



Cisco Identity Services Engine CLI Reference Guide, Release 2.3

First Published: 2017-07-28

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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 NON-INFRINGEMENT 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 OR 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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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)

© 2017 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Cisco ISE Command-Line Interface 1

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

CHAPTER 2

Cisco ISE CLI Commands in EXEC Mode 7

- Cisco ISE CLI Session Begins in EXEC Mode 8
 - application install 8
 - application configure 9
 - Monitoring Database Settings 10
 - Live Statistics of Profiling Events 13
 - Export and Import Internal CA Store 14
 - Create Missing Indexes 16
 - Enable ACS Migration 17
 - Key Performance Metrics Statistical Data 18
 - Counter Attribute Collection 18
 - Wireless Setup 19
- application remove 21
- application reset-config 22
- application reset-passwd 23
- application start 24

| | |
|------------------------------------------------------|----|
| application stop | 27 |
| application upgrade | 28 |
| backup | 31 |
| Backing up Cisco ISE Configuration Data | 33 |
| Backing up Cisco ISE Operational Data | 33 |
| backup-logs | 33 |
| clear screen | 35 |
| clock | 35 |
| cls | 37 |
| configure | 38 |
| copy | 38 |
| Running Configuration | 40 |
| Copying Running Configuration to a Remote Location | 41 |
| Copying Running Configuration from a Remote Location | 41 |
| Startup configuration | 41 |
| Copying Startup Configuration to a Remote Location | 42 |
| Copying Startup Configuration from a Remote Location | 42 |
| Copying Log files | 42 |
| crypto | 43 |
| debug | 45 |
| delete | 49 |
| dir | 50 |
| esr | 51 |
| exit | 52 |
| forceout | 52 |
| halt | 53 |
| help | 53 |
| licence esr | 54 |
| mkdir | 55 |
| nslookup | 55 |
| password | 57 |
| patch install | 57 |
| patch remove | 59 |
| ping | 60 |

| | |
|------------------------------------------------------------------------------|----|
| ping6 | 61 |
| reload | 62 |
| reset-config | 63 |
| restore | 64 |
| Restoring Cisco ISE Configuration Data from the Backup | 65 |
| Restoring Cisco ISE Operational Data from the Backup | 67 |
| Restoring Cisco ISE Configuration Data and Cisco ADE OS data from the Backup | 68 |
| rmdir | 68 |
| ssh | 69 |
| tech | 70 |
| terminal length | 72 |
| terminal session-timeout | 73 |
| terminal session-welcome | 74 |
| terminal terminal-type | 74 |
| traceroute | 75 |
| undebug | 75 |
| which | 78 |
| write | 79 |

CHAPTER 3

Cisco ISE CLI Commands in EXEC Show Mode 81

| | |
|------------------|-----|
| show | 82 |
| show application | 82 |
| show backup | 85 |
| show banner | 86 |
| show cdp | 86 |
| show clock | 87 |
| show container | 88 |
| show cpu | 92 |
| show crypto | 94 |
| show disks | 94 |
| show icmp-status | 96 |
| show interface | 97 |
| show inventory | 99 |
| show ip | 100 |

| | |
|---------------------|-----|
| show ipv6 route | 100 |
| show logging | 101 |
| show logins | 103 |
| show memory | 104 |
| show ntp | 105 |
| show ports | 105 |
| show process | 107 |
| show repository | 108 |
| show restore | 109 |
| show running-config | 110 |
| show snmp engineid | 111 |
| show snmp user | 112 |
| show startup-config | 112 |
| show tech-support | 113 |
| show terminal | 115 |
| show timezone | 116 |
| show timezones | 116 |
| show udi | 117 |
| show uptime | 118 |
| show users | 119 |
| show version | 120 |

CHAPTER 4

| | |
|-----------------------------------------------------|------------|
| Cisco ISE CLI Commands in Configuration Mode | 123 |
| Switch to Configuration Mode in EXEC Mode | 124 |
| Configuring Cisco ISE in the Configuration Mode | 125 |
| Configuring Cisco ISE in the Configuration Submode | 126 |
| CLI Configuration Command Default Settings | 126 |
| backup interface | 126 |
| cdp holdtime | 129 |
| cdp run | 130 |
| cdp timer | 131 |
| clear screen | 132 |
| clock timezone | 132 |
| Changing the Time Zone on Cisco ISE Nodes | 133 |

| | |
|--------------------------------------------------------|-----|
| Common Time Zones | 134 |
| Australia Time Zones | 135 |
| Asia Time Zones | 135 |
| cls | 136 |
| conn-limit | 136 |
| do | 137 |
| end | 140 |
| exit | 141 |
| hostname | 141 |
| icmp echo | 143 |
| interface | 143 |
| ip address | 145 |
| ip default-gateway | 146 |
| ip domain-name | 146 |
| ip host | 147 |
| ip name-server | 149 |
| ip route | 151 |
| ipv6 address | 152 |
| ipv6 address autoconfig | 154 |
| Configuring IPv6 Auto Configuration | 154 |
| Verifying the Privacy Extensions Feature | 155 |
| ipv6 address dhcp | 156 |
| ipv6 enable | 157 |
| ipv6 route | 158 |
| kron occurrence | 159 |
| kron policy-list | 161 |
| logging | 162 |
| max-ssh-sessions | 163 |
| ntp | 164 |
| ntp authenticate | 165 |
| ntp authentication-key | 166 |
| ntp server | 167 |
| Configuring Trusted Keys for NTP Server Authentication | 169 |
| Verifying the Status of Synchronization | 169 |

| | |
|-------------------------------------|-----|
| ntp trusted-key | 170 |
| rate-limit | 171 |
| password-policy | 172 |
| repository | 173 |
| service | 175 |
| shutdown | 177 |
| snmp-server enable | 178 |
| snmp-server user | 178 |
| snmp-server host | 180 |
| snmp-server community | 181 |
| snmp-server contact | 183 |
| snmp-server location | 183 |
| snmp-server trap diskThresholdLimit | 184 |
| snmp engineid | 185 |
| synflood-limit | 185 |
| username | 186 |
| which | 187 |



CHAPTER 1

Cisco ISE Command-Line Interface



Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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 1](#)
- [Cisco ISE CLI Administrator Account, on page 3](#)
- [Cisco ISE CLI User Accounts, on page 3](#)
- [Cisco ISE CLI User Account Privileges, on page 3](#)
- [Supported Hardware and Software Platforms for Cisco ISE CLI, on page 4](#)

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 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.

Step 1 Log into the Cisco ISE CLI using the CLI administrator account.

Step 2 Enter into configuration mode and run the **username** command.

```
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#
```

Step 3 Log into the Cisco ISE CLI using the CLI user account.

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`. Terminfo 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



CHAPTER 2

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 8](#)
- [application install, on page 8](#)
- [application configure, on page 9](#)
- [application remove, on page 21](#)
- [application reset-config, on page 22](#)
- [application reset-passwd, on page 23](#)
- [application start, on page 24](#)
- [application stop, on page 27](#)
- [application upgrade, on page 28](#)
- [backup, on page 31](#)
- [backup-logs, on page 33](#)
- [clear screen, on page 35](#)
- [clock, on page 35](#)
- [cls, on page 37](#)
- [configure, on page 38](#)
- [copy, on page 38](#)
- [crypto, on page 43](#)
- [debug, on page 45](#)
- [delete, on page 49](#)
- [dir, on page 50](#)
- [esr, on page 51](#)
- [exit, on page 52](#)
- [forceout, on page 52](#)
- [halt, on page 53](#)
- [help, on page 53](#)
- [licence esr, on page 54](#)
- [mkdir, on page 55](#)
- [nslookup, on page 55](#)
- [password, on page 57](#)
- [patch install, on page 57](#)

- [patch remove](#), on page 59
- [ping](#), on page 60
- [ping6](#), on page 61
- [reload](#), on page 62
- [reset-config](#), on page 63
- [restore](#), on page 64
- [rmdir](#), on page 68
- [ssh](#), on page 69
- [tech](#), on page 70
- [terminal length](#), on page 72
- [terminal session-timeout](#), on page 73
- [terminal session-welcome](#), on page 74
- [terminal terminal-type](#), on page 74
- [traceroute](#), on page 75
- [undebug](#), on page 75
- [which](#), on page 78
- [write](#), on page 79

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.

application install



Note

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. |
| <i>application-bundle</i> | Application bundle filename. Supports up to 255 alphanumeric characters. |
| <i>remote-repository-name</i> | Remote repository name. Supports up to 255 alphanumeric characters. |

Command Default

No default behavior or values.

| | |
|----------------------|------|
| Command Modes | EXEC |
|----------------------|------|

| | | |
|------------------------|----------------|---------------------|
| Command History | Release | Modification |
|------------------------|----------------|---------------------|

| | | |
|--|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |
|--|-----------|------------------------------|

| | |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| 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 | configure | Configures a specific application. |
| | <i>application-name</i> | Application name. Supports up to 255 alphanumeric characters. |

Command Default No default behavior or values.

Command Modes EXEC

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[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 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
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[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
```

```
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.

```

5
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
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[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

6

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
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[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

7
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 OSCP Responder Certificate - ise60
  Issuer:CN=Certificate Services Root CA - ise60
```

```
Serial#:0xad3ccdf-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
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[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 OSCP Responder Certificate - ise60
Issuer:CN=Certificate Services Root CA - ise60
Serial#:0xad3ccdf-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
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[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
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
```



```
[11]Enable/Disable ACS Migration
[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 MnT indexes.
Are you sure you want to proceed? y/n [n]: y
Starting to create missing MnT indexes
Completed creating missing MnT 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
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[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

11
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
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[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
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[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 the 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
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[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
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[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.

```
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
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[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 Wifisetup
Stopping container wifisetup-container
wifisetup-container
Untagged: wifisetup:0.0.15
Deleted: dff12613ae85e7a4689f48c12b05b4d3cf597f3f2ca58e942de468e8ca75bf3c
Deleted: 95fb5a455840ef26a745846736536877939e4c666751116928346d5d3e758db3
Deleted: fc3f8168728e933f353adfed0a45114682fcab3d2add7549f1855a1f7cf56451
Deleted: 4cdca485c0858f964de66979c2df213832e64af92fb6ddf923c84f668f041036
Deleted: f2a5326a7f662739242bf2581eedale41d407f92054b947187bfe01e8e0d0710

```

application remove



Note 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. |
| | <i>application-name</i> | Application name. Supports up to 255 alphanumeric characters. |
| | | Removes or uninstalls an application. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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 | reset-config | Resets the Cisco ISE application configuration and clears the Cisco ISE database. |
| | <i>application-name</i> | Name of the application configuration you want to reset. Supports up to 255 alphanumeric characters. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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...
```

```

Please rejoin to AD domains from the administrative GUI
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. |
| | <i>application-name</i> | 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

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

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

| | | | | | | | |
|---|---|---|----|---|---|---|---|
| ~ | ! | @ | \$ | & | * | - | _ |
| + | = | \ | " | , | ; | < | > |

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 | start | Enables an application bundle. |
| | <i>application-name</i> | Name of the predefined application that you want to enable. Supports up to 255 alphanumeric characters. |

| | |
|-------------|-------------------------------------|
| <i>safe</i> | Starts an application in safe mode. |
|-------------|-------------------------------------|

| | |
|------------------------|--------------------------------|
| Command Default | No default behavior or values. |
|------------------------|--------------------------------|

| | |
|----------------------|------|
| Command Modes | EXEC |
|----------------------|------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

Usage Guidelines

Enables an application.

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 *isesafe*** 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 |
|-------------------------------|---------|--------------|
| Database Listener | running | 17893 |
| Database Server | running | 62 PROCESSES |
| Application Server | running | 21962 |
| Profiler Database | running | 19443 |
| ISE Indexing Engine | running | 23331 |
| AD Connector | running | 24955 |
| M&T Session Database | running | 19351 |
| M&T Log Collector | running | 22096 |
| M&T Log Processor | running | 22010 |
| Certificate Authority Service | running | 24759 |
| EST Service | running | 891 |

| | | |
|-------------------------------------|----------|-------|
| SXP Engine Service | disabled | |
| Docker Daemon | running | 24000 |
| TC-NAC Service | disabled | |
| Wifi Setup Helper Container | running | 24465 |
| Wifi Setup Helper Vault | running | 41 |
| Wifi Setup Helper MongoDB | running | 14 |
| Wifi Setup Helper Web Server | running | 213 |
| Wifi Setup Helper Auth Service | running | 123 |
| Wifi Setup Helper Main Service | running | 159 |
| Wifi Setup Helper WLC Service | running | 197 |
| pxGrid Infrastructure Service | disabled | |
| pxGrid Publisher Subscriber Service | disabled | |
| pxGrid Connection Manager | disabled | |
| pxGrid Controller | disabled | |
| PassiveID WMI Service | disabled | |
| PassiveID Syslog Service | disabled | |
| PassiveID API Service | disabled | |
| PassiveID Agent Service | disabled | |
| PassiveID Endpoint Service | disabled | |
| PassiveID SPAN Service | disabled | |
| DHCP Server (dhcpcd) | disabled | |
| DNS Server (named) | disabled | |

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.



Note

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 Sxp Engine Service is disabled
Stopping TC-NAC Service ...
Error response from daemon: no such id: irf-core-engine-runtimeirf-core-engine-runtime is
not running
Error response from daemon: no such id: irf-rabbitmq-runtimeirf-rabbitmq-runtime is not
running
Error response from daemon: no such id: irf-mongo-runtimeirf-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 ...
38a408c9alc8
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 | stop | Disables an application. |
| | <i>application-name</i> | Name of the predefined application that you want to disable. Supports up to 255 alphanumeric characters. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

| Usage Guidelines | <p>Disables an application.</p> <p>If you have auto-failover configuration enabled in your deployment, you receive the following warning message:</p> <pre>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)?</pre> <p>Type 'y' if you want to continue or 'n' if you want to cancel.</p> |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

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.

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

| Syntax Description | upgrade | Upgrades a specific application bundle in the remote repository. |
|--------------------|---------|------------------------------------------------------------------|
|--------------------|---------|------------------------------------------------------------------|

| | |
|-------------------------------|------------------------------------------------------------------------------------------------------------|
| <i>application-bundle</i> | Application name. Supports up to 255 alphanumeric characters. |
| <i>remote-repository-name</i> | Remote repository name. Supports up to 255 alphanumeric characters. |
| cleanup | Cleans previously prepared upgrade bundle and prepares a new upgrade bundle. |
| prepare | Downloads an upgrade bundle and unzip contents to the local disk to prepare an application for an upgrade. |
| <i>application-bundle</i> | Application name. Supports up to 255 alphanumeric characters. |
| proceed | Proceeds with an upgrade using the local file. |

Command Default No default behavior or values.

Command Modes EXEC

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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.

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

| | |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <i>backup-name</i> | Name of backup file. Supports up to 100 alphanumeric characters. |
| repository | Specifies repository to store the back up file. |
| <i>repository-name</i> | Location where the files should be backed up to. Supports up to 80 alphanumeric characters. |
| ise-config | Backs up Cisco ISE configuration data (includes Cisco ISE ADE-OS). |
| ise-operational | Backs up Cisco ISE operational data. |
| encryption-key | Specifies user-defined encryption key to protect the backup. |
| hash | Specifies (Hashed encryption key for protection of backup) an encrypted (hashed) encryption key that follows. Supports up to 40 characters. |

| | |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| plain | Specifies (Plaintext encryption key for protection of backup) an unencrypted plaintext encryption key that follows. Supports up to 15 characters. |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------|

| | |
|----------------------------|------------------------------------------------------|
| <i>encryption-key name</i> | An encryption key in hash plain format for backup. |
|----------------------------|------------------------------------------------------|

| | |
|------------------------|--------------------------------|
| Command Default | No default behavior or values. |
|------------------------|--------------------------------|

| | |
|----------------------|------|
| Command Modes | EXEC |
|----------------------|------|

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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-keyplainlablab12

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 plainlablab12

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 | <i>backup-name</i> | Name of one or more files to back up. Supports up to 100 alphanumeric characters. |
| | repository | Repository command. |
| | <i>repository-name</i> | 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. |
| | <i>encryption-key name</i> | The encryption key in hash or plain format. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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

```

clear screen

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

clear screen**Syntax Description**

This command has no keywords and arguments.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History**Release****Modification**

2.0.0.306

This command was introduced.

Usage Guidelines

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

Example

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

```

ise/admin# clear screen
ise/admin#

```

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:min:ss* | *yyyy*}]

Syntax Description

set

Sets the system clock.

| | |
|-----------------|--------------------------------------------------------------------------------------------------------------|
| <i>month</i> | Current month of the year by name. Supports up to three alphabetic characters. For example, Jan for January. |
| <i>day</i> | Current day (by date) of the month. Value = 0 to 31. Supports up to two numbers. |
| <i>hh:mm:ss</i> | Current time in hours (24-hour format), minutes, and seconds. |
| <i>yyyy</i> | Current year (no abbreviation). |

Command Default No default behavior or values.

Command Modes EXEC

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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



Note

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



Note

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#
```

cls

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

cls

| | | |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Syntax Description | This command has no keywords and arguments. | |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | cls is a hidden command. Although cls is available in Cisco ISE, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. | |

Example

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

```
ise/admin# cls
ise/admin#
```

configure

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

configure terminal

| | | |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| Syntax Description | terminal | Executes configuration commands from the terminal. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | <p>Use this command to enter in to configuration mode. Note that commands in this mode write to the running configuration file as soon as you enter them.</p> <p>To exit configuration mode and return to EXEC mode, enter end, exit, or Ctrl-z.</p> <p>To view the changes made to the configuration, use the show running-config command in EXEC mode.</p> <p>If the replace option is used with this command, copies a remote configuration to the system, which overwrites the existing configuration.</p> | |

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.



Note

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 42](#) for more information.

| | | |
|---------------------------|-----------------------|----------------------------------------------------|
| Syntax Description | running-config | Represents the current running configuration file. |
|---------------------------|-----------------------|----------------------------------------------------|

| | |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| startup-config | Represents the configuration file used during initialization (startup). |
| <i>protocol</i> | Destination for copying. See Table 2-1 for protocol keyword options. |
| <i>hostname</i> | Hostname of destination. |
| <i>location</i> | Location of destination. Represents the current running configuration file. |
| logs | The system log files. |
| all | 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. |
| filename | 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. |
| <i>log_filename</i> | Name of the Cisco ISE log file, as displayed by the show logs command (up to 255 characters). |
| mgmt | 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. |
| runtime | 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. |

Command Default No default behavior or values.

Command Modes EXEC

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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)

| Keyword | Source of Destination |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| ftp | Source or destination URL for FTP network server. The syntax for this alias: ftp:[[/username [:password]@]location]/directory]/filename |
| sftp | Source or destination URL for an SFTP network server. The syntax for this alias: sftp:[[/location]/directory]/filename |
| tftp | Source or destination URL for a TFTP network server. The syntax for this alias: tftp:[[/location]/directory]/filename |

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:/

  70 May 20 2016 00:57:28  1
4096 May 20 2016 06:34:49  corefiles/
   0 May 20 2016 00:57:28  err.out
4096 May 20 2016 00:57:28  lost+found/
```

```
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 | | |
|------------------------|--|------------------------------------------------------------------------------------|
| key | | Allows you to perform crypto key operations. |
| delete | | Deletes a public/private key pair. |
| <i>hash</i> | | Hash value. Supports up to 80 characters. |
| <i>authorized_keys</i> | | Deletes authorized keys. |
| <i>rsa</i> | | Deletes an RSA key pair. |
| export | | Exports a public/private key pair to repository. |
| <i>filename</i> | | The filename to which the public key is exported to. Supports up to 80 characters. |
| <i>repository</i> | | The repository to which the public key is exported to. |
| generate | | Generates a public/private key pair. |
| <i>rsa</i> | | Generates an RSA key pair. |
| import | | Imports a public/private key pair. |
| <i>filename</i> | | The filename to which the public key is imported. Supports up to 80 characters. |
| <i>repository</i> | | The repository to which the public key is imported. |
| host_key | | Allows you to perform crypto host-key operations. |
| add | | Adds trusted host keys. |
| host | | Specifies hostname. |
| delete | | Deletes trusted host keys. |

| | |
|---------------------------|-------------------------------------------------------|
| ntp_import_autokey | Imports the public key generated from the NTP server. |
| <i>ntpkey</i> | Public key generated from the NTP server. |

Command Default No default behavior or values.

Command Modes EXEC

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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
admin public key: ssh-rsa ad:14:85:70:fa:c3:c1:e6:a9:ff:b1:b0:21:a5:28:94 admin@ise
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
admin public key: ssh-rsa 41:ab:78:26:48:d3:f1:6f:45:0d:99:d7:0f:50:9f:72 admin@ise
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# crypto key delete f8:7f:8a:79:44:b8:5d:5f:af:e1:63:b2:be:7a:fd:d4
ise/admin#
ise/admin# crypto key delete rsa
ise/admin# show crypto key
ise/admin#
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
2048 1d:72:73:6e:ad:f7:2d:11:ac:23:e7:8c:81:32:c5:ea ise (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.

debug [**all** | **application** | **backup-restore** | **cdp** | **config** | **copy** | **icmp** | **locks** | **logging** | **snmp** | **system** | **transfer** | **user** | **utils**]

| Syntax Description | | |
|--------------------|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all | | Enables all debugging. |
| application | | Enables debugging application related errors or events. <ul style="list-style-type: none"> • all—Enables all application debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • install—Enables application install debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • operation—Enables application operation debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • uninstall—Enables application uninstall debug output. Set level between 0 and 7, with 0 being severe and 7 being all. |

backup-restore

Enables debugging back up and restore related errors or events.

- **all**—Enables all debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.
- **backup**—Enables backup debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.
- **backup-logs**—Enables backup-logs debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.
- **history**—Enables history debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.
- **restore**—Enables restore debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.

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 | <p>Enables debugging the Cisco ISE configuration related errors or events.</p> <ul style="list-style-type: none"> • 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 | <p>Enables debugging copy commands. Set level between 0 and 7, with 0 being severe and 7 being all.</p> |
| icmp | <p>Enables debugging Internet Control Message Protocol (ICMP) echo response configuration related errors or events.</p> <p>all—Enable all debug output for ICMP echo response configuration. Set level between 0 and 7, with 0 being severe and 7 being all.</p> |
| locks | <p>Enables debugging resource locking related errors or events.</p> <ul style="list-style-type: none"> • 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 | <p>Enables debugging logging configuration related errors or events.</p> <p>all—Enables all logging configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</p> |
| snmp | <p>Enables debugging SNMP configuration related errors or events.</p> <p>all—Enables all SNMP configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</p> |
| system | <p>Enables debugging Cisco ISE system related errors and events.</p> <ul style="list-style-type: none"> 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. |
| transfer | <p>Enables debugging file transfer. Set level between 0 and 7, with 0 being severe and 7 being all.</p> |
| user | <p>Enables debugging user management.</p> <ul style="list-style-type: none"> all—Enables all user management debug output. Set level between 0 and 7, with 0 being severe and 7 being all. password-policy—Enables user management debug output for password-policy. Set level between 0 and 7, with 0 being severe and 7 being all. |
| utils | <p>Enables debugging utilities configuration related errors and events.</p> <p>all—Enables all utilities configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</p> |

| | |
|------------------------|--------------------------------|
| Command Default | No default behavior or values. |
|------------------------|--------------------------------|

| | |
|----------------------|------|
| Command Modes | EXEC |
|----------------------|------|

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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

Example

```
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*]

| | | |
|---------------------------|-------------------|------------------------------------------------------|
| Syntax Description | <i>filename</i> | Filename. Supports up to 80 alphanumeric characters. |
| | <i>disk:/path</i> | Location of the file in the repository. |

| | |
|------------------------|--------------------------------|
| Command Default | No default behavior or values. |
|------------------------|--------------------------------|

| | |
|----------------------|------|
| Command Modes | EXEC |
|----------------------|------|

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

| | |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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#
```

dir

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 | <i>directory-name</i> | Directory name. Supports up to 80 alphanumeric characters. Requires disk:/ preceding the directory name. |
| | recursive | (Optional). Lists directories and files in the local file system. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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/
2996022 Aug 05 2010 19:11:16 mybackup-100805-1910.tar.gz
   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/
2996022 Aug 05 2010 19:11:16 mybackup-100805-1910.tar.gz
   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#

```

esr

To enter the Embedded Services Router console, use the **esr** command in EXEC mode.

esr

| | | |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Syntax Description | This command has no keywords and arguments. | |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.2.0.470 | This command was introduced. |
| Usage Guidelines | The C5921 ESR software is bundled with Cisco ISE, Releases 2.2 and later. You need an ESR license to enable it. See Cisco 5921 Embedded Services Router Integration Guide for ESR licensing information. | |

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 |
|----------------------|------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

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 | <i>username</i> | Name of the user. Supports up to 31 alphanumeric characters. |
|---------------------------|-----------------|--------------------------------------------------------------|

| | |
|------------------------|--------------------------------|
| Command Default | No default behavior or values. |
|------------------------|--------------------------------|

| | |
|----------------------|------|
| Command Modes | EXEC |
|----------------------|------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

| | |
|-------------------------|--------------------------------------------------------------------------------------|
| 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

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

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).

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

| Usage Guidelines | <p>The help command provides a brief description of the context-sensitive help system.</p> <ul style="list-style-type: none"> • 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#
```

licence esr

To perform esr licence operation, use the **licence esr** command in EXEC mode.

license esr { **classic** | **smart** }

| | | |
|--------------------|--------------------------------|--------------------------------|
| Syntax Description | classic | Enables ESR classic licensing. |
| | smart | Enables ESR smart licensing. |
| | | |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.2.0.470 | This command was introduced. |

Usage Guidelines

The C5921 ESR software is bundled with Cisco ISE, Releases 2.2 and later. You need an ESR license to enable it. See [Cisco 5921 Embedded Services Router Integration Guide](#) for ESR licensing information.

mkdir

To create a new directory in the Cisco ISE server, use the **mkdir** command in EXEC mode.

mkdir *directory-name*

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

Command History

Release

Modification

2.0.0.306

This command was introduced.

Usage Guidelines

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

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#
```

nslookup

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

nslookup {*ip-address* |*hostname*}

nslookup [{*ip-address* |*hostname*} **name-server** {*ip-address* }]

nslookup [{*ip-address* |*hostname*} **querytype AAAA**]

| | | |
|---------------------------|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>ip-address</i> | IPv4 or IPv6 address of a remote system. Supports up to 64 alphanumeric characters. |
| | <i>hostname</i> | Hostname of a remote system. Supports up to 64 alphanumeric characters. |
| | AAAA | Queries the Internet domain name server for an IPv6 address that corresponds to a website name. |
| | name-server | Specifies an alternative name server. Supports up to 64 alphanumeric characters. |
| | querytype | 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. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

Example 1

```
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#
```

Example 2

```
ise/admin# nslookup ipv6.google.com querytype AAAA
Server:      10.106.230.244
Address:     10.106.230.244#53
Non-authoritative answer:
ipv6.google.com canonical name = ipv6.l.google.com.
ipv6.l.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.
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.

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:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200568-ISE-Password-Recovery-Mechanisms.html>

Syntax Description

| | |
|----------------------|---------------------------------|
| Enter old password | Enter the current CLI password. |
| Enter new password | Enter the new CLI password. |
| Confirm new password | Confirm the new CLI password. |

Command Modes

EXEC

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Example

```
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.

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

| | |
|----------------|------------------------------------------------------|
| install | Installs a specific patch bundle of the application. |
|----------------|------------------------------------------------------|

| | |
|---------------------|-------------------------------------------------------------------------|
| <i>patch-bundle</i> | The patch bundle file name. Supports up to 255 alphanumeric characters. |
|---------------------|-------------------------------------------------------------------------|

| | |
|-------------------|--------------------------------------------------------------------------------------------------|
| repository | Installs the patch in the specified repository name. Supports up to 255 alphanumeric characters. |
|-------------------|--------------------------------------------------------------------------------------------------|

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

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

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.

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.

Syntax Description

| | |
|-------------------------|---------------------------------------------------------------------------------------------------------------|
| remove | The command that removes a specific patch bundle version of the application. |
| <i>application_name</i> | The name of the application for which the patch is to be removed. Supports up to 255 alphanumeric characters. |
| <i>version</i> | The patch version number to be removed. Supports up to 255 alphanumeric characters. |

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.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage Guidelines

If you attempt to remove a patch that is not installed, then you receive the following error message:

```
% 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#
```

ping

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 | <i>ip-address</i> | IP address of the system to ping. Supports up to 32 alphanumeric characters. |
| | <i>hostname</i> | Hostname of the system to ping. Supports up to 32 alphanumeric characters. |
| | df | (Optional). Specification for packet fragmentation. |
| | <i>df</i> | Specify the value as 1 to prohibit packet fragmentation, or 2 to fragment the packets locally, or 3 to not set df. |
| | packetsize | (Optional). Size of the ping packet. |
| | <i>packetsize</i> | Specify the size of the ping packet; the value can be between 0 and 65507. |
| | pingcount | (Optional). Number of ping echo requests. |
| | <i>pingcount</i> | Specify the number of ping echo requests; the value can be between 1 and 10. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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*}]

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

Command Default No default behavior or values.

Command Modes EXEC

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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
PING 3ffe:302:11:2:20c:29ff:feaf:da05 (3ffe:302:11:2:20c:29ff:feaf:da05) from
3ffe:302:11:2:20c:29ff:feaf:da05 eth0: 56 data bytes
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
--- 3ffe:302:11:2:20c:29ff:feaf:da05 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3118ms
rat min./aft/max/endive = 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
PING 3ffe:302:11:2:20c:29ff:feaf:da05 (3ffe:302:11:2:20c:29ff:feaf:da05) from
3ffe:302:11:2:20c:29ff:feaf:da05 eth0: 10 data bytes
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
--- 3ffe:302:11:2:20c:29ff:feaf:da05 ping statistics ---
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

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

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 cancel.

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

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.2.0.470 | This command was introduced. |

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 | | |
|----------------------------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>filename</i> | | Name of the backed-up file that resides in the repository. Supports up to 120 alphanumeric characters. Note You must add the .tar.gpg extension after the filename (for example, myfile.tar.gpg). |
| repository | | The repository command. |
| <i>repository-name</i> | | Name of the repository from which you want to restore the backup. Supports up to 120 characters. |
| encryption-key | | (Optional). Specifies user-defined encryption key to restore backup. |
| hash | | Hashed encryption key for restoring backup. Specifies an encrypted (hashed) encryption key that follows. Supports up to 40 characters. |
| plain | | Plaintext encryption key for restoring backup. Specifies an unencrypted plaintext encryption key that follows. Supports up to 15 characters. |
| <i>encryption-key-name</i> | | Specifies encryption key in hash plain format. |

include-adeos

Restores back up and reboots Cisco ISE, if ADE-OS configuration data is present in the backup

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

Command History**Release****Modification**

2.0.0.306

This command was introduced.

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: Retrieving backup file from Repository...20% completed
% restore in progress: Decrypting backup data...25% completed
% restore in progress: Extracting backup data...30% completed
Leaving the currently connected AD domain
Please rejoin the AD domain from the administrative GUI
% restore in progress: Stopping ISE processes required for restore...35% completed
```

Restoring Cisco ISE Configuration Data from the Backup

```
% restore in progress: Restoring ISE configuration database...40% completed
% 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 2 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, OcapServiceUpgradeRegistration(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, AuthzUpgradeService(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...
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 plain lablab12
% 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#

```

rmmdir

To remove an existing directory, use the **rmmdir** command in EXEC mode.

rmmdir *directory-name*

| | | |
|---------------------------|--------------------------------|------------------------------------------------------------|
| Syntax Description | <i>directory-name</i> | Directory name. Supports up to 80 alphanumeric characters. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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.



Note 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 | | |
|--------------------|-------------------|-------------------------------------------------------------------------------|
| | <i>ip-address</i> | IPv4 address of the remote system. Supports up to 64 alphanumeric characters. |
| | <i>hostname</i> | Hostname of the remote system. Supports up to 64 alphanumeric characters. |
| | <i>username</i> | Username of the user logging in through SSH. |
| | port | (Optional). Indicates the port number of the remote host. |

| | |
|-----------------------|-------------------------------------------------------------------------------|
| <i>port number</i> | The valid range of ports is from 0 to 65,535. The default port is 22. |
| version | (Optional). Indicates the version number. |
| <i>version number</i> | 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. |
| <i>ip-address</i> | IPv4 address of the remote system. Supports up to 64 alphanumeric characters. |
| <i>hostname</i> | Hostname of the remote system. Supports up to 64 alphanumeric characters. |

Command Default Disabled.

Command Modes EXEC

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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#
```

tech

To dump traffic on a selected network interface, use the **tech** command in EXEC mode.

tech dumptcp {*interface-number* | *count* | *package-count*}

| Syntax Description | dumptcp | Dumps TCP package to the console. |
|---------------------------|----------------|-----------------------------------|
| | | |

| | |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>interface-number</i> | Gigabit Ethernet interface number (0 to 3). |
| <i>count</i> | Specifies a maximum package count, and default is continuous (no limit). |
| <i>package-count</i> | Supports 1–10000. |
| iostat | Dumps Central Processing Unit (CPU) statistics and input/output statistics for devices and partitions to the console for every 3 seconds. See Linux <code>iostat</code> command. |
| iostat | Provides accurate I/O usage per process on ISE node. |
| mpstat | Dumps processors related information sent to the console. See Linux <code>mpstat</code> command. |
| netstat | Dumps network related information sent to the console for every 3 seconds. See Linux <code>netstat</code> command. |
| top | 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. |
| support-tunnel | 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. |
| vmstat | Dumps summary information of memory, processes, and paging for every 3 seconds. See Linux <code>vmstat</code> command. |

Command Default Disabled.

Command Modes EXEC

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

Usage Guidelines If you see *bad UDP cksum* warnings in the `tech dumptcp` output, it may not be a cause for concern. The **tech dumptcp** 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 cksum*.

Example 1

```
ise/admin# tech dumptcp 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 63344
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
 12096
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*

Syntax Description

length

Sets the number of lines on the current terminal screen for the current session.

| | |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <i>integer</i> | Number of lines on the screen. Contains between 0 to 511 lines, inclusive. A value of zero (0) disables pausing between screens of output. |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|

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

Command Modes EXEC

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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 | session-timeout | Sets the inactivity timeout for all sessions. |
|---------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------|
| | <i>minutes</i> | Number of minutes for the inactivity timeout. The valid range is from 0 to 525,600. Zero (0) disables the timeout. |

Command Default The default session-timeout is 30 minutes.

Command Modes EXEC

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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 | session-welcome | Sets a welcome message on the system for all users who log in to the system. |
| | <i>string</i> | Welcome message. Supports up to 2023 alphanumeric characters. XML reserved characters are not allowed. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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*

| | | |
|---------------------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | terminal-type | Specifies the type of terminal connected. The default terminal type is VT100. |
| | <i>type</i> | Defines the terminal name and type, and permits terminal negotiation by hosts that provide that type of service. Supports up to 80 alphanumeric characters. |
| Command Default | VT100 | |
| Command Modes | EXEC | |

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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 | <i>ip-address</i> | IPv4 address of the remote system. Supports up to 64 alphanumeric characters. |
|--------------------|-------------------|-------------------------------------------------------------------------------|
| | <i>hostname</i> | Hostname of the remote system. Supports up to 64 alphanumeric characters. |

Command Default No default behavior or values.

Command Modes EXEC

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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.

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

| Syntax Description | all | Disables all debugging. |
|--------------------|------------|-------------------------|
|--------------------|------------|-------------------------|

| | |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| application | <p>Application files.</p> <ul style="list-style-type: none"> • all—Disables all application debug output. • install—Disables application install debug output. • operation—Disables application operation debug output. • uninstall—Disables application uninstall debug output. |
| backup-restore | <p>Backs up and restores files.</p> <ul style="list-style-type: none"> • all—Disables all debug output for backup-restore. • backup—Disables backup debug output for backup-restore. • backup-logs—Disables backup-logs debug output for backup-restore. • history—Disables history debug output for backup-restore. • restore—Disables restore debug output for backup-restore. |
| cdp | <p>Cisco Discovery Protocol configuration files.</p> <ul style="list-style-type: none"> • all—Disables all Cisco Discovery Protocol configuration debug output. • config—Disables configuration debug output for Cisco Discovery Protocol. • infra—Disables infrastructure debug output for Cisco Discovery Protocol. |

| | |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| config | <p>Configuration files.</p> <ul style="list-style-type: none"> • all—Disables all configuration debug output. • backup—Disables backup configuration debug output. • clock—Disables clock configuration debug output. • infra—Disables configuration infrastructure debug output. • kron—Disables command scheduler configuration debug output. • network—Disables network configuration debug output. • repository—Disables repository configuration debug output. • service—Disables service configuration debug output. |
| copy | Copy commands. |
| icmp | <p>ICMP echo response configuration.</p> <p>all—Disable all debug output for ICMP echo response configuration. Set level between 0 and 7, with 0 being severe and 7 being all.</p> |
| locks | <p>Resource locking.</p> <ul style="list-style-type: none"> • all—Disables all resource locking debug output. • file—Disables file locking debug output. |
| logging | <p>Logging configuration files.</p> <p>all—Disables all debug output for logging configuration.</p> |
| snmp | <p>SNMP configuration files.</p> <p>all—Disables all debug output for SNMP configuration.</p> |
| system | <p>System files.</p> <ul style="list-style-type: none"> • all—Disables all system files debug output. • id—Disables system ID debug output. • info—Disables system info debug output. • init—Disables system init debug output. |

which

| | |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| transfer | File transfer. |
| user | User management. <ul style="list-style-type: none"> • all—Disables all user management debug output. • password-policy—Disables user management debug output for password-policy. |
| utils | Utilities configuration files. all—Disables all utilities configuration debug output. |

Command Default No default behavior or values.

Command Modes EXEC

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

Example

```
ise/admin# undebug all
ise/admin#
```

which

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

which

Syntax Description This command has no keywords and arguments.

Command Default No default behavior or values.

Command Modes EXEC

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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

Example

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

```

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

```

write

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

write [**erase** | **memory** | **terminal**]

Syntax Description

| | |
|-----------------|-------------------------------------------------------------------------|
| erase | Erases the startup configuration. This option is disabled in Cisco ISE. |
| memory | Copies the running configuration to the startup configuration. |
| terminal | Copies the running configuration to console. |

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

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

```

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

```

Example 2

```
ise/admin# write terminal
```

 write

```
Generating configuration...  
!  
hostname ise
```




CHAPTER 3

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 82
- [show application](#), on page 82
- [show backup](#), on page 85
- [show banner](#), on page 86
- [show cdp](#), on page 86
- [show clock](#), on page 87
- [show container](#), on page 88
- [show cpu](#), on page 92
- [show crypto](#), on page 94
- [show disks](#), on page 94
- [show icmp-status](#), on page 96
- [show interface](#), on page 97
- [show inventory](#), on page 99
- [show ip](#), on page 100
- [show ipv6 route](#), on page 100
- [show logging](#), on page 101
- [show logins](#), on page 103
- [show memory](#), on page 104
- [show ntp](#), on page 105
- [show ports](#), on page 105
- [show process](#), on page 107
- [show repository](#), on page 108
- [show restore](#), on page 109
- [show running-config](#), on page 110
- [show snmp engineid](#), on page 111
- [show snmp user](#), on page 112
- [show startup-config](#), on page 112
- [show tech-support](#), on page 113
- [show terminal](#), on page 115
- [show timezone](#), on page 116

- [show timezones](#), on page 116
- [show udi](#), on page 117
- [show uptime](#), on page 118
- [show users](#), on page 119
- [show version](#), on page 120

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 |
|----------------------|------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

| | |
|-------------------------|--------------------------------------------------------------------|
| 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 *>file-name*

show application [**status** {*application_name*}]

show application [**version** {*application_name*}]

| | | |
|---------------------------|-------------------------|----------------------------------------------------------------------------|
| Syntax Description | > | Redirects output to a file. |
| | <i>file-name</i> | Name of the file to store the Cisco ISE application information. |
| | status | Displays the status of the installed application. |
| | version | Displays the application version for an installed application (Cisco ISE). |
| | <i>application_name</i> | Name of the installed application. |

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 |
|----------------------|------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

| | |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------|
| 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 | history | Displays historical information about backups on the system. |
| | progress | Displays the backup status on the system. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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 | post-login | Displays the post-login information that is configured in the Cisco ISE server for the current CLI session. |
| | pre-login | Displays the pre-login information that is configured in the Cisco ISE server for the current CLI session. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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 | all | Shows all enabled Cisco Discovery Protocol interfaces. |
| | neighbors | Shows the Cisco Discovery Protocol neighbors. |
| Command Default | No default behavior or values. | |

| | |
|----------------------|------|
| Command Modes | EXEC |
|----------------------|------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

| | |
|-------------------------|---------------------------------------------------------------------------------------------------------|
| Usage Guidelines | To view enabled Cisco Discovery Protocol interfaces and CDP neighbors, use the show cdp command. |
|-------------------------|---------------------------------------------------------------------------------------------------------|

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

CDP Neighbor: isexp-esw5
    Local Interface : GigabitEthernet0
    Device Type     : cisco WS-C3560E-24TD
    Port            : GigabitEthernet0/5
    Address          : 172.23.90.45

CDP Neighbor: 000c29e29926
    Local Interface : GigabitEthernet0
    Device Type     : ISE-1141VM-K9
    Port            : eth0
    Address          : 172.23.90.115

CDP Neighbor: 000c290fba98
    Local Interface : GigabitEthernet0
    Device Type     : ISE-1141VM-K9
    Port            : eth0
    Address          : 172.23.90.111
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 |
|----------------------|------|

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

| | | |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 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 <pre> ise/admin# show clock Fri Aug 6 10:46:39 UTC 2010 ise/admin# </pre> | |

show container

To view information about the Threat-Centric NAC adapters and Wifi 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 | tc-nac | Displays information about the Threat-Centric NAC adapters. |
| | wifi setup | Displays the Wi-Fi container setup information. |
| | all | 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. |
| | adapters | 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. |
| | inspect { container-id <i>container-id</i> container-name <i>container-name</i> } | Lists detailed information about the specific adapter. |
| | stats { container-id <i>container-id</i> container-name <i>container-name</i> } | Provides statistical information about the specific adapter. |
| | > | Redirects output to a file. |

/

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

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.2.0.470 | This command was introduced. |

Usage GuidelinesTo view information about the Threat-Centric NAC adapters, use the **show container** command.**Example 1**

ise/admin# show container tc-nac adapters

| CONTAINER ID | IMAGE | COMMAND | CREATED |
|--------------|---------------------|------------------------|--------------|
| STATUS | PORTS | | NAMES |
| 63b8904f41c6 | irf-adapter-nexpose | "/opt/CSCOcpm/vaservi" | 19 hours ago |
| Up 19 hours | | | nexpose |
| 8389f7e249cf | irf-adapter-tenable | "/opt/CSCOcpm/vaservi" | 2 days ago |
| Up 2 days | | | tenable |

ise/admin#

Example 2

ise/admin# show container tc-nac all

| CONTAINER ID | IMAGE | COMMAND | CREATED |
|--------------|---------------------|------------------------|--------------|
| STATUS | PORTS | | NAMES |
| 63b8904f41c6 | irf-adapter-nexpose | "/opt/CSCOcpm/vaservi" | 19 hours ago |

show container

```

Up 19 hours                                nexpose
8389f7e249cf          irf-adapter-tenable    "/opt/CSCOcpm/vaservi"    2 days ago
Up 2 days                                tenable
41921c1539bf          irf-core-engine:2.2.6    "/bin/sh -c 'npm star'"   3 days ago
Up 3 days                                127.0.0.1:3000->3000/tcp
irf-core-engine-runtime
c4f6ff3cf628          irf-rabbitmq:2.2.6       "/docker-entrypoint.s"    3 days ago
Up 3 days                                4369/tcp, 5671-5672/tcp, 15671-15672/tcp, 25672/tcp  irf-rabbitmq-runtime
e682a5a5ad69          irf-mongo:2.2.6          "/entrypoint.sh mongo"    3 days ago
Up 3 days                                27017/tcp                irf-mongo-runtime

ise/admin#

```

Example 3

```

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",
  "Args": [
    "start",
    "http://irf-core-engine-runtime:3000/api/adapter/instance/register",
    "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": "06ba3230bd64872b988f4506e7fffd8c6374c7ece285555ee1cc57743ea7e0",
  "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/

        63b8904f41c6ce2a58660d38eb3500104038e650e4e3365e21e0a536a1ba3044-json.log",
  "Name": "/nexpose",
  "RestartCount": 0,
  "Driver": "devicemapper",
  "ExecDriver": "native-0.2",
  "MountLabel": "",
  "ProcessLabel": "",
  "AppArmorProfile": "",
  "ExecIDs": [
    "d76578aa48118167d9d029037fcb2e56aa7dce8672b8991a736617a6d6879750"
  ],
}
]

```

```

.
.
.
"NetworkSettings": {
  "Bridge": "",
  "SandboxID": "9873fb92f86e665039a6de15bfe057bc3fd341f7b39acedee57cbd89b3f56ce0",
  "HairpinMode": false,
  "LinkLocalIPv6Address": "",
  "LinkLocalIPv6PrefixLen": 0,
  "Ports": {},
  "SandboxKey": "/var/run/docker/netns/9873fb92f86e",
  "SecondaryIPAddresses": null,
  "SecondaryIPv6Addresses": null,
  "EndpointID": "",
  "Gateway": "",
  "GlobalIPv6Address": "",
  "GlobalIPv6PrefixLen": 0,
  "IPAddress": "",
  "IPPrefixLen": 0,
  "IPv6Gateway": "",
  "MacAddress": "",
  "Networks": {
    "irf-internal-nw": {
      "EndpointID":
"8999c12319144cfd66a4e99be40f7fbc228779e43f2a7f20c48867b8b3ca7a49",
      "Gateway": "169.254.1.1",
      "IPAddress": "169.254.1.6",
      "IPPrefixLen": 24,
      "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 |
|------------|---------------------|---------------------|-------|----------|
| 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 | STATUS |
|--------------|------------------|------------------------|------------|--------|
| d51711744e7c | wifisetup:0.0.12 | "/sbin/tini -- /usr/b" | 6 days ago | Up 6 |
| days | | wifisetup-container | | |

show cpu

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 | > | Redirects output to a file. |
| | <i>file-name</i> | Name of the file to redirect. |
| | statistics | Displays CPU statistics. |
| | cpu usage | Displays the CPU usage per component for an installed application (Cisco ISE). |
| | / | Output modifier variables: <ul style="list-style-type: none"> • begin—Matched pattern. Supports up to 80 alphanumeric characters. • count—Count the number of lines in the output. Add number after the word count. <ul style="list-style-type: none"> —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. <ul style="list-style-type: none"> —Output modifier variables for last. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.1.0.474 | This command was introduced. |

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
```

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

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 | authorized_keys | Displays authorized keys information for the user who is logged in currently. |
| | host_keys | Displays host keys for the user who is logged in currently. |
| | key | Displays key information for the user who is logged in currently. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | To view authorized keys and keys for currently logged in users, use the show crypto command. | |

Example 1

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

Example 2

```
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#
```

show disks

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

show disks > *file-name*

| | | |
|---------------------------|---|-----------------------------|
| Syntax Description | > | Redirects output to a file. |
|---------------------------|---|-----------------------------|

| | |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>file-name</i> | Name of the file to redirect. |
| / | <p>Output modifier variables:</p> <ul style="list-style-type: none"> • 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 |
|----------------------|------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

| | |
|-------------------------|------------------------------------------------------------------------------------|
| Usage Guidelines | Only platforms that have a disk file system support the show disks command. |
|-------------------------|------------------------------------------------------------------------------------|

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*

| | | |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | > | Redirects output to a file. |
| | <i>file-name</i> | Name of the file to redirect. |
| | / | Output modifier commands: |
| | | <ul style="list-style-type: none"> • <i>begin</i>—Matched pattern. Supports up to 80 alphanumeric characters. • <i>count</i>—Count the number of lines in the output. Add number after the word count. <ul style="list-style-type: none"> • —Output modifier commands for count. • <i>end</i>—End with line that matches. Supports up to 80 alphanumeric characters. • <i>exclude</i>—Exclude lines that match. Supports up to 80 alphanumeric characters. • <i>include</i>—Include lines that match. Supports up to 80 alphanumeric characters. • <i>last</i>—Display last few lines of output. Add number after the word last. Supports up to 80 lines to display. Default 10. <ul style="list-style-type: none"> • —Output modifier commands for last. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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}

| | | |
|---------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | > | Redirects output to a file. |
| | <i>file-name</i> | Name of the file to redirect interface information. |
| | GigabitEthernet | Shows the specific Gigabit Ethernet interface information. |
| | 0-3 | Gigabit Ethernet number that may be one of the following: 0, 1, 2, 3. |
| | / | Output modifier variables: <ul style="list-style-type: none"> • 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 | |

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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

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. |
| | <i>file-name</i> | Name of the file to redirect hardware inventory information. |
| | / | Output modifier variables: <ul style="list-style-type: none"> • 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 | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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.

show ip route

| Syntax Description | route | Displays IP route information. |
|--------------------|---------------------------------------------|--------------------------------|
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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 eth0
0.0.0.0          172.21.79.1    0.0.0.0         UG       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 | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

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*

show logging application *application-logfile-name*

show logging container tc-nac {*container-id container-id* [*log-name name-of-log-file tail*] | *container-name container-name*}

show logging internal

show logging system *system-logfile-name*

Syntax Description

| | |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| > | Redirects output to a file. |
| <i>file-name</i> | Name of the file to redirect system logging information. |
| application | Displays application logs. |
| <i>application-logfile-name</i> | Name of the application log file. |
| container tc-nac | Displays the Threat Centric-NAC containers. |
| container-id <i>container-id</i> [log-name <i>name-of-log-file tail</i>] | Displays the log files related to the specified container (TC-NAC adapter). |
| container-name <i>container-name</i> | Displays the log files related to the specified container (TC-NAC adapter). |

| | |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| internal | Displays the syslog configuration. |
| system | Displays system syslogs. |
| <i>system-logfile-name</i> | Name of the system log file. |
| <i>system-file-name</i> | Name of the system log file name. |
| | Output modifier variables: <ul style="list-style-type: none"> • 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

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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 15:56:54  spooler
    0 Feb 25 2013 16:10:03  boot.log
    0 Feb 25 2013 16:00:03  bttmp
  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 28 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 sa/sa26
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 | cli Lists the cli login history. | |
|--------------------|----------------------------------|------------------------------|
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

show memory**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)
wtm 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.

show memory**Command Default**

No default behavior or values.

Command Modes

EXEC

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

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

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

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 1 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. |
| <i>file-name</i> | 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.
|—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

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage GuidelinesWhen 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, 127.0.0.1:8
005, 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, 127.0.0.1:8888, 0.0.0.0:9080, 0.0.0.0:62424, 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, 172.2
1.79.91:1645, 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. |
| | <i>file-name</i> | Name of the file to redirect. |
| | / | (Optional). Output modifier variables: <ul style="list-style-type: none"> • 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

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

Usage Guidelines *Table 2: Show Process Field Descriptions*

| Field | Description |
|-------|-----------------|
| USER | Logged-in user. |

| Field | Description |
|---------|-------------------------------------|
| PID | Process ID. |
| TIME | The time the command was last used. |
| TT | Terminal that controls the process. |
| COMMAND | Type of process or command used. |

Example

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

| | | |
|---------------------------|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Syntax Description | <i>repository-name</i> | Name of the repository whose contents you want to view. Supports up to 30 alphanumeric characters. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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+y5WNjGIrgfPmEpEswVY7Qjb0 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}

| | | |
|---------------------------|--------------------------------|-----------------------------------------------|
| Syntax Description | history | Displays the restore history on the system. |
| | status | Displays the status of restore on the system. |
| Command Default | No default behavior or values. | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | Example | |

```
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
%% -----
% No data found. Try 'show restore history' or ISE operation audit report
%% Operation restore status
%% -----
% 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

| | | |
|-------------------------|-----------------------------------------------------------------------------------------------|------------------------------|
| Command Default | None | |
| Command Modes | EXEC | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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 $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. 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 |

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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 | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

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 | |
|------------------------|-----------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

Usage Guidelines

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

Example

```
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/XL4tH15Knf.FfcZZr. 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 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*

Syntax Description

| | |
|-------------|---------------------------------------------------------------|
| > | Redirects output to a file. |
| file | Saves any technical support data as a file in the local disk. |

| | |
|------------------|-------------------------------------------------------------------------------------|
| <i>file-name</i> | Filename to save technical support data. Supports up to 80 alphanumeric characters. |
|------------------|-------------------------------------------------------------------------------------|

Command Default

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

Command Modes

EXEC

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

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--
(prompt 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.

show terminal

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage Guidelines

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

Table 3: Show Terminal Field Descriptions

| Field | Description |
|-----------------------------|-------------------------------------------------------------------------------|
| TTY: /dev/pts/0 | Displays standard output to type of terminal. |
| Type: "vt100" | Type of current terminal used. |
| Length: 27 lines | Length of the terminal display. |
| Width: 80 columns | Width of the terminal display, in character columns. |
| Session Timeout: 30 minutes | Length of time, in minutes, for a session, after which the connection closes. |

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.

| | |
|------------------------|--------------------------------|
| Command Default | No default behavior or values. |
|------------------------|--------------------------------|

| | |
|----------------------|------|
| Command Modes | EXEC |
|----------------------|------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

| | |
|-------------------------|----------------|
| Usage Guidelines | Example |
|-------------------------|----------------|

```
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 |
|----------------------|------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

| | |
|-------------------------|----------------------------------------------------------------------------------------------------|
| 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.

show udi

| | |
|------------------------|--------------------------------|
| Command Default | No default behavior or values. |
|------------------------|--------------------------------|

| | |
|----------------------|------|
| Command Modes | EXEC |
|----------------------|------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

| | |
|-------------------------|------------------|
| Usage Guidelines | Example 1 |
|-------------------------|------------------|

```
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.

```
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. |
| | <i>file-name</i> | Name of the file to redirect. |
| | / | Output modifier variables: |
| | | <ul style="list-style-type: none"> • 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 | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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 | > | Redirects output to a file. |
| | <i>file-name</i> | Name of the file to redirect. |
| | / | Output modifier variables: <ul style="list-style-type: none"> • 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 | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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

| | | |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | > | Redirects output to a file. |
| | <i>file-name</i> | Name of the file to redirect. |
| | history | Shows software version history information. |
| | / | Output modifier variables: <ul style="list-style-type: none"> • 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 | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| 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**



CHAPTER 4

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 124](#)
- [Configuring Cisco ISE in the Configuration Mode, on page 125](#)
- [Configuring Cisco ISE in the Configuration Submode, on page 126](#)
- [CLI Configuration Command Default Settings, on page 126](#)
- [backup interface, on page 126](#)
- [cdp holdtime, on page 129](#)
- [cdp run, on page 130](#)
- [cdp timer, on page 131](#)
- [clear screen, on page 132](#)
- [clock timezone, on page 132](#)
- [cls, on page 136](#)
- [conn-limit, on page 136](#)
- [do, on page 137](#)
- [end, on page 140](#)
- [exit, on page 141](#)
- [hostname, on page 141](#)
- [icmp echo, on page 143](#)
- [interface, on page 143](#)
- [ip address, on page 145](#)
- [ip default-gateway, on page 146](#)
- [ip domain-name, on page 146](#)
- [ip host, on page 147](#)
- [ip name-server, on page 149](#)
- [ip route, on page 151](#)
- [ipv6 address, on page 152](#)
- [ipv6 address autoconfig, on page 154](#)
- [ipv6 address dhcp, on page 156](#)
- [ipv6 enable, on page 157](#)
- [ipv6 route, on page 158](#)
- [kron occurrence, on page 159](#)

- [kron policy-list](#), on page 161
- [logging](#), on page 162
- [max-ssh-sessions](#), on page 163
- [ntp](#), on page 164
- [ntp authenticate](#), on page 165
- [ntp authentication-key](#), on page 166
- [ntp server](#), on page 167
- [ntp trusted-key](#), on page 170
- [rate-limit](#), on page 171
- [password-policy](#), on page 172
- [repository](#), on page 173
- [service](#), on page 175
- [shutdown](#), on page 177
- [snmp-server enable](#), on page 178
- [snmp-server user](#), on page 178
- [snmp-server host](#), on page 180
- [snmp-server community](#), on page 181
- [snmp-server contact](#), on page 183
- [snmp-server location](#), on page 183
- [snmp-server trap dskThresholdLimit](#), on page 184
- [snmp engineid](#), on page 185
- [synflood-limit](#), on page 185
- [username](#), on page 186
- [which](#), on page 187

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  Shutdown the interface
ise/admin(config-GigabitEthernet)#
```

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

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

CLI Configuration Command Default Settings

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

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

backup interface

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

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

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

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

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

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

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

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

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

| | | |
|---------------------------|-----------------------------------------------------------|------------------------------------------------------------------------------|
| Syntax Description | backup interface | Configures the NIC bonding feature. |
| | GigabitEthernet | Configures the Gigabit Ethernet interface specified as the backup interface. |
| | <i>0 - 3</i> | Number of the Gigabit Ethernet port to configure as the backup interface. |
| Command Default | No default behavior or values. | |
| Command Modes | Interface configuration submode (config-GigabitEthernet)# | |

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.1.0.474 | This command was introduced. |

| | |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usage Guidelines | <ul style="list-style-type: none"> As Cisco ISE supports up to six Ethernet interfaces, it can have only three bonds, bond 0, bond 1, and bond 2. You cannot change the interfaces that are part of a bond or change the role of the interface in a bond. Refer to the above table for information on which NICs can be bonded together and their role in the bond. The Eth0 interface acts as both the management interface as well as the runtime interface. The other interfaces act as runtime interfaces. Before you create a bond, the primary interface (primary NIC) must be assigned an IP address. The Eth0 interface must be assigned an IPv4 address before you create bond 0. Similarly, before you create bond 1 and 2, Eth2 and Eth4 interfaces must be assigned an IPv4 or IPv6 address, respectively. Before you create a bond, if the backup interface (Eth1, Eth3, and Eth5) has an IP address assigned, remove the IP address from the backup interface. The backup interface should not be assigned an IP address. You can choose to create only one bond (bond 0) and allow the rest of the interfaces to remain as is. In this case, bond 0 acts as the management interface and runtime interface, and the rest of the interfaces act as runtime interfaces. You can change the IP address of the primary interface in a bond. The new IP address is assigned to the bonded interface because it assumes the IP address of the primary interface. When you remove the bond between two interfaces, the IP address assigned to the bonded interface is assigned back to the primary interface. If you want to configure the NIC bonding feature on a Cisco ISE node that is part of a deployment, you must deregister the node from the deployment, configure NIC bonding, and then register the node back to the deployment. If a physical interface that acts as a primary interface in a bond (Eth0, Eth2, or Eth4 interface) has static route configured, the static routes are automatically updated to operate on the bonded interface instead of the physical interface. |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example 1 - Configure NIC Bonding

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



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

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
```



```

ise/admin(config-GigabitEthernet)# backup interface gigabitEthernet 1
Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
Stopping ISE Monitoring & Troubleshooting Log 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.

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. |
| | <i>seconds</i> | Advertised hold time value, in seconds. The value ranges from 10 to 255 seconds. |
| Command Default | The default CDP holdtime, in seconds is 180. | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | <p>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.</p> <p>The cdp holdtime command takes only one argument; otherwise, an error occurs.</p> | |

Example

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

cdp run


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

cdp run GigabitEthernet

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

no cdp run

| | | |
|---------------------------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | run | Enables the Cisco Discovery Protocol. Disables the Cisco Discovery Protocol when you use the no form of the cdp run command. |
| | <i>GigabitEthernet</i> | (Optional). Specifies the GigabitEthernet interface on which to enable the Cisco Discovery Protocol. |
| | <i>0-3</i> | Specifies the GigabitEthernet interface number on which to enable the Cisco Discovery Protocol. |
| Command Default | No default behavior or values. | |
| Command Modes | Configuration (config)# | |

| Command History | Release | Modification |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | The command has one optional argument, which is an interface name. Without an optional interface name, the command enables the Cisco Discovery Protocol on all interfaces. | |
|  | | |
| Note | The default for this command is on interfaces that are already up and running. When you are bringing up an interface, stop the Cisco Discovery Protocol first; then, start the Cisco Discovery Protocol again. | |
| Example | <pre>ise/admin(config)# cdp run GigabitEthernet 0 ise/admin(config)#</pre> | |

cdp timer

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

cdp timer *seconds*

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

no cdp timer

| Syntax Description | timer | Refreshes at the time interval specified. |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| | <i>seconds</i> | Specifies how often, in seconds, the Cisco ISE server sends Cisco Discovery Protocol updates. The value ranges from 5 to 254 seconds. |
| Command Default | The default refreshing time interval value, in seconds is 60. | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | Cisco Discovery Protocol packets transmit with a time to live, or hold time, value. The receiving device will discard the Cisco Discovery Protocol information in the Cisco Discovery Protocol packet after the hold time has elapsed. | |
| | The cdp timer command takes only one argument; otherwise, an error occurs. | |

Example

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

clear screen

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

clear screen

| | | |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Syntax Description | This command has no keywords and arguments. | |
| Command Default | No default behavior or values. | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | clear screen is a hidden command. Although clear screen is available in Cisco ISE, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. | |

Example

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

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

clock timezone

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

clock timezone *timezone*

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

no clock timezone**Note**

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

| | | |
|---------------------------|-----------------|-----------------------------|
| Syntax Description | timezone | Configures system timezone. |
|---------------------------|-----------------|-----------------------------|

| | |
|-----------------|----------------------------------------------------------------------------------------------------|
| <i>timezone</i> | Name of the time zone visible when in standard time. Supports up to 64 alphanumeric characters. |
|-----------------|----------------------------------------------------------------------------------------------------|

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

| | |
|------------------------|----------------------------------|
| Command Default | Coordinated Universal Time (UTC) |
|------------------------|----------------------------------|

| | |
|----------------------|-------------------------|
| Command Modes | Configuration (config)# |
|----------------------|-------------------------|

| Command History | <table> <tr> <th>Release</th> <th>Modification</th> </tr> <tr> <td>2.0.0.306</td> <td>This command was introduced.</td> </tr> </table> | Release | Modification | 2.0.0.306 | This command was introduced. |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------|---------|--------------|-----------|------------------------------|
| Release | Modification | | | | |
| 2.0.0.306 | This command was introduced. | | | | |

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



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

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

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

Example

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

Changing the Time Zone on Cisco ISE Nodes

Changing the time zone on 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: Table 4-1 Common Time Zones (Continued)

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

| Acronym or name | Time Zone Name |
|-----------------|-------------------------------------------|
| HST | Hawaiian Standard Time, as UTC - 10 hours |

Australia Time Zones



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

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

| Australia | | | |
|------------------------------------|-----------------------|------------------------|-------------|
| Australian Capital Territory (ACT) | Adelaide | Brisbane | Broken_Hill |
| Canberra | Currie | Darwin | Hobart |
| Lord_Howe | Lindeman | Lord Howe Island (LHI) | Melbourne |
| North | New South Wales (NSW) | Perth | Queensland |
| South | Sydney | Tasmania | Victoria |
| West | Yancowinna | | |

Asia Time Zones



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

Table 6: Table 4-3 Asia Time Zones (Continued)

| Asia | | | |
|------------|-----------|----------|-----------|
| Aden | Almaty | Amman | Anadyr |
| Aqtau | Aqtobe | Ashgabat | Ashkhabad |
| Baghdad | Bahrain | Baku | Bangkok |
| Beirut | Bishkek | Brunei | Calcutta |
| Choibalsan | Chongqing | Columbo | Damascus |
| Dhakar | Dili | Dubai | Dushanbe |

| Asia | | | |
|-----------|-------------|--------------|----------|
| Gaza | Harbin | Hong_Kong | Hovd |
| Irkutsk | Istanbul | Jakarta | Jayapura |
| Jerusalem | Kabul | Kamchatka | Karachi |
| Kashgar | Katmandu | Kuala_Lumpur | Kuching |
| Kuwait | Krasnoyarsk | | |

cls

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

cls

| Syntax Description | This command has no keywords and arguments. | | | | |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|--------------|-----------|------------------------------|
| Command Default | No default behavior or values. | | | | |
| Command Modes | Configuration (config)# | | | | |
| Command History | <table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>2.0.0.306</td><td>This command was introduced.</td></tr> </table> | Release | Modification | 2.0.0.306 | This command was introduced. |
| Release | Modification | | | | |
| 2.0.0.306 | This command was introduced. | | | | |
| Usage Guidelines | cls is a hidden command. Although cls is available in Cisco ISE, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. | | | | |

Example

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

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

conn-limit

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

| | | |
|---------------------------|----------------|------------------------------------------------------------------|
| Syntax Description | <1-2147483647> | Number of TCP connections. |
| | <i>ip</i> | (Optional). Source IP address to apply the TCP connection limit. |

| | |
|-------------|------------------------------------------------------------------------|
| <i>mask</i> | (Optional). Source IP mask to apply the TCP connection limit. |
| <i>port</i> | (Optional). Destination port number to apply the TCP connection limit. |

Command Default No default behavior or values.

Command Modes Configuration (config)#

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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

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

Example

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

do

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

do EXEC commands

| Syntax Description | EXEC commands | Specifies to execute an EXEC-system level command (see Table 7: Table 4-4 Command Options for Do Command (Continued)). |
|--------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------|
|--------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------|

Table 7: Table 4-4 Command Options for Do Command (Continued)

| Command | Description |
|---------------------------------|-------------------------------------------------------|
| application configure | Configures a specific application. |
| application install | Installs a specific application. |
| application remove | Removes a specific application. |
| application reset-config | Resets application configuration to factory defaults. |
| application reset-passwd | Resets application password for a specified user. |

| Command | Description |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| application start | Starts or enables a specific application |
| application stop | Stops or disables a specific application. |
| application upgrade | Upgrades a specific application. |
| backup | Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository. |
| backup-logs | Performs a backup of all logs in the Cisco ISE server to a remote location. |
| clock | Sets the system clock in the Cisco ISE server. |
| configure | Enters configuration mode. |
| copy | Copies any file from a source to a destination. |
| debug | Displays any errors or events for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management. |
| delete | Deletes a file in the Cisco ISE server. |
| dir | Lists files in the Cisco ISE server. |
| forceout | Forces the logout of all sessions of a specific Cisco ISE node user. |
| halt | Disables or shuts down the Cisco ISE server. |
| mkdir | Creates a new directory. |
| nslookup | Queries the IPv4 or IPv6 address or hostname of a remote system. |
| password | Updates the CLI account password. |
| patch | Installs a Patch Bundle or uninstalls an Application patch. |
| ping | Determines the IPv4 address or hostname of a remote system. |
| ping6 | Determines the IPv6 address of a remote system. |
| reload | Reboots the Cisco ISE server. |
| restore | Performs a restore and retrieves the backup out of a repository. |
| rmdir | Removes an existing directory. |

| Command | Description |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show | Provides information about the Cisco ISE server. |
| ssh | Starts an encrypted session with a remote system. |
| tech | Provides Technical Assistance Center (TAC) commands. |
| terminal length | Sets terminal line parameters. |
| terminal session-timeout | Sets the inactivity timeout for all terminal sessions. |
| terminal session-welcome | Sets the welcome message on the system for all terminal sessions. |
| terminal terminal-type | Specifies the type of terminal connected to the current line of the current session. |
| traceroute | Traces the route of a remote IP address. |
| undebg | Disables the output (display of errors or events) of the debug command for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management. |
| write | Erases the startup configuration that forces to run the setup utility and prompt the network configuration, copies the running configuration to the startup configuration, displays the running configuration on the console. |

Command Default No default behavior or values.

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

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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

Example

```
ise/admin(config)# do show run
Generating configuration...
!
hostname ise
!
ip domain-name cisco.com
!
```

end

```

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

```

end

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

This command has no keywords and arguments.

end

| | |
|------------------------|--------------------------------|
| Command Default | No default behavior or values. |
|------------------------|--------------------------------|

| | |
|----------------------|-------------------------|
| Command Modes | Configuration (config)# |
|----------------------|-------------------------|

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

| | |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usage Guidelines | <p>This command brings you back to EXEC mode regardless of what configuration mode or submode you are in.</p> <p>Use this command when you finish configuring the system and you want to return to EXEC mode to perform verification steps.</p> |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example

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

exit

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

exit

This command has no keywords and arguments.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage Guidelines

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

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

Example

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

hostname

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

hostname *hostname*

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History**Release****Modification**

2.0.0.306

This command was introduced.

Usage Guidelines**Note**

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

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

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

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

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

Example

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

```

CLI to verify all processes are in running state.
ise-1/admin#

```

icmp echo

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

icmp echo {*off* | *on*}

| | | |
|---------------------------|----------------------------------------------------------------------|--------------------------------|
| Syntax Description | echo | Configures ICMP echo response. |
| | <i>off</i> | Disables ICMP echo response |
| | <i>on</i> | Enables ICMP echo response. |
| Command Default | The system behaves as if the ICMP echo response is on (enabled). | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | Use this icmp echo to turn on or turn off ICMP echo response. | |

Example

```

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

```

interface

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



Note

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

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

| | | |
|---------------------------|------------------------|---------------------------------------------------|
| Syntax Description | GigabitEthernet | Configures the Gigabit Ethernet interface. |
| | <i>0 - 3</i> | Number of the Gigabit Ethernet port to configure. |

**Note**

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

Syntax Description

| | |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| backup | Configures the NIC bonding feature to provide high availability for the physical interfaces. |
| do | EXEC command. Allows you to perform any EXEC commands in this mode. |
| end | Exits the config-GigabitEthernet submode and returns you to EXEC mode. |
| exit | Exits the config-GigabitEthernet configuration submode. |
| ip | Sets the IP address and netmask for the Gigabit Ethernet interface. |
| ipv6 | Configures IPv6 autoconfiguration address and IPv6 address from DHCPv6 server. |
| no | Negates the command in this mode. Two keywords are available: <ul style="list-style-type: none"> • ip—Sets the IP address and netmask for the interface. • ipv6—Sets the IPv6 address for the interface. • shutdown—Shuts down the interface. |
| shutdown | Shuts down the interface. |

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-GigabitEthernet)#

Command History

| Release | Modification |
|----------------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage Guidelines

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

Example

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


ip address

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

ip address *ip-address network mask*

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

no ip address



Note

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

Syntax Description

| | |
|---------------------|-----------------------------------|
| <i>ip-address</i> | IPv4 address. |
| <i>network mask</i> | Mask of the associated IP subnet. |

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

Command Default

Enabled.

Command Modes

Interface configuration (config-GigabitEthernet)#

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage Guidelines



Note

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

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

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

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

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

Example

```
ise/admin(config)# interface GigabitEthernet 1
```

```

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

```

ip default-gateway

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

ip default-gateway *ip-address*

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

no ip default-gateway

| | | |
|---------------------------|------------------------------------------------------------------------------|-----------------------------------------------|
| Syntax Description | default-gateway | Defines a default gateway with an IP address. |
| | <i>ip-address</i> | IP address of the default gateway. |
| Command Default | Disabled. | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | If you enter more than one argument or no arguments at all, an error occurs. | |

Example

```

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

```

ip domain-name

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

ip domain-name *domain-name*

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

no ip domain-name

| | | |
|---------------------------|--------------------|--------------------------------|
| Syntax Description | domain-name | Defines a default domain name. |
|---------------------------|--------------------|--------------------------------|

| | |
|--------------------|--------------------------------------------------------------------------------------------------------|
| <i>domain-name</i> | Default domain name used to complete the hostnames. Contains at least 2 to 64 alphanumeric characters. |
|--------------------|--------------------------------------------------------------------------------------------------------|

Command Default

Enabled.

Command Modes

Configuration (config)#

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage Guidelines**Note**

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

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

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

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

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

Example

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

ip host

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

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

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

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

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

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

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

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

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

Command Default No default behavior or values.

Command Modes Configuration (config)#

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

Usage Guidelines Supported IPv6 address formats include:

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

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

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

Example 1

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

```

ip name-server

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

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

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

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



Note

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

Syntax Description

name-server

Configures the IP addresses of the name server(s).

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

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

Command Default No default behavior or values.

Command Modes Configuration (config)#

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

Usage Guidelines

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

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

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



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

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

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

Example 1

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

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

Example 2

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

```
ise/admin# show run | in name-server
ip name-server 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 | <i>prefix</i> | IP route prefix for the destination. |
| | <i>mask</i> | Prefix mask for the destination. |
| | <i>ip-address</i> | IP address of the next hop that can be used to reach that network. |
| Command Default | No default behavior or values. | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | <p>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.</p> <p>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.</p> <p>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.</p> <p>The following example describes how to configure multiple default routes:</p> | |

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

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

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

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



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

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



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

Example 2

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

ipv6 address

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

ipv6 address *ipv6-address/prefix-length*

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

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

Syntax Description

ipv6-address

IPv6 address.

prefix-length

The length of the IPv6 prefix. A decimal value between 0 and 128 that 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.

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

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

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

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-GigabitEthernet)#

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage Guidelines

Supported IPv6 address formats include:

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

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

**Note**

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

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

Example 1

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

```
processes are in running state.
ise/admin(config-GigabitEthernet)#
```

Example 2

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

ipv6 address autoconfig

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

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

ipv6 address autoconfig

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

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-GigabitEthernet)#

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage Guidelines

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

Example

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

Configuring IPv6 Auto Configuration

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

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

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

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

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

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

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

```
ise/admin# show interface GigabitEthernet 0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AF:DA:05
          inet addr:172.23.90.116  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: 3ffe:302:11:2:20c:29ff:feaf:da05/64  Scope:Global
          inet6 addr: fe80::20c:29ff:feaf:da05/64  Scope:Link
          inet6 addr: 2001:558:ff10:870:8000:29ff:fe36:200/64  Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77848 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10699801 (10.2 MiB)  TX bytes:3448374 (3.2 MiB)
          Interrupt:59 Base address:0x2000

ise/admin#
```

Verifying the Privacy Extensions Feature

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

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

The output appears similar to the following:

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

ise/admin#
```

ipv6 address dhcp

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

ipv6 address dhcp

| | | |
|-------------------------|---------------------------------------------------|------------------------------|
| Command Default | No default behavior or values. | |
| Command Modes | Interface configuration (config-GigabitEthernet)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | Example | |

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

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

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



Note

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

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

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

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

ipv6 enable

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

ipv6 enable

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

no ipv6 enable

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-GigabitEthernet)#

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage Guidelines

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

Example 1

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

Example 2

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

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

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

ipv6 route

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

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

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

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

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

| | | |
|---------------------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | <i>ipv6-address</i> | IPv6 address. |
| | <i>prefix-length</i> | 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. |
| | <i>route-specific gateway</i> | IPv6 address of the next hop that can be used to reach that network. |

Command Default No default behavior or values.

Command Modes Global configuration (config)#

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

Usage Guidelines Supported IPv6 address formats include:

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

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

Example 1

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

Example 2

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

where `::/0` indicates a default route prefix.

kron occurrence

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

kron occurrence *occurrence-name*

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

**Note**

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

| Syntax Description | at | Identifies that the occurrence is to run at a specified calendar date and time. Usage: at [<i>hh:mm</i>] [<i>day-of-week</i> <i>day-of-month</i> <i>month day-of-month</i>]. |
|--------------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | 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: <ul style="list-style-type: none"> • at—Usage: at [hh:mm] [day-of-week day-of-month month day-of-month]. • policy-list—Specifies a policy list to be run by the occurrence. Supports up to 80 alphanumeric characters. • recurring—Execution of the policy lists should be repeated. |
| policy-list | Specifies a Command Scheduler policy list to be run by the occurrence. |
| recurring | Identifies that the occurrences run on a recurring basis. Note If kron occurrence is not recurring, then the kron occurrence configuration for the scheduled backup is removed after it has run. |

Command Default No default behavior or values.

Command Modes Configuration (config-Occurance)#

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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

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



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



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

Example 1: Weekly Backup

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

Example 2: Daily Backup

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


Example 3: Weekly Backup

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

kron policy-list

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

kron policy-list *list-name*

| | | |
|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Syntax Description | policy-list | Specifies a name for Command Scheduler policies. |
| | <i>list-name</i> | Name of the policy list. Supports up to 80 alphanumeric characters. |
|  Note | After you enter the list-name in the kron policy-list command, you enter the config-Policy List configuration submode (see the following Syntax Description). | |
| | | |
| Syntax Description | cli | Command to be executed by the scheduler. Supports up to 80 alphanumeric characters. |
| | do | EXEC command. Allows you to perform any EXEC commands in this mode. |
| | end | Exits from the config-Policy List configuration submode and returns you to EXEC mode. |

| | |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| exit | Exits this submode. |
| no | Negates the command in this mode. One keyword is available: <ul style="list-style-type: none"> cli—Command to be executed by the scheduler. |

Command Default No default behavior or values.

Command Modes Configuration (config-Policy List)#

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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



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

Example

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

logging

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

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

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

no logging

| Syntax Description | loglevel | The command to configure the log level for the logging command. |
|---------------------------|-----------------|-----------------------------------------------------------------|
|---------------------------|-----------------|-----------------------------------------------------------------|

0-7

The desired priority level to set the log messages. Priority levels are (enter the number for the keyword):

- 0-emerg—Emergencies: System unusable.
- 1-alert—Alerts: Immediate action needed.
- 2-crit—Critical: Critical conditions.
- 3-err—Error: Error conditions.
- 4-warn—Warning: Warning conditions.
- 5-notif—Notifications: Normal but significant conditions.
- 6-inform—(Default) Informational messages.
- 7-debug—Debugging messages.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage Guidelines

This command requires the **loglevel** keyword.

Example

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

max-ssh-sessions

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

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

Syntax Description

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

Command Default

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

Command Modes

Configuration (config)#

| | | |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | The max-ssh-sessions parameter is not configurable from the command-line interface. The maximum number of active CLI sessions is replicated from the primary administration ISE Admin portal. | |
| | When you exceed the maximum number of CLI sessions, the “Maximum active ssh sessions reached” message is displayed in the command-line interface closing that session, and you can see the “Not connected - press Enter or Space to connect” message at the bottom. | |
| | You can log in to the CLI through the console and use the forceout username command to log out users to reduce the active SSH sessions. | |
| | The navigation path to configure the maximum number of command-line interface (CLI) sessions is in the Session tab of the Cisco ISE Admin portal in the following location: Administration > System > Admin Access > Settings > Access . | |

ntp

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

ntp authenticate

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

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

ntp trusted-key *<key>*

no ntp server

| | | |
|---------------------------|-------------------------------------------------------------|---------------------------------------------------------|
| Syntax Description | authenticate | Enables authentication of all time sources. |
| | authentication-key | Specifies authentication keys for trusted time sources. |
| | server | Specifies NTP server to use. |
| | trusted-key | Specifies key numbers for trusted time sources. |
| Command Default | None | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | Use the ntp command to specify an NTP configuration. | |

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

Example

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

ntp authenticate

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

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

ntp authenticate

| | | |
|---------------------------|-------------------------|---------------------------------------------|
| Syntax Description | authenticate | Enables authentication of all time sources. |
| Command Default | None | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

Usage Guidelines

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

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

Example

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

ntp authentication-key

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

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

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

no ntp authentication-key

Syntax Description

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

Command Default

None

Command Modes

Configuration (config)#.

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage Guidelines

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

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



Note

The **show running-config** command will always show keys that are entered in Message Digest 5 (MD5) plain format converted into hash format for security. For example, **ntp authentication-key 1 md5 hashee18afc7608ac7ecdbeefc5351ad118bc9ce1ef3**.

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 | server | Allows the system to synchronize with a specified server. |
|--------------------|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <i>ip-address</i> <i>hostname</i> | IPv4 or address or hostname of the server providing the clock synchronization. Arguments are limited to 255 alphanumeric characters. |
| | autokey | Specifies that public-key authentication should be used for NTP server. If you choose this option, ensure that you import the NTP server's public key in to the Cisco ISE node using the crypto command. |

| | |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>key</i> | <p>(Optional). Peer key number. Supports up to 65535 numeric characters.</p> <p>This key needs to be defined with a key value, by using the ntp authentication-key command, and also needs to be added as a trusted-key by using the ntp trusted-key command.</p> <p>For authentication to work, the key and the key value should be the same as that which is defined on the actual NTP server.</p> |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Command Default No servers are configured by default.

Command Modes Configuration (config)#

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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

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

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

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

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

```
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 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
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

Verifying the Status of Synchronization

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

Example 1

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

Example 2

```

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

```

ntp trusted-key

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

ntp trusted-key *key*

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

no ntp trusted-key

| | | |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax Description | trusted-key | The identifier that you want to assign to this key. |
| | <i>key</i> | Specifies key numbers for trusted time sources that needs to be defined as NTP authentication keys. Supports up to 65535 numeric characters. |
| Command Default | None | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | Define this key as an NTP authentication key and then add this key to the trusted list before you add this key to an NTP server. Keys that are added to the trusted list can only be used that allows synchronization by the NTP server with the system. | |

Example 1

```

ise/admin# configure
ise/admin(config)#
ise/admin(config)# ntp trusted-key 1
ise/admin(config)# ntp trusted-key 2
ise/admin(config)# ntp trusted-key 3

```

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

Example 2

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

rate-limit

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

rate-limit 250 ip-address net-mask port

| | | |
|---------------------------|--------------------------------|---------------------------------------------------------|
| Syntax Description | <i><1-10000></i> | An average number of TCP/UDP/ICMP packets per second. |
| | ip-address | Source IP address to apply the packet rate limit. |
| | net-mask | Source IP mask to apply the packet rate limit. |
| | port | Destination port number to apply the packet rate limit. |
| Command Default | No default behavior or values. | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | None. | |

Example

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

password-policy

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

password-policy options



Note

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



Note

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

Syntax Description

| | |
|---------------------------------|--------------------------------------------------------------------------------------|
| <i>digit-required</i> | Requires a digit in user passwords. |
| <i>disable-cisco-password</i> | Disables the ability to use the word Cisco or any combination as the password. |
| <i>disable-repeat-chars</i> | Disables the ability of the password to contain more than four identical characters. |
| <i>do</i> | Exec command. |
| <i>end</i> | Exit from configure mode. |
| <i>exit</i> | Exit from this submode. |
| <i>lower-case-required</i> | Requires a lowercase letter in user passwords. |
| <i>min-password-length</i> | Minimum number of characters for a valid password. Supports up to 40 characters. |
| <i>no</i> | Negate a command or set its defaults. |
| <i>no-previous-password</i> | Prevents users from reusing a part of their previous password. |
| <i>no-username</i> | Prohibits users from reusing their username as a part of a password. |
| <i>password-delta</i> | Number of characters to be different from the old password. |
| <i>password-expiration-days</i> | Number of days until a password expires. Supports an integer up to 3650. |

| | |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>password-expiration-enabled</i> | Enables password expiration. Note You must enter the password-expiration-enabled command before the other password-expiration commands. |
| <i>password-expiration-warning</i> | Number of days before expiration that warnings of impending expiration begin. Supports an integer up to 3650. |
| <i>password-lock-enabled</i> | Locks a password after several failures. |
| <i>password-lock-retry-count</i> | Number of failed attempts before user password locks. Supports an integer up to 20. |
| <i>password-lock-timeout</i> | Sets the time in minutes after which the account lockout is cleared. Supports time values from 5 minutes to 1440 minutes. |
| <i>special-required</i> | Requires a special character in user passwords. |
| <i>upper-case-required</i> | Requires an uppercase letter in user passwords. |

| Command Default | No default behavior or values. | | | | |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------|---------|--------------|-----------|------------------------------|
| Command Modes | Configuration (config-password-policy)# | | | | |
| Command History | <table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>2.0.0.306</td><td>This command was introduced.</td></tr> </table> | Release | Modification | 2.0.0.306 | This command was introduced. |
| Release | Modification | | | | |
| 2.0.0.306 | This command was introduced. | | | | |

Usage Guidelines None.

Example

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

repository

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

repository *repository-name*

| | | |
|---------------------------|------------------------|----------------------------------------------------------------|
| Syntax Description | <i>repository-name</i> | Name of repository. Supports up to 80 alphanumeric characters. |
|---------------------------|------------------------|----------------------------------------------------------------|



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

Syntax Description

| | |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| do | EXEC command. Allows you to perform any of the EXEC commands in this mode. |
| end | Exits the config-Repository submode and returns you to EXEC mode. |
| exit | Exits this mode. |
| no | Negates the command in this mode. Two keywords are available: <ul style="list-style-type: none"> • url—Repository URL. • user—Repository username and password for access. |
| url | URL of the repository. Supports up to 300 alphanumeric characters (see Table 4-5). |
| user | Configure the username and password for access. Supports up to 30 alphanumeric characters for username and supports 15 alphanumeric characters for password. Passwords can consist of the following characters: 0 through 9, a through z, A through Z, -, ., , @, #, \$, %, ^, &, *, (,), +, and =. |



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

Table 8: Table 4-5 URL Keywords (Continued)

| Keyword | Source of Destination |
|---------------|-------------------------------------------------------------------------------------------------------------|
| URL | Enter the repository URL, including server and path information. Supports up to 80 alphanumeric characters. |
| cdrom: | Local CD-ROM drive (read only). |

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

Command Default No default behavior or values.

Command Modes Configuration (config-Repository)#

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

service

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

service sshd

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

no service**Syntax Description**

| | |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sshd | Secure Shell Daemon. The daemon program for SSH. |
| enable | Enables sshd service. |
| encryption-algorithm | Configures SSH encryption algorithms. The supported algorithms are a, aes128-cbc, aes128-ctr, aes256-cbc, and aes256-ctr. Note This is applicable for ISE 2.3 Patch 3 and later. |
| encryption-mode | Configures SSH encryption mode on system. The supported modes are cbc and ctr. Note This is applicable for ISE 2.3 Patch 3 and later. |
| key-exchange-algorithm | Specifies allowable key exchange algorithms for sshd service. |
| diffie-hellman-group14-sha1 | Restricts key exchange algorithm to diffie-hellman-group14-sha1 |
| Loglevel | Specifies the log level of messages from sshd to secure system log. <ul style="list-style-type: none"> • 1—QUIET • 2—FATAL • 3—ERROR • 4—INFO (default) • 5—VERBOSE • 6—DEBUG • 7—DEBUG1 • 8—DEBUG2 • 9—DEBUG3 |

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

| Release | Modification |
|----------------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage Guidelines None.

Example

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

shutdown

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

This command has no keywords and arguments.

Command Default No default behavior or values.

Command Modes Configuration (config-GigabitEthernet)#

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

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

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

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

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

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

Example

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

snmp-server enable

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

snmp-server enable

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

| | |
|------------------------|-----------------------------|
| Command Default | The SNMP server is enabled. |
|------------------------|-----------------------------|

| | |
|----------------------|-------------------------|
| Command Modes | Configuration (config)# |
|----------------------|-------------------------|

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

Example

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

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 | user | Configure a new user. |
|--------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <i>username</i> | The name of the user on the host that belongs to the SNMP agent. |
| | v3 | Version of the SNMP used to send the traps. Specifies that the SNMP Version 3 security model should be used for enabling the priv and the auth keywords. |
| | { hash plain } | Password is in encrypted or plain format. Encrypted passwords must be in hexadecimal format. |
| | | |

auth-password

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

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.

priv-password

Specifies the encryption user password. 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.

Command Default

Disabled.

Command Modes

Configuration (config)#

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage Guidelines

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

Example

```
ise/admin(config)# snmp-server user testuser v3 hash 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*} **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.

Syntax Description

| | |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host | Configures hosts to receive SNMP notifications. |
| <i>ip-address</i> | IP address of the SNMP notification host. Supports up to 32 alphanumeric characters. |
| <i>hostname</i> | Name of the SNMP notification host. Supports up to 32 alphanumeric characters. |
| version { <i>1</i> <i>2c</i> <i>3</i> } | (Optional). Version of the SNMP used to send the traps. Default = 1. If you use the version keyword, specify one of the following keywords: <ul style="list-style-type: none"> • 1—SNMPv1. • 2c—SNMPv2C. • 3—SNMP v3. |
| <i>community</i> | 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 "public." Cisco ISE uses this key to determine whether the incoming SNMP request is valid. |
| <i>username</i> | (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. |

| | |
|----------------------|----------------------------------------------------------------------------------------------------|
| <i>engine_ID</i> | (Optional; required only if you choose SNMP version 3) Remote EngineID. |
| <i>auth-password</i> | (Optional; required only if you choose SNMP version 3) Specifies the authentication user password. |
| <i>priv-password</i> | (Optional; required only if you choose SNMP version 3) Specifies the encryption user password. |

Command Default

Enabled.

Command Modes

Configuration (config)#

Command History

| Release | Modification |
|-----------|------------------------------|
| 2.0.0.306 | This command was introduced. |

Usage Guidelines

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

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

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 isel version 2c public
ise/admin(config)# snmp-server community public ro
2012-09-24T18:37:59.263276+00:00 isel snmptrapd[29534]: isel.cisco.com [UDP:
[192.168.118.108]:44474]: Trap ,
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (29) 0:00:00.29, SNMPv2-MIB::snmpTrapOID.0
= OID: SNMPv2-MIB::coldStart,
SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
ise/admin(config)# snmp-server contact admin@cisco.com
2012-09-24T18:43:32.094128+00:00 isel snmptrapd[29534]: isel.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 | community | Sets SNMP community string. |
| | <i>community-string</i> | Accessing string that functions much like a password and allows access to SNMP. No blank spaces allowed. Supports up to 255 alphanumeric characters. |
| | ro | Specifies read-only access. |
| Command Default | No default behavior or values. | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | <p>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:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Product ID: entPhysicalModelName • Version ID: entPhysicalHardwareRev • Serial Number: entPhysicalSerialNumber • DISMAN-EVENT-MIB • NOTIFICATION-LOG-MIB • CISCO-CDP-MIB | |

Example

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

snmp-server contact

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

snmp-server contact *contact-name*

| | | |
|---------------------------|--------------------------------|---------------------------------------------------------------------------------------------------------------|
| Syntax Description | contact | Identifies the contact person for this managed node. Supports up to 255 alphanumeric characters. |
| | <i>contact-name</i> | String that describes the system contact information of the node. Supports up to 255 alphanumeric characters. |
| Command Default | No default behavior or values. | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | None. | |

Example

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

snmp-server location

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

snmp-server location *location*

| | | |
|---------------------------|--------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Syntax Description | location | Configures the physical location of this managed node. Supports up to 255 alphanumeric characters. |
| | <i>location</i> | String that describes the physical location information of the system. Supports up to 255 alphanumeric characters. |
| Command Default | No default behavior or values. | |
| Command Modes | Configuration (config)# | |

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 2.0.0.306 | This command was introduced. |

| | |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usage Guidelines | Cisco recommends that you use underscores (_) or hyphens (-) between the terms within the <i>word</i> string. If you use spaces between terms within the <i>word</i> string, you must enclose the string in quotation marks (“”). |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Example 1

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

Example 2

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

snmp-server trap dskThresholdLimit

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

snmp-server trap dskThresholdLimit *value*

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

| Syntax Description | <i>value</i> | Number that represents the percentage of available disk space. The value ranges from 1 to 100. |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Command Default | No default behavior or values. | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.1.0.474 | This command was introduced. |
| Usage Guidelines | <p>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.</p> <p>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.</p> | |

Example

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

snmp engineid

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

snmp engineid *engine_ID_string*

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

| | | |
|---------------------------|-------------------------|----------------------------------------------------------------|
| Syntax Description | engineid | Changes an existing engine ID to a new value that you specify. |
| | <i>engine_ID_string</i> | String of maximum 24 characters that identifies the engine ID. |
| Command Default | No command defaults. | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

Example

```
ise/admin(config)# snmp engineid Abcdef129084B
% Warning: As a result of engineID change, all SNMP users will need
           to be recreated.
ise/admin(config)#
```

synflood-limit

To configure a TCP SYN packet rate limit.

synflood-limit ?

| | | |
|---------------------------|--------------------------------|------------------------------------------------------|
| Syntax Description | synflood-limit | Average number of TCP SYN packets per second allowed |
| | ? | 1-2147483647 (Range for TCP SYN packets). |
| Command Default | No default behavior or values. | |

| | |
|----------------------|-------------------------|
| Command Modes | Configuration (config)# |
|----------------------|-------------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |

| | |
|-------------------------|--------------------------------------------------------------------------|
| Usage Guidelines | Use this synflood-limit to configure a TCP SYN packet rate limit. |
|-------------------------|--------------------------------------------------------------------------|

Example 1

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

username

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

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

For an existing user, use the following command option:

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

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

| | |
|------------------------|--------------------------------|
| Command Default | The initial user during setup. |
|------------------------|--------------------------------|

| | |
|----------------------|-------------------------|
| Command Modes | Configuration (config)# |
|----------------------|-------------------------|

| Command History | Release | Modification |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | <p>The username command requires that the username and password keywords precede the hash / plain and the admin / user options.</p> <p>Example 1</p> <pre>ise/admin(config)# username admin password hash ##### role admin ise/admin(config)#</pre> <p>Example 2</p> <pre>ise/admin(config)# username admin password plain Secr3tp@swd role admin ise/admin(config)#</pre> <p>Example 3</p> <pre>ise/admin(config)# username admin password plain Secr3tp@swd role admin email admin123@mydomain.com ise/admin(config)#</pre> | |

which

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

which

| | | |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Syntax Description | This command has no keywords and arguments. | |
| Command Default | No default behavior or values. | |
| Command Modes | Configuration (config)# | |
| Command History | Release | Modification |
| | 2.0.0.306 | This command was introduced. |
| Usage Guidelines | <p>which is a hidden command. Although which is available in Cisco ISE, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.</p> <p>Example</p> <p>The following example shows the output of which :</p> <pre>ise/admin(config)# which [1]. application configure<STRING> [2]. application install<STRING><STRING></pre> | |

which

```
[ 3]. application remove<STRING>
[ 4]. application reset-config<STRING>
[ 5]. application reset-passwd<STRING><STRING>
[ 6]. application start<STRING>
[ 7]. application start<STRING> safe
[ 8]. application stop<STRING>
[ 9]. application upgrade cleanup
[10]. application upgrade prepare<STRING><STRING>
```