The specifications and information regarding the products in this manual are subject to change without notice. All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

The software license and limited warranty for the accompanying product are set forth in the information packet that shipped with the product and are incorporated herein by this reference. If you are unable to locate the software license or limited warranty, contact your Cisco representative for a copy.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided “as is” with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential or incidental damages, including, without limitation, lost profits or loss of damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.
CONTENTS

CHAPTER 1
Cisco ISE Command-Line Interface 1
Cisco ISE Administration and Configuration Using CLI 2
Accessing the Cisco ISE CLI Using a Local System 2
Accessing the Cisco ISE CLI with Secure Shell 3
Cisco ISE CLI Administrator Account 4
Cisco ISE CLI User Accounts 5
Creating a Cisco ISE CLI User Account 5
Cisco ISE CLI User Account Privileges 6
Supported Hardware and Software Platforms for Cisco ISE CLI 7

CHAPTER 2
Cisco ISE CLI Commands in EXEC Mode 9
Cisco ISE CLI Session Begins in EXEC Mode 11
application install 12
application configure 13
  Monitoring Database Settings 14
  Live Statistics of Profiling Events 16
  Export and Import Internal CA Store 17
  Create Missing Indexes 19
  Enable ACS Migration 20
  Key Performance Metrics Statistical Data 21
  Counter Attribute Collection 22
  Wireless Setup 22
application remove 25
application reset-config 26
application reset-passwd 28
application start 29
Contents

application stop 32
application upgrade 34
backup 37
  Backing up Cisco ISE Configuration Data 38
  Backing up Cisco ISE Operational Data 39
backup-logs 40
clock 42
configure 44
copy 45
  Running Configuration 46
    Copying Running Configuration to a Remote Location 47
    Copying Running Configuration from a Remote Location 47
Startup configuration 47
  Copying Startup Configuration to a Remote Location 48
  Copying Startup Configuration from a Remote Location 48
Copying Log files 48
crypto 50
debug 53
delete 57
dir 58
exit 60
forceout 61
halt 62
help 63
mkdir 64
nslookup 65
password 67
patch install 68
patch remove 70
ping 72
ping6 73
reload 75
reset-config 76
restore 77
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>99</td>
</tr>
<tr>
<td>show application</td>
<td>100</td>
</tr>
<tr>
<td>show backup</td>
<td>103</td>
</tr>
<tr>
<td>show banner</td>
<td>104</td>
</tr>
<tr>
<td>show cdp</td>
<td>105</td>
</tr>
<tr>
<td>show clock</td>
<td>107</td>
</tr>
<tr>
<td>show container</td>
<td>108</td>
</tr>
<tr>
<td>show cpu</td>
<td>112</td>
</tr>
<tr>
<td>show crypto</td>
<td>114</td>
</tr>
<tr>
<td>show disks</td>
<td>115</td>
</tr>
<tr>
<td>show icmp-status</td>
<td>116</td>
</tr>
<tr>
<td>show interface</td>
<td>118</td>
</tr>
<tr>
<td>show inventory</td>
<td>120</td>
</tr>
<tr>
<td>show ip</td>
<td>122</td>
</tr>
<tr>
<td>show ipv6 route</td>
<td>123</td>
</tr>
<tr>
<td>show logging</td>
<td>124</td>
</tr>
<tr>
<td>show logins</td>
<td>127</td>
</tr>
<tr>
<td>show memory</td>
<td>128</td>
</tr>
<tr>
<td>show ntp</td>
<td>129</td>
</tr>
</tbody>
</table>
show ports 130
show process 132
show repository 134
show restore 135
show running-config 136
show snmp engineid 137
show snmp user 138
show startup-config 139
show tech-support 140
show terminal 142
show timezone 143
show timezones 144
show udi 145
show uptime 146
show users 147
show version 148

CHAPTER 4
Cisco ISE CLI Commands in Configuration Mode 151
Switch to Configuration Mode in EXEC Mode 153
Configuring Cisco ISE in the Configuration Mode 154
Configuring Cisco ISE in the Configuration Submode 155
CLI Configuration Command Default Settings 156
backup interface 157
cdp holdtime 161
cdp run 162
cdp timer 163
clock timezone 164

Changing the Time Zone on Cisco ISE Nodes 165
Common Time Zones 165
Australia Time Zones 166
Asia Time Zones 166
conn-limit 168
do 169
end 172
Contents

- `snmp-server enable` 222
- `snmp-server user` 223
- `snmp-server host` 225
- `snmp-server community` 227
- `snmp-server contact` 228
- `snmp-server location` 229
- `snmp-server trap dskThresholdLimit` 230
- `snmp engineid` 231
- `username` 232
- `synflood_limited` 234
Cisco ISE Command-Line Interface

This chapter provides information on the Cisco Identity Services Engine (Cisco ISE) command-line interface (CLI) that you can use to configure and maintain Cisco ISE.

- Cisco ISE Administration and Configuration Using CLI, on page 2
- Cisco ISE CLI Administrator Account, on page 4
- Cisco ISE CLI User Accounts, on page 5
- Cisco ISE CLI User Account Privileges, on page 6
- Supported Hardware and Software Platforms for Cisco ISE CLI, on page 7
Cisco ISE Administration and Configuration Using CLI

The Cisco ISE command-line interface (CLI) allows you to perform system-level configuration in EXEC mode and other configuration tasks in configuration mode (some of which cannot be performed from the Cisco ISE Admin portal), and generate operational logs for troubleshooting.

You can use either the Cisco ISE Admin portal or the CLI to apply Cisco ISE application software patches, generate operational logs for troubleshooting, and backup the Cisco ISE application data. Additionally, you can use the Cisco ISE CLI to start and stop the Cisco ISE application software, restore the application data from a backup, upgrade the application software, view all system and application logs for troubleshooting, and reload or shutdown the Cisco ISE device.

Refer to Cisco ISE CLI Commands in EXEC Mode, Cisco ISE CLI Commands in EXEC Show Mode, or Cisco ISE CLI Commands in Configuration Mode for command syntax, usage guidelines, and examples.

Accessing the Cisco ISE CLI Using a Local System

If you need to configure Cisco ISE locally without connecting to a wired Local Area Network (LAN), you can connect a system to the console port in the Cisco ISE device by using a null-modem cable. The serial console connector (port) provides access to the Cisco ISE CLI locally by connecting a terminal to the console port. The terminal is a system running terminal-emulation software or an ASCII terminal. The console port (EIA/TIA-232 asynchronous) requires only a null-modem cable.

- To connect a system running terminal-emulation software to the console port, use a DB-9 female to DB-9 female null-modem cable.

- To connect an ASCII terminal to the console port, use a DB-9 female to DB-25 male straight-through cable with a DB-25 female to DB-25 female gender changer.

The default parameters for the console port are 9600 baud, 8 data bits, no parity, 1 stop bit, and no hardware flow control.

Note

If you are using a Cisco switch on the other side of the connection, set the switchport to duplex auto, speed auto (the default).

Step 1
Connect a null-modem cable to the console port in the Cisco ISE device and to the COM port on your system.

Step 2
Set up a terminal emulator to communicate with Cisco ISE. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no hardware flow control.

Step 3
When the terminal emulator activates, press Enter.

Step 4
Enter your username and press Enter.

Step 5
Enter the password and press Enter.
Accessing the Cisco ISE CLI with Secure Shell

Cisco ISE is pre-configured through the setup utility to accept a CLI administrator. To log in with a SSH client (connecting to a wired Wide Area Network (WAN) via a system by using Windows XP or later versions), log in as an administrator.

**Before you begin**

To access the Cisco ISE CLI, use any Secure Shell (SSH) client that supports SSH v2.

---

**Step 1**
Use any SSH client and start an SSH session.

**Step 2**
Press Enter or Spacebar to connect.

**Step 3**
Enter a hostname, username, port number, and authentication method. For example, you enter ise for the hostname or the IPv4/IPv6 IP address of the remote host, admin for the username, and 22 for the port number; and, for the authentication method, choose Password from the drop-down list.

**Step 4**
Click Connect, or press Enter.

**Step 5**
Enter your assigned password for the administrator.

**Step 6**
(Optional) Enter a profile name in the Add Profile window and click Add to Profile.

**Step 7**
Click Close on the Add Profile window.
Cisco ISE CLI Administrator Account

During setup, you are prompted to enter a username and password that creates the CLI administrator account. Log into the Cisco ISE server using this account when restarting after the initial configuration for the first time.

You must always protect the CLI administrator account credentials, and use this account to explicitly create and manage additional administrator and user accounts with access to the Cisco ISE server.

CLI administrators can execute all commands to perform system-level configuration in EXEC mode (root access) and other configuration tasks in configuration mode in the Cisco ISE server. You can start and stop the Cisco ISE application software, backup and restore the Cisco ISE application data, apply software patches and upgrades to the Cisco ISE application software, view all system and application logs, and reload or shutdown the Cisco ISE devices.

A pound sign (#) appears at the end of the prompt for an administrator account, regardless of the submode.
Cisco ISE CLI User Accounts

Any user whose account you create from the Cisco ISE Admin portal cannot automatically log into the Cisco ISE CLI. You must explicitly create user accounts with access to the CLI using the CLI administrator account.

Creating a Cisco ISE CLI User Account

You must run the `username` command in configuration mode to create CLI user accounts.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log into the Cisco ISE CLI using the CLI administrator account.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter into configuration mode and run the <code>username</code> command.</td>
</tr>
</tbody>
</table>

```plaintext
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# username duke password plain Plain@123 role user email duke@cisco.com
ise/admin(config)# exit
ise/admin#
```

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Log into the Cisco ISE CLI using the CLI user account.</th>
</tr>
</thead>
</table>
Cisco ISE CLI User Account Privileges

User accounts have access to a restricted number of commands, including the following commands:

- crypto
- exit
- nslookup
- ping
- ping6
- show cdp
- show clock
- show container
- show cpu
- show disks
- show icmp_status
- show interface
- show inventory
- show logins
- show memory
- show ntp
- show ports
- show process
- show terminal
- show timezone
- show udi
- show uptime
- show version
- ssh
- terminal
- traceroute
Supported Hardware and Software Platforms for Cisco ISE CLI

You can connect to the Cisco ISE server and access the CLI using the following:

- A system running Microsoft Windows XP/Vista.
- A system running Linux, such as Red Hat or Fedora.
- An Apple computer running Mac OS X 10.4 or later.
- Any terminal device compatible with VT100 or ANSI characteristics. On VT100-type and ANSI devices, you can use cursor-control and cursor-movement keys including the left arrow, right arrow, up arrow, down arrow, Delete, and Backspace keys. The Cisco ISE CLI senses the use of the cursor-control keys and automatically uses the optimal device characteristics.

See the terminfo database (terminal capability database) for a complete listing for all terminals here: /usr/share/terminfo/*/*. These are possible locations of the compiled terminfo files: /usr/lib/terminfo/v/vt100, /usr/share/terminfo/v/vt100, /home/.../.terminfo/v/vt100, and/or /etc/terminfo/v/vt100. Terminus is a database of terminal capabilities available for every model of terminal that communicates with the application programs. It provides what escape sequences (or control characters) to send to the terminal to do things such as move the cursor to a new location, erase part of the screen, scroll the screen, change modes, change appearance (colors, brightness, blinking, underlining, reverse video etc.).

For example, typing "locate vt100" from the root may show you information about the terminal that you are using.

The following valid terminal types can access the Cisco ISE CLI:

- 1178
- 2621
- 5051
- 6053
- 8510
- altos5
- amiga
- ansi
- apollo
- Apple_Terminal
- att5425
- ibm327x
- kaypro
- vt100
Cisco ISE CLI Commands in EXEC Mode

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

- Cisco ISE CLI Session Begins in EXEC Mode, on page 11
- application install, on page 12
- application configure, on page 13
- application remove, on page 25
- application reset-config, on page 26
- application reset-passwd, on page 28
- application start, on page 29
- application stop, on page 32
- application upgrade, on page 34
- backup, on page 37
- backup-logs, on page 40
- clock, on page 42
- configure, on page 44
- copy, on page 45
- crypto, on page 50
- debug, on page 53
- delete, on page 57
- dir, on page 58
- exit, on page 60
- forceout, on page 61
- halt, on page 62
- help, on page 63
- mkdir, on page 64
- nslookup, on page 65
- password, on page 67
- patch install, on page 68
- patch remove, on page 70
- ping, on page 72
- ping6, on page 73
- reload, on page 75
• reset-config, on page 76
• restore, on page 77
• rmdir, on page 82
• ssh, on page 83
• tech, on page 85
• terminal length, on page 87
• terminal session-timeout, on page 88
• terminal session-welcome, on page 89
• terminal terminal-type, on page 90
• traceroute, on page 91
• undebug, on page 92
• write, on page 95
Cisco ISE CLI Session Begins in EXEC Mode

When you start a session in the Cisco ISE CLI, you begin in EXEC mode. In EXEC mode, you have permissions to access everything in the Cisco ISE server and perform system-level configuration and generate operational logs.
You are not allowed to run the `application install` command from the command-line interface (CLI) under normal operations because the Cisco Identity Services Engine (ISE) application is pre-installed with a Cisco IOS image on all supported appliances and VMware.

To install a specific application other than Cisco ISE, use the `application install` command in EXEC mode. To remove an application other than Cisco ISE, use the `application remove` command.

```
application [ install {application-bundle} {remote-repository-name}]
```

**Syntax Description**

- **install**
  - Installs a specific application.
- **application-bundle**
  - Application bundle filename. Supports up to 255 alphanumeric characters.
- **remote-repository-name**
  - Remote repository name. Supports up to 255 alphanumeric characters.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

Installs the specified application bundle on the appliance. The application bundle file is pulled from a specified repository.

If you issue the `application install` or `application remove` command when another installation or removal operation of an application is in progress, you will see the following warning message:

```
An existing application install, remove, or upgrade is in progress. Try again shortly.
```

**Example**

```
ise/admin# application install ise-appbundle-1.1.0.362.i386.tar.gz myrepository
Do you want to save the current configuration? (yes/no) [yes]? yes
Generating configuration...
Saved the running configuration to startup successfully
Initiating Application installation...
Extracting ISE database content...
Starting ISE database processes...
Restarting ISE database processes...
Creating ISE M&T session directory...
Performing ISE database priming...
Application successfully installed
ise/admin#
```
application configure

Use the `application configure` command in EXEC mode to:

- perform M&T operations
- refresh and display statistics related to the profiler
- export and import options to backup and restore Cisco ISE CA certificates and keys
- generate Key Performance Metrics (KPM) statistics
- enable or disable the ISE counter attribute data collection
- enable or disable wireless setup
- reset wireless setup configuration

```
application [ configure {application-name} ]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td>Configures a specific application.</td>
</tr>
<tr>
<td>application-name</td>
<td>Application name. Supports up to 255 alphanumeric characters.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Usage Guidelines

You can use this command to update M&T databases and indexes, and export and import Cisco ISE CA certificates and keys, generate Key Performance Metrics (KPM) statistics, and enable or disable ISE counter attribute data collection in a Cisco ISE node.

### Example

```
Selection ISE configuration option
[1] Reset M&T Session Database
[2] Rebuild M&T Unusable Indexes
[3] Purge M&T Operational Data
[4] Reset M&T Database
[7] Export Internal CA Store
[8] Import Internal CA Store
[9] Create Missing Config Indexes
[10] Create Missing M&T Indexes
[12] Generate Daily KPM Stats
[13] Generate KPM Stats for last 8 Weeks
[14] Enable/Disable Counter Attribute Collection
[15] View Admin Users
[16] Get all Endpoints
[17] Enable/Disable Wifi Setup
[18] Reset Config Wifi Setup
[19] Exit
```
Monitoring Database Settings

Before You begin

You must reset the monitoring database only when the Cisco ISE server is not in the deployment.

Note

We recommend to reset primary and secondary Monitoring node databases at the same time to prevent discrepancy in log files.

To configure Monitoring database related tasks, use the following options in the `application configure ise` command:

- To reset the monitoring session database, use the option 1.

  Note

  The reset option will cause ISE services to be temporarily unavailable until it restarts.

- To rebuild unusable indexes in the monitoring database, use the option 2.

- To purge monitoring operational data, use the option 3.

  The purge option is used to clean up the data and will prompt to ask the number of days to be retained.

- To reset the monitoring database, use the option 4.

  The reset option is used to reset the database to the factory default, so that all the data is be permanently deleted. You can reset the database if the files are consuming too much file system space.

  Note

  The reset option will cause ISE services to be temporarily unavailable until it restarts.

- To refresh the monitoring database statistics, use the option 5.

Example

To reset the monitoring session database, use the option 1.

```
ise/admin# application configure ise
Selection ISE configuration option
[1] Reset M&T Session Database
[2] Rebuild M&T Unusable Indexes
[3] Purge M&T Operational Data
[4] Reset M&T Database
[7] Export Internal CA Store
[8] Import Internal CA Store
[9] Create Missing Config Indexes
```
1
You are about to reset the M&T session database. Following this operation, an application
restart will be required.
Are you sure you want to proceed? y/n [n]: y
TimesTen Daemon stopped.
TimesTen Daemon startup OK.
Restarting application
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE Identity Mapping Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
CLI to verify all processes are in running state.

2
You are about to rebuild the M&T database unusable indexes.
Are you sure you want to proceed? y/n [n]: y
Starting to rebuild indexes
Completed rebuild indexes

3
Enter number of days to be retained in purging MnT Operational data [between 1 to 90 days]
For instance, Entering 20 will purge MnT Operational data older than 20 days
Enter 'exit' to return to the main menu without purging
Enter days to be retained: 20
You are about to purge M&T data older than 20 from your database.
Are you sure you want to proceed? y/n [n]: y
M&T Operational data older than 20 is getting removed from database

4
You are about to reset the M&T database. Following this operation, application will be
restarted.
Are you sure you want to proceed? y/n [n]: y
Stopping application
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE Identity Mapping Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting Database only
Creating ISE M&T database tables...
Restarting application
ISE M&T Log Collector is not running
ISE M&T Log Processor is not running
ISE Identity Mapping Service is disabled
ISE pxGrid processes are disabled
ISE Application Server process is not running
ISE Certificate Authority Service is not running
ISE Profiler Database is not running
ISE M&T Session Database is not running
ISE AD Connector is not running
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise' CLI to verify all processes are in running state.

You are about to Refresh Database statistics
Are you sure you want to proceed? y/n [n]: y
Starting to terminate long running DB sessions
Completed terminating long running DB sessions

Gathering Config schema (CEPM) stats ........
Gathering Operational schema (MNT) stats ....
Completed Refresh Database statistics

Live Statistics of Profiling Events

To display live statistics from the profiling events by probe and type, use the Display Profiler Statistics option in the application configure command. This data is collected only from the Policy Service nodes and you will not see this data in Monitoring nodes.

It leverages existing JMX counters that previously required the root patch or external JConsole to retrieve, and so there is no need to use the root patch to capture this data.

Example

ise/admin# application configure ise

Selection ISE configuration option
[1] Reset M&T Session Database
[2] Rebuild M&T Unusable Indexes
[3] Purge M&T Operational Data
[4] Reset M&T Database
[7] Export Internal CA Store
[8] Import Internal CA Store
Create an RMI connector client and connect it to the RMI connector server
Get an MBeanServerConnection
Retrieve MXBean
Press <Enter> to continue...
Timestamp, Elapsed, EndpointsProfiled, NetflowPacketsReceived, EndpointsReProfiled, EndpointsDeleted...
Press Ctrl + c

Export and Import Internal CA Store

To export Cisco ISE CA certificates and keys from the primary Administration Node (PAN) to be able to import them to the secondary Administration Node in case of a PAN failure, use the `application configure` command in EXEC mode.

When you promote your secondary Administration Node to become the primary Administration Node (PAN), you must import the Cisco ISE CA certificates and keys that you have exported from the original PAN.

- To export a copy of the Cisco ISE CA certificates and keys, use option 7 in the `application configure ise` command.

- To import a copy of the Cisco ISE CA certificates and keys, use option 8 in the `application configure ise` command.

**Example 1**

To export a copy of the Cisco ISE CA certificates and keys, use option 7.

```
ise/admin# application configure iseSelection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[17]Exit
```
Export Repository Name: sftp
Enter encryption-key for export: Test1234
Export on progress.............

The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise60':
Subject:CN=Certificate Services Root CA - ise60
Issuer:CN=Certificate Services Root CA - ise60
Serial#:0x66cfded7-2f384979-9110c0e1-50dbf656

Subject:CN=Certificate Services Endpoint Subordinate CA - ise60
Issuer:CN=Certificate Services Root CA - ise60
Serial#:0x20ff700b-d5844ef8-a029bf7d-fad64289

Subject:CN=Certificate Services Endpoint RA - ise60
Issuer:CN=Certificate Services Endpoint Subordinate CA - ise60
Serial#:0x483542bd-1f1642f4-ba71b338-8f606ee4

Subject:CN=Certificate Services OCSP Responder Certificate - ise60
Issuer:CN=Certificate Services Root CA - ise60
Serial#:0x9ad3ccdf-b64842ad-93dd5826-0b27cbd2

ISE CA keys export completed successfully

Example 2

To import a copy of the Cisco ISE CA certificates and keys, use option 8.

ise/admin# application configure ise
Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[17]Exit

8
Import Repository Name: sftp
Enter CA keys file name to import: ise_ca_key_pairs_of_ise60
Enter encryption-key: Test1234
Import on progress.............
The following 4 CA key pairs were imported:

Subject:CN=Certificate Services Root CA - ise60
Issuer:CN=Certificate Services Root CA - ise60
Serial#:0x66cfded7-2f384979-9110c0e1-50dbf656

Subject:CN=Certificate Services Endpoint Subordinate CA - ise60
Issuer:CN=Certificate Services Root CA - ise60
Serial#:0x20ff700b-d5844ef8-a029bf7d-fad64289

Subject:CN=Certificate Services Endpoint RA - ise60
Issuer:CN=Certificate Services Endpoint Subordinate CA - ise60
Serial#:0x483542bd-1f1642f4-ba71b338-8f606ee4

Subject:CN=Certificate Services OCSP Responder Certificate - ise60
Issuer:CN=Certificate Services Root CA - ise60
Serial#:0x0ad3ccdf-b64842ad-93dd5826-0b27cbd2

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully

Create Missing Indexes

To avoid upgrade failures due to missing indexes, use the `application configure` command in EXEC mode.

- To create missing CEPM database indexes, use option 9.
- To create missing monitoring database indexes, use option 10.

**Example 1**

To create the CEPM database index, use option 9.

ise/admin# application configure ise

Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[17]Exit

9

You are about to create missing config indexes.
Are you sure you want to proceed? y/n [n]: y
Starting to create missing config indexes
Completed creating missing config indexes

Example 2
To create missing Monitoring database indexes, use option 10.

```
ise/admin# application configure ise
Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[17]Exit
```

10
You are about to create missing M&T indexes.
Are you sure you want to proceed? y/n [n]: y
Starting to create missing M&T indexes
Completed creating missing M&T indexes

Enable ACS Migration
To migrate ACS configuration to ISE, use the `application configure` command in EXEC mode. To enable or disable migration of ACS configuration to ISE, use option 11.

Note
Cisco ISE, Release 1.31.4 supports migration from ACS, Release 5.5 and 5.6.

Example
To enable ACS configuration, use option 11.

```
ise/admin# application configure ise
Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
```

Cisco Identity Services Engine CLI Reference Guide, Release 2.6
ACS Migration is currently disabled. Are you sure you want to enable it? [y/n] y
ACS Migration enabled. Please make sure to disable it after you complete migration process.

Key Performance Metrics Statistical Data

To obtain key performance metrics (KPM), use the Generate Daily KPM Stats or Generate KPM Stats for last 8 Weeks option in the `application configure` command. This data is collected from the Monitoring nodes. The output of this command provides statistical information about the endpoints that connect to your deployment. You can choose to generate a report for KPM statistics daily or for the last 8 weeks. The report is saved to the local disk.

If you have reset the Monitoring database (option 4) before generating the KPM statistics, options 12 and 13 will not return any data because the Monitoring database is reset.

Example

```
ise/admin# application configure ise
Selection ISE configuration option
[1] Reset M&T Session Database
[2] Rebuild M&T Unusable Indexes
[3] Purge M&T Operational Data
[4] Reset M&T Database
[7] Export Internal CA Store
[8] Import Internal CA Store
[9] Create Missing Config Indexes
[10] Create Missing M&T Indexes
[12] Generate Daily KPM Stats
[13] Generate KPM Stats for last 8 Weeks
[14] Enable/Disable Counter Attribute Collection
[15] View Admin Users
[16] Get all Endpoints
[17] Exit

12
```
You are about to generate Daily KPM (Key Performance Metrics).
% Warning Generating KPM stats may impact ISE performance during the generation of the report. It is suggested to run this report during non-peak hours and when not conflicting with other scheduled operations of ISE.
Are you sure you want to proceed? y/n [n]: y
Starting to generate Daily KPM stats
Copying files to /localdisk
Completed generating daily KPM stats. You can find details in following files located under /localdisk
KPM_onboarding_results_27_MAR_2015.xls
KPM_trx_load_27_MAR_2015.xls

Counter Attribute Collection

ISE Counters collect threshold values for various attributes. The values for these different attributes are collected at different intervals (one at five minute interval and another greater than five minutes) and the data is presented in the ISE Counters report.

Cisco ISE, by default, collects the values for these attributes. You can choose to disable this data collection from the Cisco ISE CLI using the **application configure ise** command. Choose option 14 to enable or disable counter attribute collection.

**Example**

To disable counter attribute collection, use option 14.

```
ise/admin# application configure ise
Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[17]Exit
```

```
14
Do you want to Enable(e) or Disable(d) counter attribute collection? [e/d]d
```

Completed disabling counter attributes. It will take at most 30 minute to get effected.

Wireless Setup

To enable or disable Wireless Setup (Wifi setup), use the Enable/Disable Wifi Setup option (option 17) in the **application configure** command.

To reset the Wifi setup configuration, use the Reset Config Wifi Setup option (option 18) in the **application configure** command. This option will not reset the ISE or WLC configuration.
Example 1

To disable Wifi setup, use option 17.

ise/admin# application configure ise

Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[17]Enable/Disable Wifi Setup
[18]Reset Config Wifi Setup
[19]Exit

17
Wifi Setup is currently running. Are you sure you want to disable it? [y/n] y
Stopping container wifisetup-container

Example 2

When Wifi setup is in Disabled state, you can use option 17 to enable it again.

ise/admin# application configure ise

Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[17]Enable/Disable Wifi Setup
[18]Reset Config Wifi Setup
[19]Exit

17
Wifi Setup is currently disabled. Are you sure you want to enable it? [y/n] y
Starting container wifisetup-container
Example 3

To reset the Wifi setup configuration, use option 18.

```
ised/admin# application configure ise
Selection ISE configuration option
[1] Reset M&T Session Database
[2] Rebuild M&T Unusable Indexes
[3] Purge M&T Operational Data
[4] Reset M&T Database
[7] Export Internal CA Store
[8] Import Internal CA Store
[9] Create Missing Config Indexes
[10] Create Missing M&T Indexes
[12] Generate Daily KPM Stats
[13] Generate KPM Stats for last 8 Weeks
[14] Enable/Disable Counter Attribute Collection
[15] View Admin Users
[16] Get all Endpoints
[17] Enable/Disable Wifi Setup
[18] Reset Config Wifi Setup
[19] Exit

18
Starting Reset Config Wifi setup
Stopping container wifisetup-container
wifisetup-container Untagged: wifisetup:0.0.15
Deleted: dff12613ae85e7a4689f48c12b05b4d3c597f3f2ca58e942de468e8ca75bf3c
Deleted: 95fb5a45580ef26a745846736536877939e4c666751116928346d3e758db3
Deleted: fc3f8168728933f353adfed0a45114682fcab3d2add7549f1855a1f7cf56451
Deleted: 4dcda485c0858f964de66979c2df213832e64af92fb6d4f293c84f668f041036
Deleted: f2a5326af662739242bf2581eeda1e41d407f92054b947187bfe01e8e0d0710
```
application remove

You are not allowed to run the `application remove` command from the command-line interface (CLI) to remove Cisco ISE unless you are explicitly instructed to do so for an upgrade.

To remove a specific application other than Cisco ISE, use the `application remove` command in EXEC mode.

```
application [ remove {application-name}]`
```

When you do not want to remove any other application other than Cisco ISE, use the `no` form of this command.

```
no application [ remove {application-name}]`
```

**Syntax Description**

- **remove**: Removes or uninstalls an application.
- **application-name**: Application name. Supports up to 255 alphanumeric characters. Removes or uninstalls an application.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

Removes or uninstalls an application.

**Example**

```
ise/admin# application remove ise
Continue with application removal? [y/n] y
Application successfully uninstalled
ise/admin#
```
**application reset-config**

To reset the Cisco ISE application configuration to factory defaults or retain the existing factory settings, use the `application reset-config` command in EXEC mode. In addition to self-signed certificates, you can also reset server certificates or retain the existing server certificates.

```
application reset-config {application-name}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reset-config</td>
<td>Resets the Cisco ISE application configuration and clears the Cisco ISE database.</td>
</tr>
<tr>
<td>application-name</td>
<td>Name of the application configuration you want to reset. Supports up to 255 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

You can use the `application reset-config` command to reset the Cisco ISE configuration and clear the Cisco ISE database without reimaging the Cisco ISE appliance or VMware. The reset requires you to enter new Cisco ISE database administrator and user passwords.

**Note**

Although the `application reset-config` command resets the Cisco ISE configuration to factory defaults, the operating system (Cisco ADE-OS) configuration still remains intact. The Cisco ADE-OS configuration includes items such as the network settings, CLI password policy, and backup history.

When you reset the Cisco ISE application configuration from the CLI, it performs a leave operation disconnecting the ISE node from the Active Directory domain if it is already joined. However, the Cisco ISE node account is not removed from the Active Directory domain. We recommend that you perform a leave operation from the Cisco ISE Admin portal with the Active Directory credentials. The leave operation removes the node account from the Active Directory domain.

**Example**

If a user selects the No option, the command deletes server certificates and regenerates only self-signed certificates. If the user selects the Yes option, the command retains existing server certificates by exporting them to a location. The server certificates are then imported from this location.

```
Initialize your ISE configuration to factory defaults? (y/n): y
Leaving currently connected AD domains if any...
Retain existing ISE server certificates? (y/n): y
Reinitializing local ISE configuration to factory defaults...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
PassiveID WMI Service is disabled
PassiveID Syslog Service is disabled
PassiveID API Service is disabled
PassiveID Agent Service is disabled
PassiveID Endpoint Service is disabled
```
PassiveID SPAN 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 TC-NAC Service ...
Stopping container irf-core-engine-runtime
Stopping container irf-rabbitmq-runtime
Stopping container irf-mongo-runtime
Stopping VA Service...
Stopping ISE VA Database...
Stopping container wifisetup-container
Stopping docker daemon...
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Enter the ISE administrator username to create[admin]:
Enter the password for 'admin':
Re-enter the password for 'admin':
Extracting ISE database content...
Starting ISE database processes...
Creating ISE M&T session directory...
Creating ISE VA timesten database...
Performing ISE database priming...
Starting ISE Indexing Engine...
TimeoutStartUSec=20min
TimeoutStopUSec=20min
Cleaning up TC-NAC docker configuration...

Starting docker daemon ...
irf-core-engine-runtime is not running
irf-rabbitmq-runtime is not running
irf-mongo-runtime is not running
VA Service is not running
ISE VA Database is not running
Stopping docker daemon...
Calling wifi setup reset-config
application reset-config is success
application reset-passwd

To reset the Admin portal login password for a specified user account (usually an existing administrator account) in Cisco ISE after the administrator account has been disabled due to incorrect password entries, use the `application reset-passwd` command in EXEC mode.

`application [ reset-passwd {application-name} {administrator-ID} ]`

**Syntax Description**
- `reset-passwd` Resets the administrator account password.
- `application-name` Application name. Supports up to 255 alphanumeric characters.
- `administrator-ID` Name of a disabled administrator account for which you want to reset the password.

**Command Default**
No default behavior or values. Necessary to disable the administrator account in Cisco ISE

**Command Modes**
EXEC

**Usage Guidelines**
The following special characters are allowed when resetting the Cisco ISE Admin portal password:

<table>
<thead>
<tr>
<th>~</th>
<th>!</th>
<th>@</th>
<th>$</th>
<th>&amp;</th>
<th>*</th>
<th>-</th>
<th>_</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>=</td>
<td>\</td>
<td>&quot;</td>
<td>,</td>
<td>;</td>
<td>&lt;</td>
<td>&gt;</td>
</tr>
</tbody>
</table>

If you enter an incorrect password for an administrator user ID more than the specified number of times, then the Admin portal “locks you out” of the system. Cisco ISE suspends the credentials for it. administrator user ID until you have an opportunity to reset the password associated with it. You can reset the administrator password only in the Administration ISE node CLI.

UTF-8 admin users can change passwords only through the Cisco ISE Admin portal.

**Example**

```
ise/admin# application reset-passwd ise admin
Enter new password: *******
Confirm new password: *******
Password reset successfully.
ise/admin#
```
application start

To enable a specific application, use the application start command in EXEC mode. To disable starting an application, use the no form of this command.

```
application [ start {application-name | safe}]
no application [ start {application-name | safe}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>Enables an application bundle.</td>
</tr>
<tr>
<td>application-name</td>
<td>Name of the predefined application that you want to enable. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td>safe</td>
<td>Starts an application in safe mode.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

EXEC

Enables an application.

### Usage Guidelines

You cannot use this command to start Cisco ISE. If you try to, you will be prompted that Cisco ISE is already running.

You can use the `application start safe` command to start Cisco ISE in a safe mode that allows you to disable access control temporarily to the Admin portal and then restart the application after making necessary changes.

The safe option provides a means of recovery in the event that you as an administrator inadvertently lock out all users from accessing the Cisco ISE Admin portal. This event can happen if you configure an incorrect "IP Access" list in the Administration > Admin Access > Settings > Access page. The 'safe' option also bypasses certificate-based authentication and reverts to the default username and password authentication for logging into the Cisco ISE Admin portal.

### Example 1

```
ise/admin# application start ise
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Indexing Engine...
Starting docker daemon ...
38a408c9a1c8
Starting container wifisetup-container
Starting ISE Certificate Authority Service...
Starting ISE AD Connector...
Starting ISE EST Service...
Note: ISE Processes are initializing. Use 'show application status ise' CLI to verify all processes are in running state.
ise/admin# show application status ise
```

ISE PROCESS NAME  STATE  PROCESS ID
Starting Cisco ISE Application in Safe Mode

The purpose of the 'safe' option is to bypass access restrictions that may have been caused inadvertently. When the safe mode is used to start Cisco ISE services, the following behavior is observed:

- IP access restriction is temporarily disabled to allow administrators logging into correct IP access restrictions if they inadvertently lock themselves.

- On FIPS enabled hosts, if the 'safe' option is passed on application startup, the FIPS integrity check is temporarily disabled. Normally, if FIPS integrity check fails, Cisco ISE services are not started. Users can bypass the FIPS integrity check with the 'safe' option on application start.

- On FIPS enabled hosts, if the 'safe' option is passed on application startup, the hardware random number generator integrity check is disabled.

- If certificate-based authentication is used, the 'safe' option on application start will temporarily use username and password based authentication.

These changes are temporary and only relevant for that instance of the Cisco ISE application. If the Cisco ISE services are restarted again without the 'safe' option, all of the default functionality is restored.
ise/admin# application stop ise
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
PassiveID WMI Service is disabled
PassiveID Syslog Service is disabled
PassiveID API Service is disabled
PassiveID Agent Service is disabled
PassiveID Endpoint Service is disabled
PassiveID SPAN Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Exp Engine Service is disabled
Stopping TC-NAC Service...
Error response from daemon: no such id: irf-core-engine-runtime
irf-core-engine-runtime is not running
Error response from daemon: no such id: irf-rabbitmq-runtime
irf-rabbitmq-runtime is not running
Error response from daemon: no such id: irf-mongo-runtime
irf-mongo-runtime is not running
VA Service is not running
ISE VA Database is not running
Stopping container wifisetup-container
Stopping docker daemon...
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...

ise/admin# application start ise safe
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Indexing Engine...
Starting docker daemon ...38a408c9a1c8
Starting container wifisetup-container
Starting ISE Certificate Authority Service...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
CLI to verify all processes are in running state.
Starting ISE EST Service...
application stop

To disable a specific application, use the `application stop` command in EXEC mode. To disable stopping an application, use the `no` form of this command.

```
application [ stop {application-name}]  
no application [ stop {application-name}]  
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>stop</code></td>
<td>Disables an application.</td>
</tr>
<tr>
<td><code>application-name</code></td>
<td>Name of the predefined application that you want to disable. Supports up to 255 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

Disables an application.

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

```
PAN Auto Failover feature is enabled, therefore this operation will trigger a failover if ISE services are not restarted within the fail-over window. Do you want to continue (y/n)?
```

Type 'y' if you want to continue or 'n' if you want to abort.

**Example**

```
ise/admin# application stop ise  
Stopping ISE Monitoring & Troubleshooting Log Processor...  
Stopping ISE Monitoring & Troubleshooting Log Collector...  
Stopping ISE Identity Mapping Service...  
Stopping ISE pxGrid processes...  
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/admin# show application status ise  

+----------------+----------------+----------------+  
| ISE PROCESS NAME        | STATE           | PROCESS ID     |  
+----------------+----------------+----------------+  
| Database Listener  | not running     |                |  
| Application Server  | not running     |                |  
| Profiler Database   | not running     |                |  
| AD Connector        | not running     |                |  
| M&T Session Database | not running    |                |  
| M&T Log Collector   | not running     |                |  
| M&T Log Processor   | not running     |                |  
| Certificate Authority Service | disabled |                |  
| pxGrid Infrastructure Service | not running |                |  
| pxGrid Publisher Subscriber Service | not running |                |  
| pxGrid Connection Manager | not running |                |  
+----------------+----------------+----------------+  
```
pxGrid Controller not running
Identity Mapping Service not running
ise://admin#
# application upgrade

To upgrade a specific application bundle, use the `application upgrade` command in EXEC mode.

```bash
application [ upgrade {application-bundle | remote-repository-name} ]
```

## Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>upgrade</code></td>
<td>Upgrades a specific application bundle in the remote repository.</td>
</tr>
<tr>
<td><code>application-bundle</code></td>
<td>Application name. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td><code>remote-repository-name</code></td>
<td>Remote repository name. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td><code>cleanup</code></td>
<td>Cleans previously prepared upgrade bundle and prepares a new upgrade bundle.</td>
</tr>
<tr>
<td><code>prepare</code></td>
<td>Downloads an upgrade bundle and unzip contents to the local disk to prepare an application for an upgrade.</td>
</tr>
<tr>
<td><code>application-bundle</code></td>
<td>Application name. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td><code>proceed</code></td>
<td>Proceeds with an upgrade using the local file.</td>
</tr>
</tbody>
</table>

## Command Default

No default behavior or values.

## Command Modes

EXEC

## Usage Guidelines

Upgrades an application, and preserves any application configuration data. See the *Cisco Identity Services Engine Upgrade Guide* for more information.

- Use the `cleanup` option, if you want to try another upgrade bundle in case of a failure or use a different version.
- Use the `prepare` option to download and extract an upgrade bundle locally.
- Use the `proceed` option to upgrade Cisco ISE using the upgrade bundle you extracted with the prepare option. You can use this option after preparing an upgrade bundle instead of using the `application upgrade` command directly.
  - If upgrade is successful, this option removes the upgrade bundle.
  - If upgrade fails for any reason, this option retains the upgrade bundle.

If you issue the application upgrade command when another application upgrade operation is in progress, you will see the following warning message:

```
An existing application install, remove, or upgrade is in progress. Try again shortly.
```
Caution

Do not issue the backup or restore commands when an upgrade is in progress. This action might cause the database to be corrupted.

Note

Before attempting to use the application upgrade command, you must read the upgrade instructions in the release notes supplied with the newer release. The release notes contain important updated instructions and they must be followed.

Example 1

ise/admin# application upgrade prepare
application upgrade prepare
ise-upgradebundle-2.3.0.x.x86_64.tar.gz upgrade

Getting bundle to local machine...
Unbundling Application Package...
Verifying Application Signature...

Application upgrade preparation successful

Example 2

ise/admin# application upgrade proceed
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
- Checking VM for minimum hardware requirements
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
- Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: Taking backup of the configuration data...
STEP 5: Running ISE configuration database schema upgrade...
- Running db sanity to check and fix if any index corruption
- Auto Upgrading Schema for UPS Model
- Upgrading Schema completed for UPS Model
ISE database schema upgrade completed.
% Warning: Sanity test found some indexes missing in CEPM schema. Please recreate missing indexes after upgrade using app configure ise cli
STEP 6: Running ISE configuration data upgrade...
- Data upgrade step 1/14, UPSUpgradeHandler(2.3.0.100)... Done in 53 seconds.
- Data upgrade step 2/14, UPSUpgradeHandler(2.3.0.110)... Done in 1 seconds.
- Data upgrade step 3/14, NetworkAccessUpgrade(2.3.0.145)... Done in 0 seconds.
- Data upgrade step 4/14, NodeGroupUpgradeService(2.3.0.155)... Done in 0 seconds.
- Data upgrade step 5/14, IRFUpgradeService(2.3.0.155)... Done in 0 seconds.
- Data upgrade step 6/14, UPSUpgradeHandler(2.3.0.158)... Done in 0 seconds.
- Data upgrade step 7/14, NetworkAccessUpgrade(2.3.0.178)... Done in 0 seconds.
- Data upgrade step 8/14, NetworkAccessUpgrade(2.3.0.182)... Done in 0 seconds.
- Data upgrade step 9/14, CertMgmtUpgradeService(2.3.0.194)... Done in 3 seconds.
- Data upgrade step 10/14, UPSUpgradeHandler(2.3.0.201)... Done in 0 seconds.
- Data upgrade step 11/14, NSFUpgradeService(2.3.0.233)... Done in 0 seconds.
- Data upgrade step 12/14, ProfilerUpgradeService(2.3.0.233)... Done in 0 seconds.
- Data upgrade step 13/14, GuestAccessUpgradeService(2.3.0.233)... Done in 7 seconds.
STEP 7: Running ISE configuration data upgrade for node specific data...
STEP 8: Running ISE M&T database upgrade...
ISE M&T Log Processor is not running
ISE database M&T schema upgrade completed.

Gathering Config schema(CEPM) stats ....
Gathering Operational schema(MNT) stats ....
% NOTICE: Upgrading ADEOS. Appliance will be rebooted after upgrade completes successfully.
warning: file /opt/xgrid/gc/pxgrid-controller-1.0.4.18-dist.tar.gz: remove failed: No such file or directory

% This application Install or Upgrade requires reboot, rebooting now...
Broadcast message from root@IS137 (pts/3) (Fri Jun  2 12:22:49 2017):
Trying to stop processes gracefully. Reload might take approximately 3 mins
Broadcast message from root@IS137 (pts/3) (Fri Jun  2 12:22:49 2017):
Trying to stop processes gracefully. Reload might take approximately 3 mins
Broadcast message from root@IS137 (pts/3) (Fri Jun  2 12:23:10 2017):
The system is going down for reboot NOW
Broadcast message from root@IS137 (pts/3) (Fri Jun  2 12:23:10 2017):
The system is going down for reboot NOW
The upgrade is now complete.
**backup**

To perform a backup including Cisco ISE and Cisco ADE OS data and place the backup in a repository, use the `backup` command in EXEC mode.

**Note**

Before attempting to use the `backup` command in EXEC mode, you must copy the running configuration to a safe location, such as a network server, or save it as the Cisco ISE server startup configuration. You can use this startup configuration when you restore or troubleshoot Cisco ISE from the backup and system logs.

```plaintext
backup [{backup-name} repository {repository-name} ise-config encryption-key hash|plain {encryption-key name}]
backup [{backup-name} repository {repository-name} ise-operational encryption-key hash|plain {encryption-key name}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>backup-name</code></td>
<td>Name of backup file. Supports up to 100 alphanumeric characters.</td>
</tr>
<tr>
<td><code>repository</code></td>
<td>Specifies repository to store the backup file.</td>
</tr>
<tr>
<td><code>repository-name</code></td>
<td>Location where the files should be backed up to. Supports up to 80 alphanumeric characters.</td>
</tr>
<tr>
<td><code>ise-config</code></td>
<td>Backs up Cisco ISE configuration data (includes Cisco ISE ADE-OS).</td>
</tr>
<tr>
<td><code>ise-operational</code></td>
<td>Backs up Cisco ISE operational data.</td>
</tr>
<tr>
<td><code>encryption-key</code></td>
<td>Specifies user-defined encryption key to protect the backup.</td>
</tr>
<tr>
<td><code>hash</code></td>
<td>Specifies (Hashed encryption key for protection of backup) an encrypted (hashed) encryption key that follows. Supports up to 40 characters.</td>
</tr>
<tr>
<td><code>plain</code></td>
<td>Specifies (Plaintext encryption key for protection of backup) an unencrypted plaintext encryption key that follows. Supports up to 15 characters.</td>
</tr>
<tr>
<td><code>encryption-key name</code></td>
<td>An encryption key in hash</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

You can encrypt and decrypt backups now by using user-defined encryption keys when you perform a backup of Cisco ISE and Cisco ADE OS data in a repository with an encrypted (hashed) or unencrypted plaintext password with `ise-config`. To perform a backup of only the Cisco ISE application data without the Cisco ADE OS data, use the `ise-operational` command.
You can back up Cisco ISE operational data only from the primary or secondary Monitoring nodes.

---

**Important**

When performing a backup and restore, the restore overwrites the list of trusted certificates on the target system with the list of certificates from the source system. It is critically important to note that backup and restore functions do not include private keys associated with the Internal Certificate Authority (CA) certificates.

If you are performing a backup and restore from one system to another, you will have to choose from one of these options to avoid errors:

- **Option 1:**
  
  Export the CA certificates from the source ISE node through the CLI and import them in to the target system through the CLI.
  
  **Pros:** Any certificates issued to endpoints from the source system will continue to be trusted. Any new certificates issued by the target system will be signed by the same keys.
  
  **Cons:** Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

- **Option 2:**
  
  After the restore process, generate all new certificates for the internal CA.
  
  **Pros:** This option is the recommended and clean method, where neither the original source certificates or the original target certificates will be used. Certificates issued by the original source system will continue to be trusted.
  
  **Cons:** Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

---

### Backing up Cisco ISE Configuration Data

To backup Cisco ISE configuration data, use the following command:

```
backup mybackup repository myrepository ise-config encryption-keyplain lablab12
```

**Example**

```
ise/admin# backup test repository disk ise-config encryption-key plain Test_1234
Internal CA Store is not included in this backup. It is recommended to export it using "application configure ise" CLI command
Creating backup with timestamped filename: test-CFG-141006-1350.tar.gpg
backup in progress: Starting Backup...10% completed
backup in progress: Validating ISE Node Role...15% completed
backup in progress: Backing up ISE Configuration Data...20% completed
backup in progress: Backing up ISE Logs...45% completed
backup in progress: Completing ISE Backup Staging...50% completed
backup in progress: Backing up ADEOS configuration...55% completed
backup in progress: Moving Backup file to the repository...75% completed
backup in progress: Completing Backup...100% completed
ise/admin#
```
Backing up Cisco ISE Operational Data

To backup Cisco ISE operational data, use the following command:

```
backup mybackup repository myrepository ise-operational encryption-key plain/lablab12
```

**Example**

```
ise/admin# backup mybackup repository myrepository ise-operational encryption-key plain lablab12
backup in progress: Starting Backup...10% completed
Creating backup with timestamped filename: mybackup-OPS-130103-0019.tar.gpg
backup in progress: starting dbbackup using expdp.......20% completed
backup in progress: starting cars logic.......50% completed
backup in progress: Moving Backup file to the repository...75% completed
backup in progress: Completing Backup...100% completed
ise/admin#
```
backup-logs

To back up system logs, use the `backup-logs` command in EXEC mode. To remove this function, use the `no` form of this command.

**Note**

Before attempting to use the `backup-logs` command in EXEC mode, you must copy the running configuration to a safe location, such as a network server, or save it as the Cisco ISE server startup configuration. You can use this startup configuration when you restore or troubleshoot Cisco ISE from the backup and system logs.

```
backup-logs backup-name repository repository-name {public-key | {encryption-key { hash | plain } encryption-key name}}
```

**Syntax Description**

- `backup-name`: Name of one or more files to back up. Supports up to 100 alphanumeric characters.
- `repository`: Repository command.
- `repository-name`: Location where files should be backed up to. Supports up to 80 alphanumeric characters.
- `public-key`: Specifies that Cisco ISE will use the Cisco PKI public keys for encryption. Choose this option if you are going to provide the support bundle to Cisco TAC for troubleshooting. Only Cisco TAC can decrypt the support bundle using the private key. Choose the `encryption-key` option if you are going to troubleshoot the issues locally on premise.
- `encryption-key`: Specifies the encryption key to protect the backup logs.
- `hash`: Hashed encryption key for protection of backup logs. Specifies an encrypted (hashed) encryption key that follows. Supports up to 40 characters.
- `plain`: Plaintext encryption key for protection of backup logs. Specifies an unencrypted plaintext encryption key that follows. Supports up to 15 characters.
- `encryption-key name`: The encryption key in hash or plain format.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

Backs up system logs with an encrypted (hashed) or unencrypted plaintext password.
Example 1

ise/admin# backup-logs Test repository disk encryption-key plain Test_1234
% Creating log backup with timestamped filename: Test-141006-1351.tar.gpg
% supportbundle in progress: Copying database config files...10% completed
% supportbundle in progress: Copying debug logs...20% completed
% supportbundle in progress: Copying local logs...30% completed
% supportbundle in progress: Copying monitor logs...40% completed
% supportbundle in progress: Copying policy xml...50% completed
% supportbundle in progress: Copying system logs...60% completed
% supportbundle in progress: Moving support bundle to the repository...75% completed
% supportbundle in progress: Completing support bundle generation......100% completed
ise/admin#

Example 2

ise/admin# backup-logs test repository disk public-key
% Creating log backup with timestamped filename: new-pk-160520-0259.tar.gpg
% supportbundle in progress: Copying database config files...10% completed
% supportbundle in progress: Copying debug logs...20% completed
% supportbundle in progress: Copying local logs...30% completed
% supportbundle in progress: Copying monitor logs...40% completed
% supportbundle in progress: Copying policy xml...50% completed
% supportbundle in progress: Copying system logs...60% completed
% supportbundle in progress: Moving support bundle to the repository...75% completed
% supportbundle in progress: Completing support bundle generation......100% completed
clock

To set the system clock, use the `clock` command in EXEC mode. To disable setting the system clock, use the `no` form of this command.

```
clock [ set { month | day | hh:mm:ss | yyyy } ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Sets the system clock.</td>
</tr>
<tr>
<td>month</td>
<td>Current month of the year by name. Supports up to three alphabetic characters. For example, Jan for January.</td>
</tr>
<tr>
<td>day</td>
<td>Current day (by date) of the month. Value = 0 to 31. Supports up to two numbers.</td>
</tr>
<tr>
<td>hh:mm:ss</td>
<td>Current time in hours (24-hour format), minutes, and seconds.</td>
</tr>
<tr>
<td>yyyy</td>
<td>Current year (no abbreviation).</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

Caution

Changing the system time on a Cisco ISE appliance causes the Cisco ISE application to be unusable.

Sets the system clock. You must restart the Cisco ISE server after you reset the clock for the change to take effect. Changing system time impacts different Cisco ISE nodes types of your deployment.

To recover from the impact, use the following steps:

**Standalone or Primary ISE Node**

Changing the system time after installation is not supported on a standalone or primary ISE node.

If you inadvertently change the system time, do the following:

- Revert to the original system time (the time before it was changed).
- Run the `application reset-config ise` command from the CLI of that node.
- Restore from the last known good backup before the time change on that node.
Secondary ISE Node

Changing the system time on a secondary node renders it unusable in your deployment.

To synchronize the system time of the secondary node with the primary node, do the following:

- Deregister the secondary ISE node.
- Correct the system time to be in sync with the primary ISE node.
- Run the `application reset-config ise` command from the CLI of the primary ISE node.
- Reregister the ISE node as a secondary ISE node to the primary ISE node.

Note: To ensure that you have the correct system time set at the time of installation, the setup wizard requires you to specify an Network Time Protocol (NTP) server and tries to sync with it. You must ensure that the NTP server configured during setup is always reachable so that the system time is always kept accurate, especially in rare situations where the BIOS time can get corrupted because of power failure or CMOS battery failure. This, in turn, can corrupt the Cisco ADE-OS system time during a reboot. If you do not configure an NTP server during setup, then you have to ensure that the system BIOS time is set relative to the Universal Time Coordinated (UTC) time zone, as described in the Cisco Identity Services Engine Hardware Installation Guide.

Example

```
ise/admin# clock set August 30 18:07:20 2013
ise/admin# show clock
Fri Aug 30 18:07:26 UTC 2013
ise/admin#
```
configure

To enter into configuration mode, use the configure command in EXEC mode.

configure terminal

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>terminal</th>
<th>Executes configuration commands from the terminal.</th>
</tr>
</thead>
</table>

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use this command to enter into configuration mode. Note that commands in this mode write to the running configuration file as soon as you enter them.

To exit configuration mode and return to EXEC mode, enter end, exit, or Ctrl-z.

To view the changes made to the configuration, use the show running-config command in EXEC mode.

If the replace option is used with this command, copies a remote configuration to the system, which overwrites the existing configuration.

Example

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

To copy a file from a source to a destination, use the copy command in EXEC mode.

The copy command is supported only for the local disk and not for a repository.

Using the copy command, you can copy core files and heap dumps from Cisco ISE to a remote repository. See Example 3 under Copying Log files, on page 48 for more information.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>running-config</strong></td>
<td>Represents the current running configuration file.</td>
</tr>
<tr>
<td><strong>startup-config</strong></td>
<td>Represents the configuration file used during initialization (startup).</td>
</tr>
<tr>
<td><strong>protocol</strong></td>
<td>Destination for copying. See Table 2-1 for protocol keyword options.</td>
</tr>
<tr>
<td><strong>hostname</strong></td>
<td>Hostname of destination.</td>
</tr>
<tr>
<td><strong>location</strong></td>
<td>Location of destination. Represents the current running configuration file.</td>
</tr>
<tr>
<td><strong>logs</strong></td>
<td>The system log files.</td>
</tr>
<tr>
<td><strong>all</strong></td>
<td>Copies all Cisco ISE log files from the system to another location. All logs are packaged as iselogs.tar.gz and transferred to the specified directory on the remote host.</td>
</tr>
<tr>
<td><strong>filename</strong></td>
<td>Allows you to copy a single Cisco ISE log file and transfer it to the specified directory on the remote host, with its original name.</td>
</tr>
<tr>
<td><strong>log_filename</strong></td>
<td>Name of the Cisco ISE log file, as displayed by the show logs command (up to 255 characters).</td>
</tr>
<tr>
<td><strong>mgmt</strong></td>
<td>Copies the Cisco ISE management debug logs and Tomcat logs from the system, bundles them as mgmtlogs.tar.gz, and transfers them to the specified directory on the remote host.</td>
</tr>
<tr>
<td><strong>runtime</strong></td>
<td>Copies the Cisco ISE runtime debug logs from the system, bundles them as runtimelogs.tar.gz, and transfers them to the specified directory on the remote host.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.
Command Modes

**EXEC**

**Usage Guidelines**

The `copy` command in Cisco ISE copies a running or start up configuration and log files from the system to another location.

The fundamental function of the `copy` command allows you to copy a file (such as a system image or configuration file) from one location to another location. The source and destination for the file specified uses the Cisco ISE file system, through which you can specify any supported local or remote file location. The file system being used (a local memory source or a remote system) dictates the syntax used in the command.

You can enter all necessary source and destination information and the username and password to use; or, you can enter the `copy` command and have the server prompt you for any missing information.

The entire copying process might take several minutes and differs from protocol to protocol and from network to network.

Use the filename relative to the directory for file transfers.

Possible errors are standard File Transfer protocol (FTP) error messages.

**Table 1: Table 2-1 Protocol Prefix Keywords (Continued)**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source of Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ftp</strong></td>
<td>Source or destination URL for FTP network server. The syntax for this alias: ftp://[[username[:password]@]location]/directory/filename</td>
</tr>
<tr>
<td><strong>sftp</strong></td>
<td>Source or destination URL for an SFTP network server. The syntax for this alias: sftp://location/directory/filename</td>
</tr>
<tr>
<td><strong>tftp</strong></td>
<td>Source or destination URL for a TFTP network server. The syntax for this alias: tftp://location/directory/filename</td>
</tr>
</tbody>
</table>

**Running Configuration**

The Cisco ISE active configuration stores itself in the Cisco ISE RAM. Every configuration command you enter resides in the running configuration. If you reboot a Cisco ISE server, you lose the running configuration. If you make changes that you want to save, you must copy the running configuration to a safe location, such as a network server, or save it as the Cisco ISE server startup configuration.

If you do not save the running configuration, you will lose all your configuration changes during the next reboot of the Cisco ISE server. When you are satisfied that the current configuration is correct, copy your configuration to the startup configuration with the `copy run start` command.

**Note**

Aliases reduce the amount of typing that you need to do. For example, type `copy run` and press the Tab key, type `start` and press the Tab key, which is the abbreviated form of the `copy running-config startup-config` command.)
To replace the startup configuration with the running configuration, use the following command:

`copy run start`

To copy the running configuration to the startup configuration, use the following command:

`copy running-config startup-config`

To merge the startup configuration on top of the running configuration, use the following command:

`copy start run`

**Example 1**

```
ise/admin# copy run start
Generating configuration...
ise/admin#
```

**Example 2**

```
ise/admin# copy running-config startup-config
Generating configuration...
ise/admin#
```

### Copying Running Configuration to a Remote Location

To copy the running configuration to a remote system, use the following command:

`copy running-config [protocol://hostname/location]`

### Copying Running Configuration from a Remote Location

To copy and merge a remote file to the running configuration, use the following command:

`copy [protocol://hostname/location] running-config`—Copies and merges a remote file to the running configuration.

### Startup configuration

You cannot edit a startup configuration directly. All commands that you enter store themselves in the running configuration, which you can copy into the startup configuration.

In other words, when you boot a Cisco ISE server, the startup configuration becomes the initial running configuration. As you modify the configuration, the two diverge: the startup configuration remains the same; the running configuration reflects the changes that you have made. If you want to make your changes permanent, you must copy the running configuration to the startup configuration.

To copy the startup configuration to the running configuration, use the following command:

`copy startup-config running-config`

**Example 1**

```
ise/admin# copy start run
ise/admin#
```
Example 2

ise/admin# copy startup-config running-config
ise/admin#  

Copying Startup Configuration to a Remote Location

To copy the startup configuration to a remote system, use the following command:

```
copy startup-config [protocol://hostname/location]
```

Copying Startup Configuration from a Remote Location

To copy but does not merge a remote file to the startup configuration, use the following command:

```
copy [protocol://hostname/location] startup-config
```
—Copies but does not merge a remote file to the startup configuration

Copying Log files

Use the following `copy` command to copy log files from the Cisco ISE system to another location:

```
copy logs [protocol://hostname/location]
```

Example 1

To copy log files to the local disk, use the following command:

```
ise/admin# copy logs disk:/
  Collecting logs...
ise/admin#
```

Example 2

To copy log files to another location, use the following command:

```
ise/admin# copy disk://mybackup-100805-1910.tar.gz ftp://myftpserver/mydir
Username: 
Password: 
ise/admin#
```

Example 3

Cisco ISE moves the core files and heap dumps from the `/var/tmp` directory to the `disk:/corefiles` directory on an hourly basis. You can copy these logs from the local disk to a remote repository using the copy command. The core files and heap dumps contain critical information that would help identify the cause of a crash. These logs are created when the application crashes. You can use the `dir` command to view the core files in the local disk.

```
ise/admin# copy disk:/corefiles ftp://192.0.2.2/
Username: ftp
Password: 
ise36/admin#
ise36/admin# dir
Directory of disk:/
```
Usage for disk: filesystem
51474489344 bytes total used
123938643968 bytes free
184807632896 bytes available
crypto

To generate a new public key pair, export the current public key to a repository, and import a public key to the authorized keys list, use the crypto command in EXEC mode. It is also possible to view the public key information and delete selected keys.

crypto key [ delete {hash | authorized_keys | rsa} ]
crypto key [ export {filename | repository} ]
crypto key [ generate {rsa} ]
crypto key [ import {filename | repository} ]
crypto ntp_import_autokey ntpkey

Syntax Description

<table>
<thead>
<tr>
<th>key</th>
<th>Allows you to perform crypto key operations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete</td>
<td>Deletes a public/private key pair.</td>
</tr>
<tr>
<td>hash</td>
<td>Hash value. Supports up to 80 characters.</td>
</tr>
<tr>
<td>authorized_keys</td>
<td>Deletes authorized keys.</td>
</tr>
<tr>
<td>rsa</td>
<td>Deletes an RSA key pair.</td>
</tr>
<tr>
<td>export</td>
<td>Exports a public/private key pair to repository.</td>
</tr>
<tr>
<td>filename</td>
<td>The filename to which the public key is exported to. Supports up to 80 characters.</td>
</tr>
<tr>
<td>repository</td>
<td>The repository to which the public key is exported to.</td>
</tr>
<tr>
<td>generate</td>
<td>Generates a public/private key pair.</td>
</tr>
<tr>
<td>rsa</td>
<td>Generates an RSA key pair.</td>
</tr>
<tr>
<td>import</td>
<td>Imports a public/private key pair.</td>
</tr>
<tr>
<td>filename</td>
<td>The filename to which the public key is imported. Supports up to 80 characters.</td>
</tr>
<tr>
<td>repository</td>
<td>The repository to which the public key is imported.</td>
</tr>
<tr>
<td>host_key</td>
<td>Allows you to perform crypto host-key operations.</td>
</tr>
<tr>
<td>add</td>
<td>Adds trusted host keys.</td>
</tr>
<tr>
<td>host</td>
<td>Specifies hostname.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes trusted host keys.</td>
</tr>
<tr>
<td>ntp_import_autokey</td>
<td>Imports the public key generated from the NTP server.</td>
</tr>
<tr>
<td>ntpkey</td>
<td>Public key generated from the NTP server.</td>
</tr>
</tbody>
</table>
**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

The Cisco ADE OS supports public key authentication with out the password for SSH access to administrators and user identities.

Use the `crypto key generate rsa` command to generate a new public/private key pair with a 2048-bit length for the current user. The key attributes are fixed, and supports RSA key types. If the key pair already exists, you will be prompted to permit an over-write before continuing with a passphrase. If you provide the passphrase, you will be prompted for the passphrase whenever you access the public/private key. If the passphrase is empty, no subsequent prompts for the passphrase occurs.

Use the `crypto ntp_import_autokey` command to import the public key generated from the NTP server.

**Example 1**

```
ise/admin# crypto key generate rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
ise/admin# show crypto key
ise/admin# crypto key generate rsa
Private key for user admin already exists. Overwrite? y/n [n]: y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
ise/admin# show crypto key
ise/admin# crypto key export mykey_rsa repository myrepository
ise/admin# show crypto key
admin public key: ssh-rsa f8:7f:8a:79:44:b8:5d:5f:af:e1:63:b2:be:7a:fd:d4 admin@ise
ise/admin#
ise/admin# crypto key delete rsa
ise/admin# show crypto key
ise/admin# show crypto authorized_keys
Authorized keys for admin
ise/admin# crypto key delete authorized_keys
ise/admin# show crypto authorized_keys
ise/admin#
ise/admin# crypto key import mykey_rsa repository myrepository
ise/admin# show crypto key
admin public key: ssh-rsa f8:7f:8a:79:44:b8:5d:5f:af:e1:63:b2:be:7a:fd:d4 admin@ise
ise/admin#
```

**Example 2**

```
ise/admin# crypto host_key add host ise
host key fingerprint added
# Host ise found: line 1 type RSA
ise/admin#
ise/admin# crypto host_key delete host ise
host key fingerprint for ise removed
ise/admin#
```
Example 3

ise/admin# crypto ntp_import_autokey ntpkey repository nfs
ise/admin#
debug

To display errors or events for executed commands, use the `debug` command in EXEC mode.

dump [ all | application | backup-restore | cdp | config | copy | icmp | locks | logging | smtp | system | transfer | user | utils ]

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables all debugging.</td>
</tr>
<tr>
<td>application</td>
<td>Enables debugging application related errors or events.</td>
</tr>
<tr>
<td></td>
<td>• all—Enables all application debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>• install—Enables application install debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>• operation—Enables application operation debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>• uninstall—Enables application uninstall debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td>backup-restore</td>
<td>Enables debugging back up and restore related errors or events.</td>
</tr>
<tr>
<td></td>
<td>• all—Enables all debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>• backup—Enables backup debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>• backup-logs—Enables backup-logs debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>• history—Enables history debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>• restore—Enables restore debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
</tbody>
</table>
### cdp
Enables debugging Cisco Discovery Protocol configuration related errors or events.

- **all**—Enables all Cisco Discovery Protocol configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

- **config**—Enables configuration debug output for Cisco Discovery Protocol. Set level between 0 and 7, with 0 being severe and 7 being all.

- **infra**—Enables infrastructure debug output for Cisco Discovery Protocol. Set level between 0 and 7, with 0 being severe and 7 being all.

### config
Enables debugging the Cisco ISE configuration related errors or events.

- **all**—Enables all configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

- **backup**—Enables backup configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

- **clock**—Enables clock configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

- **infra**—Enables configuration infrastructure debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

- **kron**—Enables command scheduler configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

- **network**—Enables network configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

- **repository**—Enables repository configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

- **service**—Enables service configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

### copy
Enables debugging copy commands. Set level between 0 and 7, with 0 being severe and 7 being all.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| **icmp** | Enables debugging Internet Control Message Protocol (ICMP) echo response configuration related errors or events.  
  all—Enable all debug output for ICMP echo response configuration. Set level between 0 and 7, with 0 being severe and 7 being all. |
| **locks** | Enables debugging resource locking related errors or events.  
  • all—Enables all resource locking debug output. Set level between 0 and 7, with 0 being severe and 7 being all.  
  • file—Enables file locking debug output. Set level between 0 and 7, with 0 being severe and 7 being all. |
| **logging** | Enables debugging logging configuration related errors or events.  
  all—Enables all logging configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. |
| **snmp** | Enables debugging SNMP configuration related errors or events.  
  all—Enables all SNMP configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. |
| **system** | Enables debugging Cisco ISE system related errors and events.  
  • all—Enables all system files debug output. Set level between 0 and 7, with 0 being severe and 7 being all.  
  • id—Enables system ID debug output. Set level between 0 and 7, with 0 being severe and 7 being all.  
  • info—Enables system info debug output. Set level between 0 and 7, with 0 being severe and 7 being all.  
  • init—Enables system init debug output. Set level between 0 and 7, with 0 being severe and 7 being all. |
<p>| <strong>transfer</strong> | Enables debugging file transfer. Set level between 0 and 7, with 0 being severe and 7 being all. |</p>
<table>
<thead>
<tr>
<th>Command Default</th>
<th>EXEC</th>
</tr>
</thead>
</table>

**Usage Guidelines**

Use the `debug` command to display various errors or events in the Cisco ISE server, such as setup or configuration failures.

**Example**

```bash
ise/admin# debug all
ise/admin# mkdir disk:/1
ise/admin# 6 [15347]: utils: vsh_root_stubs.c[2742] [admin]: mkdir operation success
ise/admin# rmdir disk:/1
6 [15351]: utils: vsh_root_stubs.c[2601] [admin]: Invoked Remove Directory disk:/1 command
6 [15351]: utils: vsh_root_stubs.c[2663] [admin]: Remove Directory operation success
ise/admin#
ise/admin# undebug all
ise/admin#
```
delete

To delete a file from the Cisco ISE server, use the **delete** command in EXEC mode. To remove deleting files from the Cisco ISE server, use the **no** form of this command.

**delete [filename disk:/path]**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>filename</strong></td>
<td>Filename. Supports up to 80 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>disk:/path</strong></td>
<td>Location of the file in the repository.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

If you attempt to delete a configuration file or image, the system prompts you to confirm the deletion. Also, if you attempt to delete the last valid system image, the system prompts you to confirm the deletion.

**Example**

```
ise/admin# delete disk:/hs_err_pid19962.log
ise/admin#
```
To list a file from the Cisco ISE server, use the `dir` command in EXEC mode. To remove this function, use the `no` form of this command.

```
dir

dir disk:/logs

dir recursive
```

**Syntax Description**

- `directory-name` (Optional). Lists directories and files in the local file system.

- `recursive` (Optional). Lists directories and files in the local file system.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

None.

### Example 1

```
ise/admin# dir
Directory of disk:/
2034113 Aug 05 2010 19:58:39 ADElogs.tar.gz
4096 Jun 10 2010 02:34:03 activemq-data/
4096 Aug 04 2010 23:14:53 logs/
16384 Jun 09 2010 02:59:34 lost+found/
4096 Aug 04 2010 23:15:20 target/
4096 Aug 05 2010 12:25:55 temp/
Usage for disk: filesystem
8076189696 bytes total used
6371618816 bytes free
15234142208 bytes available
ise/admin#
```

### Example 2

```
ise/admin# dir disk:/logs
0 Aug 05 2010 11:53:52 usermgmt.log
Usage for disk: filesystem
8076189696 bytes total used
6371618816 bytes free
15234142208 bytes available
ise/admin#
```
Example 3

ise/admin# dir recursive
Directory of disk:/
  2034113 Aug 05 2010 19:58:39 ADElogs.tar.gz
  4096 Jun 10 2010 02:34:03 activemq-data/
  4096 Aug 04 2010 23:14:53 logs/
  16384 Jun 09 2010 02:59:34 lost+found/
  4096 Aug 04 2010 23:15:20 target/
  4096 Aug 05 2010 12:25:55 temp/
Directory of disk:/logs
Directory of disk:/temp
Directory of disk:/activemq-data
Directory of disk:/activemq-data/localhost
Directory of disk:/activemq-data/localhost/journal
Directory of disk:/activemq-data/localhost/kr-store
Directory of disk:/activemq-data/localhost/kr-store/data
Directory of disk:/activemq-data/localhost/kr-store/state
Directory of disk:/activemq-data/localhost/tmp_storage
Directory of disk:/target
Directory of disk:/target/logs
Directory of disk:/lost+found
Usage for disk: filesystem
  8076189696 bytes total used
  6371618816 bytes free
  15234142208 bytes available
ise/admin#
exit

To close an active terminal session by logging out of the Cisco ISE server or to move up one mode level from configuration mode, use the **exit** command in EXEC mode.

This command has no keywords and arguments.

**exit**

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Example**

```
ise/admin# config t
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# exit
ise/admin#
```
forceout

To force users out of an active terminal session by logging them out of the Cisco ISE server, use the `forceout` command in EXEC mode.

```
forceout username
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Name of the user. Supports up to 31 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

Use the `forceout` command in EXEC mode to force a user from an active session.

**Example**

```
ise/admin# forceout user1
ise/admin#
```
halt

To shut down and power off the system, use the `halt` command in EXEC mode.

This command has no keywords and arguments.

`halt`

**Command Default**
No default behavior or values.

**Command Modes**
EXEC

**Usage Guidelines**
Before you issue the `halt` command, ensure that Cisco ISE is not performing any backup, restore, installation, upgrade, or remove operation. If you issue the `halt` command while the Cisco ISE is performing any of these operations, you will get one of the following warning messages:

WARNING: A backup or restore is currently in progress! Continue with halt?
WARNING: An install/upgrade/remove is currently in progress! Continue with halt?

If you get any of these warnings, enter Yes to continue the halt operation, or enter No to cancel the halt.

If no processes are running when you use the `halt` command or if you enter Yes in response to the warning message displayed, then you must respond to the following question:

Do you want to save the current configuration?

If you enter Yes to save the existing Cisco ISE configuration, the following message is displayed:

Saved the running configuration to startup successfully

**Example**

```
ise/admin# halt
ise/admin#
```
help

To display the interactive help system for the Cisco ISE server, use the help command in EXEC mode. This command has no keywords and arguments.

help

Command Default
No default behavior or values.

Command Modes
EXEC and all Configuration (config).

Usage Guidelines
The help command provides a brief description of the context-sensitive help system.

- To list all commands available for a particular command mode, enter a question mark (?) at the system prompt.

- To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by ?. This form of help is called word help because it lists only the keywords or arguments that begin with the abbreviation that you entered.

- To list the keywords and arguments associated with a command, enter ? in place of a keyword or argument on the command line. This form of help is called command syntax help, because it lists the keywords or arguments that apply based on the command, keywords, and arguments that you enter.

Example

ise/admin# help
Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument (e.g. 'show?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?').
ise/admin#
To create a new directory in the Cisco ISE server, use the **mkdir** command in EXEC mode.

**Syntax Description**

| directory-name | Name of the directory to create. Supports up to 80 alphanumeric characters. Use `disk:/directory-name`. |

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

Use `disk:/directory-name`; otherwise, an error appears that indicates that the `disk:/directory-name` must be included.

**Example**

```plaintext
ise/admin# mkdir disk:/test
ise/admin# dir
Directory of disk:/
  4096 May 06 2010 13:34:49 activemq-data/
  4096 May 06 2010 13:40:59 logs/
  16384 Mar 01 2010 16:07:27 lost+found/
  4096 May 06 2010 13:42:53 target/
  4096 May 07 2010 12:26:04 test/
Usage for disk: filesystem
    181067776 bytes total used
    19084521472 bytes free
    20314165248 bytes available
ise/admin#
```
nslookup

To look up the hostname of a remote system in the Cisco ISE server, use the \texttt{nslookup} command in EXEC mode.

\begin{verbatim}
nslookup \{ip-address \| hostname\}
nslookup [ \{ip-address \| hostname\} name-server \{ip-address \}]
nslookup [ \{ip-address \| hostname\} querytype AAAA]
\end{verbatim}

\textbf{Syntax Description}

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{ip-address}</td>
<td>IPv4 or IPv6 address of a remote system. Supports up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td>\texttt{hostname}</td>
<td>Hostname of a remote system. Supports up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td>AAAA</td>
<td>Queries the Internet domain name server for an IPv6 address that corresponds to a website name.</td>
</tr>
<tr>
<td>\texttt{name-server}</td>
<td>Specifies an alternative name server. Supports up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td>\texttt{querytype}</td>
<td>Queries the IPv4 or IPv6 address or hostname of a remote system. It includes query types, such as PTR, A, AAAA, and SRV. Supports up to 16 alphanumeric characters.</td>
</tr>
</tbody>
</table>

\textbf{Command Default}

No default behavior or values.

\textbf{Command Modes}

EXEC

\textbf{Example 1}

\begin{verbatim}
ise/admin# nslookup 1.2.3.4
Trying "4.3.2.1.in-addr.arpa"
Received 127 bytes from 171.70.168.183#53 in 1 ms
Trying "4.3.2.1.in-addr.arpa"
Host 4.3.2.1.in-addr.arpa. not found: 3(NXDOMAIN)
Received 127 bytes from 171.70.168.183#53 in 1 ms
ise/admin#
\end{verbatim}

\textbf{Example 2}

\begin{verbatim}
ise/admin# nslookup ipv6.google.com querytype AAAA
Server: 10.106.230.244
Address: 10.106.230.244#53
Non-authoritative answer:
ipv6.1.google.com has AAAA address 2404:6800:4007:803::1001
Authoritative answers can be found from:
google.com nameserver = ns4.google.com.
google.com nameserver = ns3.google.com.
\end{verbatim}
nslookup

google.com  nameserver = ns2.google.com.
google.com  nameserver = ns1.google.com.
ns1.google.com  internet address = 216.239.32.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  internet address = 216.239.38.10
ise/admin#
password

To update the CLI account password, use the `password` command in EXEC mode.

```plaintext
password
```

---

**Note**

When you create a password for the administrator during installation or after installation in the CLI, do not use the $ character, except when it is the last character of the password. If that character is first or inside the other characters, the password is accepted, but you cannot use it to log on to the CLI.

You can fix this by logging into the console and using the CLI command, or by getting an ISE CD or ISO file. Instructions for using an ISO to reset the password are explained in the following document:


---

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter old password</td>
<td>Enter the current CLI password.</td>
</tr>
<tr>
<td>Enter new password</td>
<td>Enter the new CLI password.</td>
</tr>
<tr>
<td>Confirm new password</td>
<td>Confirm the new CLI password.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

**Example**

```plaintext
ise/admin# password
Enter old password:
Enter new password:
Confirm new password:
ise/admin#
```
patch install

Before attempting to use the `patch install` command to install a patch, you must read the patch installation instructions in the release notes supplied with the patch. The release notes contains important updated instructions; and they must be followed.

To install a patch bundle of the application on a specific node from the CLI, use the `patch install` command in EXEC mode.

```bash
patch install patch-bundle repository
```

**Note**

In a Cisco ISE distributed deployment environment, install the patch bundle from the Admin portal so that the patch bundle is automatically installed on all the secondary nodes.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>install</code></td>
<td>Installs a specific patch bundle of the application.</td>
</tr>
<tr>
<td><code>patch-bundle</code></td>
<td>The patch bundle file name. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td><code>repository</code></td>
<td>Installs the patch in the specified repository name. Supports up to 255 alphanumeric characters.</td>
</tr>
</tbody>
</table>

If you have the primary Administration node (PAN) auto-failover configuration enabled in your deployment, disable it before you install the patch. Enable the PAN auto-failover configuration after patch installation is complete on all the nodes in your deployment.

When you install a patch on Release 2.0, the patch installation process does not prompt you to verify the hash value of the software. Beginning from Release 2.0 onwards, the patch installation software automatically verifies the integrity of the patch software using digital signatures. See the example given below for a sample output of the `patch install` command.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

Installs a specific patch bundle of the application.

If you attempt to install a patch that is an older version of the existing patch, then you receive the following error message:

```
% Patch to be installed is an older version than currently installed version.
```

To view the status of a patch installation from the CLI, you must check the ade.log file in the Cisco ISE support bundle.

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.
```

Disable the PAN auto-failover configuration and enable it after patch installation is complete on all the nodes in your deployment.
Example

ise/admin# patch install ise-patchbundle-2.0.0.306-Patch2-164765.SPA.x86_64.tar.gz disk
%Warning: Patch will be installed only on this node. Install using Primary Administration node GUI to install on all nodes in deployment. Continue? (yes/no) [yes] ?
Save the current ADE-OS running configuration? (yes/no) [yes] ?
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Initiating Application Patch installation...
Getting bundle to local machine...
Unbundling Application Package...
Verifying Application Signature...
Patch successfully installed
ise/admin#
### patch remove

Before attempting to use the `patch remove` command to rollback a patch, you must read the rollback instructions of the patch in the release notes supplied with the patch. The release notes contains important updated instructions: and they must be followed.

To remove a specific patch bundle version of the application, use the `patch remove` command in EXEC mode.

```bash
patch [ remove {application_name | version}]
```

**Note**

In a Cisco ISE distributed deployment environment, removing the patch bundle from the Admin portal automatically removes the patch from the secondary nodes.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>remove</code></td>
<td>The command that removes a specific patch bundle version of the application.</td>
</tr>
<tr>
<td><code>application_name</code></td>
<td>The name of the application for which the patch is to be removed. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td><code>version</code></td>
<td>The patch version number to be removed. Supports up to 255 alphanumeric characters.</td>
</tr>
</tbody>
</table>

If you have the primary Administration node (PAN) auto-failover configuration enabled in your deployment, disable it before you remove a patch. You can enable the PAN auto-failover configuration after patch removal is complete.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>No default behavior or values.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC</td>
</tr>
<tr>
<td>Usage Guidelines</td>
<td>If you attempt to remove a patch that is not installed, then you receive the following error message:</td>
</tr>
</tbody>
</table>

```
% Patch is not installed
```

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# patch remove ise 3
Continue with application patch uninstall? [y/n] y
Application patch successfully uninstalled
ise/admin#
```

**Example 2**

```
ise/admin# patch remove ise 3
```
Continue with application patch uninstall? [y/n]  y
% Patch is not installed
ise/admin#
To diagnose the basic IPv4 network connectivity to a remote system, use the `ping` command in EXEC mode.

`ping {ip-address | hostname} [df df] [packetsize packetsize] [pingcount pingcount]`

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the system to ping. Supports up to 32 alphanumeric characters.</td>
</tr>
<tr>
<td><code>hostname</code></td>
<td>Hostname of the system to ping. Supports up to 32 alphanumeric characters.</td>
</tr>
<tr>
<td><code>df</code></td>
<td>Specify the value as 1 to prohibit packet fragmentation, or 2 to fragment the packets locally, or 3 to not set df.</td>
</tr>
<tr>
<td><code>packetsize</code></td>
<td>(Optional). Size of the ping packet.</td>
</tr>
<tr>
<td><code>packetsize</code></td>
<td>Specify the size of the ping packet; the value can be between 0 and 65507.</td>
</tr>
<tr>
<td><code>pingcount</code></td>
<td>(Optional). Number of ping echo requests.</td>
</tr>
<tr>
<td><code>pingcount</code></td>
<td>Specify the number of ping echo requests; the value can be between 1 and 10.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

The `ping` command sends an echo request packet to an address, and then waits for a reply. The ping output can help you evaluate path-to-host reliability, delays over the path, and whether or not you can reach a host.

**Example**

```
ise/admin# ping 172.16.0.1 df 2 packetsize 10 pingcount 2
PING 172.16.0.1 (172.16.0.1) 10(38) bytes of data.
18 bytes from 172.16.0.1: icmp_seq=0 ttl=40 time=306 ms
18 bytes from 172.16.0.1: icmp_seq=1 ttl=40 time=300 ms
--- 172.16.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 300.302/303.557/306.812/3.255 ms, pipe 2
ise/admin#
```
ping6

To diagnose the basic IPv6 network connectivity to a remote system, use the ping6 command in EXEC mode. This is similar to the IPv4 ping command.

```
ping6 {ip-address} [GigabitEthernet {0-3}][packetsize {packetsize}][pingcount {pingcount}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-address</strong></td>
<td>IP address of the system to ping. Supports up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>GigabitEthernet</strong></td>
<td>(Optional). Ethernet interface.</td>
</tr>
<tr>
<td><strong>0-3</strong></td>
<td>Select an Ethernet interface.</td>
</tr>
<tr>
<td><strong>packetsize</strong></td>
<td>(Optional). Size of the ping packet.</td>
</tr>
<tr>
<td><strong>packetsize</strong></td>
<td>Specify the size of the ping packet; the value can be between 0 and 65507.</td>
</tr>
<tr>
<td><strong>pingcount</strong></td>
<td>(Optional). Number of ping echo requests.</td>
</tr>
<tr>
<td><strong>pingcount</strong></td>
<td>Specify the number of ping echo requests; the value can be between 1 and 10.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

The ping6 command sends an echo request packet to an address, and then waits for a reply. The ping output can help you evaluate path-to-host reliability, delays over the path, and whether or not you can reach a host.

The ping6 command is similar to the existing ping command. The ping6 command does not support the IPv4 packet fragmentation (df, as described in the ping command) options, but it allows an optional specification of an interface. The interface option is primarily useful for pinning with link-local addresses that are interface-specific addresses. The packetsize and pingcount options work the same way as they do with the ping command.

**Example 1**

```
ise/admin# ping6 3ffe:302:11:2:20c:29ff:feaf:da05
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=0 ttl=64 time=0.599 ms
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=1 ttl=64 time=0.150 ms
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=2 ttl=64 time=0.070 ms
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=3 ttl=64 time=0.065 ms
4 packets transmitted, 4 received, 0% packet loss, time 3118ms
rt min/avg/max/mdev = 0.065/0.221/0.599/0.220 ms, pipe 2
ise/admin#
```
Example 2

ise/admin# ping6 3ffe:302:11:2:20c:29ff:feaf:da05 GigabitEthernet 0 packetsize 10 pingcount 2
18 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=0 ttl=64 time=0.073 ms
18 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=1 ttl=64 time=0.073 ms
2 packets transmitted, 2 received, 0% packet loss, time 1040ms
rat min./aft/max/endive = 0.073/0.073/0.073/0.000 ms, pipe 2
ise/admin#
reload

This command has no keywords and arguments. To reboot the Cisco ISE operating system, use the `reload` command in EXEC mode.

**reload**

**Command Default**
No default behavior or values.

**Command Modes**
EXEC

**Usage Guidelines**
The `reload` command reboots the system. Use the `reload` command after you enter configuration information into a file and save the running-configuration to the persistent startup-configuration on the CLI and save any settings in the Cisco ISE Admin portal session.

Before you issue the `reload` command, ensure that Cisco ISE is not performing any backup, restore, installation, upgrade, or remove operation. If Cisco ISE performs any of these operations and you issue the `reload` command, you will get one of the following warning messages:

WARNING: A backup or restore is currently in progress! Continue with reload?
WARNING: An install/upgrade/remove is currently in progress! Continue with reload?

If you get any of these warnings, enter Yes to continue with the reload operation, or No to cancel it.

If no processes are running when you use the `reload` command or you enter Yes in response to the warning message displayed, you must respond to the following question:

Do you want to save the current configuration?

If you enter Yes to save the existing Cisco ISE configuration, the following message is displayed:

Saved the running configuration to startup successfully

If you have auto-failover enabled in your deployment, you receive the following warning message:

PAN Auto Failover feature is enabled, therefore this operation will trigger a failover if ISE services are not restarted within the fail-over window. Do you want to continue (y/n)?

Type 'y' if you want to continue or 'n' if you want to abort.

**Example**

ise/admin# reload
Do you want to save the current configuration? (yes/no) [yes]? yes
Generating configuration...
Saved the running configuration to startup successfully
Continue with reboot? [y/n] y
Broadcast message from root (pts/0) Fri Aug 7 13:26:46 2010:
The system is going down for reboot NOW!
ise/admin#
reset-config

To reset the ADE-OS network configurations such as ip address/mask/gateway, hostname, domain name, DNS server, and NTP server using the `reset-config` command in EXEC mode. These parameters are essentially the same parameters as that is prompted during setup. The administrator will not be prompted for admin password from this CLI. This command will also not reset the current ISE configuration or operations data as these tasks are achieved by using the `application reset-config` command.

**reset-config**

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

All services will be restarted upon completion.

**Note**

Updating the hostname will cause any certificate using the old hostname to become invalid. A new self-signed certificate using the new hostname will be generated now for use with HTTPS/EAP. If CA-signed certificates are used on this node, import the new ones with the correct hostname. In addition, if this node is part of an AD domain, delete any AD memberships before proceeding.
restore

To restore a previous backup of the system, use the `restore` command in EXEC mode. A restore operation restores data related to the Cisco ISE and the Cisco ADE OS.

Use the following command to restore data related to the Cisco ISE application and Cisco ADE OS:

```
restore [{filename} repository {repository-name} encryption-key hash | plain {encryption-key-name}] 
```

```
restore [{filename} repository {repository-name} encryption-key hash | plain {encryption-key-name} include-adeos]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filename</td>
<td>Name of the backed-up file that resides in the repository. Supports up to 120 alphanumeric characters. <strong>Note</strong>: You must add the <code>.tar.gpg</code> extension after the filename (for example, <code>myfile.tar.gpg</code>).</td>
</tr>
<tr>
<td>repository</td>
<td>The repository command.</td>
</tr>
<tr>
<td>repository-name</td>
<td>Name of the repository from which you want to restore the backup. Supports up to 120 characters.</td>
</tr>
<tr>
<td>encryption-key</td>
<td>(Optional). Specifies user-defined encryption key to restore backup.</td>
</tr>
<tr>
<td>hash</td>
<td>Hashed encryption key for restoring backup. Specifies an encrypted (hashed) encryption key that follows. Supports up to 40 characters.</td>
</tr>
<tr>
<td>plain</td>
<td>Plaintext encryption key for restoring backup. Specifies an unencrypted plaintext encryption key that follows. Supports up to 15 characters.</td>
</tr>
<tr>
<td>encryption-key-name</td>
<td>Specifies encryption key in hash</td>
</tr>
<tr>
<td>include-adeos</td>
<td>Restores back up and reboots Cisco ISE, if ADE-OS configuration data is present in the backup.</td>
</tr>
</tbody>
</table>

If you have the Primary Administration Node (PAN) auto-failover configuration enabled in your deployment, disable this configuration before you restore a backup. You can enable the PAN auto-failover configuration after the restore is complete.

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Usage Guidelines

When you use restore commands in Cisco ISE, the Cisco ISE server restarts automatically.

The encryption key is optional while restoring data. To support restoring earlier backups where you have not provided encryption keys, you can use the `restore` command without the encryption key.
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.

Note

Restoring from Cisco ISE, Release 1.0 and Cisco ISE, Release 1.0 MR backups are not supported in Cisco ISE, Release 1.2.

Note

Cisco ISE, Release 1.4 supports restore from backups obtained from Release 1.2 and later.

Restoring Cisco ISE Configuration Data from the Backup

To restore Cisco ISE configuration data from the backup, use the following command:

```
restore mybackup-CFG-121025-2348.tar.gpg repository myrepository encryption-key plain lablab12
```

Example

```
ise/admin# restore latest-jul-15-CFG-140715-2055.tar.gpg repository CUSTOMER-DB-sftp encryption-key plain Test_1234
% Warning: Do not use Ctrl-C or close this terminal window until the restore completes.
Initiating restore. Please wait...
% restore in progress: Starting Restore...10% completed
% restore in progress: Decrypting backup data...25% completed
% restore in progress: Extracting backup data...30% completed
Leaving the currently connected AD domain
% restore in progress: Adjusting host data for upgrade...65% completed
UPGRADE STEP 1: Running ISE configuration DB schema upgrade...
- Running db sanity check to fix index corruption, if any...
  UPGRADE STEP 2: Running ISE configuration data upgrade...
  - Data upgrade step 1/67, NSFUpgradeService(1.2.1.127)... Done in 0 seconds.
  - Data upgrade step 2/67, NetworkAccessUpgrade(1.2.1.127)... Done in 0 seconds.
  - Data upgrade step 3/67, GuestUpgradeService(1.2.1.146)... Done in 43 seconds.
  - Data upgrade step 4/67, NetworkAccessUpgrade(1.2.1.148)... Done in 2 seconds.
  - Data upgrade step 5/67, NetworkAccessUpgrade(1.2.1.150)... Done in 2 seconds.
  - Data upgrade step 6/67, NSFUpgradeService(1.2.1.181)... Done in 0 seconds.
  - Data upgrade step 7/67, NSFUpgradeService(1.3.0.100)... Done in 0 seconds.
  - Data upgrade step 8/67, RegisterPostureTypes(1.3.0.170)... Done in 0 seconds.
  - Data upgrade step 9/67, ProfilerUpgradeService(1.3.0.187)?... Done in 5 seconds.
  - Data upgrade step 10/67, GuestUpgradeService(1.3.0.194)... Done in 2 seconds.
  - Data upgrade step 11/67, NetworkAccessUpgrade(1.3.0.200)... Done in 0 seconds.
  - Data upgrade step 12/67, GuestUpgradeService(1.3.0.208)... Done in 2 seconds.
  - Data upgrade step 13/67, GuestUpgradeService(1.3.0.220)... Done in 0 seconds.
  - Data upgrade step 14/67, RBACUpgradeService(1.3.0.228)... Done in 15 seconds.
  - Data upgrade step 15/67, NetworkAccessUpgrade(1.3.0.230)... Done in 3 seconds.
  - Data upgrade step 16/67, GuestUpgradeService(1.3.0.250)... Done in 0 seconds.
  - Data upgrade step 17/67, NetworkAccessUpgrade(1.3.0.250)... Done in 0 seconds.
  - Data upgrade step 18/67, RBACUpgradeService(1.3.0.334)... Done in 9 seconds.
  - Data upgrade step 19/67, RBACUpgradeService(1.3.0.335)... Done in 9 seconds.
```
- Data upgrade step 20/67, ProfilerUpgradeService(1.3.0.360) ... Done in 236 seconds.
- Data upgrade step 21/67, ProfilerUpgradeService(1.3.0.380) ... Done in 4 seconds.
- Data upgrade step 22/67, NSFUpgradeService(1.3.0.401) ... Done in 0 seconds.
- Data upgrade step 23/67, NSFUpgradeService(1.3.0.406) ... Done in 0 seconds.
- Data upgrade step 24/67, NSFUpgradeService(1.3.0.410) ... Done in 2 seconds.
- Data upgrade step 25/67, RBACUpgradeService(1.3.0.423) ... Done in 0 seconds.
- Data upgrade step 26/67, NetworkAccessUpgrade(1.3.0.424) ... Done in 0 seconds.
- Data upgrade step 27/67, RBACUpgradeService(1.3.0.433) ... Done in 1 seconds.
- Data upgrade step 28/67, EgressUpgradeService(1.3.0.437) ... Done in 1 seconds.
- Data upgrade step 29/67, NSFUpgradeService(1.3.0.438) ... Done in 0 seconds.
- Data upgrade step 30/67, NSFUpgradeService(1.3.0.439) ... Done in 0 seconds.
- Data upgrade step 31/67, CdaRegistration(1.3.0.446) ... Done in 2 seconds.
- Data upgrade step 32/67, RBACUpgradeService(1.3.0.452) ... Done in 16 seconds.
- Data upgrade step 33/67, NetworkAccessUpgrade(1.3.0.458) ... Done in 0 seconds.
- Data upgrade step 34/67, NSFUpgradeService(1.3.0.461) ... Done in 0 seconds.
- Data upgrade step 35/67, CertMgmtUpgradeService(1.3.0.462) ... Done in 3 seconds.
- Data upgrade step 36/67, NetworkAccessUpgrade(1.3.0.476) ... Done in 0 seconds.
- Data upgrade step 37/67, TokenUpgradeService(1.3.0.500) ... Done in 1 seconds.
- Data upgrade step 38/67, NSFUpgradeService(1.3.0.508) ... Done in 0 seconds.
- Data upgrade step 39/67, RBACUpgradeService(1.3.0.509) ... Done in 17 seconds.
- Data upgrade step 40/67, NSFUpgradeService(1.3.0.526) ... Done in 0 seconds.
- Data upgrade step 41/67, NSFUpgradeService(1.3.0.531) ... Done in 0 seconds.
- Data upgrade step 42/67, MDMUpgradeService(1.3.0.536) ... Done in 0 seconds.
- Data upgrade step 43/67, NSFUpgradeService(1.3.0.554) ... Done in 0 seconds.
- Data upgrade step 44/67, NetworkAccessUpgrade(1.3.0.561) ... Done in 3 seconds.
- Data upgrade step 45/67, RBACUpgradeService(1.3.0.563) ... Done in 19 seconds.
- Data upgrade step 46/67, CertMgmtUpgradeService(1.3.0.615) ... Done in 0 seconds.
- Data upgrade step 47/67, CertMgmtUpgradeService(1.3.0.616) ... Done in 15 seconds.
- Data upgrade step 48/67, CertMgmtUpgradeService(1.3.0.617) ... Done in 2 seconds.
- Data upgrade step 49/67, OcspServiceUpgradeRegistration(1.3.0.617) ... Done in 0 seconds.
- Data upgrade step 50/67, NSFUpgradeService(1.3.0.630) ... Done in 0 seconds.
- Data upgrade step 51/67, NSFUpgradeService(1.3.0.631) ... Done in 0 seconds.
- Data upgrade step 52/67, CertMgmtUpgradeService(1.3.0.634) ... Done in 0 seconds.
- Data upgrade step 53/67, RBACUpgradeService(1.3.0.650) ... Done in 8 seconds.
- Data upgrade step 54/67, CertMgmtUpgradeService(1.3.0.653) ... Done in 0 seconds.
- Data upgrade step 55/67, NodeGroupUpgradeService(1.3.0.655) ... Done in 1 seconds.
- Data upgrade step 56/67, RBACUpgradeService(1.3.0.670) ... Done in 4 seconds.
- Data upgrade step 57/67, ProfilerUpgradeService(1.3.0.670) ... Done in 0 seconds.
- Data upgrade step 58/67, ProfilerUpgradeService(1.3.0.671) ... Done in 0 seconds.
- Data upgrade step 59/67, ProfilerUpgradeService(1.3.0.675) ... Done in 2118 seconds.
- Data upgrade step 60/67, NSFUpgradeService(1.3.0.676) ... Done in 1 seconds.
- Data upgrade step 61/67, Auth2UpgradeService(1.3.0.676) ... Done in 20 seconds.
- Data upgrade step 62/67, GuestAccessUpgradeService(1.3.0.676) ... Done in 454 seconds.
- Data upgrade step 63/67, NSFUpgradeService(1.3.0.694) ... Done in 0 seconds.
- Data upgrade step 64/67, ProvisioningRegistration(1.3.0.700) ... Done in 0 seconds.
- Data upgrade step 65/67, RegisterPostureTypes(1.3.0.705) ... Done in 0 seconds.
- Data upgrade step 66/67, CertMgmtUpgradeService(1.3.0.727) ... Done in 0 seconds.
- Data upgrade step 67/67, ProvisioningUpgradeService(1.3.105.181) ... Done in 103 seconds.

UPGRADE STEP 3: Running ISE configuration data upgrade for node specific data...
% restore in progress: Restoring logs...75% completed
% restore in progress: Restarting ISE Services...90% completed
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE Identity Mapping Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...

Cisco Identity Services Engine CLI Reference Guide, Release 2.6

79
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise' CLI to verify all processes are in running state.
% restore in progress: Completing Restore...100% completed
ise/admin#

Restoring Cisco ISE Operational Data from the Backup

To restore Cisco ISE operational data from the backup, use the following command:

```
restore mybackup-OPS-130103-0019.tar.gpg repository myrepository encryption-key plainlablab12
```

Example

```
ise/admin# restore mybackup-OPS-130103-0019.tar.gpg repository myrepository encryption-key plainlablab12
% Warning: Do not use Ctrl-C or close this terminal window until the restore completes.
Initiating restore. Please wait...
% restore in progress: Starting Restore...10% completed
% restore in progress: Retrieving backup file from Repository...20% completed
% restore in progress: Decrypting backup data...40% completed
% restore in progress: Extracting backup data...50% completed
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Application Server...
Stopping ISE Profiler DB...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
% restore in progress: starting dbrestore.......55% completed
% restore in progress: ending dbrestore.......75% completed
checking for upgrade
Starting M&T DB upgrade
ISE Database processes already running, PID: 30124
ISE M&T Session Database is already running, PID: 484
Starting ISE Profiler DB...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Log Collector...
ISE M&T Log Processor is already running, PID: 837
Note: ISE Processes are initializing. Use 'show application status ise' CLI to verify all processes are in running state.
% restore in progress: Completing Restore...100% completed
ise/admin#
```

Restoring Cisco ISE Configuration Data and Cisco ADE OS data from the Backup

To restore Cisco ISE configuration data including Cisco ISE ADE OS data, use the following command:

```
restore mybackup-CFG-130405-0044.tar.gpg repository myrepository encryption-key plainMykey123 include-adeos
```

Example

```
ise/admin# restore mybackup-CFG-130405-0044.tar.gpg repository myrepository encryption-key
```
plain Mykey123 include-adeos
% Warning: Do not use Ctrl-C or close this terminal window until the restore completes.
Initiating restore. Please wait...
% restore in progress: Starting Restore...10% completed
% restore in progress: Retrieving backup file from Repository...20% completed
% restore in progress: Decrypting backup data...25% completed
% restore in progress: Extracting backup data...30% completed
% restore in progress: Stopping ISE processes required for restore...35% completed
% restore in progress: Restoring ISE configuration database...40% completed
% restore in progress: Updating Database metadata...70% completed
% restore in progress: Restoring logs...75% completed
% restore in progress: Performing ISE Database synchup...80% completed
% restore in progress: Completing Restore...100% completed
Broadcast message from root (pts/2) (Fri Apr  5 01:40:04 2013):
The system is going down for reboot NOW!
Broadcast message from root (pts/2) (Fri Apr  5 01:40:04 2013):
The system is going down for reboot NOW!
ise/admin#
rmdir

To remove an existing directory, use the `rmdir` command in EXEC mode.

```
rmdir directory-name
```

**Syntax Description**

- `directory-name`: Directory name. Supports up to 80 alphanumeric characters.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Example**

```
ise/admin# mkdir disk:/test
ise/admin# dir
Directory of disk:/
  4096 May 06 2010 13:34:49 activemq-data/
  4096 May 06 2010 13:40:59 logs/
  16384 Mar 01 2010 16:07:27 lost+found/
  4096 May 06 2010 13:42:53 target/
  4096 May 07 2010 12:26:04 test/
Usage for disk: filesystem
  181067776 bytes total used
  19084521472 bytes free
  20314165248 bytes available
ise/admin#
ise/admin# rmdir disk:/test
ise/admin# dir
Directory of disk:/
  4096 May 06 2010 13:34:49 activemq-data/
  4096 May 06 2010 13:40:59 logs/
  16384 Mar 01 2010 16:07:27 lost+found/
  4096 May 06 2010 13:42:53 target/
Usage for disk: filesystem
  181063680 bytes total used
  19084525568 bytes free
  20314165248 bytes available
ise/admin#
```
**ssh**

To start an encrypted session with a remote system, use the `ssh` command in EXEC mode.

An administrator or user can use this command

```
ssh [{ip-address | hostname}] [username] [ port {port number | version {1 | 2}}]

ssh delete host {ip-address | hostname}
```

**Syntax Description**

- `ip-address` - IPv4/IPv6 address of the remote system. Supports up to 64 alphanumeric characters.
- `hostname` - Hostname of the remote system. Supports up to 64 alphanumeric characters.
- `username` - Username of the user logging in through SSH.
- `port` - (Optional). Indicates the port number of the remote host.
- `port number` - The valid range of ports is from 0 to 65,535. The default port is 22.
- `version` - (Optional). Indicates the version number.
- `version number` - The SSH version number 1 and 2. The default SSH version is 2.
- `delete` - Deletes the SSH fingerprint for a specific host.
- `host` - Hostname of the remote system for which the host key will be deleted.
- `ip-address` - IPv4/IPv6 address of the remote system. Supports up to 64 alphanumeric characters.
- `hostname` - Hostname of the remote system. Supports up to 64 alphanumeric characters.

**Command Default**

Disabled.

**Command Modes**

EXEC

**Usage Guidelines**

The `ssh` command enables a system to make a secure, encrypted connection to another remote system or server. With authentication and encryption, the SSH client allows for secure communication over an insecure network.
Example 1

ise/admin# ssh 172.79.21.96 admin port 22 version 2
ssh: connect to host 172.79.21.96 port 22: No route to host
ise/admin#

Example 2

ise/admin# ssh delete host ise
ise/admin#
To dump traffic on a selected network interface, use the `tech` command in EXEC mode.

```
tech dumptcp \{interface-number | count | package-count\}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dumptcp</code></td>
<td>Dumps TCP package to the console.</td>
</tr>
<tr>
<td><code>interface-number</code></td>
<td>Gigabit Ethernet interface number (0 to 3).</td>
</tr>
<tr>
<td><code>count</code></td>
<td>Specifies a maximum package count, and default is continuous (no limit).</td>
</tr>
<tr>
<td><code>package-count</code></td>
<td>Supports 1–10000.</td>
</tr>
<tr>
<td><code>iostat</code></td>
<td>Dumps Central Processing Unit (CPU) statistics and input/output statistics to the console for every 3 seconds. See Linux <code>iostat</code> command.</td>
</tr>
<tr>
<td><code>iotop</code></td>
<td>Provides accurate I/O usage per process on ISE node.</td>
</tr>
<tr>
<td><code>mpstat</code></td>
<td>Dumps processors related information sent to the console. See Linux <code>mpstat</code> command.</td>
</tr>
<tr>
<td><code>netstat</code></td>
<td>Dumps network related information sent to the console for every 3 seconds. See Linux <code>netstat</code> command.</td>
</tr>
<tr>
<td><code>top</code></td>
<td>Dumps a dynamic real-time view of a running system, which runs in batch mode for every 5 seconds. See Linux <code>top</code> command.</td>
</tr>
<tr>
<td><code>support-tunnel</code></td>
<td>Cisco ISE uses the Cisco IronPort Tunnel infrastructure to create a secure tunnel for Cisco technical support engineers to connect to an ISE server in your deployment and troubleshoot issues with the system. Cisco ISE uses SSH to create the secure connection through the tunnel. As an administrator, you can control the tunnel access; you can choose when and how long to grant access to the support engineer. Cisco customer support cannot establish the tunnel without your intervention. You will receive notification about the service logins. You can disable the tunnel connection at any point of time.</td>
</tr>
<tr>
<td><code>vmstat</code></td>
<td>Dumps summary information of memory, processes, and paging for every 3 seconds. See Linux <code>vmstat</code> command.</td>
</tr>
</tbody>
</table>

### Command Default

Disabled.
If you see bad UDP checksum warnings in the tech dump tcp output, it may not be a cause for concern. The `tech dump tcp` command examines outgoing packets before they exit through the Ethernet microprocessor. Most modern Ethernet chips calculate checksums on outgoing packets, and so the operating system software stack does not. Hence, it is normal to see outgoing packets declared as bad UDP checksum.

**Example 1**

```
ise/admin# tech dump tcp 0 count 2
Invoking tcpdump. Press Control-C to interrupt.
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
2 packets captured
2 packets received by filter
0 packets dropped by kernel
02:38:14.869291 IP (tos 0x0, ttl 110, id 4793, offset 0, flags [DF], proto: TCP (6), length: 40) 10.77.202.52.1598 > 172.21.79.91.22: ., cksum 0xe105 (correct),
   234903779:234903779(0) ack 664498841 win 6344
02:38:14.869324 IP (tos 0x0, ttl 64, id 19495, offset 0, flags [DF], proto: TCP (6), length: 200) 172.21.79.91.22 > 10.77.202.52.1598: P 49:209(160) ack 0 win
ise/admin#
```

**Example 2**

```
ise/admin# tech iostat
Linux 2.6.18-348.el5 (ise) 02/25/13
avg-cpu: %user %nice %system %iowait %steal %idle
          7.26 0.73 4.27 0.77 0.00 86.97
Device: tps Blk_read/s Blk_wrtn/s Blk_read Blk_wrtn
    sda  16.05  415.47  1802.16  3761049  16314264
    sda1  0.01  0.23  0.00  2053     22
    sda2  0.02  0.22  0.04  1982   354
    sda3  0.01  0.29  0.02  2626   152
    sda4  0.00  0.00  0.00     14      0
    sda5  0.00  0.16  0.00  1479      0
    sda6  0.49  0.24  7.45  2189    67400
    sda7 15.51  414.27 1794.66  3750186  16246336
ise/admin#
```

**Example 3**

```
ise/admin# tech mpstat
Linux 2.6.18-348.el5 (ise) 02/25/13
02:41:25  CPU  %user  %nice  %sys  %iowait  %irq  %soft  %steal  %idle  intr/s
02:41:25   all    7.07  0.70  3.98  0.74  0.02  0.14  0.00  87.34  1015.49
ise/admin#
```
terminal length

To set the number of lines on the current terminal screen for the current session, use the terminal length command in EXEC mode.

**terminal length integer**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>length integer</td>
<td>Sets the number of lines on the current terminal screen for the current session. Number of lines on the screen. Contains between 0 to 511 lines, inclusive. A value of zero (0) disables pausing between screens of output.</td>
</tr>
</tbody>
</table>

**Command Default**
The default number of lines is 24 on the current terminal screen for the current session.

**Command Modes**
EXEC

**Usage Guidelines**
The system uses the length value to determine when to pause during multiple-screen output.

**Example**

```
ise/admin# terminal length 24
ise/admin#
```
# terminal session-timeout

To set the inactivity timeout for all sessions, use the `terminal session-timeout` command in EXEC mode.

```
terminal session-timeout minutes
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>session-timeout</code></td>
<td>Sets the inactivity timeout for all sessions.</td>
</tr>
<tr>
<td><code>minutes</code></td>
<td>Number of minutes for the inactivity timeout. The valid range is from 0 to 525,600. Zero (0) disables the timeout.</td>
</tr>
</tbody>
</table>

## Command Default

The default session-timeout is 30 minutes.

## Command Modes

EXEC

## Usage Guidelines

Setting the `terminal session-timeout` command to zero (0) results in no timeout being set.

## Example

```
ise/admin# terminal session-timeout 40
ise/admin#
```
terminal session-welcome

To set a welcome message on the system for all users who log in to the system, use the `terminal session-welcome` command in EXEC mode.

```
terminal session-welcome string
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>session-welcome</code></td>
<td>Sets a welcome message on the system for all users who log in to the system.</td>
</tr>
<tr>
<td><code>string</code></td>
<td>Welcome message. Supports up to 2023 alphanumeric characters. XML reserved characters are not allowed.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Usage Guidelines

Specify a welcome message that will appear on the screen on top of the command prompt when you log in to the CLI.

### Example

```
ise/admin# terminal session-welcome Welcome
ise/admin#
```
terminal terminal-type

To specify the type of terminal connected to the current line for the current session, use the *terminal terminal-type* command in EXEC mode.

**terminal terminal-type type**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>terminal-type</th>
<th>Specifies the type of terminal connected. The default terminal type is VT100.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>type</td>
<td>Defines the terminal name and type, and permits terminal negotiation by hosts that provide that type of service. Supports up to 80 alphanumerical characters.</td>
</tr>
</tbody>
</table>

**Command Default**

| Command Default | VT100 |

**Command Modes**

EXEC

**Usage Guidelines**

Indicate the terminal type if it is different from VT100.

**Example**

```
ise/admin# terminal terminal-type vt220
ise/admin#
```
**traceroute**

To discover the routes that packets take when traveling to their destination address, use the `traceroute` command in EXEC mode.

```
traceroute [ip-address | hostname]
```

**Syntax Description**

- **ip-address**
  - IPv4 address of the remote system. Supports up to 64 alphanumeric characters.
- **hostname**
  - Hostname of the remote system. Supports up to 64 alphanumeric characters.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Example**

```
ise/admin# traceroute 172.16.0.11
traceroute to 172.16.0.11 (172.16.0.11), 30 hops max, 38 byte packets
 1 172.16.0.11 0.067 ms 0.036 ms 0.032 ms
ise/admin#
```
# undebug

To disable debugging functions, use the `undebug` command in EXEC mode.

```plaintext
undebug [ all | application | backup-restore | cdp | config | copy | icmp | locks | logging | snmp | system | transfer | user | utils]
```

## Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Disables all debugging.</td>
</tr>
<tr>
<td><code>application</code></td>
<td>Application files.</td>
</tr>
<tr>
<td></td>
<td>• all—Disables all application debug output.</td>
</tr>
<tr>
<td></td>
<td>• install—Disables application install debug output.</td>
</tr>
<tr>
<td></td>
<td>• operation—Disables application operation debug output.</td>
</tr>
<tr>
<td></td>
<td>• uninstall—Disables application uninstall debug output.</td>
</tr>
<tr>
<td><code>backup-restore</code></td>
<td>Backs up and restores files.</td>
</tr>
<tr>
<td></td>
<td>• all—Disables all debug output for backup-restore.</td>
</tr>
<tr>
<td></td>
<td>• backup—Disables backup debug output for backup-restore.</td>
</tr>
<tr>
<td></td>
<td>• backup-logs—Disables backup-logs debug output for backup-restore.</td>
</tr>
<tr>
<td></td>
<td>• history—Disables history debug output for backup-restore.</td>
</tr>
<tr>
<td></td>
<td>• restore—Disables restore debug output for backup-restore.</td>
</tr>
<tr>
<td><code>cdp</code></td>
<td>Cisco Discovery Protocol configuration files.</td>
</tr>
<tr>
<td></td>
<td>• all—Disables all Cisco Discovery Protocol configuration debug output.</td>
</tr>
<tr>
<td></td>
<td>• config—Disables configuration debug output for Cisco Discovery Protocol.</td>
</tr>
<tr>
<td></td>
<td>• infra—Disables infrastructure debug output for Cisco Discovery Protocol.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>config</strong></td>
<td>Configuration files.</td>
</tr>
<tr>
<td>• all—Disables all configuration debug output.</td>
<td></td>
</tr>
<tr>
<td>• backup—Disables backup configuration debug output.</td>
<td></td>
</tr>
<tr>
<td>• clock—Disables clock configuration debug output.</td>
<td></td>
</tr>
<tr>
<td>• infra—Disables configuration infrastructure debug output.</td>
<td></td>
</tr>
<tr>
<td>• kron—Disables command scheduler configuration debug output.</td>
<td></td>
</tr>
<tr>
<td>• network—Disables network configuration debug output.</td>
<td></td>
</tr>
<tr>
<td>• repository—Disables repository configuration debug output.</td>
<td></td>
</tr>
<tr>
<td>• service—Disables service configuration debug output.</td>
<td></td>
</tr>
<tr>
<td><strong>copy</strong></td>
<td>Copy commands.</td>
</tr>
<tr>
<td><strong>icmp</strong></td>
<td>ICMP echo response configuration.</td>
</tr>
<tr>
<td>all—Disable all debug output for ICMP echo response configuration. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
<td></td>
</tr>
<tr>
<td><strong>locks</strong></td>
<td>Resource locking.</td>
</tr>
<tr>
<td>• all—Disables all resource locking debug output.</td>
<td></td>
</tr>
<tr>
<td>• file—Disables file locking debug output.</td>
<td></td>
</tr>
<tr>
<td><strong>logging</strong></td>
<td>Logging configuration files.</td>
</tr>
<tr>
<td>all—Disables all debug output for logging configuration.</td>
<td></td>
</tr>
<tr>
<td><strong>snmp</strong></td>
<td>SNMP configuration files.</td>
</tr>
<tr>
<td>all—Disables all debug output for SNMP configuration.</td>
<td></td>
</tr>
<tr>
<td><strong>system</strong></td>
<td>System files.</td>
</tr>
<tr>
<td>• all—Disables all system files debug output.</td>
<td></td>
</tr>
<tr>
<td>• id—Disables system ID debug output.</td>
<td></td>
</tr>
<tr>
<td>• info—Disables system info debug output.</td>
<td></td>
</tr>
<tr>
<td>• init—Disables system init debug output.</td>
<td></td>
</tr>
<tr>
<td>Command Default</td>
<td>Command Modes</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------</td>
</tr>
</tbody>
</table>
| No default behavior or values. | EXEC          | ise/admin# undebug all  
ise/admin# |

<table>
<thead>
<tr>
<th>transfer</th>
<th>File transfer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>User management.</td>
</tr>
<tr>
<td>• all—Disables all user management debug output.</td>
<td></td>
</tr>
<tr>
<td>• password-policy—Disables user management debug output for password-policy.</td>
<td></td>
</tr>
<tr>
<td>utils</td>
<td>Utilities configuration files.</td>
</tr>
<tr>
<td>all—Disables all utilities configuration debug output.</td>
<td></td>
</tr>
</tbody>
</table>
## write

To copy, display, or erase Cisco ISE server configurations, use the `write` command with the appropriate argument in EXEC mode.

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>erase</code></td>
<td>Erases the startup configuration. This option is disabled in Cisco ISE.</td>
</tr>
<tr>
<td><code>memory</code></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><code>terminal</code></td>
<td>Copies the running configuration to console.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Usage Guidelines

Using the `write` command with the `erase` option is disabled in Cisco ISE.

If you use the write command with the erase option, Cisco ISE displays the following error message:

```
% Warning: 'write erase' functionality has been disabled by application: ise
```

### Example 1

```bash
ise/admin# write memory
Generating configuration...
ise/admin#
```

### Example 2

```bash
ise/admin# write terminal
Generating configuration...
!
hostname ise
```
Cisco ISE CLI Commands in EXEC Show Mode

This chapter describes `show` commands in EXEC mode that are used to display the Cisco ISE settings and are among the most useful commands. Each of the commands in this chapter is followed by a brief description of its use, command syntax, usage guidelines, and one or more examples.

- show, on page 99
- show application, on page 100
- show backup, on page 103
- show banner, on page 104
- show cdp, on page 105
- show clock, on page 107
- show container, on page 108
- show cpu, on page 112
- show crypto, on page 114
- show disks, on page 115
- show icmp-status, on page 116
- show interface, on page 118
- show inventory, on page 120
- show ip, on page 122
- show ipv6 route, on page 123
- show logging, on page 124
- show logins, on page 127
- show memory, on page 128
- show ntp, on page 129
- show ports, on page 130
- show process, on page 132
- show repository, on page 134
- show restore, on page 135
- show running-config, on page 136
- show snmp engineid, on page 137
- show snmp user, on page 138
- show startup-config, on page 139
- show tech-support, on page 140
- show terminal, on page 142
- show timezone, on page 143
• show timezones, on page 144
• show udi, on page 145
• show uptime, on page 146
• show users, on page 147
• show version, on page 148
show

To show the running system information, use the show command in EXEC mode.

```
show keyword
```

**Command Default**
No default behavior or values.

**Command Modes**
EXEC

**Usage Guidelines**
All show commands require at least one keyword to function.

**Example**

```
ise/admin# show application
<name>       <Description>
ise           Cisco Identity Services Engine
ise/admin#
```

show application

To show installed application packages on the system, use the **show application** command in EXEC mode.

```
show application [status {application_name}]  
show application [version {application_name}]  
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>Redirects output to a file.</td>
</tr>
<tr>
<td>file-name</td>
<td>Name of the file to store the Cisco ISE application information.</td>
</tr>
<tr>
<td>status</td>
<td>Displays the status of the installed application.</td>
</tr>
<tr>
<td>version</td>
<td>Displays the application version for an installed application (Cisco ISE).</td>
</tr>
<tr>
<td>application_name</td>
<td>Name of the installed application.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Usage Guidelines

To view the application status and version about installed packages on the system, use the **show application** commands.
Example 1

ise/admin# show application
<name>         <Description>
RootPatch      Cisco ADE Root Patch
ise             Cisco Identity Services Engine
ise/admin#

Example 1

ise/admin# show application
<name>         <Description>
ise             Cisco Identity Services Engine
ise/admin#

Example 2

ise/admin# show application version ise
Cisco Identity Services Engine
---------------------------------------------
Version : 1.3.0.672
Build Date : Thu Jun 19 19:33:17 2014
Install Date : Thu Jun 19 21:06:34 2014
ise/admin#

Example 2

ise/admin# show application version ise
Cisco Identity Services Engine
---------------------------------------------
Version : 1.4.0.205
Build Date : Tue Mar 3 05:37:10 2015
Install Date : Tue Mar 3 21:06:34 2015
ise/admin#

Example 3

Cisco ISE includes the status of processes that are optional (persona-based). Processes like pxGrid, Certificate Authority, M&T, and Identity Mapping Services can be in any one of the following states:

- Running—Cisco ISE services are up and running
- Not Running—Cisco ISE services are shut down
- Disabled—Cisco ISE services are disabled

ise/admin# show application status ise
ISE PROCESS NAME      STATE  PROCESS ID
Database Listener    running   3688
Database Server      running   41 PROCESSES
Application Server   running   6041
Profiler Database    running   4533
AD Connector         running   6447
M&T Session Database running   2363
M&T Log Collector running 6297
M&T Log Processor running 6324
Certificate Authority Service running 6263
pxGrid Infrastructure Service disabled
pxGrid Publisher Subscriber Service disabled
pxGrid Connection Manager disabled
pxGrid Controller disabled
Identity Mapping Service disabled
ise/admin#

Example 4
ise/admin# show application status RootPatch
Root Patch installed, and enabled
ise/admin#

Example 5
ise/admin# show application version RootPatch
Root Patch VERSION INFORMATION
-----------------------------------
Version : 1.3.0 Vendor: Cisco Systems, Inc.
Build Date : March 21 2014 13:04PDT
ise/admin#
show backup

To display the backup history of the system or the status of the backup, use the **show backup** command in EXEC mode.

```
show backup [history | status]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>history</strong></td>
<td>Displays historical information about backups on the system.</td>
</tr>
<tr>
<td><strong>progress</strong></td>
<td>Displays the backup status on the system.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Usage Guidelines

To view the system backup history and status, use the **show backup** command.

#### Example 1

```
ise/admin# Show backup history
Wed Apr 10 02:35:29 EDT 2013: backup mybackup-CFG-130410-0226.tar.gpg to repository myrepository: success
Wed Apr 10 02:40:07 EDT 2013: backup mybackup1-OPS-130410-0239.tar.gpg to repository myrepository: success
ise/admin#
```

#### Example 2

```
ise/admin# show backup status
%% Configuration backup status
%% ----------------------------
% backup name: mybackup
% repository: myrepository
% start date: Wed Apr 10 02:26:04 EDT 2013
% scheduled: no
% triggered from: Admin web UI
% host: ise.cisco.com
% status: backup mybackup-CFG-130410-0226.tar.gpg to repository myrepository: success
%% Operation backup status
%% ------------------------
% backup name: mybackup1
% repository: myrepository
% start date: Wed Apr 10 02:39:02 EDT 2013
% scheduled: no
% triggered from: Admin web UI
% host: ise.cisco.com
% status: backup mybackup1-OPS-130410-0239.tar.gpg to repository myrepository: success
ise/admin#
```
show banner

To display pre-login and post-login banners, use the show banner command in EXEC mode.

show banner [post-login | pre-login]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>post-login</td>
<td>Displays the post-login information that is configured in the Cisco ISE server for the current CLI session.</td>
</tr>
<tr>
<td>pre-login</td>
<td>Displays the pre-login information that is configured in the Cisco ISE server for the current CLI session.</td>
</tr>
</tbody>
</table>

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use the show banner command in the active SSH sessions. If the active SSH sessions exceed the Maximum Concurrent Sessions that is configured in the Cisco ISE Admin portal, you get the “WARNING: Maximum active ssh sessions reached” message.
show cdp

To display information about all enabled Cisco Discovery Protocol (CDP) interfaces, use the `show cdp` command in EXEC mode.

`show cdp [all | neighbors]`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Shows all enabled Cisco Discovery Protocol interfaces.</td>
</tr>
<tr>
<td>neighbors</td>
<td>Shows the Cisco Discovery Protocol neighbors.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

To view enabled Cisco Discovery Protocol interfaces and CDP neighbors, use the `show cdp` command.

Note: CDP can be visualized from neighboring IPv4 and IPv6 interfaces

**Example 1**

```
ise/admin# show cdp all
CDP protocol is enabled...
  broadcasting interval is every 60 seconds.
  time-to-live of cdp packets is 180 seconds.
  CDP is enabled on port GigabitEthernet0.
ise/admin#
```

**Example 2**

```
ise/admin# show cdp neighbors
CDP Neighbor: 000c297840e5
  Local Interface : GigabitEthernet0
  Device Type : ISE-1141VM-K9
  Port : eth0
  Address : 172.23.90.114
  IPv6 Address : 2001:420:54ff:4::458:1

CDP Neighbor: ise-esw5
  Local Interface : GigabitEthernet0
  Device Type : cisco WS-C3560E-24TD
  Port : GigabitEthernet0/5
  Address : 172.23.90.45
  IPv6 Address : 2001:420:54ff:4::458:5

CDP Neighbor: 000c29e29926
  Local Interface : GigabitEthernet0
  Device Type : ISE-1141VM-K9
  Port : eth0
  Address : 172.23.90.115
  IPv6 Address : 2001:420:54ff:4::458:2

CDP Neighbor: 000c290fba98
```
show cdp

Local Interface : GigabitEthernet0
Device Type : ISE-1141VM-K9
Port : eth0
Address : 172.23.90.111
IPv6 Address : 2001:420:54ff:4::458:3
ise/admin#
show clock

To display the day, month, date, time, time zone, and year of the system software clock, use the `show clock` command in EXEC mode.

This command has no keywords and arguments.

`show clock`

**Command Default**
No default behavior or values.

**Command Modes**
EXEC

**Usage Guidelines**
The `show clock` output in the following example includes Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), Great Britain, or Zulu time.

**Example**

```
ise/admin# show clock
Fri Aug 6 10:46:39 UTC 2010
ise/admin#
```
show container

To view information about the Threat-Centric NAC adapters and Wi-Fi setup, use the `show container` command in EXEC mode.

The output of this command provides statistical information about the vulnerability assessment scans, when the adapters were created, how long the adapters were running, and their current statuses. You can further view information about each of the adapters in detail based on the container name or ID.

```
show container {tc-nac {adapters | all} inspect {container-id container-id | container-name container-name} | stats {container-id container-id | container-name container-name} | wifi setup all}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tc-nac</code></td>
<td>Displays information about the Threat-Centric NAC adapters.</td>
</tr>
<tr>
<td><code>wifi setup</code></td>
<td>Displays the Wi-Fi container setup information.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>When used with TC NAC, lists all the adapters that are available in Cisco ISE, including the container name and ID. When used with Wi-Fi Setup, displays the Wi-Fi container setup information.</td>
</tr>
<tr>
<td><code>adapters</code></td>
<td>Lists the TC NAC adapters that are configured in Cisco ISE. Lists the container ID and name, the time when the adapter was created and how long the adapter has been running, and the current status of the adapter.</td>
</tr>
<tr>
<td><code>inspect</code></td>
<td>Lists detailed information about the specific adapter.</td>
</tr>
<tr>
<td><code>stats</code></td>
<td>Provides statistical information about the specific adapter.</td>
</tr>
<tr>
<td><code>&gt;</code></td>
<td>Redirects output to a file.</td>
</tr>
</tbody>
</table>
Output modifier variables:

- **begin**—Matched pattern. Supports up to 80 alphanumeric characters.
- **count**—Count the number of lines in the output. Add number after the word count.
- **end**—End with line that matches. Supports up to 80 alphanumeric characters.
- **exclude**—Exclude lines that match. Supports up to 80 alphanumeric characters.
- **include**—Include lines that match. Supports up to 80 alphanumeric characters.
- **last**—Display last few lines of output. Add number after the word last. Supports up to 80 lines to display. Default 10.

---

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

To view information about the Threat-Centric NAC adapters, use the `show container` command.

**Example 1**

```
ise/admin# show container tc-nac adapters
```

<table>
<thead>
<tr>
<th>CONTAINER ID</th>
<th>IMAGE</th>
<th>COMMAND</th>
<th>CREATED</th>
</tr>
</thead>
<tbody>
<tr>
<td>63b8904f41c6</td>
<td>irf-adapter-nexpose</td>
<td>&quot;/opt/CSCOcpm/vaservi&quot;</td>
<td>19 hours ago</td>
</tr>
<tr>
<td>Up 19 hours</td>
<td></td>
<td>nexpose</td>
<td></td>
</tr>
<tr>
<td>8389f7e249cf</td>
<td>irf-adapter-tenable</td>
<td>&quot;/opt/CSCOcpm/vaservi&quot;</td>
<td>2 days ago</td>
</tr>
<tr>
<td>Up 2 days</td>
<td></td>
<td>tenable</td>
<td></td>
</tr>
</tbody>
</table>

ise/admin#

**Example 2**

```
ise/admin# show container tc-nac all
```

<table>
<thead>
<tr>
<th>CONTAINER ID</th>
<th>IMAGE</th>
<th>COMMAND</th>
<th>CREATED</th>
</tr>
</thead>
<tbody>
<tr>
<td>63b8904f41c6</td>
<td>irf-adapter-nexpose</td>
<td>&quot;/opt/CSCOcpm/vaservi&quot;</td>
<td>19 hours ago</td>
</tr>
<tr>
<td>Up 19 hours</td>
<td></td>
<td>nexpose</td>
<td></td>
</tr>
<tr>
<td>8389f7e249cf</td>
<td>irf-adapter-tenable</td>
<td>&quot;/opt/CSCOcpm/vaservi&quot;</td>
<td>2 days ago</td>
</tr>
<tr>
<td>Up 2 days</td>
<td></td>
<td>tenable</td>
<td></td>
</tr>
<tr>
<td>41921c1539bf</td>
<td>irf-core-engine:2.2.6</td>
<td>&quot;/bin/sh -c 'npm star&quot;</td>
<td>3 days ago</td>
</tr>
<tr>
<td>Up 3 days</td>
<td>127.0.0.1:3000-&gt;3000/tcp</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Cisco Identity Services Engine CLI Reference Guide, Release 2.6
ise/admin# show container tc-nac inspect container-name nexpose
{
  "Id": "63b8904f41c6ce2a58660d38eb3500104038e650e4e3365e21e0a536a1ba3044",
  "Created": "2016-09-22T11:38:03.146141316Z",
  "Path": "/opt/CSCOcpm/vaservice/nexposeadapter/bin/nexposeadaptercontrol.sh",
            "07bc6aee-fb9f-4845-86cb-886c7c095188"],
  "State": {
    "Status": "running",
    "Running": true,
    "Paused": false,
    "Restarting": false,
    "OOMKilled": false,
    "Dead": false,
    "Pid": 23433,
    "ExitCode": 0,
    "Error": "",
    "StartedAt": "2016-09-22T11:38:05.609439645Z",
    "FinishedAt": "0001-01-01T00:00:00Z"
  },
  "Image": "06ba3230bd64872b988f4506e7fffddc8c6374c7ece285555ee1cc57743ea7e0",
  "ResolvConfPath": "/opt/docker/runtime/containers/63b8904f41c6ce2a58660d38eb3500104038e650e4e3365e21e0a536a1ba3044/resolv.conf",
  "HostnamePath": "/opt/docker/runtime/containers/63b8904f41c6ce2a58660d38eb3500104038e650e4e3365e21e0a536a1ba3044/hostname",
  "HostsPath": "/opt/docker/runtime/containers/63b8904f41c6ce2a58660d38eb3500104038e650e4e3365e21e0a536a1ba3044/hosts",
  "LogPath": "/opt/docker/runtime/containers/63b8904f41c6ce2a58660d38eb3500104038e650e4e3365e21e0a536a1ba3044/log",
  "Name": "/nexpose",
  "RestartCount": 0,
  "Driver": "devicemapper",
  "ExecDriver": "native-0.2",
  "MountLabel": "",
  "ProcessLabel": "",
  "AppArmorProfile": "",
  "ExecIDs": ["d76578aa4481181679d0290037fcb2e56aa7dce8677b8991a736617a6d6879750"],
  "NetworkSettings": { "Bridge": ""},
"SandboxID": "9873fb92f86e665039a6de18be057bc3fd341f7b39acede57cbd89b3f56ce0",
"HairpinMode": false,
"LinkLocalIPv6Address": ",
"LinkLocalIPv6PrefixLen": 0,
"Ports": {},
"SandboxKey": "/var/run/docker/netns/9873fb92f86e",
"SecondaryIPAddresses": null,
"SecondaryIPv6Addresses": null,
"EndpointID": ",
"Gateway": ",
"GlobalIPv6Address": ",
"GlobalIPv6PrefixLen": 0,
"IPAddress": ",
"IPv6Gateway": ",
"MacAddress": ",
"Networks": {
    "irf-internal-nw": {
        "EndpointID": 
            "8999c12319144cfd66a4e99be40f7fbc228779e43f2a7f20c48867b8b3ca7a49",
        "Gateway": "169.254.1.1",
        "IPAddress": "169.254.1.6",
        "IPv6Gateway": ",
        "GlobalIPv6Address": ",
        "GlobalIPv6PrefixLen": 0,
        "MacAddress": "02:42:a9:fe:01:06"
    }
}
}
]
}

Example 4

ise/admin# show container tc-nac stats container-name nexpose
CONTAINER CPU % MEM USAGE / LIMIT MEM % NET I/O
BLOCK I/O
nexpose 0.07% 327.9 MB / 12.43 GB 2.64% 4.501 MB / 2.446 MB 106.4 MB / 21.27 MB

Example 5

ise/admin# show container wifi setup all
CONTAINER ID IMAGE COMMAND CREATED NAMES
PORTS status

d51711744e7c wifisetup:0.0.12 /sbin/tini -- /usr/b 6 days ago wifisetup-container
   Up 6 days
To display CPU information, use the `show cpu` command in EXEC mode.

To show a summary of CPU usage per Cisco ISE component, use the `show cpu usage` command in EXEC mode. The output of this command provides a snapshot of CPU usage at the moment the command is run.

```
show cpu > file-name
show cpu statistics
show cpu usage
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>Redirects output to a file.</td>
</tr>
<tr>
<td>file-name</td>
<td>Name of the file to redirect.</td>
</tr>
<tr>
<td>statistics</td>
<td>Displays CPU statistics.</td>
</tr>
<tr>
<td>cpu usage</td>
<td>Displays the CPU usage per component for an installed application (Cisco ISE).</td>
</tr>
</tbody>
</table>

### Output modifier variables:

- `begin`—Matched pattern. Supports up to 80 alphanumeric characters.
- `count`—Count the number of lines in the output. Add number after the word count. `-`—Output modifier variables for count.
- `end`—End with line that matches. Supports up to 80 alphanumeric characters.
- `exclude`—Exclude lines that match. Supports up to 80 alphanumeric characters.
- `include`—Include lines that match. Supports up to 80 alphanumeric characters.
- `last`—Display last few lines of output. Add number after the word last. Supports up to 80 lines to display. Default 10. `-`—Output modifier variables for last.

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Usage Guidelines

To view CPU information and its statistics, use the `show cpu` command.
Example 1

ise/admin# show cpu
processor: 0
model : Intel(R) Xeon(R) CPU E5320 @ 1.86GHz
speed(MHz): 1861.914
cache size: 4096 KB
ise/admin#

Example 2

ise/admin# show cpu statistics
user time: 265175
kernel time: 166835
idle time: 5356204
i/o wait time: 162676
irq time: 4055
ise/admin#

Example 3

ise/admin# show cpu usage

<table>
<thead>
<tr>
<th>ISE Function</th>
<th>% CPU Usage</th>
<th>CPU Time</th>
<th>Number of threads</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profiler Database</td>
<td>0.01</td>
<td>1:26.27</td>
<td>3</td>
</tr>
<tr>
<td>M&amp;T Session Database</td>
<td>0.01</td>
<td>1:23.06</td>
<td>18</td>
</tr>
<tr>
<td>Certificate Authority Service</td>
<td>0.04</td>
<td>6:57.38</td>
<td>31</td>
</tr>
<tr>
<td>M&amp;T Log Collector</td>
<td>0.12</td>
<td>20:29.75</td>
<td>7</td>
</tr>
<tr>
<td>M&amp;T Log Processor</td>
<td>0.09</td>
<td>15:44.23</td>
<td>60</td>
</tr>
<tr>
<td>ISE Indexing Engine</td>
<td>0.12</td>
<td>21:34.76</td>
<td>75</td>
</tr>
<tr>
<td>Database Listener</td>
<td>0.01</td>
<td>0:53.18</td>
<td>2</td>
</tr>
<tr>
<td>Database Server</td>
<td>0.36</td>
<td>62:48.64</td>
<td>64 processes</td>
</tr>
<tr>
<td>Admin Webapp</td>
<td>0.04</td>
<td>6:46.68</td>
<td>53</td>
</tr>
<tr>
<td>Profiler</td>
<td>0.00</td>
<td>0:02.94</td>
<td>26</td>
</tr>
<tr>
<td>NSF Persistence Layer</td>
<td>0.05</td>
<td>8:09.70</td>
<td>46</td>
</tr>
<tr>
<td>Guest Services</td>
<td>0.00</td>
<td>0:00.32</td>
<td>5</td>
</tr>
<tr>
<td>Syslog Processor</td>
<td>0.00</td>
<td>0:12.79</td>
<td>3</td>
</tr>
<tr>
<td>Quartz Scheduler</td>
<td>0.05</td>
<td>9:08.80</td>
<td>29</td>
</tr>
<tr>
<td>RMI Services</td>
<td>0.00</td>
<td>0:05.98</td>
<td>10</td>
</tr>
<tr>
<td>Message Queue</td>
<td>0.00</td>
<td>0:43.99</td>
<td>4</td>
</tr>
<tr>
<td>BYOD Services</td>
<td>0.00</td>
<td>0:00.00</td>
<td>1</td>
</tr>
<tr>
<td>Admin Process JVM Threads</td>
<td>0.19</td>
<td>32:50.67</td>
<td>10</td>
</tr>
<tr>
<td>Miscellaneous services</td>
<td>0.17</td>
<td>30:30.47</td>
<td>3557</td>
</tr>
<tr>
<td>Identity Mapping Service</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>SXP Engine Service</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Threat Centric NAC Docker Service</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Threat Centric NAC MongoDB Container</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Threat Centric NAC RabbitMQ Container</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Threat Centric NAC Core Engine Container</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Vulnerability Assessment Database</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Vulnerability Assessment Service</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
show crypto

To display information about the public keys and authorized keys for the logged in administrators and users, use the `show crypto` command.

- `show crypto authorized_keys`
- `show crypto host-keys`
- `show crypto key`

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>authorized_keys</code></td>
<td>Displays authorized keys information for the user who is logged in currently.</td>
</tr>
<tr>
<td><code>host_keys</code></td>
<td>Displays host keys for the user who is logged in currently.</td>
</tr>
<tr>
<td><code>key</code></td>
<td>Displays key information for the user who is logged in currently.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

To view authorized keys and keys for currently logged in users, use the `show crypto` command.

**Example 1**

```plaintext
ise/admin# show crypto authorized_keys
Authorized keys for admin
ise/admin#
```

**Example 2**

```plaintext
ise/admin# show crypto key
admin public key: ssh-rsa f8:7f:8a:79:44:5d:5f:af:e1:63:b2:be:7a:fd:d4 admin@ise
ise/admin#
```
show disks

To display the disks file-system information, use the `show disks` command in EXEC mode.

```
show disks > file-name
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>Redirects output to a file.</td>
</tr>
<tr>
<td>file-name</td>
<td>Name of the file to redirect.</td>
</tr>
</tbody>
</table>

Output modifier variables:

- **begin**—Matched pattern. Supports up to 80 alphanumeric characters.
- **count**—Count the number of lines in the output. Add number after the word count.
- **end**—End with line that matches. Supports up to 80 alphanumeric characters.
- **exclude**—Exclude lines that match. Supports up to 80 alphanumeric characters.
- **include**—Include lines that match. Supports up to 80 alphanumeric characters.
- **last**—Display last few lines of output. Add number after the word last. Supports up to 80 lines to display. Default 10.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>No default behavior or values.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC</td>
</tr>
<tr>
<td>Usage Guidelines</td>
<td>Only platforms that have a disk file system support the <code>show disks</code> command.</td>
</tr>
</tbody>
</table>

**Example**

```
ise/admin# show disks
disk repository: 24% used (3325484 of 14877092)
Internal filesystems:
/ : 5% used ( 24124436 of 540283556)
/storedconfig : 7% used ( 5693 of 93327)
/tmp : 2% used ( 35960 of 1976268)
/boot : 4% used ( 17049 of 489992)
/dev/shm : 0% used ( 0 of 1943756)
  all internal filesystems have sufficient free space
ise/admin#
```
show icmp-status

To display the Internet Control Message Protocol (ICMP) echo response configuration information, use the show icmp_status command in EXEC mode.

show icmp_status > file-name

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>Redirects output to a file.</td>
</tr>
<tr>
<td>file-name</td>
<td>Name of the file to redirect.</td>
</tr>
</tbody>
</table>

Output modifier commands:

- **begin**—Matched pattern. Supports up to 80 alphanumeric characters.
- **count**—Count the number of lines in the output. Add number after the word count.
  - |—Output modifier commands for count.
- **end**—End with line that matches. Supports up to 80 alphanumeric characters.
- **exclude**—Exclude lines that match. Supports up to 80 alphanumeric characters.
- **include**—Include lines that match. Supports up to 80 alphanumeric characters.
- **last**—Display last few lines of output. Add number after the word last. Supports up to 80 lines to display. Default 10.
  - |—Output modifier commands for last.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

To view the Internet Control Message Protocol (ICMP) echo response configuration information, use the show icmp_status command.

**Example 1**

ise/admin# show icmp_status
icmp echo response is turned on
ise/admin#
Example 2

ise/admin# show icmp_status
icmp echo response is turned off
ise/admin#
show interface

To display the usability status of interfaces configured for IP, use the **show interface** command in EXEC mode.

```
show interface > file-name
show interface GigabitEthernet {0-3}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>file-name</td>
<td>Name of the file to redirect interface information.</td>
</tr>
<tr>
<td>GigabitEthernet</td>
<td>Shows the specific Gigabit Ethernet interface information.</td>
</tr>
<tr>
<td>0-3</td>
<td>Gigabit Ethernet number that may be one of the following: 0, 1, 2, 3.</td>
</tr>
</tbody>
</table>

Output modifier variables:
- **begin**—Matched pattern. Supports up to 80 alphanumeric characters.
- **count**—Count the number of lines in the output. Add number after the word count.
- **end**—End with line that matches. Supports up to 80 alphanumeric characters.
- **exclude**—Exclude lines that match. Supports up to 80 alphanumeric characters.
- **include**—Include lines that match. Supports up to 80 alphanumeric characters.
- **last**—Display last few lines of output. Add number after the word last. Supports up to 80 lines to display. Default 10.

Command Default
No default behavior or values.

Command Modes
EXEC

Usage Guidelines
In the **show interface GigabitEthernet 0** output, you can find that the interface has three IPv6 addresses. The first internet address (starting with 3ffe) is the result of using stateless autoconfiguration. For this to work, you need to 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 always see a link local address regardless of the IPv6 autoconfiguration or DHCPv6 configuration. The last address (starting with 2001) is the result obtained from a IPv6 DHCP server.
Example 1

```
ise/admin# show interface
eth0  Link encap:Ethernet  HWaddr 00:0C:29:6A:88:C4
      inet addr:172.23.90.113  Bcast:172.23.90.255  Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fe6a:88c4/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:48536  errors:0  dropped:0  overruns:0  frame:0
      TX packets:14152  errors:0  dropped:0  overruns:0  carrier:0
      collisions:0  txqueuelen:1000
      RX bytes:6507290 (6.2 MiB)  TX bytes:12443568 (11.8 MiB)
      Interrupt:59  Base address:0x2000

lo   Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:1195025  errors:0  dropped:0  overruns:0  frame:0
      TX packets:1195025  errors:0  dropped:0  overruns:0  carrier:0
      collisions:0  txqueuelen:0
      RX bytes:649425800 (619.3 MiB)  TX bytes:649425800 (619.3 MiB)

sit0  Link encap:IPv6-in-IPv4
      NOARP  MTU:1480  Metric:1
      RX packets:0  errors:0  dropped:0  overruns:0  frame:0
      TX packets:0  errors:0  dropped:0  overruns:0  carrier:0
      collisions:0  txqueuelen:0
      RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
ise/admin#```

Example 2

```
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: ffff:302:11:2:20c:29ff:feaf:da05/64 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#```
show inventory

To display information about the hardware inventory, including the Cisco ISE appliance model and serial number, use the `show inventory` command in EXEC mode.

```
show inventory > file-name
```

### Syntax Description

- **>` Redirects output to a file.
- **file-name** Name of the file to redirect hardware inventory information.

### Output modifier variables:

- **begin**—Matched pattern. Supports up to 80 alphanumeric characters.
- **count**—Count the number of lines in the output. Add number after the word count.
- **end**—End with line that matches. Supports up to 80 alphanumeric characters.
- **exclude**—Exclude lines that match. Supports up to 80 alphanumeric characters.
- **include**—Include lines that match. Supports up to 80 alphanumeric characters.
- **last**—Display last few lines of output. Add number after the word last. Supports up to 80 lines to display. Default 10.

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Usage Guidelines

To view the Cisco ISE appliance information, use the `show inventory` command.

### Example

```
ise/admin# show inventory
NAME: "ISE-VM-K9 chassis", DESCR: "ISE-VM-K9 chassis"
PID: ISE-VM-K9 , VID: V01, SN: H8JESGOFHGG
Total RAM Memory: 1035164 kB
CPU Core Count: 1
CPU 0: Model Info: Intel(R) Xeon(R) CPU E5320 @ 1.86GHz
Hard Disk Count(*): 1
Disk 0: Device Name: /dev/sda
Disk 0: Capacity: 64.40 GB
Disk 0: Geometry: 255 heads 63 sectors/track 7832 cylinders
NIC Count: 1
NIC 0: Device Name: eth0
NIC 0: HW Address: 00:0C:29:6A:88:C4
```
NIC 0: Driver Descr: eth0: registered as PCnet/PCI II 79C970A
(*) Hard Disk Count may be Logical.
ise/admin#
show ip

To display the IP route information, use the **show ip** command in EXEC mode.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route</td>
<td>Displays IP route information.</td>
</tr>
</tbody>
</table>

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

This command displays the IP routing table.

Example

```
ise/admin# show ip route
Kernel IP routing table
Destination     Gateway          Genmask Flags Metric Ref Use Iface
172.21.79.0      0.0.0.0          255.255.255.0  U      0      0      0      0      eth0
0.0.0.0           172.21.79.1     0.0.0.0          UG     0      0      0      0      eth0
ise/admin#
```
show ipv6 route

To display the IPv6 route information, use the **show ipv6 route** command in EXEC mode.

**show ipv6 route**

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

This command displays the IPv6 routing table.

**Example 1**

```
ise/admin# show ipv6 route
Destination          Gateway       Iface
-------------------  -----------  -----
2001:DB8:cc00:1::/64 2001:DB8:cc00:1::1  eth0
ff02::1:2/128       ff02::1:2       eth0
ise/admin#
```

**Example 2**

```
ise/admin# show ipv6 route
Destination          Gateway       Iface
-------------------  -----------  -----
2001:db8::/64        ::           eth0
2015:db8::/64        ::           eth3
2020:db8::/64        2001:db8::5   eth0
default              2001:db8::5   eth0
ise/admin#
```
show logging

To display the state of system logging (syslog) and the contents of the standard system logging buffer, use the show logging command in EXEC mode.

- `show logging > file-name` redirects output to a file.
- `show logging application application-logfile-name` displays application logs.
- `show logging container tc-nac {container-id container-id [log-name name-of-log-file tail] | container-name container-name}` displays the Threat Centric-NAC containers.
- `show logging internal` displays the syslog configuration.
- `show logging system system-logfile-name` displays system syslogs.

### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&gt;</code></td>
<td>Redirects output to a file.</td>
</tr>
<tr>
<td><code>file-name</code></td>
<td>Name of the file to redirect system logging information.</td>
</tr>
<tr>
<td><code>application</code></td>
<td>Displays application logs.</td>
</tr>
<tr>
<td><code>application-logfile-name</code></td>
<td>Name of the application log file.</td>
</tr>
<tr>
<td><code>container tc-nac</code></td>
<td>Displays the Threat Centric-NAC containers.</td>
</tr>
<tr>
<td><code>container-id container-id [log-name name-of-log-file tail]</code></td>
<td>Displays the log files related to the specified container (TC-NAC adapter).</td>
</tr>
<tr>
<td><code>container-name container-name</code></td>
<td>Displays the log files related to the specified container (TC-NAC adapter).</td>
</tr>
<tr>
<td><code>internal</code></td>
<td>Displays the syslog configuration.</td>
</tr>
<tr>
<td><code>system</code></td>
<td>Displays system syslogs.</td>
</tr>
<tr>
<td><code>system-logfile-name</code></td>
<td>Name of the system log file.</td>
</tr>
<tr>
<td><code>system-file-name</code></td>
<td>Name of the system log file name.</td>
</tr>
</tbody>
</table>
Output modifier variables:

- **begin**—Matched pattern. Supports up to 80 alphanumeric characters.
- **count**—Count the number of lines in the output. Add number after the word count.
- **end**—End with line that matches. Supports up to 80 alphanumeric characters.
- **exclude**—Exclude lines that match. Supports up to 80 alphanumeric characters.
- **include**—Include lines that match. Supports up to 80 alphanumeric characters.
- **last**—Display last few lines of output. Add number after the word last. Supports up to 80 lines to display. Default 10.

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Usage Guidelines

This command displays the state of syslog error and event logging, including host addresses, and for which, logging destinations (console, monitor, buffer, or host) logging is enabled.

#### Example 1

```
ise/admin# show logging system
  0 Feb 25 2013 15:57:43  tallylog
  1781 Feb 26 2013 02:01:02 maillog
  4690 Feb 26 2013 02:40:01  cron
  0 Feb 25 2013 15:56:58  spooler
  0 Feb 25 2013 16:10:03 boot.log
  0 Feb 25 2013 16:00:03 btmp
  38784 Feb 26 2013 02:19:48 wtmp
  16032 Feb 26 2013 02:19:47 faillog
  32947 Feb 26 2013 00:38:02 dmesg
  63738 Feb 26 2013 02:19:49 messages
  146292 Feb 26 2013 02:19:48 lastlog
  13877 Feb 26 2013 01:48:32 rpmpkgs
  129371 Feb 26 2013 02:40:22 secure
  27521 Feb 25 2013 16:10:02 anaconda.syslog
  345031 Feb 25 2013 16:10:02 anaconda.log
  0 Jul 26 2011 00:56:37 mail/statistics
  1272479 Feb 26 2013 02:42:52 ade/ADE.log
  567306 Feb 26 2013 02:40:22 audit/audit.log
  24928 Feb 26 2013 02:40:01 aa/aa26
  0 Feb 25 2013 16:01:40 pm/suspend.log
ise/admin#
```

#### Example 2

To view application log files on Cisco ISE nodes, use the following command:
ise/admin# show logging application
  61 Oct 07 2016 03:02:43   dbalert.log
  4569 Oct 07 2016 03:21:18    ad_agent.log
          0 Oct 07 2016 03:13:18 ise-elasticsearch_index_indexing_slowlog.log
          0 Oct 07 2016 03:02:59    edf.log
          124 Oct 07 2016 03:21:59    diagnostics.log
          8182 Oct 07 2016 03:26:45    caservice.log
          426 Oct 07 2016 03:19:17    redis.log
         1056 Oct 07 2016 03:13:07    caservice_bootstrap.log
         49637 Oct 07 2016 03:27:40    passiveid-mgmt.log
          0 Oct 07 2016 03:02:59    passiveid.log
          0 Oct 07 2016 03:13:18 ise-elasticsearch_index_search_slowlog.log
         14152 Oct 07 2016 03:26:03    collector.log
          0 Oct 07 2016 03:02:59    idc-endpoint.log
          134 Oct 07 2016 03:22:34    ocsp.log
          0 Oct 07 2016 03:02:59    dbconn.log
          0 Oct 07 2016 03:02:59    idc-kerberos.log
        100958 Oct 07 2016 03:24:43    crypto.log
          0 Oct 07 2016 03:02:59    idc-syslog.log
          0 Oct 07 2016 03:02:59    replication.log.2016-10-04.1
        10394 Oct 07 2016 03:24:01    guest.log
          0 Oct 07 2016 03:02:59    guest.log.2016-10-07.1
          0 Oct 07 2016 03:02:59    vcs.log.2016-10-04.1
       288624 Oct 07 2016 03:27:25    ise-psc.log
ise/admin#
show logins

To display the state of system logins, use the `show logins` command in EXEC mode.

```
show logins cli
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cli</td>
<td>Lists the cli login history.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

Requires the `cli` keyword; otherwise, an error occurs.

**Example**

```
ise/admin# show logins cli
admin pts/0 10.77.137.60 Fri Aug 6 09:45 still logged in
admin pts/0 10.77.137.60 Fri Aug 6 08:56 - 09:30 (00:33)
admin pts/0 10.77.137.60 Fri Aug 6 07:17 - 08:43 (01:26)
reboot system boot 2.6.18-164.el5PA Thu Aug 5 18:17 (17:49)
admin tty1 Thu Aug 5 18:15 - down (00:00)
reboot system boot 2.6.18-164.el5PA Thu Aug 5 18:09 (00:06)
setup tty1 Thu Aug 5 17:43 - 18:07 (00:24)
reboot system boot 2.6.18-164.el5PA Thu Aug 5 16:05 (02:02)
wtmp begins Thu Aug 5 16:05:36 2010
ise/admin#
```
show memory

To display the memory usage of all running processes, use the show memory command in EXEC mode. This command has no keywords and arguments.

Command Default
No default behavior or values.

Command Modes
EXEC

Usage Guidelines
To view used memory, use the show memory command.

Example

ise/admin# show memory
total memory: 4394380 kB
free memory: 206060 kB
cached: 1111752 kB
swap-cached: 9072 kB

output of free command:
total used free shared buffers cached
Mem: 4394380 4188576 205804 0 147504 1111748
-/+ buffers/cache: 2929324 1465056
Swap: 8185108 192728 7992380
ise/admin#
show ntp

To show the status of the Network Translation Protocol (NTP) associations, use the **show ntp** command in EXEC mode.

This command has no keywords and arguments.

**show ntp**

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

To view the Network Translation Protocol (NTP) associations, use the **show ntp** command.

**Example**

ise/admin# show ntp
Primary NTP : ntp.esl.cisco.com
Secondary NTP : 171.68.10.150
Tertiary NTP : 171.68.10.80
synchronised to local net at stratum 11
time correct to within 11 ms
polling server every 128 s
remote     refid  st  t when poll reach delay offset jitter
-----------------------------------------------------------------------------
  *127.127.1.0 .LOCL. 10 l 9   64 377  0.000  0.000  0.001
  171.68.10.80 .RMOT. 16 u 11  64 0   0.000  0.000  0.000
  171.68.10.150 .INIT. 16 u 11  64 0   0.000  0.000  0.000

Warning: Output results may conflict during periods of changing synchronization.
ise/admin#
show ports

To display information about all processes listening on active ports, use the show ports command in EXEC mode.

**show ports > file-name**

**Syntax Description**
- `>` Redirects output to a file.
- `file-name` Name of the file to redirect.
- `|` Output modifier variables:
  - `begin`—Matched pattern. Supports up to 80 alphanumeric characters.
  - `count`—Count the number of lines in the output. Add number after the word count.
  - `end`—End with line that matches. Supports up to 80 alphanumeric characters.
  - `exclude`—Exclude lines that match. Supports up to 80 alphanumeric characters.
  - `include`—Include lines that match. Supports up to 80 alphanumeric characters.
  - `last`—Display last few lines of output. Add number after the word last. Supports up to 80 lines to display. Default 10.

**Command Default**
No default behavior or values.

**Command Modes**
EXEC

**Usage Guidelines**
When you run the show ports command, the port must have an associated active session.

**Example**

```
ise/admin# show ports
Process : java (22648)
tcp: 0.0.0.0:9024, 127.0.0.1:2020, 0.0.0.0:9060, 0.0.0.0:37252, 127.0.0.1:805, 0.0.0.0:9990, 0.0.0.0:8009, 0.0.0.0:8905, 0.0.0.0:5514, 0.0.0.0:1099, 0.0.0.0:61616, 0.0.0.0:80, 0.0.0.0:9080, 0.0.0.0:62424, 0.0.0.0:443, 0.0.0.0:8443, 0.0.0.0:443, 0.0.0.0:8444
udp: 172.21.79.91:1812, 172.21.79.91:1813, 172.21.79.91:1700, 0.0.0.0:48425, 172.21.79.91:8905, 172.21.79.91:3799, 0.0.0.0:54104, 172.21.79.91:57696, 172.21.79.91:1645, 172.21.79.91:1646
Process : timestenrepd (21516)
```
tcp: 127.0.0.1:56513, 0.0.0.0:51312
Process : timestensubd (21421)
tcp: 127.0.0.1:50598
Process : rpc.statd (3042)
tcp: 0.0.0.0:680
udp: 0.0.0.0:674, 0.0.0.0:677
Process : ttcserver (21425)
tcp: 0.0.0.0:53385, 127.0.0.1:49293
Process : timestensubd (21420)
tcp: 127.0.0.1:51370
Process : redis-server (21535)
tcp: 0.0.0.0:6379
Process : portmap (2999)
tcp: 0.0.0.0:111
udp: 0.0.0.0:111
Process : Decap_main (22728)
--More--
show process

To display information about active processes, use the show process command in EXEC mode.

```
show process > file-name
```

**Syntax Description**

- **>** Redirects output to a file.
- **file-name** Name of the file to redirect.

(Optional). Output modifier variables:

- **begin**—Matched pattern. Supports up to 80 alphanumeric characters.
- **count**—Count the number of lines in the output. Add number after the word count.
- **end**—End with line that matches. Supports up to 80 alphanumeric characters.
- **exclude**—Exclude lines that match. Supports up to 80 alphanumeric characters.
- **include**—Include lines that match. Supports up to 80 alphanumeric characters.
- **last**—Display last few lines of output. Add number after the word last. Supports up to 80 lines to display. Default 10.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

*Table 2: Show Process Field Descriptions*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER</td>
<td>Logged-in user.</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID.</td>
</tr>
<tr>
<td>TIME</td>
<td>The time the command was last used.</td>
</tr>
<tr>
<td>TT</td>
<td>Terminal that controls the process.</td>
</tr>
<tr>
<td>COMMAND</td>
<td>Type of process or command used.</td>
</tr>
</tbody>
</table>

**Example**

```
ise/admin# show process
```
<table>
<thead>
<tr>
<th>USER</th>
<th>PID</th>
<th>TIME</th>
<th>TT</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>1</td>
<td>00:00:02</td>
<td>?</td>
<td>init</td>
</tr>
<tr>
<td>root</td>
<td>2</td>
<td>00:00:00</td>
<td>?</td>
<td>migration/0</td>
</tr>
<tr>
<td>root</td>
<td>3</td>
<td>00:00:00</td>
<td>?</td>
<td>ksoftirqd/0</td>
</tr>
<tr>
<td>root</td>
<td>4</td>
<td>00:00:00</td>
<td>?</td>
<td>watchdog/0</td>
</tr>
<tr>
<td>root</td>
<td>5</td>
<td>00:00:00</td>
<td>?</td>
<td>events/0</td>
</tr>
<tr>
<td>root</td>
<td>6</td>
<td>00:00:00</td>
<td>?</td>
<td>khelper</td>
</tr>
<tr>
<td>root</td>
<td>7</td>
<td>00:00:00</td>
<td>?</td>
<td>kthread</td>
</tr>
<tr>
<td>root</td>
<td>10</td>
<td>00:00:01</td>
<td>?</td>
<td>kblockd/0</td>
</tr>
<tr>
<td>root</td>
<td>11</td>
<td>00:00:00</td>
<td>?</td>
<td>kacpid</td>
</tr>
<tr>
<td>root</td>
<td>170</td>
<td>00:00:00</td>
<td>?</td>
<td>cqueue/0</td>
</tr>
<tr>
<td>root</td>
<td>173</td>
<td>00:00:00</td>
<td>?</td>
<td>khubd</td>
</tr>
<tr>
<td>root</td>
<td>175</td>
<td>00:00:00</td>
<td>?</td>
<td>kseriod</td>
</tr>
<tr>
<td>root</td>
<td>239</td>
<td>00:00:32</td>
<td>?</td>
<td>kswapd0</td>
</tr>
<tr>
<td>root</td>
<td>240</td>
<td>00:00:00</td>
<td>?</td>
<td>aio/0</td>
</tr>
<tr>
<td>root</td>
<td>458</td>
<td>00:00:00</td>
<td>?</td>
<td>kpsmoused</td>
</tr>
<tr>
<td>root</td>
<td>488</td>
<td>00:00:00</td>
<td>?</td>
<td>mpt_poll_0</td>
</tr>
<tr>
<td>root</td>
<td>489</td>
<td>00:00:00</td>
<td>?</td>
<td>scsi_eh_0</td>
</tr>
<tr>
<td>root</td>
<td>492</td>
<td>00:00:00</td>
<td>?</td>
<td>ata/0</td>
</tr>
<tr>
<td>root</td>
<td>493</td>
<td>00:00:00</td>
<td>?</td>
<td>ata_aux</td>
</tr>
<tr>
<td>root</td>
<td>500</td>
<td>00:00:00</td>
<td>?</td>
<td>kstriped</td>
</tr>
<tr>
<td>root</td>
<td>509</td>
<td>00:00:07</td>
<td>?</td>
<td>kjournald</td>
</tr>
<tr>
<td>root</td>
<td>536</td>
<td>00:00:00</td>
<td>?</td>
<td>kauditd</td>
</tr>
<tr>
<td>root</td>
<td>569</td>
<td>00:00:00</td>
<td>?</td>
<td>udevd</td>
</tr>
<tr>
<td>root</td>
<td>1663</td>
<td>00:00:00</td>
<td>?</td>
<td>kmpathd/0</td>
</tr>
<tr>
<td>root</td>
<td>1664</td>
<td>00:00:00</td>
<td>?</td>
<td>kmpath_handlerd</td>
</tr>
<tr>
<td>root</td>
<td>1691</td>
<td>00:00:00</td>
<td>?</td>
<td>kjournald</td>
</tr>
<tr>
<td>root</td>
<td>1693</td>
<td>00:00:00</td>
<td>?</td>
<td>kjournald</td>
</tr>
<tr>
<td>root</td>
<td>1695</td>
<td>00:00:00</td>
<td>?</td>
<td>kjournald</td>
</tr>
<tr>
<td>root</td>
<td>1697</td>
<td>00:00:00</td>
<td>?</td>
<td>kjournald</td>
</tr>
<tr>
<td>root</td>
<td>2284</td>
<td>00:00:00</td>
<td>?</td>
<td>auditd</td>
</tr>
<tr>
<td>root</td>
<td>2286</td>
<td>00:00:00</td>
<td>?</td>
<td>audispd</td>
</tr>
<tr>
<td>root</td>
<td>2318</td>
<td>00:00:10</td>
<td>?</td>
<td>debug</td>
</tr>
<tr>
<td>rpc</td>
<td>2350</td>
<td>00:00:00</td>
<td>?</td>
<td>portmap</td>
</tr>
<tr>
<td>root</td>
<td>2381</td>
<td>00:00:00</td>
<td>?</td>
<td>rpciod/0</td>
</tr>
</tbody>
</table>

--More--

ise/admin#
show repository

To display the file contents of the repository, use the show repository command in EXEC mode.

```
show repository repository-name
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>repository-name</td>
<td>Name of the repository whose contents you want to view. Supports up to 30 alphanumeric characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>No default behavior or values.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To view the contents of the repository, use the show repository command.

**Example**

```
ise/admin# show repository myrepository
back1.tar.gpg
back2.tar.gpg
ise/admin#
```

**Note**

To use this command for an SFTP repository, the admin needs to generate the public key from the ISE CLI in addition to generating it from the ISE GUI. This is required because when the SFTP repository is configured from the ISE GUI, the public key on ISE is generated for the root user only and not for the admin user (user with which all commands can be run from the CLI). Follow these steps to verify and configure the public key from the ISE CLI:

1. Verify whether the crypto key is yet generated or not. If the output for the following command is empty it means that the crypto key is not generated.
   ```
   ise24/admin# show crypto key
   ```

2. Hence from the CLI EXEC mode generate the key using the command: `crypto key generate rsa passphrase <secretkey>`. 

3. From the following we can now confirm that the crypto key is generated successfully:
   ```
   ise24/admin# show crypto key
   admin public key: ssh-rsa SHA256:eEziR/ARPyFo1WptgI+y5WNjG1rgfPmEpEswVY7Qjb0 admin@ise24
   ```

4. After this, the admin needs to export the public key for 'admin' user using the command:`crypto key export <sample-name> repository <another-repository-name>`. 

5. Now open the file saved to the `<another-repository-name>` and add it to `/home/<username>/.ssh/authorized_keys` folder in the SFTP server.
show restore

To display the restore history and the status of restore, use the **show restore** command in EXEC mode.

```
show restore {history | status}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>history</td>
<td>Displays the restore history on the system.</td>
</tr>
<tr>
<td>status</td>
<td>Displays the status of restore on the system.</td>
</tr>
</tbody>
</table>

**Command Default**
No default behavior or values.

**Command Modes**
EXEC

**Usage Guidelines**

```
ise/admin# show restore history
Wed Apr 10 03:32:24 PDT 2013: restore mybackup-CFG-130410-0228.tar.gpg from repository myrepository: success
Wed Apr 10 03:45:19 PDT 2013: restore mybackup1-OPS-130410-0302.tar.gpg from repository myrepository: success
ise/admin#
ise/admin# show restore status
%% Configuration restore status
%% Operation restore status
%% ------------------------
%% No data found. Try 'show restore history' or ISE operation audit report
%% ------------------------
%% No data found. Try 'show restore history' or ISE operation audit report
ise/admin#
```
show running-config

To display the contents of the currently running configuration file or the configuration, use the `show running-config` command in EXEC mode.

This command has no keywords and arguments.

**show running-config**

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show running-config` command displays all of the running configuration information.

**Example**

```
ise/admin# show running-config
Generating configuration...
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 171.70.168.183
!
ip default-gateway 172.23.90.1
!
clock timezone UTC
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHV$GwMz/XL4tH15KnF.FeEZr. role admin
!
service sshd
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
cdp timer 60
!
cdp holdtime 180
!
cdp run GigabitEthernet 0
!
icmp echo on
!
ise/admin#
```
show snmp engineid

To display the default or configured engine ID, use the `show snmp engineid` command in EXEC mode. This command displays the identification of the local SNMP engine and all remote engines that have been configured on the device.

`show snmp engineid`

**Command Default**
No default behavior or values.

**Command Modes**
EXEC

**Example**

```
ise/admin# show snmp engineid
Local SNMP EngineID: 0x1234567

ise/admin#
```
**show snmp user**

To display a list of defined snmp users, use the **show snmp user** command in EXEC mode.

```
show snmp user
```

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Example**

```
ise/admin# show snmp user
User: snmp3
  EngineID: 80001f88044b4951504a375248374c55
  Auth Protocol: sha
  Priv Protocol: aes-128

ise/admin#
```
show startup-config

To display the contents of the startup configuration file or the configuration, use the `show startup-config` command in EXEC mode.

This command has no keywords and arguments.

`show startup-config`

**Command Default**

None

**Usage Guidelines**

The `show startup-config` command displays all of the startup configuration information.

**Example**

```bash
ise/admin# show startup-config
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 171.70.168.183
!
ip default-gateway 172.23.90.1
!
clock timezone UTC
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/Xl5Knf.FfcZz. role admin
!
service sshd
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
cdp timer 60
!
ise/admin#
```
show tech-support

To display technical support information, including e-mail, use the `show tech-support` command in EXEC mode.

```
show tech-support > file-name
show tech-support file file-name
```

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&gt;</code></td>
<td>Redirects output to a file.</td>
</tr>
<tr>
<td><code>file</code></td>
<td>Saves any technical support data as a file in the local disk.</td>
</tr>
<tr>
<td><code>file-name</code></td>
<td>Filename to save technical support data. Supports up to 80 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Command Default**

Passwords and other security information do not appear in the output.

**Command Modes**

EXEC

**Usage Guidelines**

The `show tech-support` command is useful for collecting a large amount of information about the Cisco ISE server for troubleshooting purposes. You can then provide output to technical support representatives when reporting a problem.

**Example**

```
ise/admin# show tech-support
******************************************************************************
Displaying ISE version ...                                    
******************************************************************************
Cisco Identity Services Engine                                    
******************************************************************************
Version : 1.3.0.862
Build Date : Tue Oct 14 19:02:08 2014
Install Date : Wed Oct 15 09:08:53 2014

******************************************************************************
Displaying Clock ...                                            
******************************************************************************
Tue Oct 21 11:24:08 IST 2014

******************************************************************************
Displaying UDI ...                                              
******************************************************************************
ISE-VM-K9

******************************************************************************
Displaying ISE application status ...                           
******************************************************************************
ISE PROCESS NAME STATE PROCESS ID
--More--
(press Spacebar to continue)
ise/admin#
```
Example

ise/admin# show tech-support
************************************************
Displaying ISE version ...
************************************************
Cisco Identity Services Engine
************************************************
Version : 1.4.0.205
Build Date : Tue 03 Mar 2015 05:37:10 AM UTC
Install Date : Tue 03 Mar 2015 08:25:37 PM UTC

************************************************
Displaying Clock ...
************************************************
Mon Mar 16 03:51:35 UTC 2015

************************************************
Displaying UDI ...
************************************************
ISE-VM-K9

************************************************
Displaying ISE application status ....
************************************************
ISE PROCESS NAME STATE PROCESS ID
--More--
(press Spacebar to continue)
ise/admin#
**show terminal**

To obtain information about the terminal configuration parameter settings, use the `show terminal` command in EXEC mode.

This command has no keywords and arguments.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

The following table describes the fields of the `show terminal` output.

**Table 3: Show Terminal Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTY: /dev/pts/0</td>
<td>Displays standard output to type of terminal.</td>
</tr>
<tr>
<td>Type: “vt100”</td>
<td>Type of current terminal used.</td>
</tr>
<tr>
<td>Length: 27 lines</td>
<td>Length of the terminal display.</td>
</tr>
<tr>
<td>Width: 80 columns</td>
<td>Width of the terminal display, in character columns.</td>
</tr>
<tr>
<td>Session Timeout: 30 minutes</td>
<td>Length of time, in minutes, for a session, after which the connection closes.</td>
</tr>
</tbody>
</table>

**Example**

```
ise/admin# show terminal
TTY: /dev/pts/0 Type: "vt100"
Length: 27 lines, Width: 80 columns
Session Timeout: 30 minutes
ise/admin#
```
show timezone

To display the time zone as set on the system, use the show timezone command in EXEC mode.
This command has no keywords and arguments.

show timezone
This command has no keywords and arguments.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Command Modes</th>
<th>Usage Guidelines</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EXEC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| No default behavior or values. |                  |                  | ise/admin# show timezone
|                  |                |                  | UTC
|                  |                |                  | ise/admin#      |
show timezones

To obtain a list of time zones from which you can select, use the `show timezones` command in EXEC mode.

This command has no keywords and arguments.

**show timezones**

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

See the clock timezone section, for examples of the time zones available for the Cisco ISE server.

**Example**

```
ise/admin# show timezones
Africa/Cairo
Africa/Banjul
Africa/Nouakchott
Africa/Gaborone
Africa/Bangui
Africa/Malabo
Africa/Lusaka
Africa/Conakry
Africa/Freetown
Africa/Bamako
--More--
(press Spacebar to continue)
ise/admin#
```
show udi

To display information about the Unique Device Identifier (UDI) of the Cisco ISE appliance, use the **show udi** command in EXEC mode.

This command has no keywords and arguments.

```markdown
show udi
```

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

**Example 1**

```bash
ise/admin# show udi
SPID: ISE-3415-K9
VPID: V01
Serial: LAB12345678
ise/admin#
```

**Example 2**

The following output appears when you run the **show udi** command on VMware servers.

```bash
ise/admin# show udi
SPID: ISE-VM-K9
VPID: V01
Serial: 5C79C84ML9H
ise/admin#
```
show uptime

To display the length of time, the Cisco ISE server has been up since the last reboot, use the `show uptime` command in EXEC mode.

`show uptime > file-name`

**Syntax Description**

> Redirects output to a file.

`file-name` Name of the file to redirect.

<table>
<thead>
<tr>
<th>Output modifier variables:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• begin—Matched pattern. Supports up to 80 alphanumeric characters.</td>
</tr>
<tr>
<td>• count—Count the number of lines in the output. Add number after the word count.</td>
</tr>
<tr>
<td>• end—End with line that matches. Supports up to 80 alphanumeric characters.</td>
</tr>
<tr>
<td>• exclude—Exclude lines that match. Supports up to 80 alphanumeric characters.</td>
</tr>
<tr>
<td>• include—Include lines that match. Supports up to 80 alphanumeric characters.</td>
</tr>
<tr>
<td>• last—Display last few lines of output. Add number after the word last. Supports up to 80 lines to display. Default 10.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

Use this `show uptime` to check for how long the Cisco ISE server has been up since the last reboot.

**Example**

```
ise/admin# show uptime
3 day(s), 18:55:02
ise/admin#
```
show users

To display the list of users logged in to the Cisco ISE server, use the `show users` command in EXEC mode.

```
show users > file-name
```

### Syntax Description

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>Redirects output to a file.</td>
</tr>
<tr>
<td>file-name</td>
<td>Name of the file to redirect.</td>
</tr>
</tbody>
</table>

### Output modifier variables:

- **begin**—Matched pattern. Supports up to 80 alphanumeric characters.
- **count**—Count the number of lines in the output. Add number after the word count.
- **end**—End with line that matches. Supports up to 80 alphanumeric characters.
- **exclude**—Exclude lines that match. Supports up to 80 alphanumeric characters.
- **include**—Include lines that match. Supports up to 80 alphanumeric characters.
- **last**—Display last few lines of output. Add number after the word last. Supports up to 80 lines to display. Default 10.

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Usage Guidelines

Use this `show users` command to check the list of users logged into the Cisco ISE server.

### Example

```
ise/admin# show users
USERNAME ROLE HOST TTY LOGIN DATETIME
admin Admin 10.77.202.52 pts/0 Tue Feb 26 20:36:41 2013

-------------------

DETACHED SESSIONS:
-------------------

USERNAME ROLE STARTDATE
% No disconnected user sessions present
ise/admin#
```
**show version**

To display information about the software version of the system and software installation information, use the `show version` command in EXEC mode.

```
show version > file-name
show version history
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>Redirects output to a file.</td>
</tr>
<tr>
<td><code>file-name</code></td>
<td>Name of the file to redirect.</td>
</tr>
<tr>
<td><code>history</code></td>
<td>Shows software version history information.</td>
</tr>
<tr>
<td>Output modifier variables:</td>
<td></td>
</tr>
<tr>
<td>• <code>begin</code>—Matched pattern. Supports up to 80 alphanumeric characters.</td>
<td></td>
</tr>
<tr>
<td>• <code>count</code>—Count the number of lines in the output. Add number after the word count.</td>
<td></td>
</tr>
<tr>
<td>• <code>end</code>—End with line that matches. Supports up to 80 alphanumeric characters.</td>
<td></td>
</tr>
<tr>
<td>• <code>exclude</code>—Exclude lines that match. Supports up to 80 alphanumeric characters.</td>
<td></td>
</tr>
<tr>
<td>• <code>include</code>—Include lines that match. Supports up to 80 alphanumeric characters.</td>
<td></td>
</tr>
<tr>
<td>• <code>last</code>—Display last few lines of output. Add number after the word last. Supports up to 80 lines to display. Default 10.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

This command displays version information about the Cisco ADE-OS software running in the Cisco ISE server, and also displays the Cisco ISE version.

**Example 1**

```
ise/admin# show version

Cisco Application Deployment Engine OS Release: 3.0
ADE-OS Build Version: 3.0.3.030
ADE-OS System Architecture: x86_64

Copyright (c) 2005-2014 by Cisco Systems, Inc.
All rights reserved.
Hostname: docs-ise-23-lnx
```
Version information of installed applications
--------------------------------------------

Cisco Identity Services Engine
--------------------------------------------
Version : 2.3.0.297
Build Date : Mon Jul 24 18:51:29 2017
Install Date : Wed Jul 26 13:59:41 2017
ise/admin#

Example 2
ise/admin# show version history
--------------------------------------------
Install Date: Wed Jul 26 19:02:13 UTC 2017
Application: ise
Version: 2.3.0.297
Install type: Application Install
Bundle filename: ise.tar.gz
Repository: SystemDefaultPkgRepos
ise/admin#
show version
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, on page 153
- Configuring Cisco ISE in the Configuration Mode, on page 154
- Configuring Cisco ISE in the Configuration Submode, on page 155
- CLI Configuration Command Default Settings, on page 156
- backup interface, on page 157
- cdp holdtime, on page 161
- cdp run, on page 162
- cdp timer, on page 163
- clock timezone, on page 164
- conn-limit, on page 168
- do, on page 169
- end, on page 172
- exit, on page 173
- hostname, on page 174
- icmp echo, on page 176
- interface, on page 177
- ipv6 address autoconfig, on page 179
- ipv6 address dhcp, on page 181
- ip address, on page 182
- ipv6 address, on page 184
- ipv6 enable, on page 186
- ip default-gateway, on page 187
- ip domain-name, on page 188
- ip host, on page 189
- ip mtu, on page 191
- ip name-server, on page 192
- ip route, on page 194
- ipv6 route, on page 196
- kron occurrence, on page 198
- kron policy-list, on page 200
• logging, on page 202
• max-ssh-sessions, on page 203
• ntp, on page 204
• ntp authenticate, on page 205
• ntp authentication-key, on page 206
• ntp server, on page 208
• ntp trusted-key, on page 212
• rate-limit, on page 213
• password-policy, on page 214
• repository, on page 216
• service, on page 219
• shutdown, on page 221
• snmp-server enable, on page 222
• snmp-server user, on page 223
• snmp-server host, on page 225
• snmp-server community, on page 227
• snmp-server contact, on page 228
• snmp-server location, on page 229
• snmp-server trap dskThresholdLimit, on page 230
• snmp engineid, on page 231
• username, on page 232
• synflood_limited, on page 234
Switch to Configuration Mode in EXEC Mode

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

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

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

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

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

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

- `copy running-config startup-config`
- `write memory`
Configuring Cisco ISE in the Configuration Mode

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

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

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

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

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

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

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

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

```
ise/admin(config)# exit
ise/admin# exit
```
Configuring Cisco ISE in the Configuration Submode

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

---

**Step 1**

Enter `configure terminal` to enter into the configuration mode.

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

**Step 2**

Enter into the configuration submode.

ise/admin# configure terminal
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config-GigabitEthernet)# ?
Configure ethernet interface:
  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 Shut down 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 into 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.

<table>
<thead>
<tr>
<th>Cisco ISE Physical NIC Name</th>
<th>Linux Physical NIC Name</th>
<th>Role in Bonded NIC</th>
<th>Bonded NIC Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet 0</td>
<td>Eth0</td>
<td>Primary</td>
<td>Bond 0</td>
</tr>
<tr>
<td>Gigabit Ethernet 1</td>
<td>Eth1</td>
<td>Backup</td>
<td></td>
</tr>
<tr>
<td>Gigabit Ethernet 2</td>
<td>Eth2</td>
<td>Primary</td>
<td>Bond 1</td>
</tr>
<tr>
<td>Gigabit Ethernet 3</td>
<td>Eth3</td>
<td>Backup</td>
<td></td>
</tr>
<tr>
<td>Gigabit Ethernet 4</td>
<td>Eth4</td>
<td>Primary</td>
<td>Bond 2</td>
</tr>
<tr>
<td>Gigabit Ethernet 5</td>
<td>Eth5</td>
<td>Backup</td>
<td></td>
</tr>
</tbody>
</table>

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. |
Configure the Gigabit Ethernet interfaces specified as the backup interface.

**GigabitEthernet**

- **Number of the Gigabit Ethernet port to configure as the backup interface.**
- **0 - 3**

**Command Default**

No default behavior or values.

**Command Modes**

Interface configuration submode (config-GigabitEthernet)#

**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.
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.

**Note**

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 Collector...
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 Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise' CLI to verify all processes are in running state.
ise/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.

```
is/admin# show interface
bond0: flags=5187<UP,BROADCAST,RUNNING,MASTER,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,SLAVE,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,SLAVE,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 seconds. |

### Command Default

The default CDP holdtime, in seconds is 180.

### Command Modes

Configuration (config)#

### 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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>run</code></td>
<td>Enables the Cisco Discovery Protocol. Disables the Cisco Discovery Protocol when you use the <code>no</code> form of the <code>cdp run</code> command.</td>
</tr>
<tr>
<td><code>GigabitEthernet</code></td>
<td>(Optional). Specifies the GigabitEthernet interface on which to enable the Cisco Discovery Protocol.</td>
</tr>
<tr>
<td><code>0-3</code></td>
<td>Specifies the GigabitEthernet interface number on which to enable the Cisco Discovery Protocol.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

Configuration (config)#

### 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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>timer</code></td>
<td>Refreshes at the time interval specified.</td>
</tr>
<tr>
<td><code>seconds</code></td>
<td>Specifies how often, in seconds, the Cisco ISE server sends Cisco Discovery Protocol updates. The value ranges from 5 to 254 seconds.</td>
</tr>
</tbody>
</table>

**Command Default**

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

**Command Modes**

Configuration (config)#

**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
```

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

```
no clock timezone
```

---

**Note**

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>timezone</code></td>
<td>Configures system timezone.</td>
</tr>
<tr>
<td><code>timezone</code></td>
<td>Name of the time zone visible when in standard time. Supports up to 64 alphanumeric characters.</td>
</tr>
</tbody>
</table>

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)#

**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(config)# show timezone
EST
ise/admin#
```
Changing the Time Zone on Cisco ISE Nodes

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

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

To recover from the impact, use the following steps:

**Standalone or Primary Cisco ISE Node**

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

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

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

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

**Secondary ISE Node**

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

- Export the necessary certificates.
- Deregister the secondary node.
- Re-image the node.
- Import the necessary certificates, if required.
- Re-register the node as a secondary node to the primary node.
- Rejoin Active Directory and apply any per-node configurations for ISE profiling probes, LDAP, etc.

Common Time Zones

Table 4-1 Common Time Zones (Continued)

<table>
<thead>
<tr>
<th>Acronym or name</th>
<th>Time Zone Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td>Greenwich Mean Time, as UTC</td>
</tr>
<tr>
<td>GMT, GMT0, GMT-0, GMT+0, UTC, Greenwich, Universal, Zulu</td>
<td>Greenwich Mean Time, as UTC</td>
</tr>
<tr>
<td>GB</td>
<td>British</td>
</tr>
<tr>
<td>GB-Eire, Eire</td>
<td>Irish</td>
</tr>
</tbody>
</table>
### Australia Time Zones

<table>
<thead>
<tr>
<th>Acronym or name</th>
<th>Time Zone Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>WET</td>
<td>Western Europe Time, as UTC</td>
</tr>
<tr>
<td>CET</td>
<td>Central Europe Time, as UTC + 1 hour</td>
</tr>
<tr>
<td>EET</td>
<td>Eastern Europe Time, as UTC + 2 hours</td>
</tr>
<tr>
<td>United States and Canada</td>
<td></td>
</tr>
<tr>
<td>EST, EST5EDT</td>
<td>Eastern Standard Time, as UTC - 5 hours</td>
</tr>
<tr>
<td>CST, CST6CDT</td>
<td>Central Standard Time, as UTC - 6 hours</td>
</tr>
<tr>
<td>MST, MST7MDT</td>
<td>Mountain Standard Time, as UTC - 7 hours</td>
</tr>
<tr>
<td>PST, PST8PDT</td>
<td>Pacific Standard Time, as UTC - 8 hours</td>
</tr>
<tr>
<td>HST</td>
<td>Hawaiian Standard Time, as UTC - 10 hours</td>
</tr>
</tbody>
</table>

**Note**

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

**Table 5: Table 4-2 Australia Time Zones (Continued)**

<table>
<thead>
<tr>
<th>Australia</th>
<th>Adelaide</th>
<th>Brisbane</th>
<th>Broken_Hill</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australian Capital</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Territory (ACT)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canberra</td>
<td>Currie</td>
<td>Darwin</td>
<td>Hobart</td>
</tr>
<tr>
<td>Lord_Howe</td>
<td>Lindeman</td>
<td>Lord Howe Island (LHI)</td>
<td>Melbourne</td>
</tr>
<tr>
<td>North</td>
<td>New South Wales (NSW)</td>
<td>Perth</td>
<td>Queensland</td>
</tr>
<tr>
<td>South</td>
<td>Sydney</td>
<td>Tasmania</td>
<td>Victoria</td>
</tr>
<tr>
<td>West</td>
<td>Yancowinna</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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>
<thead>
<tr>
<th>Asia</th>
<th>Aden</th>
<th>Almaty</th>
<th>Amman</th>
<th>Anadyr</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Aqtau</td>
<td>Aqtobe</td>
<td>Ashgabat</td>
<td>Ashkhabad</td>
</tr>
<tr>
<td></td>
<td>Baghdad</td>
<td>Bahrain</td>
<td>Baku</td>
<td>Bangkok</td>
</tr>
<tr>
<td></td>
<td>Beirut</td>
<td>Bishkek</td>
<td>Brunei</td>
<td>Calcutta</td>
</tr>
<tr>
<td></td>
<td>Choibalsan</td>
<td>Chongqing</td>
<td>Columbo</td>
<td>Damascus</td>
</tr>
<tr>
<td></td>
<td>Dhakar</td>
<td>Dili</td>
<td>Dubai</td>
<td>Dushanbe</td>
</tr>
<tr>
<td></td>
<td>Gaza</td>
<td>Harbin</td>
<td>Hong_Kong</td>
<td>Hovd</td>
</tr>
<tr>
<td></td>
<td>Irkutsk</td>
<td>Istanbul</td>
<td>Jakarta</td>
<td>Jayapura</td>
</tr>
<tr>
<td></td>
<td>Jerusalem</td>
<td>Kabul</td>
<td>Kamchatka</td>
<td>Karachi</td>
</tr>
<tr>
<td></td>
<td>Kashgar</td>
<td>Katmandu</td>
<td>Kuala_Lumpur</td>
<td>Kuching</td>
</tr>
<tr>
<td></td>
<td>Kuwait</td>
<td>Krasnoyarsk</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**conn-limit**

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

**Syntax Description**

```
<1-2147483647>  Number of TCP connections.

ip             (Optional). Source IP address to apply the TCP connection limit.

mask           (Optional). Source IP mask to apply the TCP connection limit.

port           (Optional). Destination port number to apply the TCP connection limit.
```

**Command Default**

No default behavior or values.

**Command Modes**

Configuration (config)#

**Usage Guidelines**

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

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

**Example**

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application configure</td>
<td>Configures a specific application.</td>
</tr>
<tr>
<td>application install</td>
<td>Installs a specific application.</td>
</tr>
<tr>
<td>application remove</td>
<td>Removes a specific application.</td>
</tr>
<tr>
<td>application reset-config</td>
<td>Resets application configuration to factory defaults.</td>
</tr>
<tr>
<td>application reset-passwd</td>
<td>Resets application password for a specified user.</td>
</tr>
<tr>
<td>application start</td>
<td>Starts or enables a specific application</td>
</tr>
<tr>
<td>application stop</td>
<td>Stops or disables a specific application.</td>
</tr>
<tr>
<td>application upgrade</td>
<td>Upgrades a specific application.</td>
</tr>
<tr>
<td>backup</td>
<td>Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.</td>
</tr>
<tr>
<td>backup-logs</td>
<td>Performs a backup of all logs in the Cisco ISE server to a remote location.</td>
</tr>
<tr>
<td>clock</td>
<td>Sets the system clock in the Cisco ISE server.</td>
</tr>
<tr>
<td>configure</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>copy</td>
<td>Copies any file from a source to a destination.</td>
</tr>
<tr>
<td>debug</td>
<td>Displays any errors or events for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a file in the Cisco ISE server.</td>
</tr>
<tr>
<td>dir</td>
<td>Lists files in the Cisco ISE server.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>forceout</td>
<td>Forces the logout of all sessions of a specific Cisco ISE node user.</td>
</tr>
<tr>
<td>halt</td>
<td>Disables or shuts down the Cisco ISE server.</td>
</tr>
<tr>
<td>mkdir</td>
<td>Creates a new directory.</td>
</tr>
<tr>
<td>nslookup</td>
<td>Queries the IPv4 or IPv6 address or hostname of a remote system.</td>
</tr>
<tr>
<td>password</td>
<td>Updates the CLI account password.</td>
</tr>
<tr>
<td>patch</td>
<td>Installs a Patch Bundle or uninstalls an Application patch.</td>
</tr>
<tr>
<td>ping</td>
<td>Determines the IPv4 address or hostname of a remote system.</td>
</tr>
<tr>
<td>ping6</td>
<td>Determines the IPv6 address of a remote system.</td>
</tr>
<tr>
<td>reload</td>
<td>Reboots the Cisco ISE server.</td>
</tr>
<tr>
<td>restore</td>
<td>Performs a restore and retrieves the backup out of a repository.</td>
</tr>
<tr>
<td>rmdir</td>
<td>Removes an existing directory.</td>
</tr>
<tr>
<td>show</td>
<td>Provides information about the Cisco ISE server.</td>
</tr>
<tr>
<td>ssh</td>
<td>Starts an encrypted session with a remote system.</td>
</tr>
<tr>
<td>tech</td>
<td>Provides Technical Assistance Center (TAC) commands.</td>
</tr>
<tr>
<td>terminal length</td>
<td>Sets terminal line parameters.</td>
</tr>
<tr>
<td>terminal session-timeout</td>
<td>Sets the inactivity timeout for all terminal sessions.</td>
</tr>
<tr>
<td>terminal session-welcome</td>
<td>Sets the welcome message on the system for all terminal sessions.</td>
</tr>
<tr>
<td>terminal terminal-type</td>
<td>Specifies the type of terminal connected to the current line of the current session.</td>
</tr>
<tr>
<td>traceroute</td>
<td>Traces the route of a remote IP address.</td>
</tr>
<tr>
<td>undebug</td>
<td>Disables the output (display of errors or events) of the debug command for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>write</strong></td>
<td>Erases the startup configuration that forces to run the setup utility and prompt the network configuration, copies the running configuration to the startup configuration, displays the running configuration on the console.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

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

**Usage Guidelines**

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

**Example**

ise/admin(config)# do show run
Generating configuration...
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
    ip address 172.23.90.113 255.255.255.0
    ipv6 address autoconfig
!
ip name-server 171.70.168.183
!
ip default-gateway 172.23.90.1
!
clock timezone EST
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. role admin
!
service sshd
!
backup-staging-url nfs://loc-filer02a:/vol/local1/private1/jdoe
!
password-policy
    lower-case-required
    upper-case-required
    digit-required
    no-username
    disable-cisco-passwords
    min-password-length 6
!
logging localhost
logging loglevel 6
!
--More--
ise/admin(config)#
**end**

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

This command has no keywords and arguments.

**Command Default**

No default behavior or values.

**Command Modes**

Configuration (config)#

**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)#

**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Name of the host. Supports up to 19 alphanumeric characters and an underscore (_). The hostname must begin with a character that is not a space.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Configuration (config)#

**Usage Guidelines**

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

The workaround for this is to issue another 'hostname' configuration CLI to set the hostname to the desired value.

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.

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

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

**Example**

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

ise-1/admin#
icmp echo

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

```
icmp echo {off | on}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>off</code></td>
<td>Disables ICMP echo response.</td>
</tr>
<tr>
<td><code>on</code></td>
<td>Enables ICMP echo response.</td>
</tr>
<tr>
<td><code>echo</code></td>
<td>Configures ICMP echo response.</td>
</tr>
</tbody>
</table>

**Command Default**

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

**Command Modes**

Configuration (config) #

**Usage Guidelines**

Use this `icmp echo` to turn on or turn off ICMP echo response.

**Example**

```
isec/admin(config)# icmp echo off
ise/admin(config) #
```
**interface**

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

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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet</td>
<td>Configures the Gigabit Ethernet interface.</td>
</tr>
<tr>
<td>0 - 3</td>
<td>Number of the Gigabit Ethernet port to configure.</td>
</tr>
</tbody>
</table>

---

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup</td>
<td>Configures the NIC bonding feature to provide high availability for the physical interfaces.</td>
</tr>
<tr>
<td>do</td>
<td>EXEC command. Allows you to perform any EXEC commands in this mode.</td>
</tr>
<tr>
<td>end</td>
<td>Exits the config-GigabitEthernet submode and returns you to EXEC mode.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits the config-GigabitEthernet configuration submode.</td>
</tr>
<tr>
<td>ip</td>
<td>Sets the IP address and netmask for the Gigabit Ethernet interface.</td>
</tr>
<tr>
<td>ipv6</td>
<td>Configures IPv6 autoconfiguration address and IPv6 address from DHCPv6 server.</td>
</tr>
<tr>
<td>no</td>
<td>Negates the command in this mode. Two keywords are available:</td>
</tr>
<tr>
<td></td>
<td>• ip—Sets the IP address and netmask for the interface.</td>
</tr>
<tr>
<td></td>
<td>• ipv6—Sets the IPv6 address for the interface.</td>
</tr>
<tr>
<td></td>
<td>• shutdown—Shuts down the interface.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the interface.</td>
</tr>
</tbody>
</table>
**Command Default**
No default behavior or values.

**Command Modes**
Interface configuration (config-GigabitEthernet)#

**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)#
```
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.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Nodefaultbehaviororvalues.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Interface configuration (config-GigabitEthernet)#</td>
</tr>
</tbody>
</table>

**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
```

**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
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:302:11:2:20c: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.

**Command Default**

No default behavior or values.

**Command Modes**

Interface configuration (config-GigabitEthernet)#

**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
!
```
**ip address**

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

```
ip address ip-address network mask
```

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

```
no ip address
```

---

**Note**

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

---

**Syntax Description**

- `ip-address`  
  IPv4 address.

- `network mask`  
  Mask of the associated IP subnet.

---

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)#

---

**Usage Guidelines**

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.

---

**Note**

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)#
**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.

```shell
ipv6 address ipv6-address/prefix-length
```

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

```shell
no ipv6 address ipv6-address/prefix-length
```

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>ipv6-address</strong></th>
<th>IPv6 address.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>prefix-length</strong></td>
<td>The length of the IPv6 prefix. A decimal value between 0 and 128 that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</td>
</tr>
</tbody>
</table>

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)#

**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 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)#

**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
erethernet 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 5247 (5.1 KiB)
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# show interface gigabitEthernet 1
GigabitEthernet 1
flags=4163 UP,BROADCAST, RUNNING, MULTICAST mtu 1500
erethernet 00:0c:29:83:a6:10 txqueuelen 1000 (Ethernet)
RX packets 6 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
```
ip default-gateway

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

```
ip default-gateway ip-address
```

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

```
no ip default-gateway
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default-gateway</code></td>
<td>Defines a default gateway with an IP address.</td>
</tr>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the default gateway.</td>
</tr>
</tbody>
</table>

### Command Default

Disabled.

### Command Modes

Configuration (config)#

### Usage Guidelines

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

### Example

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

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

**ip domain-name** *domain-name*

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

**no ip domain-name**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>domain-name</strong></td>
<td>Defines a default domain name.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Default Domain Name Used to Complete the Hostnames.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>domain-name</strong></td>
<td>Contains at least 2 to 64 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Command Default**

Enabled.

**Command Modes**

Configuration (config)#

**Usage Guidelines**

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

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

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

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

*Warning:* Updating the domain name will cause any certificate using the old domain name to become invalid. Therefore, a new self-signed certificate using the new domain name will be generated now for use with HTTPS/EAP. If CA-signed certificates were used on this node, please import them with the correct domain name. In addition, if this ISE node will be joining a new Active Directory domain, please leave your current Active Directory domain before proceeding.

**Example**

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

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

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

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

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

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

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4-address</td>
<td>IPv4 address of the network interface.</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>IPv6 address of the network interface.</td>
</tr>
<tr>
<td>host-alias</td>
<td>Host alias is the name that you assign to the network interface.</td>
</tr>
<tr>
<td>FQDN-string</td>
<td>Fully qualified domain name (FQDN) of the network interface.</td>
</tr>
</tbody>
</table>

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)#

**Usage Guidelines**

Supported IPv6 address formats include:

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

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

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

Example 1

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

Example 2

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

<table>
<thead>
<tr>
<th>mtu</th>
<th>Configures the MTU on an ISE interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>The size in bytes of the MTU from 1300 to 1500. The default MTU value is 1500.</td>
</tr>
</tbody>
</table>

### Command Default

The MTU is set as 1500.

### Command Modes

Interface configuration (config-GigabitEthernet)#

### 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:

```plaintext
ise/admin(config)# int GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ip mtu ?
<1300-1500> Select MTU value in range of 1300 to 1500
```

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

```plaintext
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name-server</td>
<td>Configures the IP addresses of the name server(s).</td>
</tr>
<tr>
<td>ip-address</td>
<td>Address of a name server.</td>
</tr>
<tr>
<td>ip-address*</td>
<td>(Optional). IP addresses of additional name servers.</td>
</tr>
</tbody>
</table>

**Note**

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

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)#

**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 171.70.168.183 171.68.226.120
3201:db8:0:20:f41d:eee:7e66:4eba
ise/admin#

Example 3

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

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

```
ip route prefix mask gateway ip-address
no ip route prefix mask
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix</td>
<td>IP route prefix for the destination.</td>
</tr>
<tr>
<td>mask</td>
<td>Prefix mask for the destination.</td>
</tr>
<tr>
<td>ip-address</td>
<td>IP address of the next hop that can be used to reach that network.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

Configuration (config)#

### 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
192.168.117.10 192.168.117.0 192.168.117.1
```

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
```
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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-address</td>
<td>IPv6 address.</td>
</tr>
<tr>
<td>prefix-length</td>
<td>The length of the IPv6 prefix. A decimal value between 0 and 128 that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</td>
</tr>
<tr>
<td>route-specific gateway</td>
<td>IPv6 address of the next hop that can be used to reach that network.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

Global configuration (config)#

### 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

<table>
<thead>
<tr>
<th>occurrence</th>
<th>Schedules Command Scheduler commands.</th>
</tr>
</thead>
<tbody>
<tr>
<td>occurrence-name</td>
<td>Name of the occurrence. Supports up to 80 alphanumeric characters. (See the following note and Syntax Description.)</td>
</tr>
</tbody>
</table>

**Note**

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

## Syntax Description

| at              | Identifies that the occurrence is to run at a specified calendar date and time. Usage: `at [hh:mm] [day-of-week | day-of-month | month day-of-month]`. |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| do              | EXEC command. Allows you to perform any EXEC commands in this mode.                                                                 |
| end             | Exits the kron-occurrence configuration submode and returns you to EXEC mode.                                                                 |
| exit            | Exits the kron-occurrence configuration mode.                                                                                                                                                             |
| no              | Negates the command in this mode. Three keywords are available:                                                                                                                                           |
|                 | * at—Usage: `at [hh:mm] [day-of-week | day-of-month | month day-of-month]`.                                                                                                                       |
|                 | * policy-list—Specifies a policy list to be run by the occurrence. Supports up to 80 alphanumeric characters.                                                                                           |
|                 | * recurring—Execution of the policy lists should be repeated.                                                                                                                                              |
| policy-list     | Specifies a Command Scheduler policy list to be run by the occurrence.                                                                                                                                    |
Identifies that the occurrences run on a recurring basis.

**Note** If kron occurrence is not recurring, then the kron occurrence configuration for the scheduled backup is removed after it has run.

---

**Command Default**
No default behavior or values.

**Command Modes**
Configuration (config-Occurrence)#

**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 timestamp) 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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>policy-list</strong></td>
<td>Specifies a name for Command Scheduler policies.</td>
</tr>
<tr>
<td><strong>list-name</strong></td>
<td>Name of the policy list. Supports up to 80 alphanumeric characters.</td>
</tr>
</tbody>
</table>

#### 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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>cli</strong></td>
<td>Command to be executed by the scheduler. Supports up to 80 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>do</strong></td>
<td>EXEC command. Allows you to perform any EXEC commands in this mode.</td>
</tr>
<tr>
<td><strong>end</strong></td>
<td>Exits from the config-Policy List configuration submode and returns you to EXEC mode.</td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td>Exits this submode.</td>
</tr>
<tr>
<td><strong>no</strong></td>
<td>Negates the command in this mode. One keyword is available:</td>
</tr>
<tr>
<td></td>
<td>• cli—Command to be executed by the scheduler.</td>
</tr>
</tbody>
</table>

#### Command Default

No default behavior or values.

#### Command Modes

Configuration (config-Policy List)#

#### 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

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

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Usage Guidelines

This command requires the `loglevel` keyword.

Example

```
ise/admin(config)# logging loglevel 0
ise/admin(config)#
```
max-ssh-sessions

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>1-10</th>
<th>Number of concurrent SSH sessions. The default is 5.</th>
</tr>
</thead>
</table>

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

**Command Modes**
Configuration (config)#

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

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

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

The navigation path to configure the maximum number of command-line interface (CLI) sessions is in the Session tab of the Cisco ISE Admin portal in the following location: Administration > System > Admin Access > Settings > Access.
To specify an NTP configuration, use the `ntp` command in configuration mode with `authenticate`, `authentication-key`, `server`, and `trusted-key` commands.

**ntp authenticate**

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

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

**ntp trusted-key** `<key>`

**no ntp server**

---

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>authenticate</code></td>
<td>Enables authentication of all time sources.</td>
</tr>
<tr>
<td><code>authentication-key</code></td>
<td>Specifies authentication keys for trusted time sources.</td>
</tr>
<tr>
<td><code>server</code></td>
<td>Specifies NTP server to use.</td>
</tr>
<tr>
<td><code>trusted-key</code></td>
<td>Specifies key numbers for trusted time sources.</td>
</tr>
</tbody>
</table>

---

**Command Default**

None

**Command Modes**

Configuration (config)#

**Usage Guidelines**

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

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

**Example**

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

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

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

**ntp authenticate**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>authenticate</th>
<th>Enables authentication of all time sources.</th>
</tr>
</thead>
</table>

**Command Default**

None

**Command Modes**

Configuration (config)#

**Usage Guidelines**

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

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

**Example**

```
ise/admin(config)# ntp authenticate
ise/admin(config)#
```
ntp authentication-key

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

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

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

**no ntp authentication-key**

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication-key</td>
<td>Configures authentication keys for trusted time sources.</td>
</tr>
<tr>
<td>key id</td>
<td>The identifier that you want to assign to this key. Supports numeric values from 1–65535.</td>
</tr>
<tr>
<td>md5</td>
<td>The encryption type for the authentication key.</td>
</tr>
<tr>
<td>hash</td>
<td>Hashed key for authentication. Specifies an encrypted (hashed) key that follows the encryption type. Supports up to 40 characters.</td>
</tr>
<tr>
<td>plain</td>
<td>Plaintext key for authentication. Specifies an unencrypted plaintext key that follows the encryption type. Supports up to 15 characters.</td>
</tr>
<tr>
<td>key value</td>
<td>The key value in the format matching either md5 plain</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Configuration (config)#.

**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**

**Example 1**

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

**Example 2**

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

**Example 3**

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

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

Cisco ISE also supports public-key authentication for NTP servers. NTPv4 uses symmetric-key cryptography and also provides a new Autokey scheme based on public-key cryptography. Public-key cryptography is generally considered more secure than symmetric-key cryptography because the security is based on a private value, which is generated by each server and never revealed. With Autokey, all key distribution and management functions involve only public values, which considerably simplifies key distribution and storage. We recommend that you use the IFF (identify Friend or Foe) Identification scheme as this scheme is most widely used.

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} {autokey | key <peer key number>}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Allows the system to synchronize with a specified server.</td>
</tr>
<tr>
<td>ip-address</td>
<td>IPv4 or IPv6 address or hostname of the server providing the clock synchronization. Arguments are limited to 255 alphanumeric characters. Ensure that the ISE eth0 interface is statically configured with an IPv6 address if you want to add an NTP server with an IPv6 address.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies that public-key authentication should be used for NTP server. If you choose this option, ensure that you import the NTP server's public key in to the Cisco ISE node using the <code>crypto</code> command.</td>
</tr>
<tr>
<td>autokey</td>
<td>(Optional). Peer key number. Supports up to 65535 numeric characters.</td>
</tr>
<tr>
<td>key</td>
<td>This key needs to be defined with a key value, by using the <code>ntp authentication-key</code> command, and also needs to be added as a trusted-key by using the <code>ntp trusted-key</code> command. For authentication to work, the key and the key value should be the same as that which is defined on the actual NTP server.</td>
</tr>
</tbody>
</table>

### Command Default

No servers are configured by default.

### Command Modes

Configuration (config)#
Usage Guidelines

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

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

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

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

To define an NTP server configuration and authentication keys from the Cisco ISE Admin portal, see the System Time and NTP Server Settings section in the *Cisco Identity Services Engine Administration Guide*. You can configure Autokey for NTP server only from the Cisco ISE CLI in Configuration Mode. After you configure Autokey for NTP server, be sure to import the public keys generated from the NTP server. See the **crypto** command for more information.

---

**Note**

When you use public-key authentication for NTP servers:

- Ensure that the NTP server available in the network is configured with Autokey. The NTP server must be reachable through DNS/hostname address. For information on how to configure Autokey for NTP servers, see the NTP Support Web.

- Generate key pairs on the NTP server using the **ntp-keygen-T** command and obtain the trusted public key of the NTP server. Import the public key in to Cisco ISE using the **crypto** command.

---

**Note**

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

---

**Example**

```plaintext
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# ntp server 209.165.200.225 autokey

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 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
ntp trusted-key nn
ntp server 209.165.200.228 key nn
ntp server 209.165.200.229
ntp server 209.165.200.225 autokey

Configuring Trusted Keys for NTP Server Authentication

To allow for software clock synchronization by the NTP server for the system, use the `ntp server` command in configuration mode.

ise/admin(config)# ntp server ntp.esl.cisco.com key 1
% WARNING: Key 1 needs to be defined as a ntp trusted-key.
ise/admin(config)# ntp trusted-key 1
% WARNING: Key 1 needs to be defined as a ntp authentication-key.
ise/admin(config)# ntp authentication-key 1 md5 plain SharedWithServe
ise/admin(config)#
ise/admin(config)# ntp server ntp.esl.cisco.com 1
ise/admin(config)# ntp server 171.68.10.80 2
ise/admin(config)# ntp server 171.68.10.150 3
ise/admin(config)#
ise/admin(config)# do show running-config
Generating configuration...

hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 10.105.171.218 255.255.255.0
  ipv6 address 2001:420:54ff:4::420:101/112
  ipv6 address autoconfig
  ipv6 enable
  !ip name-server 10.105.171.200 2001:420:54ff:4::420:200
  !ip default-gateway 172.21.79.1
  ipv6 route ::/0 gateway 2001:420:54ff:4::420:10
  !
clock timezone UTC
!
ntp authentication-key 1 md5 hash ee18afc7608ac7ecdbbeefc5351ad118bc9ce1eef3
ntp authentication-key 2 md5 hash f1ef7b05c0d1cd4c18c8b70e8c76f37f33c33b59
ntp authentication-key 3 md5 hash ee18afc7608ac7ec2d7ac6d09226111dce07da37
ntp trusted-key 1
ntp trusted-key 2
ntp trusted-key 3
ntp authenticate
ntp server 10.105.171.10 key 1
ntp server 2001:420:54ff:4::420:111 key 2
ntp server clock.cisco.com key 3
!
--More--
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 1 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 1 35 64 377    0.000   0.000   0.001
171.68.10.80  144.254.15.122 2 u 36 64 377 1.474   7.381   2.095
*171.68.10.150 144.254.15.122 2 u 33 64 377 0.922   10.485   2.198
Warning: Output results may conflict during periods of changing synchronization.
ise/admin#
```
ntp trusted-key

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

**ntp trusted-key key**

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

**no ntp trusted-key**

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Command Default</th>
<th>Command Modes</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>trusted-key</td>
<td>The identifier that you want to assign to this key.</td>
<td>Configuration (config)#</td>
<td>Define this key as an NTP authentication key and then add this key to the trusted list before you add this key to an NTP server. Keys that are added to the trusted list can only be used that allows synchronization by the NTP server with the system.</td>
</tr>
<tr>
<td>key</td>
<td>Specifies key numbers for trusted time sources that needs to be defined as NTP authentication keys. Supports up to 65535 numeric characters.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Configuration (config)#

### Usage Guidelines

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

**Example 1**

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

**Example 2**

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

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

rate-limit 250 ip-address net-mask port

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-10000&gt;</td>
<td>An average number of TCP/UDP/ICMP packets per second.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Source IP address to apply the packet rate limit.</td>
</tr>
<tr>
<td>net-mask</td>
<td>Source IP mask to apply the packet rate limit.</td>
</tr>
<tr>
<td>port</td>
<td>Destination port number to apply the packet rate limit.</td>
</tr>
</tbody>
</table>

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Usage Guidelines

None.

Example

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

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

#### password-policy options

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>digit-required</code></td>
<td>Requires a digit in user passwords.</td>
</tr>
<tr>
<td><code>disable-cisco-password</code></td>
<td>Disables the ability to use the word Cisco or any combination as the password.</td>
</tr>
<tr>
<td><code>disable-repeat-chars</code></td>
<td>Disables the ability of the password to contain more than four identical characters.</td>
</tr>
<tr>
<td><code>do</code></td>
<td>Exec command.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Exit from configure mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exit from this submode.</td>
</tr>
<tr>
<td><code>lower-case-required</code></td>
<td>Requires a lowercase letter in user passwords.</td>
</tr>
<tr>
<td><code>min-password-length</code></td>
<td>Minimum number of characters for a valid password. Supports up to 40 characters.</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Negate a command or set its defaults.</td>
</tr>
<tr>
<td><code>no.previous-password</code></td>
<td>Prevents users from reusing a part of their previous password.</td>
</tr>
<tr>
<td><code>no-username</code></td>
<td>Prohibits users from reusing their username as a part of a password.</td>
</tr>
<tr>
<td><code>password-delta</code></td>
<td>Number of characters to be different from the old password.</td>
</tr>
<tr>
<td><code>password-expiration-days</code></td>
<td>Number of days until a password expires. Supports an integer up to 3650.</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>Command</th>
<th>Default</th>
<th>Modes</th>
<th>Guidelines</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>password-expiration-enabled</strong></td>
<td>Enables password expiration.</td>
<td>You must enter the <code>password-expiration-enabled</code> command before the other password-expiration commands.</td>
<td></td>
<td><code>ise/admin(config)# password-policy</code>&lt;br&gt;<code>ise/admin(config-password-policy)# password-expiration-days 30</code>&lt;br&gt;<code>ise/admin(config-password-policy)# exit</code>&lt;br&gt;<code>ise/admin(config)#</code></td>
</tr>
<tr>
<td><strong>password-expiration-warning</strong></td>
<td>Number of days before expiration that warnings of impending expiration begin. Supports an integer up to 3650.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>password-lock-enabled</strong></td>
<td>Locks a password after several failures.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>password-lock-retry-count</strong></td>
<td>Number of failed attempts before user password locks. Supports an integer up to 20.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>password-time-lockout</strong></td>
<td>Sets the time in minutes after which the account lockout is cleared. Supports time values from 5 minutes to 1440 minutes.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>special-required</strong></td>
<td>Requires a special character in user passwords.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>upper-case-required</strong></td>
<td>Requires an uppercase letter in user passwords.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**repository**

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

```
repository repository-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>repository-name</code></td>
<td>Name of repository. Supports up to 80 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>do</code></td>
<td>EXEC command. Allows you to perform any of the EXEC commands in this mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Exits the config-Repository submode and returns you to EXEC mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits this mode.</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Negates the command in this mode.</td>
</tr>
<tr>
<td><code>url</code></td>
<td>URL of the repository. Supports up to 300 alphanumeric characters (see Table 4-3).</td>
</tr>
<tr>
<td><code>user</code></td>
<td>Configure the username and password for access. Supports up to 30 alphanumeric characters for username and supports 15 alphanumeric characters for password.</td>
</tr>
</tbody>
</table>

```
Password can consist of the following characters: 0 through 9, a through z, A through Z, ' ', @, #, $, %, ^, &, *, ( ), +, and =.
```

**Note**

Server is the server name and path refers to /subdir/subsubdir. Remember that a colon(:) is required after the server for an NFS network server.
Table 8: Table 4-5 URL Keywords (Continued)

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source of Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Enter the repository URL, including server and path information. Supports up to 80 alphanumeric characters.</td>
</tr>
<tr>
<td>cdrom:</td>
<td>Local CD-ROM drive (read only).</td>
</tr>
<tr>
<td>disk:</td>
<td>Local storage. You can run the <code>show repository repository_name</code> to view all files in the local repository.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> All local repositories are created on the <code>/localdisk</code> partition. When you specify disk:// in the repository URL, the system creates directories in a path that is relative to <code>/localdisk</code>. For example, if you entered disk://backup, the directory is created at <code>/localdisk/backup</code>.</td>
</tr>
<tr>
<td>ftp:</td>
<td>Source or destination URL for an FTP network server. Use <code>url ftp://server/path</code></td>
</tr>
<tr>
<td>http:</td>
<td>Source or destination URL for an HTTP network server (read only).</td>
</tr>
<tr>
<td>https:</td>
<td>Source or destination URL for an HTTPS network server (read only).</td>
</tr>
<tr>
<td>nfs:</td>
<td>Source or destination URL for an NFS network server. Use <code>url nfs://server:/path</code></td>
</tr>
<tr>
<td>sftp:</td>
<td>Source or destination URL for an SFTP network server. Use <code>url sftp://server/path</code></td>
</tr>
<tr>
<td>tftp:</td>
<td>Source or destination URL for a TFTP network server. Use <code>url tftp://server/path</code></td>
</tr>
</tbody>
</table>

**Command Default**
No default behavior or values.

**Command Modes**
Configuration (config-Repository)#

**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 `no` form of `host-key host` command in the submode.
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.
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sshd</code></td>
<td>Secure Shell Daemon. The daemon program for SSH.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables sshd service.</td>
</tr>
<tr>
<td><code>encryption-algorithm</code></td>
<td>Configures SSH encryption algorithms. The supported algorithms are a, aes128-cbc, aes128-ctr, aes256-cbc, and aes256-ctr.</td>
</tr>
<tr>
<td><code>encryption-mode</code></td>
<td>Configures SSH encryption mode on system. The supported modes are cbc and ctr.</td>
</tr>
<tr>
<td><code>key-exchange-algorithm</code></td>
<td>Specifies allowable key exchange algorithms for sshd service.</td>
</tr>
<tr>
<td><code>diffie-hellman-group14-sha1</code></td>
<td>Restricts key exchange algorithm to diffie-hellman-group14-sha1</td>
</tr>
<tr>
<td><code>Loglevel</code></td>
<td>Specifies the log level of messages from sshd to secure system log.</td>
</tr>
<tr>
<td></td>
<td>• 1—QUIET</td>
</tr>
<tr>
<td></td>
<td>• 2—FATAL</td>
</tr>
<tr>
<td></td>
<td>• 3—ERROR</td>
</tr>
<tr>
<td></td>
<td>• 4—INFO (default)</td>
</tr>
<tr>
<td></td>
<td>• 5—VERBOSE</td>
</tr>
<tr>
<td></td>
<td>• 6—DEBUG</td>
</tr>
<tr>
<td></td>
<td>• 7—DEBUG1</td>
</tr>
<tr>
<td></td>
<td>• 8—DEBUG2</td>
</tr>
<tr>
<td></td>
<td>• 9—DEBUG3</td>
</tr>
</tbody>
</table>

#### Command Default

No default behavior or values.

#### Command Modes

Configuration (config)#

#### 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-shal
ise/admin(config)# service sshd loglevel 4
ise/admin(config)#
shutdown

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

This command has no keywords and arguments.

**Command Default**
No default behavior or values.

**Command Modes**
Configuration (config-GigabitEthernet)#

**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.

```plaintext
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)#

**Example**

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

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

```
snmp-server user username v3 {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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>Configure a new user.</td>
</tr>
<tr>
<td>username</td>
<td>The name of the user on the host that belongs to the SNMP agent.</td>
</tr>
<tr>
<td>v3</td>
<td>Version of the SNMP used to send the traps.</td>
</tr>
<tr>
<td></td>
<td>Specifies that the SNMP Version 3 security model should be used for enabling the priv and the auth keywords.</td>
</tr>
<tr>
<td>{hash</td>
<td>plain}</td>
</tr>
<tr>
<td>auth-password</td>
<td>Specifies the authentication user password. The minimum length for a password is one character; however, we recommend that you use at least eight characters for security</td>
</tr>
<tr>
<td>priv-password</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

If you forget a password, you cannot recover it, and must reconfigure the user. You can specify a plain-text password or a localized digest. The localized digest must match the authentication algorithm selected for the user, which can be either MD5 or SHA. When the user configuration is displayed on the console or is written to a file (for example, the startup-configuration file), the localized authentication and privacy digests are always displayed instead of the plain-text password.
Specifiestheencryptionuserpassword. The minimum length for a password is one character; however, we recommend that you use at least eight characters for security.

**Note** If you forget a password, you cannot recover it, and must reconfigure the user. You can specify a plain-text password or a localized digest. The localized digest must match the authentication algorithm selected for the user, which can be either MD5 or SHA. When the user configuration is displayed on the console or is written to a file (for example, the startup-configuration file), the localized authentication and privacy digests are always displayed instead of the plain-text password.

---

<table>
<thead>
<tr>
<th><strong>Command Default</strong></th>
<th>Disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command Modes</strong></td>
<td>Configuration (config)#</td>
</tr>
<tr>
<td><strong>Usage Guidelines</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Example**

```
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.

```
snmp-server host {ip-address | hostname} trap version {1 | 2c} community | 3 username engine_ID {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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>host</strong></td>
<td>Configures hosts to receive SNMP notifications.</td>
</tr>
<tr>
<td><strong>ip-address</strong></td>
<td>IP address of the SNMP notification host. Supports up to 32 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>hostname</strong></td>
<td>Name of the SNMP notification host. Supports up to 32 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>trap</strong></td>
<td>Limits the NMS to receiving traps only.</td>
</tr>
<tr>
<td><strong>version</strong> {1</td>
<td>2c</td>
</tr>
<tr>
<td></td>
<td>• 1—SNMPv1.</td>
</tr>
<tr>
<td></td>
<td>• 2c—SNMPv2C.</td>
</tr>
<tr>
<td></td>
<td>• 3—SNMP v3.</td>
</tr>
<tr>
<td><strong>community</strong></td>
<td>Specifies the shared secret key between Cisco ISE and the NMS. Case-sensitive value that can be up to 32 characters in length. Spaces are not allowed. The default community-string is &quot;public.&quot; Cisco ISE users this key to determine whether the incoming SNMP request is valid.</td>
</tr>
<tr>
<td><strong>username</strong></td>
<td>(Optional; required only if you choose SNMP version 3) Associates a user with the host when SNMP Version 3 hosts are configured in Cisco ISE.</td>
</tr>
<tr>
<td><strong>engine_ID</strong></td>
<td>(Optional; required only if you choose SNMP version 3) Remote EngineID.</td>
</tr>
</tbody>
</table>
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 encryption user password.

Command Default
Enabled.

Command Modes
Configuration (config)#

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
2012-09-24T18:43:45:32.094128+00:00 ise1 snmtrapd[29534]: ise1.cisco.com [UDP: [192.168.118.108]:44474]: 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 contact admin@cisco.com
2012-09-24T18:43:45:32.094128+00:00 ise1 snmtrapd[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)#
```
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>community</code></td>
<td>Sets SNMP community string.</td>
</tr>
<tr>
<td><code>community-string</code></td>
<td>Accessing string that functions much like a password and allows access to SNMP. No blank spaces allowed. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td><code>ro</code></td>
<td>Specifies read-only access.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

Configuration (config)#

### Usage Guidelines

The `snmp-server community` command requires a community string and the `ro` argument; otherwise, an error occurs.

The SNMP agent on the Cisco ISE provides read-only SNMP-v1 and SNMP-V2c access to the following MIBs:

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

### Example

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

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

**snmp-server contact**  **contact-name**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>contact</strong></td>
<td>Identifies the contact person for this managed node. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>contact-name</strong></td>
<td>String that describes the system contact information of the node. Supports up to 255 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Command Default**  
No default behavior or values.

**Command Modes**  
Configuration (config)#

**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>location</td>
<td>Configures the physical location of this managed node. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td>location</td>
<td>String that describes the physical location information of the system. Supports up to 255 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Configuration (config)#

**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>value</th>
<th>Number that represents the percentage of available disk space. The value ranges from 1 to 100.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>No default behavior or values.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Configuration (config)#</th>
</tr>
</thead>
</table>

| 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 cron 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>engineid</code></td>
<td>Changes an existing engine ID to a new value that you specify.</td>
</tr>
<tr>
<td><code>engine_ID_string</code></td>
<td>String of maximum 24 characters that identifies the engine ID.</td>
</tr>
</tbody>
</table>

### Command Default

No command defaults.

### Command Modes

Configuration (config)#

### 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)#
```
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>username</code></td>
<td>Only one word for the username argument. Blank spaces and quotation marks (&quot;&quot;&quot;) are not allowed. Supports up to 31 alphanumeric characters.</td>
</tr>
<tr>
<td><code>password</code></td>
<td>Specifies password.</td>
</tr>
<tr>
<td><code>password</code></td>
<td>Password character length up to 40 alphanumeric characters. You must specify the password for all new users.</td>
</tr>
<tr>
<td>`hash</td>
<td>plain`</td>
</tr>
<tr>
<td>`role admin</td>
<td>user`</td>
</tr>
<tr>
<td><code>disabled</code></td>
<td>Disables the user according to the user’s email address.</td>
</tr>
<tr>
<td><code>email</code></td>
<td>Sets user’s email address.</td>
</tr>
<tr>
<td><code>email-address</code></td>
<td>Specifies the user’s email address. For example, <a href="mailto:user1@mydomain.com">user1@mydomain.com</a>.</td>
</tr>
</tbody>
</table>

**Command Default**

The initial user during setup.

**Command Modes**

Configuration (config)#

**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)#
### synflood_limited

To configure a TCP SYN packet rate limit.

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>synflood-limit</td>
<td>Average number of TCP SYN packets per second allowed</td>
</tr>
<tr>
<td>?</td>
<td>1-2147483647 (Range for TCP SYN packets).</td>
</tr>
</tbody>
</table>

#### Command Default

No default behavior or values.

#### Command Modes

Configuration (config)#

#### Usage Guidelines

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

#### Example 1

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