THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMA-
TION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS 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.

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: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface ix
  Purpose ix
  Who Should Refer This Guide ix
  How To Use This Guide x
  How This Guide Is Organized x
  Document Conventions x
  Related Documentation xii
  Obtaining Documentation and Submitting a Service Request xiii

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 10
      Monitoring Database Settings 11
      Live Statistics of Profiling Events 13
      Export and Import Internal CA Store 13
      Create Missing Indexes 15
Enable ACS Migration 16

application remove 17
application reset-config 18
application reset-passwd 19
application start 20
application stop 23
application upgrade 24
backup 27

Backing up Cisco ISE Configuration Data 29
Backing up Cisco ISE Operational Data 29
backup-logs 29
clock 31
configure 32
copy 33

Running Configuration 35

Copying Running Configuration to a Remote Location 36
Copying Running Configuration from a Remote Location 36

Startup configuration 36

Copying Startup Configuration to a Remote Location 36
Copying Startup Configuration from a Remote Location 36

Copying Log files 37
crypto 37
debug 39
delete 43
dir 43
exit 45
forceout 45
halt 46
help 46
mkdir 47
nslookup 48
password 49
patch install 50
patch remove 51
ping 52
ping6  53
reload  55
restore  56

    Restoring Cisco ISE Configuration Data from the Backup  57
    Restoring Cisco ISE Operational Data from the Backup  59
    Restoring Cisco ISE Configuration Data and Cisco ADE OS data from the Backup  59
rmdir  60
ssh  61
tech  62
telnet  64
terminal length  64
terminal session-timeout  65
terminal session-welcome  66
terminal terminal-type  66
traceroute  67
undebug  67
write  70

C H A P T E R  3  
Cisco ISE CLI Commands in EXEC Show Mode  71

    show  72
    show application  72
    show backup  75
    show banner  76
    show cdp  76
    show clock  77
    show crypto  78
    show disks  79
    show icmp-status  80
    show interface  82
    show inventory  83
    show ip  84
    show logging  85
    show logins  87
    show memory  88
    show ntp  88
show ports 89
show process 91
show repository 92
show restore 93
show running-config 94
show startup-config 95
show tech-support 96
show terminal 97
show timezone 98
show timezones 98
show udi 99
show uptime 100
show users 101
show version 102

Chapter 4
Cisco ISE CLI Commands in Configuration Mode 105
Switch to Configuration Mode in EXEC Mode 106
Configuring Cisco ISE in the Configuration Mode 107
Configuring Cisco ISE in the Configuration Submode 108
CLI Configuration Command Default Settings 108
cdp holdtime 108
cdp run 109
cdp timer 110
clock timezone 111
   Restoring the Time Zone in Cisco ISE Nodes 112
   Common Time Zones 113
   Australia Time Zones 113
   Asia Time Zones 114
conn-limit 115
do 115
end 118
exit 119
hostname 119
icmpecho 121
interface 121
Preface

• Purpose, page ix
• Who Should Refer This Guide, page ix
• How To Use This Guide, page x
• How This Guide Is Organized, page x
• Document Conventions, page x
• Related Documentation, page xii
• Obtaining Documentation and Submitting a Service Request, page xiii

Purpose

This guide describes how you can configure and maintain Cisco Identity Services Engine (Cisco ISE) using the command-line interface (CLI). Each command topic provides details on how to use the Cisco ISE CLI in Cisco Application Deployment Engine (ADE) OS Release 3.0, which runs on supported appliances.

There is no ISO image for Inline Posture in Release 1.3. You can continue to use your Release 1.2 Inline Posture nodes in the new deployment. See the Cisco Identity Services Engine CLI Reference Guide, Release 1.2 for information on how to install Inline Posture nodes with Release 1.2 image and how to configure certificates on these nodes.

Throughout this guide, the term Admin portal, refers to the user interface of the Primary Administration Node.

Who Should Refer This Guide

Cisco ISE CLI administrators and users with appropriate privileges can use this CLI reference guide. The majority of the commands in this guide are straightforward; however, a few are complex. Therefore, only experienced users should use these commands.

Note

Use this guide in conjunction with the documentation listed in Related Documentation.
How To Use This Guide

• Refer the document in its entirety. Subsequent sections build on information and recommendations discussed in previous sections.

• Use this document for all-inclusive information about Cisco ISE when running the CLI commands.

• Do not vary the command-line conventions described in Document Conventions.

How This Guide Is Organized

• Chapter 1, Cisco ISE Command-Line Interface—Provides an overview of the Cisco ISE CLI environment and command modes

• Chapter 2, Cisco ISE CLI Commands in EXEC Mode—Provides a brief description of its use in EXEC mode, command syntax, usage guidelines, and one or more examples

• Chapter 3, Cisco ISE CLI Commands in EXEC Show Mode—Provides a brief description of its use in EXEC show mode, command syntax, usage guidelines, and one or more examples

• Chapter 4, Cisco ISE CLI Commands in Configuration Mode—Provides a brief description of its use in Configuration mode, command syntax, usage guidelines, and one or more examples

Document Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (help)</td>
<td>Lists available commands and description at the command prompt for all modes (Exec, Exec show, and Configuration modes), keywords, and arguments with description for each command.</td>
</tr>
<tr>
<td>&lt;cr&gt;</td>
<td>Carriage return. Press Enter to complete the command.</td>
</tr>
<tr>
<td>Tab</td>
<td>Completes the partial commands and keywords entered at the command prompt.</td>
</tr>
<tr>
<td>Ctrl-C</td>
<td>Aborts any executing command and returns to the previous mode.</td>
</tr>
<tr>
<td>End, Exit, Ctrl-Z</td>
<td>Exits configuration mode and returns to the previous mode.</td>
</tr>
<tr>
<td>ise</td>
<td>Host name of the Cisco ISE server.</td>
</tr>
<tr>
<td>admin</td>
<td>CLI administrator account.</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><em>Italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
<tr>
<td>[x]</td>
<td>Keywords or arguments in square brackets are optional.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts appear in square brackets.</td>
</tr>
<tr>
<td></td>
<td>A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
<tr>
<td><strong>Courier font</strong></td>
<td>Examples of screen displays, prompts and scripts in a monospace, fixed width font.</td>
</tr>
<tr>
<td><strong>Bold Courier font</strong></td>
<td>Examples of information you enter.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters (for example, passwords) appear in angle brackets.</td>
</tr>
</tbody>
</table>

**Reader Alert Conventions**

This document uses the following conventions for reader alerts:

- **Note**
  Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

- **Tip**
  Means *the following information will help you solve a problem, or could be some useful information.*
Caution
Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Timesaver
Means the described action saves time. You can save time by performing the action described in the paragraph.

Warning
Means reader be warned. In this situation, you might perform an action that could result in bodily injury.

Related Documentation

Release-Specific Documents

Table 1: Product Documentation for Cisco Identity Services Engine

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Identity Services Engine Upgrade Guide, Release 1.3</td>
<td></td>
</tr>
<tr>
<td>Cisco Identity Services Engine, Release 1.3 Migration Tool Guide</td>
<td></td>
</tr>
<tr>
<td>Regulatory Compliance and Safety Information for Cisco Identity Services Engine 3400 Series Appliance and Cisco 3400 Secure Access Control System</td>
<td></td>
</tr>
</tbody>
</table>
Platform-Specific Documents

Links to other platform-specific documentation are available at the following locations:

<table>
<thead>
<tr>
<th>Platform-Specific Documents</th>
<th>URL</th>
</tr>
</thead>
</table>

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.
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, page 1
- Cisco ISE CLI Administrator Account, page 3
- Cisco ISE CLI User Accounts, page 3
- Cisco ISE CLI User Account Privileges, page 3
- Supported Hardware and Software Platforms for Cisco ISE CLI, 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 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 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
• telnet
• 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

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, page 8
- application install, page 8
- application configure, page 10
- application remove, page 17
- application reset-config, page 18
- application reset-passwd, page 19
- application start, page 20
- application stop, page 23
- application upgrade, page 24
- backup, page 27
- backup-logs, page 29
- clock, page 31
- configure, page 32
- copy, page 33
- crypto, page 37
- debug, page 39
- delete, page 43
- dir, page 43
- exit, page 45
- forceout, page 45
- halt, page 46
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>install</td>
<td>Installs a specific application.</td>
</tr>
<tr>
<td>application-bundle</td>
<td>Application bundle filename. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td>remote-repository-name</td>
<td>Remote repository name. Supports up to 255 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

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

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

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

**Example**

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

**Related Topics**

- application configure, on page 10
- application remove, on page 17
- application reset-config, on page 18
- application reset-passwd, on page 19
- application start, on page 20
- application stop, on page 23
- application upgrade, on page 24
- show application, on page 72
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

application [ configure {application-name}]}

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

You can use this command to update M&T databases and indexes, and export and import Cisco ISE CA certificates and keys, in a Cisco ISE node.

Example

ise/admin# application configure ise
Selection ISE configuration option
[1] Reset M&T Session Database
[2] Rebuild M&T Unusable Indexes
[3] Purge M&T Operational Data
[4] Reset M&T Database
[7] Export Internal CA Store
[8] Import Internal CA Store
[9] Create Missing Config Indexes
[10] Create Missing M&T Indexes
[12] Exit

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

Related Topics

application install, on page 8
application remove, on page 17
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.
- To rebuild unusable indexes in the monitoring database, use the option 2.
- To purge monitoring operational data, use the option 3.
- To reset the monitoring database, use the option 4.
- To refresh the monitoring database statistics, use the option 5.

**Example**

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

```
ise/admin# application configure ise
Selection ISE configuration option
[1] Reset M&T Session Database
[2] Rebuild M&T Unusable Indexes
[3] Purge M&T Operational Data
[4] Reset M&T Database
[7] Export Internal CA Store
[8] Import Internal CA Store
[9] Create Missing Config Indexes
[10] Create Missing M&T Indexes
[12] 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.
You are about to Refresh Database statistics
Are you sure you want to proceed? y/n [n]: y
Starting to terminate long running DB sessions
Completed terminating long running DB sessions

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

Live Statistics of Profiling Events

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

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

Example

```
ise/admin$ application configure ise
Selection ISE configuration option
[1] Reset M&T Session Database
[2] Rebuild M&T Unusable Indexes
[3] Purge M&T Operational Data
[4] Reset M&T Database
[7] Export Internal CA Store
[8] Import Internal CA Store
[9] Create Missing Config Indexes
[10] Create Missing M&T Indexes
[12] Exit
```

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 ise
Selection ISE configuration option
[1] Reset M&T Session Database
[2] Rebuild M&T Unusable Indexes
[3] Purge M&T Operational Data
[4] Reset M&T Database
[7] Export Internal CA Store
[8] Import Internal CA Store
[9] Create Missing Config Indexes
[10] Create Missing M&T Indexes
[12] 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 OCSP Responder Certificate - ise60
  Issuer:CN=Certificate Services Root CA - ise60
  Serial#:0x0ad3cccdf-b64842ad-93dd5826-0b27cbd2

ISE CA keys export completed successfully
```

**Example 2**

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

```
ise/admin# application configure ise
Selection ISE configuration option
[1] Reset M&T Session Database
[2] Rebuild M&T Unusable Indexes
[3] Purge M&T Operational Data
[4] Reset M&T Database
[7] Export Internal CA Store
[8] Import Internal CA Store
[9] Create Missing Config Indexes
[10] Create Missing M&T Indexes
[12] Exit

8
Import Repository Name: sftp
Enter encryption-key for import: Test1234
Import on progress..............
ISE CA keys import completed successfully
```
Import Repository Name: sftp
Enter CA keys file name to import: ise_ca_key_pairs_of_ise60
Enter encryption-key: Test1234
Import on progress...............

The following 4 CA key pairs were imported:
  Subject:CN=Certificate Services Root CA - ise60
  Issuer:CN=Certificate Services Root CA - ise60
  Serial#:0x66cfded7-2f384979-9110c0e1-50dbf656
  Subject:CN=Certificate Services Endpoint Subordinate CA - ise60
  Issuer:CN=Certificate Services Root CA - ise60
  Serial#:0x20ff700b-d5844ef8-a029bf7d-fad64289
  Subject:CN=Certificate Services Endpoint RA - ise60
  Issuer:CN=Certificate Services Endpoint Subordinate CA - ise60
  Serial#:0x483542bd-1f1642f4-ba71b338-8f606ee4
  Subject:CN=Certificate Services OCSP Responder Certificate - ise60
  Issuer:CN=Certificate Services Root CA - ise60
  Serial#:0x0ad3ccdf-b64842ad-93dd5826-0b27cbd2

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

Create Missing Indexes

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

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

**Example 1**

To create the CEPM database index, use option 9.

```
ise/admin# application configure ise
Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Exit

9
You are about to create missing config indexes.
Are you sure you want to proceed? y/n [n]: y
Starting to create missing config indexes
Completed creating missing config indexes
```
Example 2

To create missing Monitoring database indexes, use option 10.

ise/admin# application configure ise
Selection ISE configuration option
[1] Reset M&T Session Database
[2] Rebuild M&T Unusable Indexes
[3] Purge M&T Operational Data
[4] Reset M&T Database
[7] Export Internal CA Store
[8] Import Internal CA Store
[9] Create Missing Config Indexes
[10] Create Missing M&T Indexes
[12] Exit

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

Enable ACS Migration

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

Note
Cisco ISE, Release 1.3 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
[7] Export Internal CA Store
[8] Import Internal CA Store
[9] Create Missing Config Indexes
[10] Create Missing M&T Indexes
[12] 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.
application remove

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

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

application [ remove {application-name}]

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

no application [ remove {application-name}]

Syntax Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>remove</td>
<td>Removes or uninstalls an application.</td>
</tr>
<tr>
<td>application-name</td>
<td>Application name. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>Removes or uninstalls an application.</td>
</tr>
</tbody>
</table>

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Removes or uninstalls an application.

Example

ise/admin# application remove ise
Continue with application removal? [y/n] y
Application successfully uninstalled
ise/admin#

Related Topics

application configure, on page 10
application install, on page 8
application reset-config, on page 18
application reset-passwd, on page 19
application start, on page 20
application stop, on page 23
application upgrade, on page 24
show application, on page 72
application reset-config

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

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

**Note**

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

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

**Example**

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

```
ise/admin# application reset-config ise
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...
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...
Enter the ISE administrator username to create[admin]: 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...
Performing ISE database priming...
application reset-config is success
ise/admin#

Related Topics

- application configure, on page 10
- application install, on page 8
- application remove, on page 17
- application start, on page 20
- application stop, on page 23
- application upgrade, on page 24
- show application, on page 72

---

**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. You can also use this command to reset the Cisco ISE database administrator and user passwords.

```
application [ reset-passwd {application-name} {administrator-ID | internal-database-admin | internal-database-user} ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reset-passwd</td>
<td>Resets the administrator account password.</td>
</tr>
<tr>
<td>application-name</td>
<td>Application name. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td>administrator-ID</td>
<td>Name of a disabled administrator account for which you want to reset the password.</td>
</tr>
<tr>
<td>internal-database-admin</td>
<td>Identifies the Cisco ISE database system-level password. You must create this password (there is no default). The password must be a minimum of 11 characters in length and include at least one lowercase letter, at least one uppercase letter, and at least one number (0-9).</td>
</tr>
<tr>
<td>internal-database-user</td>
<td>Identifies the Cisco ISE database access-level password. You must create this password (there is no default). The password must be a minimum of 11 characters in length and include at least one lowercase letter, at least one uppercase letter, and at least one number (0 to 9).</td>
</tr>
</tbody>
</table>
internal-comm-user

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

**Command Modes**
EXEC

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

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

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

Typically, you need to specify the Cisco ISE database administrator and user passwords only once during an initial configuration or upgrade. If it is necessary to change either of these passwords later, you can use the `application reset-passwd` command.

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#
```

**Related Topics**

- application configure, on page 10
- application install, on page 8
- application remove, on page 17
- application reset-config, on page 18
- application start, on page 20
- application stop, on page 23
- application upgrade, on page 24
- show application, on page 72

**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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

EXEC

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

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

Example 1

```bash
test-admin# application start ise
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.
```

```bash
test-admin# show application status ise

<table>
<thead>
<tr>
<th>ISE PROCESS NAME</th>
<th>STATE</th>
<th>PROCESS ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Listener</td>
<td>running</td>
<td>30171</td>
</tr>
<tr>
<td>Database Server</td>
<td>running</td>
<td>33 PROCESSES</td>
</tr>
<tr>
<td>Application Server</td>
<td>initializing</td>
<td></td>
</tr>
<tr>
<td>Profiler Database</td>
<td>running</td>
<td>31315</td>
</tr>
<tr>
<td>AD Connector</td>
<td>running</td>
<td>1732</td>
</tr>
<tr>
<td>M&amp;T Session Database</td>
<td>running</td>
<td>31225</td>
</tr>
<tr>
<td>M&amp;T Log Collector</td>
<td>running</td>
<td>1625</td>
</tr>
<tr>
<td>M&amp;T Log Processor</td>
<td>running</td>
<td>1584</td>
</tr>
<tr>
<td>Certificate Authority Service</td>
<td>running</td>
<td>1532</td>
</tr>
</tbody>
</table>
```
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...
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/admin# application start ise safe

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/admin#

Related Topics

application configure, on page 10
application install, on page 8
application remove, on page 17
application stop

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

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

### Syntax Description

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

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Usage Guidelines

Disables an application.

### 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  
```

<table>
<thead>
<tr>
<th>ISE PROCESS NAME</th>
<th>STATE</th>
<th>PROCESS ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Listener</td>
<td>not running</td>
<td></td>
</tr>
<tr>
<td>Application Server</td>
<td>not running</td>
<td></td>
</tr>
<tr>
<td>Profiler Database</td>
<td>not running</td>
<td></td>
</tr>
<tr>
<td>AD Connector</td>
<td>not running</td>
<td></td>
</tr>
<tr>
<td>M&amp;T Session Database</td>
<td>not running</td>
<td></td>
</tr>
<tr>
<td>M&amp;T Log Collector</td>
<td>not running</td>
<td></td>
</tr>
<tr>
<td>M&amp;T Log Processor</td>
<td>not running</td>
<td></td>
</tr>
<tr>
<td>Certificate Authority Service</td>
<td>disabled</td>
<td></td>
</tr>
</tbody>
</table>
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**

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

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

Upgrades an application, and preserves any application configuration data. See the *Cisco Identity Services Engine Upgrade Guide* for more information.
• Use the **cleanup** option, if you want to try another upgrade bundle in case of a failure or use a different version.

• Use the **prepare** option to download and extract an upgrade bundle locally.

• Use the **proceed** option to upgrade Cisco ISE using the upgrade bundle you extracted with the prepare option. You can use this option after preparing an upgrade bundle instead of using the application upgrade command directly.
  
  ◦ If upgrade is successful, this option removes the upgrade bundle.
  
  ◦ If upgrade fails for any reason, this option retains the upgrade bundle.

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

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

⚠️ **Caution**

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

⚠️ **Note**

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

---

**Example 1**

```
ise/admin# application upgrade prepare ise-upgradebundle=1.2.x-to-1.3.0.693.x86_64.tar.gz
upgrade
Getting bundle to local machine...
md5: de9e7c83679897f792ad3e9f74879c51
sha256: e3358ca424d977af67f88b2bb3574b3e559ce9578d2f36c44cd8ba9e6dddef6
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y]Y
Getting bundle to local machine...
md5: de9e7c83679897f792ad3e9f74879c51
sha256: e3358ca424d977af67f88b2bb3574b3e559ce9578d2f36c44cd8ba9e6dddef6
```

**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 DB schema upgrade...
- Running db sanity check to fix index corruption, if any...
ISE Database schema upgrade completed.
STEP 6: Running ISE configuration data upgrade...
- Data upgrade step 1/59, NSFUpgradeService(1.2.1.127)... Done in 0 seconds.
- Data upgrade step 2/59, NetworkAccessUpgrade(1.2.1.127)... Done in 0 seconds.
```
- Data upgrade step 3/59, GuestUpgradeService(1.2.1.146)... Done in 50 seconds.
- Data upgrade step 4/59, NetworkAccessUpgrade(1.2.1.148)... Done in 2 seconds.
- Data upgrade step 5/59, NetworkAccessUpgrade(1.2.1.150)... Done in 2 seconds.
- Data upgrade step 6/59, NSFUpgradeService(1.3.0.100)... Done in 0 seconds.
- Data upgrade step 7/59, RegisterPostureTypes(1.3.0.170)... Done in 0 seconds.
- Data upgrade step 8/59, ProfilerUpgradeService(1.3.0.187)... Done in 5 seconds.
- Data upgrade step 9/59, GuestUpgradeService(1.3.0.194)... Done in 2 seconds.
- Data upgrade step 10/59, NetworkAccessUpgrade(1.3.0.200)... Done in 2 seconds.
- Data upgrade step 11/59, GuestUpgradeService(1.3.0.208)... Done in 2 seconds.
- Data upgrade step 12/59, GuestUpgradeService(1.3.0.250)... Done in 0 seconds.
- Data upgrade step 13/59, RBACUpgradeService(1.3.0.250)... Done in 15 seconds.
- Data upgrade step 14/59, NetworkAccessUpgrade(1.3.0.250)... Done in 3 seconds.
- Data upgrade step 15/59, GuestUpgradeService(1.3.0.250)... Done in 0 seconds.
- Data upgrade step 16/59, NetworkAccessUpgrade(1.3.0.250)... Done in 0 seconds.
- Data upgrade step 17/59, RBACUpgradeService(1.3.0.334)... Done in 9 seconds.
- Data upgrade step 18/59, RBACUpgradeService(1.3.0.335)... Done in 9 seconds.
- Data upgrade step 19/59, ProfileUpgradeService(1.3.0.380)... Done in 215 seconds.
- Data upgrade step 20/59, ProfileUpgradeService(1.3.0.380)... Done in 0 seconds.
- Data upgrade step 21/59, NSFUpgradeService(1.3.0.401)... Done in 0 seconds.
- Data upgrade step 22/59, NSFUpgradeService(1.3.0.406)... Done in 0 seconds.
- Data upgrade step 23/59, NSFUpgradeService(1.3.0.410)... Done in 1 seconds.
- Data upgrade step 24/59, RBACUpgradeService(1.3.0.423)... Done in 0 seconds.
- Data upgrade step 25/59, NetworkAccessUpgrade(1.3.0.424)... Done in 0 seconds.
- Data upgrade step 26/59, RBACUpgradeService(1.3.0.433)... Done in 1 seconds.
- Data upgrade step 27/59, EgressUpgradeService(1.3.0.437)... Done in 0 seconds.
- Data upgrade step 28/59, NSFUpgradeService(1.3.0.438)... Done in 0 seconds.
- Data upgrade step 29/59, NSFUpgradeService(1.3.0.439)... Done in 0 seconds.
- Data upgrade step 30/59, CsdbRegistration(1.3.0.446)... Done in 2 seconds.
- Data upgrade step 31/59, RBACUpgradeService(1.3.0.452)... Done in 17 seconds.
- Data upgrade step 32/59, NetworkAccessUpgrade(1.3.0.458)... Done in 0 seconds.
- Data upgrade step 33/59, NSFUpgradeService(1.3.0.461)... Done in 0 seconds.
- Data upgrade step 34/59, CertMgmtUpgradeService(1.3.0.462)... Done in 0 seconds.
- Data upgrade step 35/59, NetworkAccessUpgrade(1.3.0.476)... Done in 0 seconds.
- Data upgrade step 36/59, NSFUpgradeService(1.3.0.508)... Done in 0 seconds.
- Data upgrade step 37/59, RBACUpgradeService(1.3.0.509)... Done in 17 seconds.
- Data upgrade step 38/59, NSFUpgradeService(1.3.0.526)... Done in 0 seconds.
- Data upgrade step 39/59, NSFUpgradeService(1.3.0.531)... Done in 0 seconds.
- Data upgrade step 40/59, MDMUpgradeService(1.3.0.536)... Done in 0 seconds.
- Data upgrade step 41/59, NSFUpgradeService(1.3.0.554)... Done in 0 seconds.
- Data upgrade step 42/59, NetworkAccessUpgrade(1.3.0.561)... Done in 4 seconds.
- Data upgrade step 43/59, RBACUpgradeService(1.3.0.563)... Done in 20 seconds.
- Data upgrade step 44/59, CertMgmtUpgradeService(1.3.0.615)... Done in 0 seconds.
- Data upgrade step 45/59, CertMgmtUpgradeService(1.3.0.616)... Done in 22 seconds.
- Data upgrade step 46/59, CertMgmtUpgradeService(1.3.0.617)... Done in 2 seconds.
- Data upgrade step 47/59, OcspServiceUpgradeRegistration(1.3.0.617)... Done in 0 seconds.
- Data upgrade step 48/59, NSFUpgradeService(1.3.0.630)... Done in 0 seconds.
- Data upgrade step 49/59, NSFUpgradeService(1.3.0.631)... Done in 0 seconds.
- Data upgrade step 50/59, CertMgmtUpgradeService(1.3.0.634)... Done in 0 seconds.
- Data upgrade step 51/59, RBACUpgradeService(1.3.0.650)... Done in 8 seconds.
- Data upgrade step 52/59, CertMgmtUpgradeService(1.3.0.653)... Done in 0 seconds.
- Data upgrade step 53/59, NodeGroupUpgradeService(1.3.0.659)... Done in 1 seconds.
- Data upgrade step 54/59, RBACUpgradeService(1.3.0.670)... Done in 4 seconds.
- Data upgrade step 55/59, ProfilerUpgradeService(1.3.0.670)... Done in 0 seconds.
- Data upgrade step 56/59, NSFUpgradeService(1.3.0.676)... Done in 0 seconds.
- Data upgrade step 57/59, AuthzUpgradeService(1.3.0.676)... Done in 10 seconds.
- Data upgrade step 58/59, GuestAccessUpgradeService(1.3.0.676)... Done in 231 seconds.
- Data upgrade step 59/59, ProvisioningUpgradeService(1.3.105.181)... Done in 51 seconds.

STEP 7: Running ISE configuration data upgrade for node specific data...
STEP 8: Running ISE M&T DB upgrade...
ISE Database Mnt schema upgrade completed.

Gathering Config schema(CEPM) stats .......
Gathering Operational schema(MNT) stats ......
Stopping ISE Database processes...

% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS. During this time
progress of the upgrade is visible on console. It could take up to 30 minutes for this to
complete.
Rebooting to do Identity Service Engine upgrade...

Related Topics
application configure, on page 10
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 {encryption-key name}]  
backup [{backup-name} repository {repository-name} ise-operational encryption-key {encryption-key name}]  
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup-name</td>
<td>Name of backup file. Supports up to 100 alphanumeric characters.</td>
</tr>
<tr>
<td>repository</td>
<td>Specifies repository to store the backup file.</td>
</tr>
<tr>
<td>repository-name</td>
<td>Location where the files should be backed up to. Supports up to 80 alphanumeric characters.</td>
</tr>
<tr>
<td>ise-config</td>
<td>Backs up Cisco ISE configuration data (includes Cisco ISE ADE-OS).</td>
</tr>
<tr>
<td>ise-operational</td>
<td>Backs up Cisco ISE operational data.</td>
</tr>
<tr>
<td>encryption-key</td>
<td>Specifies user-defined encryption key to protect the backup.</td>
</tr>
<tr>
<td>hash</td>
<td>Specifies (Hashed encryption key for protection of backup) an encrypted (hashed) encryption key that follows. Supports up to 40 characters.</td>
</tr>
<tr>
<td>plain</td>
<td>Specifies (Plaintext encryption key for protection of backup) an unencrypted plaintext encryption key that follows. Supports up to 15 characters.</td>
</tr>
<tr>
<td>encryption-key name</td>
<td>An encryption key in hash</td>
</tr>
</tbody>
</table>
**Command Default**
No default behavior or values.

**Command Modes**
EXEC

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

You can back up Cisco ISE operational data only from the primary or secondary Monitoring nodes.

---

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

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

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

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

---

**Related Topics**
- backup-logs, on page 29
- repository, on page 148
- restore, on page 56
- show backup, on page 75
- show repository, on page 92
- show restore, on page 93
Backing up Cisco ISE Configuration Data

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

```
backup mybackup repository myrepository ise-config encryption-key plain lablab12
```

Example

```
ise/admin# backup test repository disk ise-config encryption-key plain Test_1234
```

```
Internal CA Store is not included in this backup. It is recommended to export it using "application configure ise" CLI command
Creating backup with timestamped filename: test-CFG-141006-1350.tar.gpg
```

```
backup in progress: Starting Backup...10% completed
```

```
backup in progress: Validating ISE Node Role...15% completed
```

```
backup in progress: Backing up ISE Configuration Data...20% completed
```

```
backup in progress: Backing up ISE Logs...45% completed
```

```
backup in progress: Completing ISE Backup Staging...50% completed
```

```
backup in progress: Backing up ADEOS configuration...55% completed
```

```
backup in progress: Moving Backup file to the repository...75% completed
```

```
backup in progress: Completing Backup...100% completed
```

ise/admin#

Backing up Cisco ISE Operational Data

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

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

Example

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

```
backup in progress: Starting Backup...10% completed
```

```
Creating backup with timestamped filename: mybackup-OPS-130103-0019.tar.gpg
```

```
backup in progress: starting dbbackup using expdp.......20% completed
```

```
backup in progress: starting cars logic.......50% completed
```

```
backup in progress: Moving Backup file to the repository...75% completed
```

```
backup in progress: Completing Backup...100% completed
```

ise/admin#

backup-logs

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

Note

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

```
backup-logs backup-name repository repository-name {encryption-key { hash | plain } encryption-key name}
```
### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>backup-name</code></td>
<td>Name of one or more files to back up. Supports up to 100 alphanumeric characters.</td>
</tr>
<tr>
<td><code>repository</code></td>
<td>Repository command.</td>
</tr>
<tr>
<td><code>repository-name</code></td>
<td>Location where files should be backed up to. Supports up to 80 alphanumeric characters.</td>
</tr>
<tr>
<td><code>encryption-key</code></td>
<td>Specifies the encryption key to protect the backup logs.</td>
</tr>
<tr>
<td><code>hash</code></td>
<td>Hashed encryption key for protection of backup logs. Specifies an encrypted (hashed) encryption key that follows. Supports up to 40 characters.</td>
</tr>
<tr>
<td><code>plain</code></td>
<td>Plaintext encryption key for protection of backup logs. Specifies an unencrypted plaintext encryption key that follows. Supports up to 15 characters.</td>
</tr>
<tr>
<td><code>encryption-key name</code></td>
<td>The encryption key in hash or plain format.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Usage Guidelines

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

### Example 1

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

### Related Topics

- backup, on page 27
- restore, on page 56
- repository, on page 148
- show backup, on page 75
- show restore, on page 93
clock

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

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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

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

Caution

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#
```

Related Topics

- `show clock`, on page 77

configure

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

configure terminal

Syntax Description

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

Command Default

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

EXEC

**Usage Guidelines**

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

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

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

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

**Example**

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

**Related Topics**

- `show running-config`, on page 94
- `show startup-config`, on page 95

---

**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.

---

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>running-config</code></td>
<td>Represents the current running configuration file.</td>
</tr>
<tr>
<td><code>startup-config</code></td>
<td>Represents the configuration file used during initialization (startup).</td>
</tr>
<tr>
<td><code>protocol</code></td>
<td>Destination for copying. See Table 2-1 for protocol keyword options.</td>
</tr>
<tr>
<td><code>hostname</code></td>
<td>Hostname of destination.</td>
</tr>
<tr>
<td><code>location</code></td>
<td>Location of destination.</td>
</tr>
<tr>
<td><code>logs</code></td>
<td>The system log files.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Copies all Cisco ISE log files from the system to another location. All logs are packaged as <code>iselogs.tar.gz</code> and transferred to the specified directory on the remote host.</td>
</tr>
</tbody>
</table>
**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.

**log_filename**

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

**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) or Secure Copy (SCP) error messages.

**Table 3: Table 2-1 Protocol Prefix Keywords (Continued)**

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

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.

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

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#
```

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}] 
```

### Syntax Description

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

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

The Cisco ADE OS supports public key authentication without 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.

**Example 1**

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

Example 2

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

Related Topics

- show crypto, on page 78

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables all debugging.</td>
</tr>
<tr>
<td>application</td>
<td>Enables debugging application related errors or events.</td>
</tr>
<tr>
<td></td>
<td>- all—Enables all application debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>- install—Enables application install debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>- operation—Enables application operation debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>- uninstall—Enables application uninstall debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
</tbody>
</table>
### 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.
### Cisco ISE CLI Commands in EXEC Mode

#### debug

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Enables debugging the Cisco ISE configuration related errors or events.</td>
</tr>
<tr>
<td></td>
<td>- all—Enables all configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>- backup—Enables backup configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>- clock—Enables clock configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>- infra—Enables configuration infrastructure debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>- kron—Enables command scheduler configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>- network—Enables network configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>- repository—Enables repository configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>- service—Enables service configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td>copy</td>
<td>Enables debugging copy commands. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td>icmp</td>
<td>Enables debugging Internet Control Message Protocol (ICMP) echo response configuration related errors or events.</td>
</tr>
<tr>
<td></td>
<td>- all—Enable all debug output for ICMP echo response configuration. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td>locks</td>
<td>Enables debugging resource locking related errors or events.</td>
</tr>
<tr>
<td></td>
<td>- all—Enables all resource locking debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td></td>
<td>- file—Enables file locking debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td>logging</td>
<td>Enables debugging logging configuration related errors or events.</td>
</tr>
<tr>
<td></td>
<td>- all—Enables all logging configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
<tr>
<td>snmp</td>
<td>Enables debugging SNMP configuration related errors or events.</td>
</tr>
<tr>
<td></td>
<td>- all—Enables all SNMP configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.</td>
</tr>
</tbody>
</table>
**system**

Enables debugging Cisco ISE system related errors and events.

- **all**—Enables all system files debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
- **id**—Enables system ID debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
- **info**—Enables system info debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
- **init**—Enables system init debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

**transfer**

Enables debugging file transfer. Set level between 0 and 7, with 0 being severe and 7 being all.

**user**

Enables debugging user management.

- **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**

Enables debugging utilities configuration related errors and events.

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

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**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#
```
Related Topics
   unsubscribe, on page 67

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**

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

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

**Command Modes**
EXEC

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

**Example**

```
ise/admin# delete disk:/hs_err_pid19962.log
ise/admin#
```

Related Topics
   dir, on page 43

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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>directory-name</code></td>
<td>Directory name. Supports up to 80 alphanumeric characters. Requires <code>disk:</code> preceding the directory name.</td>
</tr>
</tbody>
</table>
`dir` (Optional). Lists directories and files in the local file system.

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

**Command Modes**
EXEC

**Usage Guidelines**
None.

**Example 1**

iseg/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**

iseg/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**

iseg/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#

Related Topics
delete, on page 43

exit

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

This command has no keywords and arguments.

**exit**

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

**Command Modes**
EXEC

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

Related Topics
delete, on page 43

forceout

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

**forceout username**

**Syntax Description**

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

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

**Command Modes**
EXEC
Usage Guidelines

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

Example

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

halt

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

This command has no keywords and arguments.

```
halt
```

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

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

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

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

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

```
Do you want to save the current configuration?
```

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

```
Saved the running configuration to startup successfully
```

Example

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

Related Topics

`reload`, on page 55

help

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

```
help
```

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

**Command Modes**
EXEC and all Configuration (config).

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

- To list all commands available for a particular command mode, enter a question mark (?) at the system prompt.
- To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by ?. This form of help is called word help because it lists only the keywords or arguments that begin with the abbreviation that you entered.
- To list the keywords and arguments associated with a command, enter ? in place of a keyword or argument on the command line. This form of help is called command syntax help, because it lists the keywords or arguments that apply based on the command, keywords, and arguments that you enter.

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

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

```
mkdir directory-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>directory-name</th>
<th>Name of the directory to create. Supports up to 80 alphanumeric characters. Use <code>disk:/directory-name</code>.</th>
</tr>
</thead>
</table>

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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-address</strong></td>
<td>IPv4 or IPv6 address of a remote system. Supports up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>hostname</strong></td>
<td>Hostname of a remote system. Supports up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>AAAA</strong></td>
<td>Queries the Internet domain name server for an IPv6 address that corresponds to a website name.</td>
</tr>
<tr>
<td><strong>name-server</strong></td>
<td>Specifies an alternative name server. Supports up to 64 alphanumeric characters.</td>
</tr>
</tbody>
</table>
**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

**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.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**

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Enter old password</code></td>
<td>Enter the current CLI password.</td>
</tr>
<tr>
<td><code>Enter new password</code></td>
<td>Enter the new CLI password.</td>
</tr>
<tr>
<td><code>Confirm new password</code></td>
<td>Confirm the new CLI password.</td>
</tr>
</tbody>
</table>
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 contain 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.
- `patch-bundle` 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.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

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

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

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

**Example 1**

ise/admin# patch install ise-patchbundle-1.1.0.362-3.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 Patch installation...
Patch successfully installed
ise/admin#

**Example 2**

ise/admin# patch install ise-patchbundle-1.1.0.362-3.i386.tar.gz myrepository
Do you want to save the current configuration? [yes/no] [yes]? no
Initiating Application Patch installation...
Patch successfully installed
ise/admin#

**Example 3**

ise/admin# patch install ise-patchbundle-1.1.0.362-2.i386.tar.gz disk
Do you want to save the current configuration? [yes/no] [yes]? yes
Generating configuration...
Saved the running configuration to startup successfully
Initiating Application Patch installation...
% Patch to be installed is an older version than currently installed version.
ise/admin#

**Related Topics**

- patch remove, on page 51
- show version, on page 102

**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.

application_name
The name of the application for which the patch is to be removed. Supports up to 255 alphanumeric characters.

version
The patch version number to be removed. Supports up to 255 alphanumeric characters.

Command Default
No default behavior or values.

Command Modes
EXEC

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

% Patch is not installed

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#

Related Topics
patch install, on page 50
show version, on page 102

ping

To diagnose the basic IPv4 network connectivity to a remote system, use the ping command in EXEC mode.

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

Syntax Description

ip-address
IP address of the system to ping. Supports up to 32 alphanumeric characters.
**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}]
```

**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.

```
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#
```

**Related Topics**

`ping6`, on page 53
### Syntax Description

- **ip-address**: IP address of the system to ping. Supports up to 64 alphanumeric characters.
- **GigabitEthernet**: (Optional). Ethernet interface.
- **0-3**: Select an Ethernet interface.
- **packetsize**: (Optional). Size of the ping packet.
- **packetsize**: Specify the size of the ping packet; the value can be between 0 and 65507.
- **pingcount**: (Optional). Number of ping echo requests.
- **pingcount**: 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

### 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

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

#### Example 2

```plaintext
ise/admin# ping6 3ffe:302:11:2:20c:29ff:feaf:da05 GigabitEthernet 0 packetsize 10 pingcount 2
```
reload

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

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

**Command Modes**
EXEC

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

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

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

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

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

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

Saved the running configuration to startup successfully

**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#
```
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}]
```

### Syntax Description

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

### Command Default
No default behavior or values.

### Command Modes
EXEC

### Usage Guidelines
When you use restore commands in Cisco ISE, the Cisco ISE server restarts automatically.
The encryption key is optional while restoring data. To support restoring earlier backups where you have not provided encryption keys, you can use the `restore` command without the encryption key.

**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.

---

**Related Topics**

backup, on page 27
backup-logs, on page 29
repository, on page 148
show repository, on page 92
show backup, on page 75
show restore, on page 93

---

**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
% restore in progress: Stopping ISE processes required for restore...35% completed
% 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.
```
Restoring Cisco ISE Configuration Data from the Backup

Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Certificate Authority Service...
Starting ISE Application Server...
Starting ISE Profiler Database...
Starting ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Stopping ISE AD Connector...
Stopping ISE Identity Mapping Service...
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...

- 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(1.3.0.230) ... 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, NFSUpgradeService(1.3.0.401) ... Done in 0 seconds.
- Data upgrade step 23/67, NFSUpgradeService(1.3.0.406) ... Done in 0 seconds.
- Data upgrade step 24/67, NFSUpgradeService(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, NFSUpgradeService(1.3.0.438) ... Done in 0 seconds.
- Data upgrade step 30/67, NFSUpgradeService(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, NFSUpgradeService(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, NFSUpgradeService(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, NFSUpgradeService(1.3.0.526) ... Done in 0 seconds.
- Data upgrade step 41/67, NFSUpgradeService(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, NFSUpgradeService(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(1.3.0.564) ... Done in 0 seconds.
- Data upgrade step 47/67, CertMgmtUpgradeService(1.3.0.616) ... Done in 15 seconds.
- Data upgrade step 48/67, CertMgmtUpgradeService(1.3.0.617) ... Done in 2 seconds.
- Data upgrade step 49/67, OcspServiceUpgradeRegistration(1.3.0.617) ... Done in 0 seconds.
- Data upgrade step 50/67, NFSUpgradeService(1.3.0.630) ... Done in 0 seconds.
- Data upgrade step 51/67, CertMgmtUpgradeService(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 0 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 plain/lablab12
```

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
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 plain/Mykey123 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
```
To remove an existing directory, use the **rmdir** command in EXEC mode.

```
rmdir directory-name
```

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Example**

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

**Related Topics**

- **dir**, on page 43
- **rmdir**, on page 60
**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**

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

**Command Default**

Disabled.

**Command Modes**

EXEC

**Usage Guidelines**

The `ssh` command enables a system to make a secure, encrypted connection to another remote system or server. This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted. 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#

technology

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

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

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

Dumps summary information of memory, processes, and paging for every 3 seconds. See Linux vmstat command.

**Command Default**

Disabled.

**Command Modes**

EXEC

**Usage Guidelines**

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

**Example 1**

```
ise/admin# tech dump tcp 0 count 2
Invoking tcpdump. Press Control-C to interrupt.
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
2 packets captured
2 packets received by filter
0 packets dropped by kernel
02:38:14.869291 IP (tos 0x0, ttl 110, id 4793, offset 0, flags [DF], proto: TCP (6), length: 40) 10.77.202.52.1598 > 172.21.79.91.22: ., cksum 0xe105 (correct),
234903779:234903779(0) ack 664488841 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 0.01 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#
```
**telnet**

To log in to a host that supports Telnet, administrators and operators can use the **telnet** command in EXEC mode.

`telnet {ip-address | hostname} port {portnumber}`

**Syntax Description**

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

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

- **port**
  Specifies the destination telnet port.

- **portnumber**
  (Optional). Indicates the port number of the remote host. From 0 to 65,535.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Example**

```bash
ise/admin# telnet 172.16.0.11 port 23
ise.cisco.com login: admin
password: 
Last login: Mon Jul 2 08:45:24 on ttyS0
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.

- **integer**
  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

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

Example
ise/admin# terminal length 24
ise/admin#

terminal session-timeout

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

terminal session-timeout minutes

Syntax Description

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

Command Default
The default session-timeout is 30 minutes.

Command Modes
EXEC

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

Example
ise/admin# terminal session-timeout 40
ise/admin#

Related Topics
terminal session-welcome, on page 66
terminal session-welcome

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

```
terminal session-welcome string
```

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

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

**Example**

```
is/admin# terminal session-welcome Welcome
is/admin#
```

**Related Topics**

terminal session-timeout, on page 65

---

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**

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

VT100

Command Modes

EXEC

Usage Guidelines

Indicate the terminal type if it is different from VT100.

Example

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

trace

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

```
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IPv4 address of the remote system. Supports up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td>hostname</td>
<td>Hostname of the remote system. Supports up to 64 alphanumeric characters.</td>
</tr>
</tbody>
</table>
```

Command Default

No default behavior or values.

Command Modes

EXEC

Example

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

undebug

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

```
undebug | all | application | backup-restore | cdp | config | copy | icmp | locks | logging | snmp | system | transfer | user | utils |
```
### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>all</strong></td>
<td>Disables all debugging.</td>
</tr>
<tr>
<td><strong>application</strong></td>
<td>Application files.</td>
</tr>
<tr>
<td>• all</td>
<td>Disables all application debug output.</td>
</tr>
<tr>
<td>• install</td>
<td>Disables application install debug output.</td>
</tr>
<tr>
<td>• operation</td>
<td>Disables application operation debug output.</td>
</tr>
<tr>
<td>• uninstall</td>
<td>Disables application uninstall debug output.</td>
</tr>
<tr>
<td><strong>backup-restore</strong></td>
<td>Backs up and restores files.</td>
</tr>
<tr>
<td>• all</td>
<td>Disables all debug output for backup-restore.</td>
</tr>
<tr>
<td>• backup</td>
<td>Disables backup debug output for backup-restore.</td>
</tr>
<tr>
<td>• backup-logs</td>
<td>Disables backup-logs debug output for backup-restore.</td>
</tr>
<tr>
<td>• history</td>
<td>Disables history debug output for backup-restore.</td>
</tr>
<tr>
<td>• restore</td>
<td>Disables restore debug output for backup-restore.</td>
</tr>
<tr>
<td><strong>cdp</strong></td>
<td>Cisco Discovery Protocol configuration files.</td>
</tr>
<tr>
<td>• all</td>
<td>Disables all Cisco Discovery Protocol configuration debug output.</td>
</tr>
<tr>
<td>• config</td>
<td>Disables configuration debug output for Cisco Discovery Protocol.</td>
</tr>
<tr>
<td>• infra</td>
<td>Disables infrastructure debug output for Cisco Discovery Protocol.</td>
</tr>
<tr>
<td><strong>config</strong></td>
<td>Configuration files.</td>
</tr>
<tr>
<td>• all</td>
<td>Disables all configuration debug output.</td>
</tr>
<tr>
<td>• backup</td>
<td>Disables backup configuration debug output.</td>
</tr>
<tr>
<td>• clock</td>
<td>Disables clock configuration debug output.</td>
</tr>
<tr>
<td>• infra</td>
<td>Disables configuration infrastructure debug output.</td>
</tr>
<tr>
<td>• kron</td>
<td>Disables command scheduler configuration debug output.</td>
</tr>
<tr>
<td>• network</td>
<td>Disables network configuration debug output.</td>
</tr>
<tr>
<td>• repository</td>
<td>Disables repository configuration debug output.</td>
</tr>
<tr>
<td>• service</td>
<td>Disables service configuration debug output.</td>
</tr>
<tr>
<td><strong>copy</strong></td>
<td>Copy commands.</td>
</tr>
</tbody>
</table>
### undebug

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `icmp`  | ICMP echo response configuration.  
|         | all—Disable all debug output for ICMP echo response configuration.  
|         | Set level between 0 and 7, with 0 being severe and 7 being all. |
| `locks` | Resource locking.  
|         | • all—Disables all resource locking debug output.  
|         | • file—Disables file locking debug output. |
| `logging` | Logging configuration files.  
|         | all—Disables all debug output for logging configuration. |
| `snmp`  | SNMP configuration files.  
|         | all—Disables all debug output for SNMP configuration. |
| `system` | System files.  
|         | • 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. |
| `transfer` | File transfer. |
| `user`  | User management.  
|         | • 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

**Example**

ise/admin# undebug all  
ise/admin#
Related Topics

debug, on page 39

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 ]
```

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

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

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

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

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

Example 1

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

Example 2

```
ise/admin# write terminal
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, page 72
- show application, page 72
- show backup, page 75
- show banner, page 76
- show cdp, page 76
- show clock, page 77
- show crypto, page 78
- show disks, page 79
- show icmp-status, page 80
- show interface, page 82
- show inventory, page 83
- show ip, page 84
- show logging, page 85
- show logins, page 87
- show memory, page 88
- show ntp, page 88
- show ports, page 89
- show process, page 91
- show repository, page 92
- show restore, page 93
- show running-config, page 94
show

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

`show keyword`

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

**Command Modes**
EXEC

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

**Example**

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

**show application**

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

```
show application > file-name
show application [status {application_name}]
show application [version {application_name}]
```

**Syntax Description**

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

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

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

**Command Modes**
EXEC

**Usage Guidelines**
To view the application status and version about installed packages on the system, use the `show application` commands.

**Example 1**
ise/admin# show application

<table>
<thead>
<tr>
<th>&lt;name&gt;</th>
<th>&lt;Description&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>RootPatch</td>
<td>Cisco ADE Root Patch</td>
</tr>
<tr>
<td>ise</td>
<td>Cisco Identity Services Engine</td>
</tr>
</tbody>
</table>

ise/admin#

**Example 2**
ise/admin# show application version ise

Cisco Identity Services Engine
---------------------------------------------------------------
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#

Related Topics

application configure, on page 10
application install, on page 8
application remove, on page 17
application reset-config, on page 18
application reset-passwd, on page 19
application start, on page 20
application stop, on page 23
application upgrade, on page 24
**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]`

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

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

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

**Example 1**

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

**Example 2**

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

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

```
show banner [post-login | pre-login]
```

### Syntax Description

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

### Command Default

No default behavior or values.

### Command Modes

EXEC

### Usage Guidelines

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

---

**show cdp**

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

```
show cdp [all | neighbors]
```

### Syntax Description

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

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

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

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#

Related Topics

cdp holdtime, on page 108

cdp run, on page 109

cdp timer, on page 110

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
show crypto

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

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

**Syntax Description**

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

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

**Command Modes**
EXEC

**Usage Guidelines**
To view authorized keys and keys for currently logged in users, use the `show crypto` command.
Example 1

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#

Related Topics

crypto, on page 37

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. |
| file-name | Name of the file to redirect. |
| | Output modifier variables: |
| • begin—Matched pattern. Supports up to 80 alphanumeric characters. |
| • count—Count the number of lines in the output. Add number after the word count. |
| | —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.
show icmp-status

Show function: To display the Internet Control Message Protocol (ICMP) echo response configuration information, use the show icmp-status command in EXEC mode.

show icmp-status

Syntax Description

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

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#

Related Topics

show memory, on page 88
Output modifier commands:

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

---

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

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

**Example 1**

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

**Example 2**

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

**Related Topics**

- `icmp echo`, on page 121
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**

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

**|** Output modifier variables:

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

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

In the **show interface GigabitEthernet 0** output, you can find that the interface has three IPv6 addresses. The first internet address (starting with 3ffe) is the result of using stateless autoconfiguration. For this to work, you need to have IPv6 route advertisement enabled on that subnet. The next address (starting with fe80) is a link local address that does not have any scope outside the host. You always see a link local address regardless of the IPv6 autoconfiguration or DHCPv6 configuration. The last address (starting with 2001) is the result obtained from a IPv6 DHCP server.
Example 1

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

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

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

Example 2

ise/admin# show interface GigabitEthernet 0
eth0 Link encap:Ethernet HWaddr 00:0C:29:AF:DA:05
inet addr:172.23.90.116 Bcast:172.23.90.255 Mask:255.255.255.0
inet6 addr: 3ffe:3021:22:20c:29ff:feaf:da05/64 Scope:Global
inet6 addr: fe80::20c:29ff:feaf:da05/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:77848 errors:0 dropped:0 overruns:0 frame:0
TX packets:23131 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:10699801 (10.2 MiB) TX bytes:3448374 (3.2 MiB)
Interrupt:59 Base address:0x2000
ise/admin#

Related Topics
  interface, on page 121
  ipv6 address autoconfig, on page 123
  ipv6 address dhcp, on page 125

show inventory

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

show inventory > file-name

Syntax Description

| >                      | Redirects output to a file. |
| file-name             | Name of the file to redirect hardware inventory information. |
Output modifier variables:

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

---

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

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

**Example**

```bash
ise/admin# show inventory
NAME: "ISE-VM-K9 chassis", DESCR: "ISE-VM-K9 chassis"
PID: ISE-VM-K9 , VID: V01 , SN: H8JES2OFKGG
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

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 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}
save logging internal
show logging system system-logfile-name

Syntax Description

> Redirects output to a file.

file-name Name of the file to redirect system logging information.

application Displays application logs.

application-logfile-name Name of the application log file.

container tc-nac Displays the Threat Centric-NAC containers.

container-id container-id [log-name name-of-log-file tail] Displays the log files related to the specified container (TC-NAC adapter).
**container-name**

**internal**

**system**

**system-logfile-name**

**system-file-name**

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

---

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

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 btmp
                     38784 Feb 26 2013 02:19:48 wtmp
                    16032 Feb 26 2013 02:19:47 faillog
                    32947 Feb 26 2013 00:38:02 dmesg
                    63738 Feb 26 2013 02:19:49 messages
                    146292 Feb 26 2013 02:19:48 lastlog
                    13877 Feb 26 2013 01:48:32 rpmpkgs
```
Example 2

To view application log files on Cisco ISE nodes, use the following command:

```plaintext
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 03:26:03 collector.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 ocap.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.

**Syntax Description**

| cli | Lists the cli login history. |

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

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

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

Example

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

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

show ntp

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

This command has no keywords and arguments.

```
show ntp
```

Command Default
No default behavior or values.
Command Modes

EXEC

Usage Guidelines

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

Example

ise/admin# show ntp
Primary NTP : ntp.es1.cisco.com
Secondary NTP : 171.68.10.150
Tertiary NTP : 171.68.10.80
synchronised to local net at stratum 11
time correct to within 11 ms
polling server every 128 s
remote refid st t when poll reach delay offset jitter
==============================================================================
*127.127.1.0 .LOCL. 10 l 9 64 377 0.000 0.000 0.001
171.68.10.80 .RMOT. 16 u 11 64 0 0.000 0.000 0.000
171.68.10.150 .INIT. 16 u 11 64 0 0.000 0.000 0.000
Warning: Output results may conflict during periods of changing synchronization.
ise/admin#

Related Topics

ntp, on page 139
ntp server, on page 142

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

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

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

Command Default
No default behavior or values.

Command Modes
EXEC

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

Example

ise/admin# show ports
Process : java (22648)
tcp: 0.0.0.0:9024, 127.0.0.1:2020, 0.0.0.0:9060, 0.0.0.0:37252, 127.0.0.1:805, 0.0.0.0:9990, 0.0.0.0:8009, 0.0.0.0:8005, 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, 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, 172.21.79.91:1813, 172.21.79.91:1700, 0.0.0.0:48425, 172.21.79.91:8905, 172.21.79.91:3799, 0.0.0.0:54104, 172.21.79.91:57696, 172.21.79.91:1645, 172.21.79.91:1646
Process : timestenrepd (21516)
tcp: 127.0.0.1:56513, 0.0.0.0:51312
Process : timestensubd (21421)
tcp: 127.0.0.1:50598
tcp: rpc.statd (3042)
tcp: 0.0.0.0:680
udp: 0.0.0.0:674, 0.0.0.0:677
Process : ttcs server (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
show process

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

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

**Syntax Description**

- `>` Redirects output to a file.

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

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

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

**Table 4: Show Process Field Descriptions**

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

#### Example

```
ise/admin# show process
```

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

```

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

| repository-name | Name of the repository whose contents you want to view. Supports up to 30 alphanumeric characters. |
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**

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

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

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
```

**Related Topics**

- backup, on page 27
- restore, on page 56
- repository, on page 148
- show backup, on page 75
- show restore, on page 93
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#

Related Topics
backup, on page 27
restore, on page 56
repository, on page 148
show backup, on page 75
show repository, on page 92

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

**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 $1$JbbHvKVGSxMZ/XL4tH15Knf.FfcEZz. role admin
! service sshd
```
Related Topics

show startup-config, on page 95

**show startup-config**

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

This command has no keywords and arguments.

**show startup-config**

**Command Default**

None

**Usage Guidelines**

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

**Example**

```
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 $1$JbbHvKVGSxM/ZXL4tH15Knf.FfcZZr. role admin
!
service sshd
!
password-policy
```
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

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

Command Default

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

Command Modes

EXEC

Usage Guidelines

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

Example

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

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

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

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

Related Topics
             show interface, on page 82
             show process, on page 91
             show running-config, on page 94

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
Usage Guidelines        The following table describes the fields of the show terminal output.

Table 5: Show Terminal Field Descriptions

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

**Example**

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

**show timezone**

To display the time zone as set on the system, use the `show timezone` command in EXEC mode.

This command has no keywords and arguments.

**show timezone**

This command has no keywords and arguments.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

**Example**

```
ise/admin# show timezone
UTC
ise/admin#
```

**Related Topics**

- `clock timezone`, on page 111
- `show timezones`, on page 98

**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**
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

**Usage Guidelines**

**Example 1**

```
ise/admin# show udi
SPID: ISE-3315-K9
VVID: 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 that you have been logged into the Cisco ISE server, use the `show uptime` command in EXEC mode.

```
show uptime > file-name
```

### Syntax Description

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

### Command Default
No default behavior or values.

### Command Modes
EXEC

### Usage Guidelines
Use this `show uptime` to check for how long you have been logged into the Cisco ISE server.
Example

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

show users

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

**show users > file-name**

**Syntax Description**

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

**Output modifier variables:**

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

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

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

**Example**

ise/admin# show users

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>ROLE</th>
<th>HOST</th>
<th>TTY</th>
<th>LOGIN DATETIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Admin</td>
<td>10.77.202.52</td>
<td>pts/0</td>
<td>Tue Feb 26 20:36:41 2013</td>
</tr>
</tbody>
</table>

DETACHED SESSIONS:
show version

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

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

**Syntax Description**

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

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

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

This command displays version information about the Cisco ADE-OS software running in the Cisco ISE server, and also displays the Cisco ISE version.
Example 1

ise/admin# show version
Cisco Application Deployment Engine OS Release: 2.2
ADE-OS Build Version: 2.2.0.127
ADE-OS System Architecture: x86_64

Copyright (c) 2005-2014 by Cisco Systems, Inc.
All rights reserved.
Hostname: Positron

Version information of installed applications
---------------------------------------------

Root Patch VERSION INFORMATION
-----------------------------------
Version : 1.3.0 Vendor: Cisco Systems, Inc.
Build Date : June 13 2014 15:39PDT

Cisco Identity Services Engine
---------------------------------------------
Version : 1.3.0.673
Build Date : Fri Jun 20 19:32:13 2014
Install Date : Fri Jun 20 21:06:00 2014

ise/admin#

Example 2

ise/admin# show version history
---------------------------------------------
Install Date: Fri Jun 20 21:06:46 PDT 2014
Application: ise
Version: 1.3.0.673
Install type: Application Install
Bundle filename: ise.tar.gz
Repository: SystemDefaultPkgRepos
---------------------------------------------
Install Date: Fri Jun 20 21:57:46 PDT 2014
Application: RootPatch
Version: UNKNOWN
Install type: Application Install
Bundle filename: RootPatch-appbundle-allinone-x86_64.tar.gz
Repository: carsapps
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, page 106
• Configuring Cisco ISE in the Configuration Mode, page 107
• Configuring Cisco ISE in the Configuration Submode, page 108
• CLI Configuration Command Default Settings, page 108
• cdp holdtime, page 108
• cdp run, page 109
• cdp timer, page 110
• clock timezone, page 111
• conn-limit, page 115
• do, page 115
• end, page 118
• exit, page 119
• hostname, page 119
• icmp echo, page 121
• interface, page 121
• ipv6 address autoconfig, page 123
• ipv6 address dhcp, page 125
• ip address, page 126
• ip default-gateway, page 127
• ip domain-name, page 128
• ip host, page 129
Switch to Configuration Mode in EXEC Mode

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

**Step 2**

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

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

**Step 3**

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

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

**Step 4**

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

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

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

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

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

**Step 2**
Enter into the configuration submode.

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

Configure ethernet interface:
- `do` EXEC command
- `end` Exit from configure mode
- `exit` Exit from this submode
- `ip` Configure IP features
- `ipv6` Configure IPv6 features
- `no` Negate a command or set its defaults
- `shutdown` Shutdown the interface

```
ise/admin(config-GigabitEthernet)# ip ?
```

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

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

**CLI Configuration Command Default Settings**

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

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

**cdp holdtime**

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

```
cdp holdtime seconds
```

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

```
no cdp holdtime
```
Syntax Description

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

Command Default

The default CDP holdtime, in seconds is 180.

Command Modes

Configuration (config)#

Usage Guidelines

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

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

Example

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

Related Topics

- cdp timer, on page 110
- cdp run, on page 109

### cdp run

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

**cdp run GigabitEthernet**

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

**no cdp run**

Syntax Description

<table>
<thead>
<tr>
<th>run</th>
<th>Enables the Cisco Discovery Protocol. Disables the Cisco Discovery Protocol when you use the <strong>no</strong> form of the <strong>cdp run</strong> command.</th>
</tr>
</thead>
</table>

**GigabitEthernet** (Optional). Specifies the GigabitEthernet interface on which to enable the Cisco Discovery Protocol.

| 0-3 | Specifies the GigabitEthernet interface number on which to enable the Cisco Discovery Protocol. |


**cdp timer**

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

```plaintext
 cdp timer seconds
```

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

```plaintext
 no cdp timer
```

**Syntax Description**

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

**Command Default**

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

**Command Modes**

Configuration (config)#
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)#
```

Related Topics

- `cdp holdtime`, on page 108
- `cdp run`, on page 109

**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
```

**Syntax Description**

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

**Command Default**

Coordinated Universal Time (UTC)

**Command Modes**

Configuration (config)#

**Usage Guidelines**

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

**Note**

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

Warning 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 ISE Node**

Changing the time zone after installation is not supported on a Standalone or Primary ISE node. If you inadvertently change the time zone, do the following:

- Revert to the time zone back. (the time zone before it changed).
- Run the `application reset-config ise` command from the CLI of that node.
- Restore from the last known good backup before the time zone change on that node.

**Secondary ISE Node**

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

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:

- Deregister the secondary node.
- Correct the time zone to be the same as the primary node.
- Run the `application reset-config ise` command from the CLI of that node.
- Reregister the node as a secondary node to the primary node.

---

Example

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

**Related Topics**

- show timezones, on page 98
- show timezone, on page 98
- Restoring the Time Zone in Cisco ISE Nodes, on page 112
- Common Time Zones, on page 113
- Australia Time Zones, on page 113
- Asia Time Zones, on page 114
# Common Time Zones

Table 6: Table 4-1 Common Time Zones (Continued)

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

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

<table>
<thead>
<tr>
<th>Australia</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Australian Capital Territory (ACT)</td>
<td>Adelaide</td>
<td>Brisbane</td>
<td>Broken_Hill</td>
</tr>
</tbody>
</table>
### Australia

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Canberra</td>
<td>Currie</td>
<td>Darwin</td>
<td>Hobart</td>
</tr>
<tr>
<td>Lord_Howe</td>
<td>Lindeman</td>
<td>Lord Howe Island (LHI)</td>
<td>Melbourne</td>
</tr>
<tr>
<td>North</td>
<td>New South Wales (NSW)</td>
<td>Perth</td>
<td>Queensland</td>
</tr>
<tr>
<td>South</td>
<td>Sydney</td>
<td>Tasmania</td>
<td>Victoria</td>
</tr>
<tr>
<td>West</td>
<td>Yancowinna</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Asia Time Zones

**Note**

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

---

**Table 8: Table 4-3 Asia Time Zones (Continued)**

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Number of TCP connections.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-2147483647&gt;</td>
<td>(Optional). Source IP address to apply the TCP connection limit.</td>
</tr>
<tr>
<td>ip</td>
<td>(Optional). Source IP mask to apply the TCP connection limit.</td>
</tr>
<tr>
<td>mask</td>
<td>(Optional). Destination port number to apply the TCP connection limit.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Configuration (config)#

**Usage Guidelines**

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

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

**Example**

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

**Related Topics**

rate-limit, on page 146

---

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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Specifies to execute an EXEC-system level command (see Table 9: Table 4-4 Command Options for Do Command (Continued)).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>application configure</td>
<td>Configures a specific application.</td>
</tr>
<tr>
<td>application install</td>
<td>Installs a specific application.</td>
</tr>
<tr>
<td>application remove</td>
<td>Removes a specific application.</td>
</tr>
<tr>
<td>application reset-config</td>
<td>Resets application configuration to factory defaults.</td>
</tr>
<tr>
<td>application reset-passwd</td>
<td>Resets application password for a specified user.</td>
</tr>
<tr>
<td>application start</td>
<td>Starts or enables a specific application</td>
</tr>
<tr>
<td>application stop</td>
<td>Stops or disables a specific application.</td>
</tr>
<tr>
<td>application upgrade</td>
<td>Upgrades a specific application.</td>
</tr>
<tr>
<td>backup</td>
<td>Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.</td>
</tr>
<tr>
<td>backup-logs</td>
<td>Performs a backup of all logs in the Cisco ISE server to a remote location.</td>
</tr>
<tr>
<td>clock</td>
<td>Sets the system clock in the Cisco ISE server.</td>
</tr>
<tr>
<td>configure</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>copy</td>
<td>Copies any file from a source to a destination.</td>
</tr>
<tr>
<td>debug</td>
<td>Displays any errors or events for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a file in the Cisco ISE server.</td>
</tr>
<tr>
<td>dir</td>
<td>Lists files in the Cisco ISE server.</td>
</tr>
<tr>
<td>forceout</td>
<td>Forces the logout of all sessions of a specific Cisco ISE node user.</td>
</tr>
<tr>
<td>halt</td>
<td>Disables or shuts down the Cisco ISE server.</td>
</tr>
<tr>
<td>mkdir</td>
<td>Creates a new directory.</td>
</tr>
<tr>
<td>nslookup</td>
<td>Queries the IPv4 or IPv6 address or hostname of a remote system.</td>
</tr>
<tr>
<td>password</td>
<td>Updates the CLI account password.</td>
</tr>
<tr>
<td>patch</td>
<td>Installs a Patch Bundle or uninstalls an Application patch.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ping</td>
<td>Determines the IPv4 address or hostname of a remote system.</td>
</tr>
<tr>
<td>ping6</td>
<td>Determines the IPv6 address of a remote system.</td>
</tr>
<tr>
<td>reload</td>
<td>Reboots the Cisco ISE server.</td>
</tr>
<tr>
<td>restore</td>
<td>Performs a restore and retrieves the backup out of a repository.</td>
</tr>
<tr>
<td>rmdir</td>
<td>Removes an existing directory.</td>
</tr>
<tr>
<td>show</td>
<td>Provides information about the Cisco ISE server.</td>
</tr>
<tr>
<td>ssh</td>
<td>Starts an encrypted session with a remote system.</td>
</tr>
<tr>
<td>tech</td>
<td>Provides Technical Assistance Center (TAC) commands.</td>
</tr>
<tr>
<td>telnet</td>
<td>Establishes a Telnet connection to a remote system.</td>
</tr>
<tr>
<td>terminal length</td>
<td>Sets terminal line parameters.</td>
</tr>
<tr>
<td>terminal session-timeout</td>
<td>Sets the inactivity timeout for all terminal sessions.</td>
</tr>
<tr>
<td>terminal session-welcome</td>
<td>Sets the welcome message on the system for all terminal sessions.</td>
</tr>
<tr>
<td>terminal terminal-type</td>
<td>Specifies the type of terminal connected to the current line of the current session.</td>
</tr>
<tr>
<td>traceroute</td>
<td>Traces the route of a remote IP address.</td>
</tr>
<tr>
<td>unddebug</td>
<td>Disables the output (display of errors or events) of the debug command for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.</td>
</tr>
<tr>
<td>write</td>
<td>Erases the startup configuration that forces to run the setup utility and prompt the network configuration, copies the running configuration to the startup configuration, displays the running configuration on the console.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

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

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

Example

```
ise/admin(config)# do show run
Generating configuration...
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 171.70.168.183
!
ip default-gateway 172.23.90.1
!
clock timezone EST
!
tp server time.nist.gov
!
username admin password hash $1$JbbHVKGxMZ/ XL4tH15KnF.FfcZEr. 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)#
```

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

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

Related Topics
exit, on page 119

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

exit
This command has no keywords and arguments.

Command Default
No default behavior or values.

Command Modes
Configuration (config)#

Usage Guidelines
The exit command is used in the Cisco ISE server to exit the current command mode to the next highest command mode in the CLI mode hierarchy.
For example, use the exit command in configuration mode to return to EXEC mode. Use the exit command in the configuration submodes to return to configuration mode. At the highest level, EXEC mode, the exit command exits EXEC mode and disconnects from the Cisco ISE server.

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

Related Topics
end, on page 118
exit, on page 119

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

Syntax Description

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

Command Default
No default behavior or values.

Command Modes
Configuration (config)#

Usage Guidelines

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

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

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

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

% Warning: Updating the hostname will cause any certificate using the old hostname to become invalid. Therefore, a new self-signed certificate using the new hostname will be generated now for use with HTTPs/EAP. If CA-signed certs were used on this node, please 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 AD Connector...
Stopping ISE Database processes...
ISE Database processes already running, PID: 9651
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise' CLI to verify all processes are in running state.
ise=1/admin#

**icmp echo**

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

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

**Syntax Description**

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

**Command Default**

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

**Command Modes**

Configuration (config)#

**Usage Guidelines**

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

**Example**

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

**Related Topics**

`show icmp-status`, on page 80

**interface**

To configure an interface type and enter the interface configuration mode, use the `interface` command in configuration mode. This command does not have a `no` form.
VMware virtual machine may have a number of interfaces available that depends on how many network interfaces (NIC) are added to the virtual machine.

```plaintext
interface GigabitEthernet {0 | 1 | 2 | 3}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>note</strong></td>
<td>Configure the Gigabit Ethernet interface.</td>
</tr>
<tr>
<td><strong>number</strong></td>
<td>Number of the Gigabit Ethernet port to configure.</td>
</tr>
<tr>
<td><strong>0 - 3</strong></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>do</strong></td>
<td>EXEC command. Allows you to perform any EXEC commands in this mode.</td>
</tr>
<tr>
<td><strong>end</strong></td>
<td>Exits the config-GigabitEthernet submode and returns you to EXEC mode.</td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td>Exits the config-GigabitEthernet configuration submode.</td>
</tr>
<tr>
<td><strong>ip</strong></td>
<td>Sets the IP address and netmask for the Gigabit Ethernet interface.</td>
</tr>
<tr>
<td><strong>ipv6</strong></td>
<td>Configures IPv6 autoconfiguration address and IPv6 address from DHCPv6 server.</td>
</tr>
<tr>
<td><strong>no</strong></td>
<td>Negates the command in this mode. Two keywords are available:</td>
</tr>
<tr>
<td></td>
<td>- ip—Sets the IP address and netmask for the interface.</td>
</tr>
<tr>
<td></td>
<td>- ipv6—Sets the IPv6 address for the interface.</td>
</tr>
<tr>
<td></td>
<td>- shutdown—Shuts down the interface.</td>
</tr>
<tr>
<td><strong>shutdown</strong></td>
<td>Shuts down the interface.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Interface configuration (config-GigabitEthernet)#
Usage Guidelines

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

Example

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

Related Topics

do, on page 115
ip address, on page 126
ipv6 address autoconfig, on page 123
ipv6 address dhcp, on page 125
shutdown, on page 152

**ipv6 address autoconfig**

To enable IPv6 stateless autoconfiguration, use the interface GigabitEthernet 0 command in configuration mode. This command does not have a no form.

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.

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

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

Interface configuration (config-GigabitEthernet)#

**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)#

**Related Topics**

- show interface, on page 82
Configuring IPv6 Auto Configuration

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

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

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

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

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

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

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

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

Verifying the Privacy Extensions Feature

To verify that the privacy extensions feature is enabled, you can use the `show interface GigabitEthernet 0` command. You can see two autoconfiguration addresses: one address is without the privacy extensions, and the other is with the privacy extensions.
In the example below, the MAC is 3ffe:302:11:2:20c:29ff:feaf:da05/64 and the non-RFC3041 address contains the MAC, and the privacy-extension address is 302:11:2:9d65:e608:59a9:d4b9/64.

The output appears similar to the following:

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

### ipv6 address dhcp

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

```
ipv6 address dhcp
```

**Command Default**

No default behavior or values.

**Command Modes**

Interface configuration (config-GigabitEthernet)#

**Usage Guidelines**

**Example**

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

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

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

**Note**

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

You can use the **show interface** command to display what IPv6 addresses are in use for a particular interface.
When both the IPv6 stateless autoconfiguration and IPv6 address DHCP are enabled, the running configuration shows the interface settings similar to the following:

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

**Related Topics**
- show interface, on page 82
- ip address, on page 126
- shutdown, on page 152
- ipv6 address autoconfig, on page 123
- show running-config, on page 94

## 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IPv4 address.</td>
</tr>
<tr>
<td>network mask</td>
<td>Mask of the associated IP subnet.</td>
</tr>
</tbody>
</table>

**Command Default**

Enabled.

**Command Modes**

Interface configuration (config-GigabitEthernet)#
Usage Guidelines

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

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

Note

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

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)#

Related Topics

- shutdown, on page 152
- ip default-gateway, on page 127
- interface, on page 121
- show interface, on page 82

ip default-gateway

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

ip default-gateway ip-address
To disable this function, use the no form of this command.

no ip default-gateway

Syntax Description

default-gateway
Defines a default gateway with an IP address.

ip-address
IP address of the default gateway.

Command Default

Disabled.

Command Modes

Configuration (config)#
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)#

Related Topics

ip address, on page 126

**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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-name</td>
<td>Defines a default domain name.</td>
</tr>
<tr>
<td>domain-name</td>
<td>Default domain name used to complete the hostnames. Contains at least 2 to 64 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Command Default**

Enabled.

**Command Modes**

Configuration (config)#

**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)#

Related Topics

ip name-server, on page 131

### 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]
```

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

**Command Default**

No default behavior or values.

**Command Modes**

Configuration (config)#

**Usage Guidelines**

Supported IPv6 address formats include:

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

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

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

**Example 1**

```plaintext
ise/admin(config)# ip host 172.21.79.96 ise1 ise1.cisco.com
Host alias was modified. You must restart ISE for change to take effect.
Do you want to restart ISE now? (yes/no) yes
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Application Server...
Stopping ISE Profiler DB...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting 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**

```plaintext
ise/admin(config)# ipv6 host 2001:db8:cc00:1::1 ise1 ise1.cisco.com
Host alias was modified. You must restart ISE for change to take effect.
Do you want to restart ISE now? (yes/no) yes
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Application Server...
Stopping ISE Profiler DB...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting 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)#
```

**Related Topics**

- **ip domain-name**, on page 128
**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 four 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 name servers from the configuration. Using the `no` form of this command and one of the IP names removes only that name server.

---

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

**Command Default**

No default behavior or values.

**Command Modes**

Configuration (config)#

**Usage Guidelines**

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

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

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

**Note**

If you modified this setting for AD connectivity, you must restart Cisco ISE for the changes to take effect. Also, ensure that all DNS servers configured in Cisco ISE are able to resolve all relevant AD DNS records. If the configured AD join points are not correctly resolved after the DNS settings are changed, you must manually perform the Leave operation and re-join the AD join point.
Example 1

ise/admin(config)# ip name-server ?
<A.B.C.D> Primary DNS server IP address
<A.B.C.D> DNS server 2 IP address
<A.B.C.D> DNS server 3 IP address
<X:X:X::X> IPv6 DNS server 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 64.102.6.247
ip name-server 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)

Related Topics
ip domain-name, on page 128

ip route

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

ip route prefix mask gateway ip-address
no ip route prefix mask

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix</td>
<td>IP route prefix for the destination.</td>
</tr>
<tr>
<td>mask</td>
<td>Prefix mask for the destination.</td>
</tr>
<tr>
<td>ip-address</td>
<td>IP address of the next hop that can be used to reach that network.</td>
</tr>
</tbody>
</table>

Command Default

No default behavior or values.

Command Modes

Configuration (config)#
### Usage Guidelines

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

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

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

The following example describes how to configure multiple default routes:

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

<table>
<thead>
<tr>
<th>ISE Interface</th>
<th>IP Network</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>192.168.114.10</td>
<td>192.168.114.0 192.168.114.1</td>
</tr>
<tr>
<td></td>
<td>192.168.115.10</td>
<td>192.168.115.0 192.168.115.1</td>
</tr>
<tr>
<td></td>
<td>192.168.117.10</td>
<td>192.168.117.0 192.168.117.1</td>
</tr>
</tbody>
</table>

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

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

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

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

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

```bash
ise/admin(config)# ip route 192.168.0.0 255.255.0.0 gateway 172.23.90.2
ise/admin(config)#
```
To schedule one or more Command Scheduler commands to run at a specific date and time or a recurring level, use the `kron occurrence` command in configuration mode. To delete this schedule, use the `no` form of this command.

**kron occurrence occurrence-name**

### Syntax Description

<table>
<thead>
<tr>
<th>occurrence</th>
<th>Schedules Command Scheduler commands.</th>
</tr>
</thead>
<tbody>
<tr>
<td>occurrence-name</td>
<td>Name of the occurrence. Supports up to 80 alphanumeric characters. (See the following note and Syntax Description.)</td>
</tr>
</tbody>
</table>

**Note**

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

### Syntax Description

| at | Identifies that the occurrence is to run at a specified calendar date and time. Usage: at [hh:mm] [day-of-week | day-of-month | month day-of-month]. |
| do | EXEC command. Allows you to perform any EXEC commands in this mode. |
| end | Exits the kron-occurrence configuration submode and returns you to EXEC mode. |
| exit | Exits the kron-occurrence configuration mode. |
| no | Negates the command in this mode. Three keywords are available: |
|    | • at—Usage: at [hh:mm] [day-of-week | day-of-month | month day-of-month]. |
|    | • policy-list—Specifies a policy list to be run by the occurrence. Supports up to 80 alphanumeric characters. |
|    | • recurring—Execution of the policy lists should be repeated. |
| policy-list | Specifies a Command Scheduler policy list to be run by the occurrence. |
Identify that the occurrences run on a recurring basis.

**Note** If a kron occurrence is not recurring, then the kron occurrence configuration for the scheduled backup is removed after it has run.

**Command Default**

No default behavior or values.

**Command Modes**

Configuration (config-Occurrence)#

**Usage Guidelines**

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

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

**Note** When you run the **kron** command, backup bundles are created with a unique name (by adding a 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**

```plaintext
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**

```plaintext
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**

```plaintext
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)#
```
Related Topics

kron policy-list, on page 136

kron policy-list

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

kron policy-list list-name

Syntax Description

<table>
<thead>
<tr>
<th>syntax</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy-list</td>
<td>Specifies a name for Command Scheduler policies.</td>
</tr>
<tr>
<td>list-name</td>
<td>Name of the policy list. Supports up to 80 alphanumeric characters.</td>
</tr>
</tbody>
</table>

Note

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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Configuration (config-Policy List)#
Usage Guidelines

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

**Note**

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

Example

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

**Related Topics**

- **kron occurrence**, on page 134

logging

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

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

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

```
no logging
```

**Syntax Description**

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

**Usage Guidelines**

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

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

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

The navigation path to configure the maximum number of command-line interface (CLI) sessions is in the Session tab of the Cisco ISE Admin portal in the following location: **Administration > System > Admin Access > Settings > Access**.
To specify an NTP configuration, use the `ntp` command in configuration mode with `authenticate`, `authentication-key`, `server`, and `trusted-key` commands.

**ntp authenticate**

**ntp authentication-key** `<key id> md5|plain <key value>`

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

**ntp trusted-key** `<key>`

**no ntp server**

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>authenticate</code></td>
<td>Enables authentication of all time sources.</td>
</tr>
<tr>
<td><code>authentication-key</code></td>
<td>Specifies authentication keys for trusted time sources.</td>
</tr>
<tr>
<td><code>server</code></td>
<td>Specifies NTP server to use.</td>
</tr>
<tr>
<td><code>trusted-key</code></td>
<td>Specifies key numbers for trusted time sources.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Configuration (config)#

### Usage Guidelines

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

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

### Example

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

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

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

**ntp authenticate**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>authenticate</th>
<th>Enables authentication of all time sources.</th>
</tr>
</thead>
</table>

**Command Default**

None

**Command Modes**

Configuration (config)#

**Usage Guidelines**

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

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

**Example**

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

**Related Topics**

- ntp, on page 139
- ntp authentication-key, on page 141
- ntp server, on page 142
- ntp trusted-key, on page 145
- show ntp, on page 88
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** | **plain** *key value*

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

**no ntp authentication-key**

**Syntax Description**

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

**Command Default**

None

**Command Modes**

Configuration (config)#.

**Usage Guidelines**

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

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

**Note**

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

**Example 1**

```
ise/admin# configure
ise/admin(config)#
ise/admin(config)# ntp authentication-key 1 md5 plain SharedWithServe
```
To allow for software clock synchronization by the NTP server for the system, use the `ntp server` command in configuration mode. Allows up to three servers each with a key in a separate line. The key is an optional parameter but the key is required for NTP authentication.

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

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

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

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

### Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Allows the system to synchronize with a specified server.</td>
</tr>
<tr>
<td>`ip-address</td>
<td>hostname`</td>
</tr>
<tr>
<td>autokey</td>
<td>Specifies that public-key authentication should be used for NTP server. If you choose this option, ensure that you import the NTP server's public key in to the Cisco ISE node using the <code>crypto</code> command.</td>
</tr>
</tbody>
</table>
This key needs to be defined with a key value, by using the `ntp authentication-key` command, and also needs to be added as a trusted-key by using the `ntp trusted-key` command.

For authentication to work, the key and the key value should be the same as that which is defined on the actual NTP server.

---

**Command Default**

No servers are configured by default.

**Command Modes**

Configuration (config)#

**Usage Guidelines**

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

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

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

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

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

---

**Note**

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

**Related Topics**

- `ntp`, on page 139
- `ntp authenticate`, on page 140
- `ntp authentication-key`, on page 141
- `ntp trusted-key`, on page 145
- `show ntp`, on page 88
- Configuring Trusted Keys for NTP Server Authentication, on page 144
- Verifying the Status of Synchronization, on page 144
Configuring Trusted Keys for NTP Server Authentication

To allow for software clock synchronization by the NTP server for the system, use the `ntp server` command in configuration mode.

```
ise/admin(config)# ntp server ntp.esl.cisco.com key 1
% WARNING: Key 1 needs to be defined as a ntp trusted-key.
ise/admin(config)#
ise/admin(config)# ntp trusted-key 1
% WARNING: Key 1 needs to be defined as a ntp authentication-key.
ise/admin(config)#
ise/admin(config)# ntp authentication-key 1 md5 plain SharedWithServe
ise/admin(config)#
ise/admin(config)# ntp server ntp.esl.cisco.com 1
ise/admin(config)# ntp server 171.68.10.80 2
ise/admin(config)# ntp server 171.68.10.150 3
ise/admin(config)#
ise/admin(config)# do show running-config
Generating configuration...
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
   ip address 172.21.79.246 255.255.255.0
   ipv6 address autoconfig
!
ip name-server 171.70.168.183
!
ip default-gateway 172.21.79.1
!
clock timezone UTC
!
ntp authentication-key 1 md5 hash ee18afc7608ac7ecdbbeefc5351ad118bc9ce1ef3
ntp authentication-key 2 md5 hash f1ef7b05c0d1c0d8c8b70e8c76f37f33c33b59
ntp authentication-key 3 md5 hash ee18afc7608ac7ecdbbeefc5351ad118bc9ce1ef3
ntp trusted-key 1
ntp trusted-key 2
ntp trusted-key 3
ntp authenticate
ntp server ntp.esl.cisco.com key 1
ntp server 171.68.10.80 key 2
ntp server 171.68.10.150 key 3
!
--More--
```

Verifying the Status of Synchronization

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

```
Example 1

ise/admin# show ntp
Primary NTP : ntp.esl.cisco.com
Secondary NTP : 171.68.10.80
Tertiary NTP : 171.68.10.150
synchronised to local net at stratum 11
time correct to within 448 ms
polling server every 64 s
remote refid st t when poll reach delay offset jitter
+127.127.1.0 .LOCL. 10 l 46 64 37 0.000 0.000 0.001
```

Cisco Identity Services Engine CLI Reference Guide, Release 1.3
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**

<table>
<thead>
<tr>
<th>trusted-key</th>
<th>The identifier that you want to assign to this key.</th>
</tr>
</thead>
<tbody>
<tr>
<td>key</td>
<td>Specifies key numbers for trusted time sources that needs to be defined as NTP authentication keys. Supports up to 65535 numeric characters.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Configuration (config)#

**Usage Guidelines**

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

**Example 1**

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
rate-limit

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

```
rate-limit 250 ip-address net-mask port
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-10000&gt;</code></td>
<td>An average number of TCP/UDP/ICMP packets per second.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Source IP address to apply the packet rate limit.</td>
</tr>
<tr>
<td>net-mask</td>
<td>Source IP mask to apply the packet rate limit.</td>
</tr>
<tr>
<td>port</td>
<td>Destination port number to apply the packet rate limit.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Configuration (config)#

**Usage Guidelines**

None.

**Example**

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

Related Topics
    conn-limit, on page 115

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>digit-required</td>
<td>Requires a digit in user passwords.</td>
</tr>
<tr>
<td>disable-cisco-password</td>
<td>Disables the ability to use the word Cisco or any combination as the password.</td>
</tr>
<tr>
<td>disable-repeat-chars</td>
<td>Disables the ability of the password to contain more than four identical characters.</td>
</tr>
<tr>
<td>do</td>
<td>Exec command.</td>
</tr>
<tr>
<td>end</td>
<td>Exit from configure mode.</td>
</tr>
<tr>
<td>exit</td>
<td>Exit from this submode.</td>
</tr>
<tr>
<td>lower-case-required</td>
<td>Requires a lowercase letter in user passwords.</td>
</tr>
<tr>
<td>min-password-length</td>
<td>Minimum number of characters for a valid password. Supports up to 40 characters.</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults.</td>
</tr>
<tr>
<td>no-previous-password</td>
<td>Prevents users from reusing a part of their previous password.</td>
</tr>
<tr>
<td>no-username</td>
<td>Prohibits users from reusing their username as a part of a password.</td>
</tr>
<tr>
<td>password-delta</td>
<td>Number of characters to be different from the old password.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>password-expiration-days</td>
<td>Number of days until a password expires. Supports an integer up to 3650.</td>
</tr>
<tr>
<td>password-expiration-enabled</td>
<td>Enables password expiration.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You must enter the <strong>password-expiration-enabled</strong> command before the other password-expiration commands.</td>
</tr>
<tr>
<td>password-expiration-warning</td>
<td>Number of days before expiration that warnings of impending expiration begin. Supports an integer up to 3650.</td>
</tr>
<tr>
<td>password-lock-enabled</td>
<td>Locks a password after several failures.</td>
</tr>
<tr>
<td>password-lock-retry-count</td>
<td>Number of failed attempts before user password locks. Supports an integer up to 20.</td>
</tr>
<tr>
<td>password-time-lockout</td>
<td>Sets the time in minutes after which the account lockout is cleared. Supports time values from 5 minutes to 1440 minutes.</td>
</tr>
<tr>
<td>special-required</td>
<td>Requires a special character in user passwords.</td>
</tr>
<tr>
<td>upper-case-required</td>
<td>Requires an uppercase letter in user passwords.</td>
</tr>
</tbody>
</table>

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

**Command Modes**
Configuration (config-password-policy)#

**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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>repository-name</td>
<td>Name of repository. Supports up to 80 alphanumeric characters.</td>
</tr>
</tbody>
</table>
After you enter the name of the repository in the `repository` command, you enter the `config-Repository` configuration submode (see the Syntax Description).

**Syntax Description**

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

---

**Note**

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

**Table 10: Table 4-5 URL Keywords (Continued)**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Source of Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Enter the repository URL, including server and path information. Supports up to 80 alphanumeric characters.</td>
</tr>
<tr>
<td>cdrom:</td>
<td>Local CD-ROM drive (read only).</td>
</tr>
</tbody>
</table>
You can run the `show repository` repository_name to view all files in the local repository.

**Note** All local repositories are created on the /localdisk partition. When you specify disk:// in the repository URL, the system creates directories in a path that is relative to /localdisk. For example, if you entered disk://backup, the directory is created at /localdisk/backup.

## Command Default
No default behavior or values.

## Command Modes
Configuration (config-Repository)#

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

To disable this function, use the `no` form of `host-key host` command in the submode.

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

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

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

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

### Command Default

No default behavior or values.

### Command Modes

Configuration (config)#
shutdown

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

This command has no keywords and arguments.

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

**Command Modes**
Configuration (config-GigabitEthernet)#

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

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

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

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

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

**Example**

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

**Related Topics**
- `interface`, on page 121
- `ip address`, on page 126
- `show interface`, on page 82
- `ip default-gateway`, on page 127
**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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>community</td>
<td>Sets SNMP community string.</td>
</tr>
<tr>
<td><code>community-string</code></td>
<td>Accessing string that functions much like a password and allows access to SNMP. No blank spaces allowed. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td><code>ro</code></td>
<td>Specifies read-only access.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Configuration (config)#

**Usage Guidelines**

The `snmp-server community` command requires a community string and the `ro` argument; otherwise, an error occurs.

The SNMP agent on the Cisco ISE provides read-only SNMP-v1 and SNMP-V2c access to the following MIBs:

- SNMPv2-MIB
- RFC1213-MIB
- IF-MIB
- IP-MIB
- IP-FORWARD-MIB
- TCP-MIB
- UDP-MIB
- HOST-RESOURCES-MIB

- ENTITY-MIB-Only 3 MIB variables are supported on the ENTITY-MIB:
  - Product ID: entPhysicalModelName
  - Version ID: entPhysicalHardwareRev
  - Serial Number: entPhysicalSerialNumber
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>contact</code></td>
<td>Identifies the contact person for this managed node. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td><code>contact-name</code></td>
<td>String that describes the system contact information of the node. Supports up to 255 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Configuration (config)#

**Usage Guidelines**

None.

**Example**

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

**Related Topics**

- `snmp-server community`, on page 153
- `snmp-server location`, on page 155
snmp-server location

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

**snmp-server location location**

**Syntax Description**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>location</td>
<td>Configures the physical location of this managed node. Supports up to 255 alphanumeric characters.</td>
</tr>
<tr>
<td>location</td>
<td>String that describes the physical location information of the system. Supports up to 255 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Configuration (config)#

**Usage Guidelines**

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

**Example 1**

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

**Example 2**

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

**Related Topics**

- snmp-server community, on page 153
- snmp-server location, on page 155

username

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

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

For an existing user, use the following command option:

**username username password role admin | user {password}**
### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>username</code></td>
<td>Only one word for the username argument. Blank spaces and quotation marks (&quot; &quot;) are not allowed. Supports up to 31 alphanumeric characters.</td>
</tr>
<tr>
<td><code>password</code></td>
<td>Specifies password.</td>
</tr>
<tr>
<td><code>password</code></td>
<td>Password character length up to 40 alphanumeric characters. You must specify the password for all new users.</td>
</tr>
<tr>
<td>`hash</td>
<td>plain`</td>
</tr>
<tr>
<td>`role admin</td>
<td>user`</td>
</tr>
<tr>
<td><code>disabled</code></td>
<td>Disables the user according to the user's email address.</td>
</tr>
<tr>
<td><code>email</code></td>
<td>Sets user's email address.</td>
</tr>
<tr>
<td><code>email-address</code></td>
<td>Specifies the user’s email address. For example, <a href="mailto:user1@mydomain.com">user1@mydomain.com</a>.</td>
</tr>
</tbody>
</table>

### Command Default

The initial user during setup.

### Command Modes

Configuration (config)#

### Usage Guidelines

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

#### Example 1

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

#### Example 2

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

#### Example 3

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

### Related Topics

- `password-policy`, on page 147
- `show users`, on page 101