Cisco Identity Services Engine CLI Reference Guide, Release 3.3

First Published: 2023-07-05

Last Modified: 2024-04-18

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

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

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

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

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

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

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

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

© 2023 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Cisco ISE Command-Line Interface** 1

Communications, Services, and Additional Information 2

Cisco Bug Search Tool 2

Documentation Feedback 2

Cisco ISE Administration and Configuration Using CLI 3

Accessing the Cisco ISE CLI Using a Local System 3

Accessing the Cisco ISE CLI with Secure Shell 4

Cisco ISE CLI Administrator Account 5

Cisco ISE CLI User Accounts 6

Creating a Cisco ISE CLI User Account 6

Cisco ISE CLI User Account Privileges 7

Supported Hardware and Software Platforms for Cisco ISE CLI 8

CHAPTER 2 **Cisco ISE CLI Commands in EXEC Mode** 9

Cisco ISE CLI Session Begins in EXEC Mode 11

application install 12

application configure ise 13

Monitoring Database Settings 14

Live Statistics of Profiling Events 17

Export and Import Internal CA Store 17

Create Missing Indexes 20

Key Performance Metrics Statistical Data 21

Counter Attribute Collection 22

Localized ISE Installation 23

application remove 25

application reset-config 26

application reset-passwd 28
application start 29
application stop 32
application upgrade 34
backup 37
Backing up Cisco ISE Configuration Data 38
Backing up Cisco ISE Operational Data 39
backup-logs 40
clock 42
cls 44
configure 45
copy 46
Copying Log files 47
crypto 49
debug 52
delete 55
dir 56
esr 58
exit 59
forceout 60
generate-password 61
halt 62
idle-timeout 63
licence esr 64
mkdir 65
nslookup 66
password 68
patch install 69
patch remove 71
permit rootaccess 73
ping 75
ping6 76
reload 78
reset-config 80

restore 81
Restoring Cisco ISE Configuration Data from the Backup 82
Restoring Cisco ISE Operational Data from the Backup 84
Restoring Cisco ISE Configuration Data and Cisco ADE OS data from the Backup 84
rmdir 86
screen-length 87
screen-width 88
ssh 89
tech 91
Interpreting CPU and Memory Usage Data 92
terminal 94
traceroute 95
undebug 96
who 98

CHAPTER 3 Cisco ISE CLI Commands in EXEC Show Mode 99
show 101
show application 102
show backup 105
show banner 107
show cdp 108
show clock 110
show container 111
show cpu 115
show crypto 117
show disks 118
show esr status 120
show icmp-status 121
show interface 123
show inventory 125
show ip 127
show ipv6 route 128
show logging 129
show logins 132

show memory 133
show ntp 134
show ports 135
show process 137
show repository 139
show restore 141
show running-config 142
show snmp-server engineid 143
show snmp-server user 144
show tech-support 145
show terminal 147
show timezone 148
show timezones 149
show udi 150
show uptime 151
show users 152
show version 153

CHAPTER 4 **Cisco ISE CLI Commands in Configuration Mode** 155
Switch to Configuration Mode in EXEC Mode 157
Configuring Cisco ISE in the Configuration Mode 158
Configuring Cisco ISE in the Configuration Submode 160
CLI Configuration Command Default Settings 161
backup interface 162
cdp holdtime 166
cdp run 167
cdp timer 168
clock timezone 169
Changing the Time Zone on Cisco ISE Nodes 169
Common Time Zones 170
Australia Time Zones 170
Asia Time Zones 171
cls 172
conn-limit 173

service cache 174
do 175
end 178
exit 179
hostname 180
icmp echo 182
identity-store 183
interface 184
ip address 186
ip default-gateway 188
ip domain-name 189
ip host 191
ip mtu 193
ip name-server 194
ip route 196
ipv6 address 198
ipv6 address autoconfig 200
Configuring IPv6 Auto Configuration 200
Verifying the Privacy Extensions Feature 201
ipv6 address dhcp 202
ipv6 enable 203
ipv6 route 205
kron occurrence 207
kron policy-list 209
logging 211
ntp 212
ntp authentication-key 214
ntp maxdistance 216
ntp server 217
Verifying the Status of Synchronization 218
rate-limit 220
password-policy 222
repository 224
service 227

shutdown 229
snmp-server enable 230
snmp-server user 232
snmp-server host 235
snmp-server community 238
snmp-server contact 239
snmp-server location 240
snmp-server trap dskThresholdLimit 241
snmp engineid 242
synflood-limit 243
username 245
Additional References 247

Cisco ISE Command-Line Interface

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

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

- Communications, Services, and Additional Information, on page 2
- Cisco ISE Administration and Configuration Using CLI, on page 3
- Cisco ISE CLI Administrator Account, on page 5
- Cisco ISE CLI User Accounts, on page 6
- Cisco ISE CLI User Account Privileges, on page 7
- Supported Hardware and Software Platforms for Cisco ISE CLI, on page 8

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

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 If you use SNS appliances, connect a null-modem cable to the console port in the Cisco ISE device and to the COM port on your system.

In the case of virtual machines or public cloud platforms, carry out the required alternative steps to connect to the console.

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

Step 3 When the terminal emulator activates, press Enter.

Step 4 Enter your username and press Enter.

Step 5 Enter the password and press Enter.

Accessing the Cisco ISE CLI with Secure Shell

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

Before you begin

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

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

Step 2 Press Enter or Spacebar to connect.

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

Step 4 Click Connect, or press Enter.

Step 5 Enter your assigned password for the administrator.

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

Step 7 Click Close on the Add Profile window.

Cisco ISE CLI Administrator Account

During the intial 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 when you restart Cisco ISE after the initial configuration.

After the intial setup, the passwords for Cisco ISE GUI and Cisco ISE CLI are managed independantly. Updating one password does not affect the other password.

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. Use the command **generate-password <username>** to generate a password that complies with the Cisco ISE Password Policy for a CLI user 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.

From Cisco ISE Release, 3.3, a newly added user is prompted to change their password on the first login.

Cisco ISE CLI User Account Privileges

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

- crypto: Crypto operations
- exit: Exit the management session
- generate-password: Username for which password has to be generated
- license: License operations
- nslookup: DNS lookup for an IP address or hostname
- password: Update Password
- ping: Ping a remote ip address
- ping6: Ping a remote ipv6 address
- show: Show information about the system
- terminal: Set terminal type
- traceroute: Trace the route to a remote ip address

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 10 or later releases.
- 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.

Cisco ISE CLI Commands in EXEC Mode

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

- Cisco ISE CLI Session Begins in EXEC Mode, on page 11
- application install, on page 12
- application configure ise, on page 13
- application remove, on page 25
- application reset-config, on page 26
- application reset-passwd, on page 28
- application start, on page 29
- application stop, on page 32
- application upgrade, on page 34
- backup, on page 37
- backup-logs, on page 40
- clock, on page 42
- cls, on page 44
- configure, on page 45
- copy, on page 46
- crypto, on page 49
- debug, on page 52
- delete, on page 55
- dir, on page 56
- esr, on page 58
- exit, on page 59
- forceout, on page 60
- generate-password, on page 61
- halt, on page 62
- idle-timeout, on page 63
- licence esr, on page 64
- mkdir, on page 65
- nslookup, on page 66
- password, on page 68
- patch install, on page 69

- patch remove, on page 71
- permit rootaccess, on page 73
- ping, on page 75
- ping6, on page 76
- reload, on page 78
- reset-config, on page 80
- restore, on page 81
- rmdir, on page 86
- screen-length, on page 87
- screen-width, on page 88
- ssh, on page 89
- tech, on page 91
- terminal , on page 94
- traceroute, on page 95
- undebug, on page 96
- who, on page 98

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 The **application install** command must only be used for installing hot patches.

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

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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

Example

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

application configure ise

Use the **application configure ise** command in EXEC mode to:

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

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

Syntax Description

configure	Configures a specific application.
application-name	Application name. Supports up to 255 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.0	Wireless setup support was removed.

Usage Guidelines

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

Example

```
ise/admin# application configure ise

Selection configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[19]Establish Trust with controller
```

```
[20]Reset Context Visibility
[21]Synchronize Context Visibility With Database
[22]Generate Heap Dump
[23]Generate Thread Dump
[24]Force Backup Cancellation
[25]Recreate undotablespace
[26]Configure TCP params
[27]Reset Upgrade Tables and Proceed with upgrade
[28]Recreate Temp tablespace
[29]Clear Sysaux tablespace
[30]Fetch SGA/PGA Memory usage
[31]Generate Self-Signed Admin Certificate
[32]View Certificates in NSSDB or CA_NSSDB
[33]Recreate REPLOGNS tablespace
[34]View Native IPSec status
[0]Exit
```

Note Cisco ISE 3.0 and later does not support Wireless Setup (Wifi setup).

Note Cisco ISE 3.1 and later does not support ACS migration.

Monitoring Database Settings

Before You begin

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

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

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

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

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

- To rebuild unusable indexes in the monitoring database, use the option 2.
- To purge monitoring operational data, use the option 3.

  The purge option is used to clean up the data and will prompt to ask the number of days to be retained.
- To reset the monitoring database, use the option 4.

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

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

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

Example

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

```
ise/admin# application configure ise

Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
.
.
.
[xx]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 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 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 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 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 AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.

5
You are about to Refresh Database statistics
Are you sure you want to proceed? y/n [n]: y
Starting to terminate long running DB sessions
Completed terminating long running DB sessions

Gathering Config schema(CEPM) stats ........
```

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

Live Statistics of Profiling Events

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

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

Example

```
ise/admin# application configure ise

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



6


Create an RMI connector client and connect it to the RMI connector server
Get an MBeanServerConnection
Retrieve MXBean

Press <Enter> to continue...
Timestamp,Elapsed,EndpointsProfiled,NetflowPacketsReceived,
EndpointsReProfiled,EndpointsDeleted...
Press Ctrl + c
```

Export and Import Internal CA Store

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

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

- To export a copy of the Cisco ISE CA certificates and keys, use option 7 in the **application configure ise** command.
- To import a copy of the Cisco ISE CA certificates and keys, use option 8 in the **application configure ise** command.

Example 1

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

```
ise/admin# application configure iseSelection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
.
.
.
[xx]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#:0x0ad3ccdf-b64842ad-93dd5826-0b27cbd2

ISE CA keys export completed successfully
```

Example 2

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

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



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



The following 4 CA key pairs were imported:
        Subject:CN=Certificate Services Root CA - ise60
        Issuer:CN=Certificate Services Root CA - ise60
        Serial#:0x66cfded7-2f384979-9110c0e1-50dbf656

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

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

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

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

Create Missing Indexes

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

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

Example 1

To create the CEPM database index, use option 9.

```
ise/admin# application configure ise

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

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

Example 2

To create missing Monitoring database indexes, use option 10.

```
ise/admin# application configure ise

Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
```

```
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
.
.
.
[xx]Exit
```

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

Key Performance Metrics Statistical Data

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

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

Example

```
ise/admin# application configure ise

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

```
.
[xx]Exit


12

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

Counter Attribute Collection

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

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

Example

To disable counter attribute collection, use option 14.

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

14
```

```
Do you want to Enable(e) or Disable(d) counter attribute collection? [e/d]d
Completed disabling counter attributes. It will take at the most 30 minute to get effected.
```

Localized ISE Installation

While reinstalling Cisco ISE, you can use the **Localized ISE Install** option (option 38) in the **application configure ise** command to reduce the installation time. By using this option, you can reduce the reinstallation time from an average of 5-7 hours, to approximately 1-2 hours. Though this option can be used for both Cisco Secure Network Server and virtual appliances, it significantly reduces the reinstallation time for Cisco Secure Network Servers.

Note

-
- You can use this option to reinstall the current version and higher versions. You cannot install a version that is older than the current version.

To install Cisco ISE using the **Localized ISE Install** option:

1. Copy a Cisco ISE ISO file to the local disk (`disk://`) using the **copy** command. Here is an example:

   ```
   ise/admin#copy ftp://xx.xx.xxx.xx//iseBuild/3.x.x.xxx/ise-3.x.x.xxx.SPA.x86_64.iso disk://
   Enter username:admin
   Enter password:
   ```

2. Run the **application configure ise** command.

   The following options are displayed:

   ```
   Selection configuration option
   [1]Reset M&T Session Database
   [2]Rebuild M&T Unusable Indexes
   [3]Purge M&T Operational Data
   [4]Reset M&T Database
   [5]Refresh Database Statistics
   [6]Display Profiler Statistics
   [7]Export Internal CA Store
   [8]Import Internal CA Store
   [9]Create Missing Config Indexes
   [10]Create Missing M&T Indexes
   [12]Generate Daily KPM Stats
   [13]Generate KPM Stats for last 8 Weeks
   [14]Enable/Disable Counter Attribute Collection
   [15]View Admin Users
   [16]Get all Endpoints
   [19]Establish Trust with controller
   [20]Reset Context Visibility
   [21]Synchronize Context Visibility With Database
   [22]Generate Heap Dump
   [23]Generate Thread Dump
   [24]Force Backup Cancellation
   [25]CleanUp ESR 5921 IOS Crash Info Files
   [26]Recreate undotablespace
   [27]Reset Upgrade Tables
   [28]Recreate Temp tablespace
   [29]Clear Sysaux tablespace
   [30]Fetch SGA/PGA Memory usage
   [31]Generate Self-Signed Admin Certificate
   [32]View Certificates in NSSDB or CA_NSSDB
   [33]Recreate REPLOGNS tablespace
   ```

```
[34]View Native IPSec status
[35]Enable/Disable/Current_status of Audit-Session-ID Uniqueness
[36]Check and Repair Filesystem
[37]Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS
[38]Localised ISE Install
[0]Exit
```

3. Choose the **Localized ISE Install** option (option 38).

   The ISO files that are stored in the local disk are listed.

4. Choose the ISO file that you want to install.

5. Verify the MD5 hash value of the chosen ISO file.

   If the MD5 checksum of the ISO file is not correct, the following error message is displayed:

   ```
   Error in mounting ISO
   ```

   You might face this error if the ISO file download was interupted due to any network issue. In this case, download the ISO file and verify the MD5 checksum again.

6. Enter **Y** to proceed with installation.

   The contents of the ISO file will be copied to the installer directories, and the appliance will reboot to install the chosen Cisco ISE release. Here is an example:

   ```
   ISO files present in the disk are:
   [1] ise-3.x.x.xxx.SPA.x86_64.iso
   Choose the ISO you want to install: 1

   Computing MD5 hash value of the selected ISO...
   File selected: ise-3.x.x.xxx.SPA.x86_64.iso (MD5: 8c3a2a73620bed0e3024044af9ccdf8e)

   Warning: Verify the MD5 checksum of the ISO before you proceed.

   Proceed with Installation? [y/n] y

   Copying ISO contents to installer directories. The copy may take around 5 minutes.

   % Notice: The appliance will reboot to install the chosen Cisco ISE release now.
   ```

application remove

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

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

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

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

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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Removes or uninstalls an application.

Example

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

application reset-config

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

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

Syntax Description

reset-config	Resets the Cisco ISE application configuration and clears the Cisco ISE datal
application-name	Name of the application configuration you want to reset. Supports up to 255 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

Example

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

```
iseadmin#application reset-config ise
Initialize your Application 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 Application server certificates? (y/n): n
Reinitializing local configuration to factory defaults...
Stopping ISE Monitoring & Troubleshooting Log Processor...
PassiveID WMI Service is disabled
PassiveID Syslog Service is disabled
```

```
PassiveID API Service is disabled
PassiveID Agent Service is disabled
PassiveID Endpoint Service is disabled
PassiveID SPAN Service is disabled
Stopping ISE Application Server...
Stopping ISE Process Monitoring Service...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping TC-NAC Service ...
VA Service is not running
ISE VA Database is not running
Segmentation Policy Service is disabled
REST Auth Service is disabled
Stopping ISE Messaging Service...
Stopping ISE API Gateway Service...
Stopping edda-url-fetcher-service Service...
Stopping ISE API Gateway Database Service...
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Stopping ISE Node Exporter...
Stopping ISE Prometheus Service...
Stopping ISE Grafana Service...
ISE MNT LogAnalytics Elasticsearch Service is not running.
ISE Logstash Service is not running.
ISE Kibana service is not running.
Enter the administrator username to create[admin]: iseadmin
Enter the password for 'iseadmin':
Re-enter the password for 'iseadmin':
Extracting ISE database content...
Starting ISE database processes...
Creating ISE M&T session directory...
Creating ISE VA timesten database...
Performing ISE database priming...
Starting ISE Indexing Engine...
TimeoutStartUSec=20min
TimeoutStopUSec=20min
You (oracle) are not allowed to use this program (crontab)
See crontab(1) for more information
mkdir: cannot create directory ‘/opt/podman’: File exists
Cleaning up TC-NAC docker configuration...
Starting ISE Messaging Service...
Stopping ISE Messaging Service...
Starting ISE API Gateway Database Service...
Stopping ISE API Gateway Database Service...
Smart Licensing is Enabled. Removing the configuration during reset-config
Smart Licensing configuration files are deleted.
application reset-config is success
```

application reset-passwd

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

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

Syntax Description

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

Command Default

No default behavior or values. necessary to disable the administrator account in Cisco ISE

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

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

Example

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

application start

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

application [**start** {*application-name* [*safe*]}]

no application [**start** {*application-name* [*safe*]}]

Syntax Description

start	Enables an application bundle.
application-name	Name of the predefined application that you want to enable. Supports u 255 alphanumeric characters.
safe	Starts an application in safe mode.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Enables an application.

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

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

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

Example 1

```
ise/iseadmin#application start ise

ISE Database processes already running, PID: xxxxxxx
Starting ISE Messaging Service...
Starting ISE API Gateway Database Service...
Starting ISE Profiler Database...
Starting ISE API Gateway Service...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting edda-url-fetcher-service Service...
Starting ISE Process Monitoring Service...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Indexing Engine...
```

```
Starting ISE Certificate Authority Service...
NSS database for CA Service is ready
ISE EST service is already running, PID: xxxxxxx
Starting ISE AD Connector...
Starting ISE Node Exporter...
Starting ISE Prometheus Service...
Starting ISE Grafana Service...
ISE MNT LogAnalytics Elasticsearch Service is disabled
ISE Logstash Service is disabled
ISE Kibana Service is disabled
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
```

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

  Cisco ISE uses embedded FIPS 140-2 validated cryptographic modules. For details of the FIPS compliance claims, see the FIPS Compliance Letter.
- 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/iseadmin#application stop ise

Stopping ISE Monitoring & Troubleshooting Log Processor...
PassiveID WMI Service is disabled
PassiveID Syslog Service is disabled
PassiveID API Service is disabled
PassiveID Agent Service is disabled
PassiveID Endpoint Service is disabled
PassiveID SPAN Service is disabled
Stopping ISE Application Server...
Stopping ISE Process Monitoring Service...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping TC-NAC Service ...
VA Service is not running
ISE VA Database is not running
```

```
Segmentation Policy Service is disabled
REST Auth Service is disabled
Stopping ISE Messaging Service...
Stopping ISE API Gateway Service...
Stopping edda-url-fetcher-service Service...
Stopping ISE API Gateway Database Service...
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Stopping ISE Node Exporter...
Stopping ISE Prometheus Service...
Stopping ISE Grafana Service...
ISE MNT LogAnalytics Elasticsearch Service is not running.
ISE Logstash Service is not running.
ISE Kibana service is not running.


ise/iseadmin#application start ise safe
ISE Database processes already running, PID: xxxxxx
Starting ISE Messaging Service...
Starting ISE API Gateway Database Service...
Starting ISE Profiler Database...
Starting ISE API Gateway Service...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting edda-url-fetcher-service Service...
Starting ISE Process Monitoring Service...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
NSS database for CA Service is ready
ISE EST service is already running, PID: xxxxxx
Starting ISE AD Connector...
Starting ISE Node Exporter...
Starting ISE Prometheus Service...
Starting ISE Grafana Service...
ISE MNT LogAnalytics Elasticsearch Service is disabled
ISE Logstash Service is disabled
ISE Kibana Service is disabled
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
```

application stop

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

application [**stop** {*application-name*}]

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

Syntax Description

stop	Disables an application.
application-name	Name of the predefined application that you want to disable. Supports up to alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Disables an application.

If the autofailover configuration is enabled in your deployment, you receive the following warning message:

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

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

Example

```
iseadmin#application stop ise

Stopping ISE Monitoring & Troubleshooting Log Processor...
PassiveID WMI Service is disabled
PassiveID Syslog Service is disabled
PassiveID API Service is disabled
PassiveID Agent Service is disabled
PassiveID Endpoint Service is disabled
PassiveID SPAN Service is disabled
Stopping ISE Application Server...
Stopping ISE Process Monitoring Service...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping TC-NAC Service ...
VA Service is not running
ISE VA Database is not running
Segmentation Policy Service is disabled
REST Auth Service is disabled
Stopping ISE Messaging Service...
Stopping ISE API Gateway Service...
Stopping edda-url-fetcher-service Service...
```

```
Stopping ISE API Gateway Database Service...
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Stopping ISE Node Exporter...
Stopping ISE Prometheus Service...
Stopping ISE Grafana Service...
ISE MNT LogAnalytics Elasticsearch Service is not running.
ISE Logstash Service is not running.
ISE Kibana service is not running.
```

application upgrade

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

application [upgrade {*application-bundle remote-repository-name*|*cleanup*|*prepare*|*proceed*|*start*}]

Syntax Description

upgrade	Upgrades a specific application bundle in the remote repository.
application-bundle	Application name. Supports up to 255 alphanumeric characters.
remote-repository-name	Remote repository name. Supports up to 255 alphanumeric characters.
cleanup	Cleans previously prepared upgrade bundle and prepares a new upgrade bu
prepare	Downloads an upgrade bundle and unzip contents to the local disk to prepa application for an upgrade.
application-bundle	Application name. Supports up to 255 alphanumeric characters.
remote-repository-name	Remote repository name. Supports up to 255 alphanumeric characters.
proceed	Proceeds with an upgrade using the local file.
Start	Starts the upgrade using the local prepared bundle.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

Example 1

```
ise/admin# application upgrade prepare ise-upgradebundle-3.x.0.x.x86_64.tar.gz local

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

Application upgrade preparation successful
```

Example 2

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

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

% This application Install or Upgrade requires reboot, rebooting now...

Broadcast message from root@IS137 (pts/3) (Fri Jun  2 12:22:49 2017):

Trying to stop processes gracefully. Reload might take approximately 3 mins

Broadcast message from root@IS137 (pts/3) (Fri Jun  2 12:22:49 2017):

Trying to stop processes gracefully. Reload might take approximately 3 mins

Broadcast message from root@IS137 (pts/3) (Fri Jun  2 12:23:10 2017):

The system is going down for reboot NOW

Broadcast message from root@IS137 (pts/3) (Fri Jun  2 12:23:10 2017):

The system is going down for reboot NOW
The upgrade is now complete.
```

backup

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

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

backup [{*backup-name*} **repository** {*repository-name*} **ise-config encryption-key hash| plain** {*encryption-key name*}]

backup [{*backup-name*} **repository** {*repository-name*} **ise-operational encryption-key hash| plain** {*encryption-key name*}]

Syntax Description

backup-name	Name of backup file. Supports up to 100 alphanumeric characters.
repository	Specifies repository to store the back up file.
repository-name	Location where the files should be backed up to. Supports up to 80 alpha characters.
ise-config	Backs up Cisco ISE configuration data (includes Cisco ISE ADE-OS).
ise-operational	Backs up Cisco ISE operational data.
encryption-key	Specifies user-defined encryption key to protect the backup.
hash	Specifies (Hashed encryption key for protection of backup) an encrypted encryption key that follows. Supports up to 40 characters.
plain	Specifies (Plaintext encryption key for protection of backup) an unencr plaintext encryption key that follows. Supports up to 15 characters.
encryption-key name	An encryption key in hash | plain format for backup.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

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

- **Option 1:**

  Export the CA certificates from the source ISE node through the CLI and import them in to the target system through the CLI.

  Pros: Any certificates issued to endpoints from the source system will continue to be trusted. Any new certificates issued by the target system will be signed by the same keys.

  Cons: Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

- **Option 2:**

  After the restore process, generate all new certificates for the internal CA.

  Pros: This option is the recommended and clean method, where neither the original source certificates or the original target certificates will be used. Certificates issued by the original source system will continue to be trusted.

  Cons: Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

Backing up Cisco ISE Configuration Data

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

backup *mybackup* **repository** *myrepository* **ise-config encryption-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* {**public-key** | {**encryption-key** { **hash** | **plain** } *encryption-key name*}}

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example 1

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

Example 2

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

clock

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

clock [**set** {*month day hh:min:ss yyyy*}]

Syntax Description

set	Sets the system clock.
month	Current month of the year by name. Supports up to three alphabetic charact For example, Jan for January.
day	Current day (by date) of the month. Value = 0 to 31. Supports up to two num
hh:mm:ss	Current time in hours (24-hour format), minutes, and seconds.
yyyy	Current year (no abbreviation).

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

To recover from the impact, use the following steps:

Standalone or Primary ISE Node

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

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

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

Secondary ISE Node

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

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

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

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

Example

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

cls

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

cls

Syntax Description

This command has no keywords and arguments.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

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

configure

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

configure terminal

Syntax Description

terminal	Executes configuration commands from the terminal.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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)#
```

copy

To copy a file (such as a system image or configuration file) from local disk to a repository, use the following **copy** command in EXEC mode.

copy disk:/ *filename* **repository** *repository_name*

To copy a file from a repository to local disk, use the following **copy** command in EXEC mode.

copy repository *repo_name* **file** *file_name localdisk_destination_path*

Using the following **copy** command, you can copy core files and heap dumps from Cisco ISE to a remote repository. See Copying Log files, on page 47 for more information.

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

Syntax Description

protocol	
ftp	Source or destination URL for FTP network server. The syntax for this alias: **ftp**:[[[//*username* [:*password*]@]*location*]/*directory*]/*filename*
sftp	Source or destination URL for an SFTP network server. The syntax for this alias: **sftp**:[[//*location*]/*directory*]/*filename*
tftp	Source or destination URL for a TFTP network server. The syntax for this alias: **tftp**:[[//*location*]/*directory*]/*filename*
location	Location of destination. Represents the current running configuration file.
logs	The system log files.
all	Copies all Cisco ISE log files from the system to another location. All logs are packaged as iselogs.tar.gz and transferred to the specified directory on the remote host.
filename	Allows you to copy a single Cisco ISE log file and transfer it to the specified directory on the remote host, with its original name.
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.
disk	The localdisk from where files can be downloaded or uploaded.
repository	The repository from where files can be downloaded or uploaded.

Command Default No default behavior or values.

Command Modes EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	This command was modified to no longer support running-config and startup-config functions.

Usage Guidelines The source and destination for the file specified uses the Cisco ISE file system, through which you can specify any supported local or remote file location. The file system being used (a local memory source or a remote system) dictates the syntax used in the command.

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

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

Use the filename relative to the directory for file transfers.

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

Copying Log files

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

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

Example 1

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

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

Example 2

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

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

Example 3

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

logs are created when the application crashes. You can use the dir command to view the core files in the local disk.

```
ise/admin# copy disk:/corefiles ftp://192.0.2.2/
Username: ftp
Password:
ise36/admin#
ise36/admin# dir

Directory of disk:/

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

           Usage for disk: filesystem
                51474489344 bytes total used
                123938643968 bytes free
                184807632896 bytes available
```

crypto

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

crypto key [**delete** {*hash* | *authorized_keys* | *rsa*}]

crypto key [**export** {*filename* | *repository*}]

crypto key [**generate** {*rsa*}]

crypto key [**import** {*filename* | *repository*}]

crypto [**host_key** {*add* | *delete*}]

Syntax Description

key	Allows you to perform crypto key operations.
delete	Deletes a public/private key pair.
hash	Hash value. Supports up to 80 characters.
authorized_keys	Deletes authorized keys.
rsa	Deletes an RSA key pair.
export	Exports a public/private key pair to repository.
filename	The filename to which the public key is exported to. Supports up to 80 ch
repository	The repository to which the public key is exported to.
generate	Generates a public/private key pair.
rsa	Generates an RSA key pair.
import	Imports a public/private key pair.
filename	The filename to which the public key is imported. Supports up to 80 ch
repository	The repository to which the public key is imported.
host_key	Allows you to perform crypto host key operations.
add	Add trusted host key.
delete	Delete trusted host key.
add	Adds trusted host keys.
host	Specifies hostname.
delete	Deletes trusted host keys.
ntpkey	Public key generated from the NTP server.

Command Default No default behavior or values.

Command Modes EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

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

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

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

Example 1

The following example shows the key management for SFTP repositories.

```
ise/admin# crypto key generate rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
ise/admin# show crypto key
admin public key: ssh-rsa ad:14:85:70:fa:c3:c1:e6:a9:ff:b1:b0:21:a5:28:94 admin@ise
ise/admin# crypto key generate rsa
Private key for user admin already exists. Overwrite? y/n [n]: y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
ise/admin# show crypto key
admin public key: ssh-rsa 41:ab:78:26:48:d3:f1:6f:45:0d:99:d7:0f:50:9f:72 admin@ise
ise/admin# crypto key export mykey_rsa repository myrepository
ise/admin# show crypto key
admin public key: ssh-rsa f8:7f:8a:79:44:b8:5d:5f:af:e1:63:b2:be:7a:fd:d4 admin@ise
ise/admin# crypto key delete  f8:7f:8a:79:44:b8:5d:5f:af:e1:63:b2:be:7a:fd:d4
ise/admin#
ise/admin# crypto key delete rsa
ise/admin# show crypto key
ise/admin#
```

Example 2

The following example shows the key management for public keys that can be used to log in to Cisco ISE.

```
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 3

```
ise/admin# crypto host_key add host ise
host key fingerprint added
# Host ise found: line 1 type RSA
2048 1d:72:73:6e:ad:f7:2d:11:ac:23:e7:8c:81:32:c5:ea ise (RSA)
ise/admin#
ise/admin# crypto host_key delete host ise
host key fingerprint for ise removed
ise/admin#
```

debug

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

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

Syntax Description

all	Enables all debugging.
application	Enables debugging application related errors or events. • all—Enables all application debug output. Set level between 0 and 7, 0 being severe and 7 being all. • install—Enables application install debug output. Set level between 0 7, with 0 being severe and 7 being all. • operation—Enables application operation debug output. Set level betw 0 and 7, with 0 being severe and 7 being all. • uninstall—Enables application uninstall debug output. Set level betwe and 7, with 0 being severe and 7 being all.
backup-restore	Enables debugging back up and restore related errors or events. • all—Enables all debug output for backup-restore. Set level between 0 7, with 0 being severe and 7 being all. • backup—Enables backup debug output for backup-restore. Set level betw 0 and 7, with 0 being severe and 7 being all. • backup-logs—Enables backup-logs debug output for backup-restore. S level between 0 and 7, with 0 being severe and 7 being all. • history—Enables history debug output for backup-restore. Set level betw 0 and 7, with 0 being severe and 7 being all. • restore—Enables restore debug output for backup-restore. Set level betw 0 and 7, with 0 being severe and 7 being all.
cdp	Enables debugging Cisco Discovery Protocol configuration related errors o events. • all—Enables all Cisco Discovery Protocol configuration debug output level between 0 and 7, with 0 being severe and 7 being all. • config—Enables configuration debug output for Cisco Discovery Proto Set level between 0 and 7, with 0 being severe and 7 being all. • infra—Enables infrastructure debug output for Cisco Discovery Proto Set level between 0 and 7, with 0 being severe and 7 being all.

config	Enables debugging the Cisco ISE configuration related errors or events • all—Enables all configuration debug output. Set level between 0 an 0 being severe and 7 being all. • backup—Enables backup configuration debug output. Set level be and 7, with 0 being severe and 7 being all. • clock—Enables clock configuration debug output. Set level betwe 7, with 0 being severe and 7 being all. • infra—Enables configuration infrastructure debug output. Set level 0 and 7, with 0 being severe and 7 being all. • kron—Enables command scheduler configuration debug output. S between 0 and 7, with 0 being severe and 7 being all. • network—Enables network configuration debug output. Set level 0 and 7, with 0 being severe and 7 being all. • repository—Enables repository configuration debug output. Set level 0 and 7, with 0 being severe and 7 being all. • service—Enables service configuration debug output. Set level bet and 7, with 0 being severe and 7 being all.
copy	Enables debugging copy commands. Set level between 0 and 7, with 0 severe and 7 being all.
locks	Enables debugging resource locking related errors or events. • all—Enables all resource locking debug output. Set level between with 0 being severe and 7 being all. • file—Enables file locking debug output. Set level between 0 and 7 being severe and 7 being all.
logging	Enables debugging logging configuration related errors or events. all—Enables all logging configuration debug output. Set level between with 0 being severe and 7 being all.
snmp	Enables debugging SNMP configuration related errors or events. all—Enables all SNMP configuration debug output. Set level between with 0 being severe and 7 being all.

system	Enables debugging Cisco ISE system related errors and events. • all—Enables all system files debug output. Set level between 0 and 7, 0 being severe and 7 being all. • id—Enables system ID debug output. Set level between 0 and 7, with being severe and 7 being all. • info—Enables system info debug output. Set level between 0 and 7, w being severe and 7 being all. • init—Enables system init debug output. Set level between 0 and 7, wit being severe and 7 being all.
transfer	Enables debugging file transfer. Set level between 0 and 7, with 0 being sev and 7 being all.
user	Enables debugging user management. • all—Enables all user management debug output. Set level between 0 a 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 b all.
utils	Enables debugging utilities configuration related errors and events. all—Enables all utilities configuration debug output. Set level between 0 a with 0 being severe and 7 being all.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

delete

To delete a file from the Cisco ISE server, use the **delete** command in EXEC mode.

delete [*filename disk:/path*]

Syntax Description

filename	Filename. Supports up to 80 alphanumeric characters.
disk:/path	Location of the file in the repository.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

dir

To list a file from the Cisco ISE server, use the **dir** command in EXEC mode.

dir

dir *disk:/logs*

dir recursive

Syntax Description

directory-name	Directory name. Supports up to 80 alphanumeric characters. Requires **disk:/** preceding the directory name.
recursive	(Optional). Lists directories and files in the local file system.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

None.

Example 1

```
iseadmin#dir

Directory of disk:/

 4096 Jun 19 2022 00:01:31 corefileanalysis/
 4096 Jun 18 2022 21:33:58 corefiles/
 4096 Jun 18 2022 23:22:31 CSD-config-backup/
 4096 Jun 20 2022 14:33:12 gc/
16552 Jun 18 2022 21:35:15 upgraderpms.log

  Usage for disk: filesystem
   42673885184 bytes total used
   220581744640 bytes free
   277419163648 bytes available
```

Example 2

```
iseadmin#dir disk:/corefiles

Directory of disk:/


  Usage for disk: filesystem
   42674413568 bytes total used
   220581216256 bytes free
   277419163648 bytes available
```

Example 3

```
iseadmin#dir recursive

Directory of disk:/

.:
 4096 Jun 19 2022 00:01:31 corefileanalysis/
 4096 Jun 18 2022 21:33:58 corefiles/
 4096 Jun 18 2022 23:22:31 CSD-config-backup/
 4096 Jun 20 2022 14:33:12 gc/
16552 Jun 18 2022 21:35:15 upgraderpms.log

./corefileanalysis:

./corefiles:

./CSD-config-backup:

./gc:
490314 Jun 20 2022 15:01:01 gc_app.log.20220620143312.0.current

  Usage for disk: filesystem
   42674921472 bytes total used
   220580708352 bytes free
   277419163648 bytes available
```

esr

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

esr

Syntax Description

This command has no keywords and arguments.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.2.0.470	This command was introduced.

Usage Guidelines

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

exit

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

This command has no keywords and arguments.

exit

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Example

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

forceout

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

forceout *username*

Syntax Description

username	Name of the user. Supports up to 31 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

generate-password

To generate a user password that complies with the Cisco ISE password policy, use the command **generate-password** in EXEC mode..

Syntax Description

<word>	Username for which password has to be generated (maximum length is

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

You can also generate a user password through the Cisco ISE GUI when you add a new admin user. In the Cisco ISE GUI, from the main menu, choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Users** > **Add New User**. In the **Password** area, click **Generate Password** to automatically generate and assign a password for the admin user you are adding.

In the Cisco ISE CLI, you can generate an admin user password that complies with the Cisco ISE password policy using the **generate-password** command.

Example

```
ise/admin# generate-password <username>
1pNn
ise/admin#configure terminal
Entering configuration mode terminal
ise/admin(config)#username <username> ?
Possible completions:
 password  Password and user role
ise/admin(config)#username <username> password plain ?
Description: Password. Use of % character must be escaped with (Max Size - 127)
Possible Completions:
 <AES encrypted string, min: 1 units, max: 200 units>
ise/admin(config)#username <username> password plain 1pNn ?
Possible completions:
 role
ise/admin(config)#username <username> password plain 1pNn role admin ?
Possible completions:
 disabled  User is diabled
 email  User email address
 <cr>
```

halt

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

This command has no keywords and arguments.

halt

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Before you issue the **halt** command, ensure that Cisco ISE is not performing any backup, restore, installation, upgrade, or remove operation. First, run the **application stop ise** command to stop Cisco ISE processes. Then, run the **halt** command.

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#
```

idle-timeout

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

idle-timeout *seconds*

Syntax Description

session-timeout	Sets the inactivity timeout for all sessions.
seconds	Number of seconds for the inactivity timeout. The valid range is from 0 to

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
3.2	This command was introduced.

Usage Guidelines

Setting the **idle-timeout** command to zero (0) results in no timeout being set.

Example

```
ise/admin# idle-timeout 40
```

licence esr

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

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

Syntax Description

classic	Enables ESR classic licensing.
smart	Enables ESR smart licensing.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.2.0.470	This command was introduced.

For information on how to disable **licence esr**, see "Configure RADIUS IPSec on Cisco ISE" in the chapter "Secure Access" in the *Cisco ISE Administrator Guide* Release 2.7 and above.

Usage Guidelines

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

mkdir

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

mkdir *directory-name*

Syntax Description

directory-name	Name of the directory to create. Supports up to 80 alphanumeric charact *disk:/directory-name*.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

nslookup

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

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

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

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

Syntax Description

ip-address	IPv4 or IPv6 address of a remote system. Supports up to 64 alphanumeric characters.
hostname	Hostname of a remote system. Supports up to 64 alphanumeric characters.
name-server	Specifies an alternative name server. Supports up to 64 alphanumeric charac
querytype	Queries the IPv4 or IPv6 address or hostname of a remote system. It includ query types, such as PTR, A, AAAA, and SRV. Supports up to 16 alphanun characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Example 1

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

Example 2

```
ise/admin# nslookup ipv6.google.com querytype AAAA
Server:         10.106.230.244
Address:        10.106.230.244#53
Non-authoritative answer:
ipv6.google.com canonical name = ipv6.l.google.com.
ipv6.l.google.com       has AAAA address 2404:6800:4007:803::1001
Authoritative answers can be found from:
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns2.google.com.
```

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

password

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

In Cisco ISE Release 3.2, to create a password with the hash symbol (#) or exclamation mark (!), you must first enter the backslash symbol (\). For example: **abc\!23**, **abc\12#**, and so on.

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

You can fix this by logging into the console and using the CLI command, or by getting an ISE CD or ISO file. Instructions for using an ISO to reset the password are explained in the following document: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200568-ISE-Password-Recovery-Mechanisms.html

Syntax Description

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

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	To create a password with the hash symbol (#) or exclamation mark (!), you must first enter the backslash symbol (\). For example: **abc\!23**, **abc\12#**, and so on.

Example

```
ise/admin# password
Enter old password:
Enter new password:
Confirm new password:
ise/admin#
```

patch install

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

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

patch install *patch-bundle* **repository**

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

Syntax Description

install	Installs a specific patch bundle of the application.
patch-bundle	The patch bundle file name. Supports up to 255 alphanumeric character
repository	Installs the patch in the specified repository name. Supports up to 255 alphanumeric characters.

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

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

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Installs a specific patch bundle of the application.

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

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

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

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

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

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

Example

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

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

Patch successfully installed
ise/admin#
```

patch remove

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

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

patch [**remove** {*application_name* | *version*}]

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

Syntax Description

remove	The command that removes a specific patch bundle version of the appli
application_name	The name of the application for which the patch is to be removed. Supp to 255 alphanumeric characters.
version	The patch version number to be removed. Supports up to 255 alphanum characters.

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

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

```
% Patch is not installed
```

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

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

Example 1

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

Example 2

```
ise/admin# patch remove ise 3
Continue with application patch uninstall? [y/n] y
% Patch is not installed
ise/admin#
```

permit rootaccess

To access the root of the Cisco ISE CLI, use the **permit rootaccess** command in EXEC mode.

permit rootaccess

Note You must submit the Challenge Token Request as a part of TAC case to obtain the Challenge Response. This TAC case is valid only for 15 minutes. If you did not receive a Challenge Response within 15 minutes, then you must submit it again. The root access received from TAC will be locked by the challenge/response process once you exit the root level access.

Syntax Description

This command has no keywords and arguments.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.7.0.349	This command was introduced.

Example

The following example shows how to access the root of the Cisco ISE CLI:

```
ise/admin##
ise/admin# permit rootaccess
1.  Generate Challenge Token Request
2.  Enter Challenge Response for Root Access
3.  Show History
4.  Exit
Enter CLI Option:
1
Generating Challenge.....................................
Challenge String (Please copy everything between the asterisk lines exclusively):
********************************************************************************
GlXZgWQEBAQWWBgEWWWWAClmUgbOnitBWQLw+ED3pn7HnJy3OQAWWAhGANUUHWZUVEQQJANUUJACJJD2NQNjgvLTWtEWOWZS0wZjYTTdlZDlMQQM2WNQ=
********************************************************************************
Starting background timer of 15mins
1.  Generate Challenge Token Request
2.  Enter Challenge Response for Root Access
3.  Show History
4.  Exit
Enter CLI Option:
2
Please input the response when you are ready .........................
[redacted]
Response Signature Verified successfully !
Granting shell access
sh-4.2# ls
2.4backup                               config          CT_Deme_Test_Rpm
ct_rolling.txt     lost+found            threadHeapDumpGntr.sh
backup_anc-2.7.0-115.jar                corefiles       CT_engine-2.7.0-1.0.x86_64.rpm
```

```
err.out            prrt-server.log         tomcat-process-log.txt
backup_guestaccess-upgrade-2.7.0-115.jar  corestacks.txt  ct_persistent.txt
Heap_dump20190705  libciscosafec.so.4.0.1  Thread_dump_2019-07-05-19:07:30
sh-4.2# exit
exit
Root shell exited
1.  Generate Challenge Token Request
2.  Enter Challenge Response for Root Access
3.  Show History
4.  Exit
Enter CLI Option:
3
**********************************
                SN No : 1
**********************************
Challenge
3/wyAAMQEBAQAAAAAAAAAAM89hCTWAAAAAAAAAA
```

ping

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

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

Syntax Description

ip-address	IP address of the system to ping. Supports up to 32 alphanumeric chara
hostname	Hostname of the system to ping. Supports up to 32 alphanumeric chara
df	(Optional). Specification for packet fragmentation.
df	Specify the value as 1 to prohibit packet fragmentation, or 2 to fragmen packets locally, or 3 to not set df.
packetsize	(Optional). Size of the ping packet.
packetsize	Specify the size of the ping packet; the value can be between 0 and 655
pingcount	(Optional). Number of ping echo requests.
pingcount	Specify the number of ping echo requests; the value can be between 1 a

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

ping6

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

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

Syntax Description

ip-address	IP address of the system to ping. Supports up to 64 alphanumeric character
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

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

Example 1

```
ise/admin# ping6 3ffe:302:11:2:20c:29ff:feaf:da05
PING 3ffe:302:11:2:20c:29ff:feaf:da05(3ffe:302:11:2:20c:29ff:feaf:da05) from
3ffe:302:11:2:20c:29ff:feaf:da05 eth0: 56 data bytes
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=0 ttl=64 time=0.599 ms
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=1 ttl=64 time=0.150 ms
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=2 ttl=64 time=0.070 ms
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=3 ttl=64 time=0.065 ms
--- 3ffe:302:11:2:20c:29ff:feaf:da05 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3118ms
rat min./aft/max/endive = 0.065/0.221/0.599/0.220 ms, pipe 2
ise/admin#
```

Example 2

```
ise/admin# ping6 3ffe:302:11:2:20c:29ff:feaf:da05 GigabitEthernet 0 packetsize 10 pingcount
 2
PING 3ffe:302:11:2:20c:29ff:feaf:da05(3ffe:302:11:2:20c:29ff:feaf:da05) from
3ffe:302:11:2:20c:29ff:feaf:da05 eth0: 10 data bytes
18 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=0 ttl=64 time=0.073 ms
18 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=1 ttl=64 time=0.073 ms
--- 3ffe:302:11:2:20c:29ff:feaf:da05 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1040ms
rat min./aft/max/endive = 0.073/0.073/0.073/0.000 ms, pipe 2
ise/admin#
```

reload

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

reload [**cli**]

Syntax Description

cli	Restart the underlying Confd processes and generate the CLI again with upd values.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	The cli variable is introduced.

Usage Guidelines

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

Before you issue the **reload** command, ensure that Cisco ISE is not performing any backup, restore, installation, upgrade, or remove operation. First, run the **application stop ise** command to stop Cisco ISE processes. Then, run the **reload** command.

If Cisco ISE performs any of these operations and you issue the **reload** command, you get one of the following warning messages:

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

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

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

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

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

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

If automatic failover is enabled in your deployment, you receive the following warning message:

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

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

In Cisco ISE 3.1 and earlier releases, when you carry out an operation such as adding a new NIC card to Cisco ISE, the running-config and other appropriate commands are updated automatically to reflect the change. In Cisco ISE Release 3.2, you must enter the **reload cli** command to reload the Cisco ISE CLI. Then, the newly added NIC card information is displayed in running-config and other related areas.

Note The Cisco ISE CLI service is interrupted for a few minutes when you run the **reload cli** command.

Example 1

```
ise/admin# reload
Continue with reboot? [y/n]
```

Example 2

```
ise/iseadmin#reload cli
%WARNING: : The Cisco ISE CLI will restart now and will be unavailable for a few minutes.
 Do you want to continue (yes/no) [no] ?yes
Connection to ise closed.
```

reset-config

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

reset-config

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.2.0.470	This command was introduced.

Usage Guidelines

All services will be restarted upon completion.

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

restore

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

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

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

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

Syntax Description

filename	Name of the backed-up file that resides in the repository. Supports up to alphanumeric characters. **Note** You must add the .tar.gpg extension after the filename (for ex myfile.tar.gpg).
repository	The repository command.
repository-name	Name of the repository from which you want to restore the backup. Sup to 120 characters.
encryption-key	(Optional). Specifies user-defined encryption key to restore backup.
hash	Hashed encryption key for restoring backup. Specifies an encrypted (ha encryption key that follows. Supports up to 40 characters.
plain	Plaintext encryption key for restoring backup. Specifies an unencrypted p encryption key that follows. Supports up to 15 characters.
encryption-key-name	Specifies encryption key in hash | plain format.
include-adeos	Restores back up and reboots Cisco ISE, if ADE-OS configuration data is in the backup

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

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

Restoring Cisco ISE Configuration Data from the Backup

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

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

Example

```
ise/admin# restore latest-jul-15-CFG-140715-2055.tar.gpg repository CUSTOMER-DB-sftp
encryption-key plain Test_1234
% Warning: Do not use Ctrl-C or close this terminal window until the restore completes.
Initiating restore.  Please wait...
% restore in progress: Starting Restore...10% completed
% restore in progress: Retrieving backup file from Repository...20% completed
% restore in progress: Decrypting backup data...25% completed
% restore in progress: Extracting backup data...30% completed
 Leaving the currently connected AD domain
Please rejoin the AD domain from the administrative GUI
% restore in progress: Stopping ISE processes required for restore...35% completed
% restore in progress: Restoring ISE configuration database...40% completed
% restore in progress: Adjusting host data for upgrade...65% completed
UPGRADE STEP 1: Running ISE configuration DB schema upgrade...
- Running db sanity check to fix index corruption, if any...

UPGRADE STEP 2: Running ISE configuration data upgrade...
- Data upgrade step 1/67, NSFUpgradeService(1.2.1.127)... Done in 0 seconds.
- Data upgrade step 2/67, NetworkAccessUpgrade(1.2.1.127)... Done in 0 seconds.
- Data upgrade step 3/67, GuestUpgradeService(1.2.1.146)... Done in 43 seconds.
- Data upgrade step 4/67, NetworkAccessUpgrade(1.2.1.148)... Done in 2 seconds.
- Data upgrade step 5/67, NetworkAccessUpgrade(1.2.1.150)... Done in 2 seconds.
- Data upgrade step 6/67, NSFUpgradeService(1.2.1.181)... Done in 0 seconds.
- Data upgrade step 7/67, NSFUpgradeService(1.3.0.100)... Done in 0 seconds.
- Data upgrade step 8/67, RegisterPostureTypes(1.3.0.170)... Done in 0 seconds.
- Data upgrade step 9/67, ProfilerUpgradeService(1.3.0.187)... Done in 5 seconds.
- Data upgrade step 10/67, GuestUpgradeService(1.3.0.194)... Done in 2 seconds.
- Data upgrade step 11/67, NetworkAccessUpgrade(1.3.0.200)... Done in 0 seconds.
- Data upgrade step 12/67, GuestUpgradeService(1.3.0.208)... Done in 2 seconds.
- Data upgrade step 13/67, GuestUpgradeService(1.3.0.220)... Done in 0 seconds.
- Data upgrade step 14/67, RBACUpgradeService(1.3.0.228)... Done in 15 seconds.
- Data upgrade step 15/67, NetworkAccessUpgrade(1.3.0.230)... Done in 3 seconds.
- Data upgrade step 16/67, GuestUpgradeService(1.3.0.250)... Done in 0 seconds.
- Data upgrade step 17/67, NetworkAccessUpgrade(1.3.0.250)... Done in 0 seconds.
- Data upgrade step 18/67, RBACUpgradeService(1.3.0.334)... Done in 9 seconds.
- Data upgrade step 19/67, RBACUpgradeService(1.3.0.335)... Done in 9 seconds.
```

```
- Data upgrade step 20/67, ProfilerUpgradeService(1.3.0.360)... ...Done in 236 seconds.
- Data upgrade step 21/67, ProfilerUpgradeService(1.3.0.380)... Done in 4 seconds.
- Data upgrade step 22/67, NSFUpgradeService(1.3.0.401)... Done in 0 seconds.
- Data upgrade step 23/67, NSFUpgradeService(1.3.0.406)... Done in 0 seconds.
- Data upgrade step 24/67, NSFUpgradeService(1.3.0.410)... Done in 2 seconds.
- Data upgrade step 25/67, RBACUpgradeService(1.3.0.423)... Done in 0 seconds.
- Data upgrade step 26/67, NetworkAccessUpgrade(1.3.0.424)... Done in 0 seconds.
- Data upgrade step 27/67, RBACUpgradeService(1.3.0.433)... Done in 1 seconds.
- Data upgrade step 28/67, EgressUpgradeService(1.3.0.437)... Done in 1 seconds.
- Data upgrade step 29/67, NSFUpgradeService(1.3.0.438)... Done in 0 seconds.
- Data upgrade step 30/67, NSFUpgradeService(1.3.0.439)... Done in 0 seconds.
- Data upgrade step 31/67, CdaRegistration(1.3.0.446)... Done in 2 seconds.
- Data upgrade step 32/67, RBACUpgradeService(1.3.0.452)... Done in 16 seconds.
- Data upgrade step 33/67, NetworkAccessUpgrade(1.3.0.458)... Done in 0 seconds.
- Data upgrade step 34/67, NSFUpgradeService(1.3.0.461)... Done in 0 seconds.
- Data upgrade step 35/67, CertMgmtUpgradeService(1.3.0.462)... Done in 2 seconds.
- Data upgrade step 36/67, NetworkAccessUpgrade(1.3.0.476)... Done in 0 seconds.
- Data upgrade step 37/67, TokenUpgradeService(1.3.0.500)... Done in 1 seconds.
- Data upgrade step 38/67, NSFUpgradeService(1.3.0.508)... Done in 0 seconds.
- Data upgrade step 39/67, RBACUpgradeService(1.3.0.509)... Done in 17 seconds.
- Data upgrade step 40/67, NSFUpgradeService(1.3.0.526)... Done in 0 seconds.
- Data upgrade step 41/67, NSFUpgradeService(1.3.0.531)... Done in 0 seconds.
- Data upgrade step 42/67, MDMUpgradeService(1.3.0.536)... Done in 0 seconds.
- Data upgrade step 43/67, NSFUpgradeService(1.3.0.554)... Done in 0 seconds.
- Data upgrade step 44/67, NetworkAccessUpgrade(1.3.0.561)... Done in 3 seconds.
- Data upgrade step 45/67, RBACUpgradeService(1.3.0.563)... Done in 19 seconds.
- Data upgrade step 46/67, CertMgmtUpgradeService(1.3.0.615)... Done in 0 seconds.
- Data upgrade step 47/67, CertMgmtUpgradeService(1.3.0.616)... Done in 15 seconds.
- Data upgrade step 48/67, CertMgmtUpgradeService(1.3.0.617)... Done in 2 seconds.
- Data upgrade step 49/67, OcspServiceUpgradeRegistration(1.3.0.617)... Done in 0 seconds.
- Data upgrade step 50/67, NSFUpgradeService(1.3.0.630)... Done in 0 seconds.
- Data upgrade step 51/67, NSFUpgradeService(1.3.0.631)... Done in 0 seconds.
- Data upgrade step 52/67, CertMgmtUpgradeService(1.3.0.634)... Done in 0 seconds.
- Data upgrade step 53/67, RBACUpgradeService(1.3.0.650)... Done in 8 seconds.
- Data upgrade step 54/67, CertMgmtUpgradeService(1.3.0.653)... Done in 0 seconds.
- Data upgrade step 55/67, NodeGroupUpgradeService(1.3.0.655)... Done in 1 seconds.
- Data upgrade step 56/67, RBACUpgradeService(1.3.0.670)... Done in 4 seconds.
- Data upgrade step 57/67, ProfilerUpgradeService(1.3.0.670)... Done in 0 seconds.
- Data upgrade step 58/67, ProfilerUpgradeService(1.3.0.671)... Done in 0 seconds.
- Data upgrade step 59/67, ProfilerUpgradeService(1.3.0.675)...
.................................Done in 2118 seconds.
- Data upgrade step 60/67, NSFUpgradeService(1.3.0.676)... Done in 1 seconds.
- Data upgrade step 61/67, 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 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 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 Application Server...
Stopping ISE Profiler DB...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
% restore in progress: starting dbrestore.......55% completed
% restore in progress: ending dbrestore.......75% completed
 checking for upgrade
Starting M&T DB upgrade
ISE Database processes already running, PID: 30124
ISE M&T Session Database is already running, PID: 484
Starting ISE Profiler DB...
Starting ISE Application Server...
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
% restore in progress: Restoring ISE configuration database...40% completed
% restore in progress: Updating Database metadata...70% completed
% restore in progress: Restoring logs...75% completed
% restore in progress: Performing ISE Database synchup...80% completed
% restore in progress: Completing Restore...100% completed
Broadcast message from root (pts/2) (Fri Apr  5 01:40:04 2013):
The system is going down for reboot NOW!
Broadcast message from root (pts/2) (Fri Apr  5 01:40:04 2013):
The system is going down for reboot NOW!
ise/admin#
```

rmdir

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

rmdir *directory-name*

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Example

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

screen-length

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

screen-length *integer*

Syntax Description

length	Sets the number of rows on the current terminal screen for the current s
integer	Number of rows on the screen. The valid range is from 0 to 511 rows. A of zero (0) disables pausing between screens of output.

Command Default

The default number of rows on the current terminal screen for the current session is 24.

Command Modes

EXEC

Command History

Release	Modification
3.2	This command was introduced.

Usage Guidelines

The system uses the length value to determine when to pause during multiple-screen output. The valid range is from 0 to 511.

Example

```
ise/admin# screen-length 24
```

screen-width

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

screen-width *integer*

Syntax Description

width	Sets the number of columns on the current terminal screen for the current ses
integer	Number of columns on the screen. The default value is 0, which correspond full screen. The valid range is from 0 to 511.

Command Default

The default value is 0, which corresponds to full screen.

Command Modes

EXEC

Command History

Release	Modification
3.2	This command was introduced.

Usage Guidelines

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

Example

```
ise/admin# screen-width 124
```

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

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

Command Default

Disabled.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

Example 1

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

Example 2

```
ise/admin# ssh delete host ise
ise/admin#
```

tech

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

Syntax Description

dumptcp	Dumps TCP package to the console.
interface	Specify interface name.
stop	Stops all the running TCP dump processes on the node.
iostat	Dumps Central Processing Unit (CPU) statistics and input/output statist devices and partitions to the console for every 3 seconds. See Linux ios command.
iotop	Provides accurate I/O usage per process on ISE node.
killgdb	Kills the GDB process based on the ProcessID
mpstat	Dumps processors related information sent to the console. See Linux m command.
netstat	Dumps network related information sent to the console for every 3 seco Linux netstat command.
top	Dumps a dynamic real-time view of a running system, which runs in bat for every 5 seconds. See Linux top command.
vmstat	Dumps summary information of memory, processes, and paging for eve seconds. See Linux vmstat command.

Command Default

Disabled.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

From Cisco ISE Release 3.0 onwards, the **tech dumptcp** command has the following options as available interfaces:

- br-<...>
- docker0
- GigabitEthernet0 (and other GigabitEthernet interfaces if available)

- lo
- veth<...>

Example 1

```
ise/admin# tech dumptcp 0 count 2
Invoking tcpdump. Press Control-C to interrupt.
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
2 packets captured
2 packets received by filter
0 packets dropped by kernel
02:38:14.869291 IP (tos 0x0, ttl 110, id 4793, offset 0, flags [DF], proto: TCP (6), length:
 40) 10.77.202.52.1598 > 172.21.79.91.22: ., cksum 0xe105 (correct),
 234903779:234903779(0) ack 664498841 win 63344
02:38:14.869324 IP (tos 0x0, ttl  64, id 19495, offset 0, flags [DF], proto: TCP (6), length:
 200) 172.21.79.91.22 > 10.77.202.52.1598: P 49:209(160) ack 0 win
12096
ise/admin#
```

Example 2

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

Example 3

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

Interpreting CPU and Memory Usage Data

Usage Guidelines

The **tech top** command output has the following options that provide information on memory and CPU usage:

- top shows uptime information
- Tasks shows process status information.
- %Cpu(s) shows various processor values.

- MiB Mem displays physical memory utilization. This value is based on the total amount of physical RAM installed on the system and provides the following information:
  - total shows total installed memory.
  - free shows available memory.
  - Used shows consumed memory.
  - buff/cache shows the amount of information cached to be written later.
- MiB Swap displays virtual memory utilization. OS can take advantage of virtual memory when physical memory space is used by borrowing storage space from storage disks. The process of swapping data back and forth between physical RAM and storage drives is time-consuming and uses system resources, so it is best to minimize the use of virtual memory. MiB Swap output provides the following information:
  - total shows total swap space.
  - free shows available swap space.
  - used shows consumed swap space.
  - buff/cache shows the amount of information cached for future reads.
- Load Average: The load average is broken down into three time increments. The first value displays the load for the last one minute, the second value for the last five minutes, and the final value for the last fifteen-minutes. For Cisco ISE high load average, use the five-minute interval. If the five-minute interval value goes beyond the cores allocated to the node, the load average alarm is triggered.

  Do not consider individual core usage, always monitor the load average for CPU or I/O consumption.

Example:

```
ise/admin# tech top
top - 06:33:08 up 13:03, 1 user
Tasks: 559 total, 1 running, 557 sleeping, 0 stopped, 1 zombie
%Cpu(s): 1.8 us, 0.7 sy, 0.0 ni, 97.3 id, 0.0 wa, 0.2 hi, 0.1 si, 0.0 st
MiB Mem: 31928.6 total, 5691.9 free, 22647.7 used, 3589.1 buff/cache
MiB Swap: 8000.0 total, 7126.7 free, 873.2 used. 6765.0 avail Mem
load average: 0.30, 0.38, 0.66
ise/admin#
```

terminal

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

terminal

Syntax Description

type	Defines the terminal name and type, and permits terminal negotiation by ho that provide that type of service. Supports up to 80 alphanumeric character

Command Default

VT100

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	The command is updated and no longer supports the variable *terminal-type*

Usage Guidelines

Indicates the terminal type if it is different from VT100.

You can also use the **show terminal** command to view the information on terminal type.

Example

```
ise/admin# terminal vt220
ise/admin#
```

traceroute

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

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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Example

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

undebug

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

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

Syntax Description

all	Disables all debugging.
application	Application files. • all—Disables all application debug output. • install—Disables application install debug output. • operation—Disables application operation debug output. • uninstall—Disables application uninstall debug output.
backup-restore	Backs up and restores files. • all—Disables all debug output for backup-restore. • backup—Disables backup debug output for backup-restore. • backup-logs—Disables backup-logs debug output for backup-restore. • history—Disables history debug output for backup-restore. • restore—Disables restore debug output for backup-restore.
cdp	Cisco Discovery Protocol configuration files. • all—Disables all Cisco Discovery Protocol configuration debug outpu • config—Disables configuration debug output for Cisco Discovery Prot • infra—Disables infrastructure debug output for Cisco Discovery Proto
config	Configuration files. • all—Disables all configuration debug output. • backup—Disables backup configuration debug output. • clock—Disables clock configuration debug output. • infra—Disables configuration infrastructure debug output. • kron—Disables command scheduler configuration debug output. • network—Disables network configuration debug output. • repository—Disables repository configuration debug output. • service—Disables service configuration debug output.

copy	Copy commands.
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

Command History

Release	Modification
2.0.0.306	This command was introduced.

Example

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

who

To display the details of the current user, use the **who** command in EXEC mode.

who

Syntax Description

This command has no keywords and arguments.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
3.2	This command was introduced.

Usage Guidelines

None.

Example

The following example shows the output of the **who** command:

```
ise/admin# who
Session User  Context From          Proto Date     Mode
*188    admin cli     xx.xxx.xxx.xx ssh   17:05:50 operational
```

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.

Note From Cisco ISE Release 3.0 onwards, if there is an escape character required after running certain show commands, press **Ctrl+C** and then press **Q**.

- show, on page 101
- show application, on page 102
- show backup, on page 105
- show banner, on page 107
- show cdp, on page 108
- show clock, on page 110
- show container, on page 111
- show cpu, on page 115
- show crypto, on page 117
- show disks, on page 118
- show esr status, on page 120
- show icmp-status, on page 121
- show interface, on page 123
- show inventory, on page 125
- show ip, on page 127
- show ipv6 route, on page 128
- show logging, on page 129
- show logins, on page 132
- show memory, on page 133
- show ntp, on page 134
- show ports, on page 135
- show process, on page 137
- show repository, on page 139
- show restore, on page 141
- show running-config, on page 142

- show snmp-server engineid, on page 143
- show snmp-server user, on page 144
- show tech-support, on page 145
- show terminal, on page 147
- show timezone, on page 148
- show timezones, on page 149
- show udi, on page 150
- show uptime, on page 151
- show users, on page 152
- show version, on page 153

show

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

show *keyword*

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

show application

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

show application > *file-name*

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

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

Syntax Description

>	Redirects output to a file.
file-name	Name of the file to store the Cisco ISE application information.
status	Displays the status of the installed application.
version	Displays the application version for an installed application (Cisco ISE).
application_name	Name of the installed application.
|	Output modifier variables: • begin—Matched pattern. Supports up to 80 alphanumeric characters. • count—Count the number of lines in the output. Add number after the v count. |—Output modifier variables for count. • end—End with line that matches. Supports up to 80 alphanumeric charac • exclude—Exclude lines that match. Supports up to 80 alphanumeric characters. • include—Include lines that match. Supports up to 80 alphanumeric characters. • last—Display last few lines of output. Add number after the word last Supports up to 80 lines to display. Default 10. |—Output modifier variables for last.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example 1

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

Example 2

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

Example 2

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

Example 3

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

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

```
iseadmin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      not running
Application Server                     not running
Profiler Database                      not running
ISE Indexing Engine                    not running
AD Connector                           not running
M&T Session Database                   not running
M&T Log Processor                      not running
Certificate Authority Service          not running
EST Service                            not running
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
```

```
PassiveID SPAN Service                disabled
DHCP Server (dhcpd)                   disabled
DNS Server (named)                    disabled
ISE Messaging Service                 not running
ISE API Gateway Database Service      not running
ISE API Gateway Service               not running
ISE EDDA Service                      not running
Segmentation Policy Service           disabled
REST Auth Service                     disabled
SSE Connector                         disabled
Hermes (pxGrid Cloud Agent)           disabled
McTrust (Meraki Sync Service)         disabled
ISE Node Exporter                     not running
ISE Prometheus Service                not running
ISE Grafana Service                   not running
ISE MNT LogAnalytics Elasticsearch    disabled
ISE Logstash Service                  disabled
ISE Kibana Service                    disabled
```

show backup

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

show backup [**history** | **status**]

Syntax Description

history	Displays historical information about backups on the system.
progress	Displays the backup status on the system.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example 1

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

Example 2

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

```
success
ise/admin#
```

show banner

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

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

The banners are configured in the Cisco ISE GUI in the following window:

Administration > **System** > **Admin Access** > **Settings** > **Access**. The **Session** tab contains the fields for configuring the pre-login and post-login banners for Cisco ISE CLI and GUI.

Syntax Description

post-login	Displays the post-login information that is configured in the Cisco ISE s the current CLI session.
pre-login	Displays the pre-login information that is configured in the Cisco ISE s the current CLI session.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

show cdp

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

show cdp [**all** | **neighbors**]

Syntax Description

all	Shows all enabled Cisco Discovery Protocol interfaces.
neighbors	Shows the Cisco Discovery Protocol neighbors.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Note CDP can be visualized from neighboring IPv4 and IPv6 interfaces

Example 1

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

Example 2

```
ise/admin# show cdp neighbors
CDP Neighbor: 000c297840e5
        Local Interface : GigabitEthernet0
        Device Type     : ISE-1141VM-K9
        Port            : eth0
        Address         : 172.23.90.114
        IPv6 Address    : 2001:420:54ff:4::458:1
CDP Neighbor: isexp-esw5
        Local Interface : GigabitEthernet0
        Device Type     : cisco WS-C3560E-24TD
        Port            : GigabitEthernet0/5
        Address         : 172.23.90.45
       IPv6 Address     : 2001:420:54ff:4::458:5
CDP Neighbor: 000c29e29926
        Local Interface : GigabitEthernet0
        Device Type     : ISE-1141VM-K9
```

```
        Port            : eth0
        Address         : 172.23.90.115
       IPv6 Address     : 2001:420:54ff:4::458:2
CDP Neighbor: 000c290fba98
        Local Interface : GigabitEthernet0
        Device Type     : ISE-1141VM-K9
        Port            : eth0
        Address         : 172.23.90.111
       IPv6 Address     : 2001:420:54ff:4::458:3
ise/admin#
```

show clock

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

This command has no keywords and arguments.

show clock

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

show container

To view information about the Threat-Centric NAC adapters, use the **show container** command in EXEC mode.

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

show container tc-nac {**adapters** | **all** | **inspect** {**container-id** *container-id* | **container-name** *container-name*} | **stats** {**container-id** *container-id* | **container-name** *container-name*}} |}

Syntax Description

tc-nac	Displays information about the Threat-Centric NAC adapters.
all	When used with TC NAC, lists all the adapters that are available in Cis including the container name and ID. When used with Wi-Fi Setup, displays the Wi-Fi container setup inform
adapters	Lists the TC NAC adapters that are configured in Cisco ISE. Lists the c ID and name, the time when the adapter was created and how long the a has been running, and the current status of the adapter.
inspect {**container-id** *container-id* | **container-name** *container-name*}	Lists detailed information about the specific adapter.
stats {**container-id** *container-id* | **container-name** *container-name*}	Provides statistical information about the specific adapter.
>	Redirects output to a file.
|	Output modifier variables: • begin—Matched pattern. Supports up to 80 alphanumeric characte • count—Count the number of lines in the output. Add number after t count. |—Output modifier variables for count. • end—End with line that matches. Supports up to 80 alphanumeric ch • exclude—Exclude lines that match. Supports up to 80 alphanumer characters. • include—Include lines that match. Supports up to 80 alphanumeric characters. • last—Display last few lines of output. Add number after the word Supports up to 80 lines to display. Default 10. |—Output modifier variables for last.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.2.0.470	This command was introduced.
3.1	This command no longer includes Wi-Fi configurations.

Usage Guidelines

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

Example 1

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

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

ise/admin#
```

Example 2

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

CONTAINER ID        IMAGE                   COMMAND                  CREATED
STATUS              PORTS                                                NAMES
63b8904f41c6        irf-adapter-nexpose     "/opt/CSCOcpm/vaservi"   19 hours ago
Up 19 hours                                                              nexpose
8389f7e249cf        irf-adapter-tenable     "/opt/CSCOcpm/vaservi"   2 days ago
Up 2 days                                                                tenable
41921c1539bf        irf-core-engine:2.2.6   "/bin/sh -c 'npm star"   3 days ago
Up 3 days           127.0.0.1:3000->3000/tcp
irf-core-engine-runtime
c4f6ff3cf628        irf-rabbitmq:2.2.6      "/docker-entrypoint.s"   3 days ago
Up 3 days          4369/tcp, 5671-5672/tcp, 15671-15672/tcp, 25672/tcp   irf-rabbitmq-runtime
e682a5a5ad69        irf-mongo:2.2.6         "/entrypoint.sh mongo"   3 days ago
Up 3 days           27017/tcp                                            irf-mongo-runtime

ise/admin#
```

Example 3

```
ise/admin#  show container tc-nac inspect container-name nexpose
[
{
    "Id": "63b8904f41c6ce2a58660d38eb3500104038e650e4e3365e21e0a536a1ba3044",
    "Created": "2016-09-22T11:38:03.146141316Z",
    "Path": "/opt/CSCOcpm/vaservice/nexposeadapter/bin/nexposeadaptercontrol.sh",
    "Args": [
        "start",
        "http://irf-core-engine-runtime:3000/api/adapter/instance/register",
        "07bc6aee-fb9f-4845-86cb-886c7c095188"
    ],
```

```
    "State": {
        "Status": "running",
        "Running": true,
        "Paused": false,
        "Restarting": false,
        "OOMKilled": false,
        "Dead": false,
        "Pid": 23433,
        "ExitCode": 0,
        "Error": "",
        "StartedAt": "2016-09-22T11:38:05.609439645Z",
        "FinishedAt": "0001-01-01T00:00:00Z"
    },
    "Image": "06ba3230bd64872b988f4506e7fffddc8c6374c7ece285555ee1cc57743ea7e0",
    "ResolvConfPath":
"/opt/docker/runtime/containers/63b8904f41c6ce2a58660d38eb3500104038e650e4e3365e21e0a536a1ba3044/resolv.conf",

    "HostnamePath":
"/opt/docker/runtime/containers/63b8904f41c6ce2a58660d38eb3500104038e650e4e3365e21e0a536a1ba3044/hostname",

    "HostsPath":
"/opt/docker/runtime/containers/63b8904f41c6ce2a58660d38eb3500104038e650e4e3365e21e0a536a1ba3044/hosts",

    "LogPath":
"/opt/docker/runtime/containers/63b8904f41c6ce2a58660d38eb3500104038e650e4e3365e21e0a536a1ba3044/

            63b8904f41c6ce2a58660d38eb3500104038e650e4e3365e21e0a536a1ba3044-json.log",
    "Name": "/nexpose",
    "RestartCount": 0,
    "Driver": "devicemapper",
    "ExecDriver": "native-0.2",
    "MountLabel": "",
    "ProcessLabel": "",
    "AppArmorProfile": "",
    "ExecIDs": [
        "d76578aa48118167d9d029037fcb2e56aa7dce8672b8991a736617a6d6879750"
    ],
    .
    .
    .
    "NetworkSettings": {
        "Bridge": "",
        "SandboxID": "9873fb92f86e665039a6de15bfe057bc3fd341f7b39acedee57cbd89b3f56ce0",
        "HairpinMode": false,
        "LinkLocalIPv6Address": "",
        "LinkLocalIPv6PrefixLen": 0,
        "Ports": {},
        "SandboxKey": "/var/run/docker/netns/9873fb92f86e",
        "SecondaryIPAddresses": null,
        "SecondaryIPv6Addresses": null,
        "EndpointID": "",
        "Gateway": "",
        "GlobalIPv6Address": "",
        "GlobalIPv6PrefixLen": 0,
        "IPAddress": "",
        "IPPrefixLen": 0,
        "IPv6Gateway": "",
        "MacAddress": "",
        "Networks": {
            "irf-internal-nw": {
                "EndpointID":
"8999c12319144cfd66a4e99be40f7fbc228779e43f2a7f20c48867b8b3ca7a49",
                "Gateway": "169.254.1.1",
                "IPAddress": "169.254.1.6",
```

```
                "IPPrefixLen": 24,
                "IPv6Gateway": "",
                "GlobalIPv6Address": "",
                "GlobalIPv6PrefixLen": 0,
                "MacAddress": "02:42:a9:fe:01:06"
            }
        }
    }
}
]
```


Example 4

```
ise/admin#  show container tc-nac stats container-name nexpose

CONTAINER           CPU %               MEM USAGE / LIMIT     MEM %               NET I/O
             BLOCK I/O
nexpose             0.07%               327.9 MB / 12.43 GB   2.64%               4.501 MB
 / 2.446 MB   106.4 MB / 21.27 MB
```

show cpu

To display CPU information, use the **show cpu** command in EXEC mode.

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

show cpu > *file-name*

show cpu statistics

show cpu usage

Syntax Description

>	Redirects output to a file.
file-name	Name of the file to redirect.
statistics	Displays CPU statistics.
cpu usage	Displays the CPU usage per component for an installed application (Cis
|	Output modifier variables: • begin—Matched pattern. Supports up to 80 alphanumeric characte • count—Count the number of lines in the output. Add number after t count. |—Output modifier variables for count. • end—End with line that matches. Supports up to 80 alphanumeric ch • exclude—Exclude lines that match. Supports up to 80 alphanumer characters. • include—Include lines that match. Supports up to 80 alphanumeric characters. • last—Display last few lines of output. Add number after the word Supports up to 80 lines to display. Default 10. |—Output modifier variables for last.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.1.0.474	This command was introduced.

Usage Guidelines

To view CPU information and its statistics, use the **show cpu** command.

Example 1

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

Example 2

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

Example 3

```
ise/admin# show cpu usage

ISE Function                          % CPU Usage           CPU Time     Number of threads
-------------------------------------------------------------------------------------------
Profiler Database                        0.01              1:26.27              3
M&T Session Database                     0.01              1:23.06             18
Certificate Authority Service            0.04              6:57.38             31
M&T Log Processor                        0.09             15:44.23             60
ISE Indexing Engine                      0.12             21:34.76             75
Database Listener                        0.01              0:53.18              2
Database Server                         0.36             62:48.64             64 processes

Admin Webapp                             0.04              6:46.68             53
Profiler                                 0.00              0:02.94             26
NSF Persistence Layer                    0.05              8:09.70             46
Guest Services                           0.00              0:00.32              5
Syslog Processor                         0.00              0:12.79              3
Quartz Scheduler                         0.05              9:08.80             29
RMI Services                             0.00              0:05.98             10
Message Queue                            0.00              0:43.99              4
BYOD Services                            0.00              0:00.00              1
Admin Process JVM Threads                0.19             32:50.67             10
Miscellaneous services                   0.17             30:30.47           3557
Identity Mapping Service                  N/A
SXP Engine Service                        N/A
Threat Centric NAC Docker Service         N/A
Threat Centric NAC MongoDB Container      N/A
Threat Centric NAC RabbitMQ Container     N/A
Threat Centric NAC Core Engine Container  N/A
Vulnerability Assessment Database         N/A
Vulnerability Assessment Service          N/A
```

show crypto

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

show crypto authorized_keys

show crypto host-keys

show crypto key

Syntax Description

authorized_keys	Displays authorized keys information for the user who is logged in curr
host_keys	Displays host keys for the user who is logged in currently.
key	Displays key information for the user who is logged in currently.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example 1

```
ise/iseadmin#show crypto authorized_keys
Authorized keys for iseadmin
ssh-rsa in netadmin@cjb
```

Example 2

```
ise/iseadmin#show crypto key
iseadmin public key: ssh-rsa in iseadmin@ise-1
```

show disks

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

show disks

Syntax Description

|	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 w count. |—Output modifier variables for count. • end—End with line that matches. Supports up to 80 alphanumeric charac • exclude—Exclude lines that match. Supports up to 80 alphanumeric characters. • include—Include lines that match. Supports up to 80 alphanumeric characters. • last—Display last few lines of output. Add number after the word last Supports up to 80 lines to display. Default 10. |—Output modifier variables for last.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	The filename variable is no longer supported.

Usage Guidelines

Only platforms that have a disk file system support the **show disks** command.

Example

```
ise/admin# show disks
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#
```

Note In Cisco ISE 3.0, the localdisk partition is allocated dynamically.

show esr status

To show the Embedded Services Router status, use the **show esr status** command in EXEC mode.

show esr status

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
3.2	This command was introduced.

Usage Guidelines

The comand **show esr status** replaces the command **service esr status** that was used in Cisco ISE Release 3.1 and earlier releases.

Examples

```
ise49/admin# show esr status
% ESR 5921 is enabled on eth1
```

```
ise49/admin# show esr status
% ESR 5921 is disabled
```

show icmp-status

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

show icmp_status | save *file_name*

Syntax Description

| save	Redirects output to a file.
file-name	Name of the file to redirect.
|	Output modifier commands: • *begin*—Matched pattern. Supports up to 80 alphanumeric characte • *count*—Count the number of lines in the output. Add number after t count. • |—Output modifier commands for count. • *end*—End with line that matches. Supports up to 80 alphanumeric ch • *exclude*—Exclude lines that match. Supports up to 80 alphanumer characters. • *include*—Include lines that match. Supports up to 80 alphanumeric characters. • last—Display last few lines of output. Add number after the word Supports up to 80 lines to display. Default 10. • |—Output modifier commands for last.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	To redirect the command output to a file, you must use **| save *file_name*** instead of **> *file-name***.

Usage Guidelines

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

Example 1

```
ise/admin# show icmp_status
```

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

Example 2

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

show interface

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

show interface | save *file_name*

show interface GigabitEthernet {*0-3*}

Syntax Description

| save	Redirects output to a file.
file-name	Name of the file to redirect interface information.
GigabitEthernet	Shows the specific Gigabit Ethernet interface information.
0-3	Gigabit Ethernet number that may be one of the fallowing: 0. 1, 2, 3.
|	Output modifier variables: • begin—Matched pattern. Supports up to 80 alphanumeric characte • count—Count the number of lines in the output. Add number after t count. • end—End with line that matches. Supports up to 80 alphanumeric ch • exclude—Exclude lines that match. Supports up to 80 alphanumer characters. • include—Include lines that match. Supports up to 80 alphanumeric characters. • last—Display last few lines of output. Add number after the word Supports up to 80 lines to display. Default 10.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	To redirect the command output to a file, you must use **| save *file_name*** instead of **> *file-name***.

Usage Guidelines

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

Example 1

```
ise/admin# show interface
eth0      Link encap:Ethernet  HWaddr 00:0C:29:6A:88:C4
          inet addr:172.23.90.113  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6a:88c4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:48536 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14152 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6507290 (6.2 MiB)  TX bytes:12443568 (11.8 MiB)
          Interrupt:59 Base address:0x2000
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1195025 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1195025 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:649425800 (619.3 MiB)  TX bytes:649425800 (619.3 MiB)
sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
ise/admin#
```

Example 2

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

show inventory

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

show inventory | save *file_name*

Syntax Description

| save	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 characte • count—Count the number of lines in the output. Add number after t count. • end—End with line that matches. Supports up to 80 alphanumeric ch • exclude—Exclude lines that match. Supports up to 80 alphanumer characters. • include—Include lines that match. Supports up to 80 alphanumeric characters. • last—Display last few lines of output. Add number after the word Supports up to 80 lines to display. Default 10.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	To redirect the command output to a file, you must use **| save *file_name*** instead of **> *file-name***.

Usage Guidelines

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

Example

```
ise/admin# show inventory
inventory
NAME: "ISE-VM-K9 chassis", DESCR: "ISE-VM-K9 chassis"
PID: ISE-VM-K9, VID: V01, SN: H8JESGOFHGG

Manufacturer: VMware, Inc.
Product Name: VMware7,1
Total RAM Memory: 16211484 kB
CPU Core Count: 4
```

```
CPU 0: Model Info: Intel(R) Xeon(R) Platinum 8280 CPU @ 2.70GHz
CPU 1: Model Info: Intel(R) Xeon(R) Platinum 8280 CPU @ 2.70GHz
CPU 2: Model Info: Intel(R) Xeon(R) Platinum 8280 CPU @ 2.70GHz
CPU 3: Model Info: Intel(R) Xeon(R) Platinum 8280 CPU @ 2.70GHz
Hard Disk Count(*): 1
Disk 0: Device Name: /dev/sda:
Disk 0: Capacity: 300GiB
NIC Count: 1
NIC 0: Device Name: eth0:
NIC 0: HW Address: 00:50:56:bx:aa:bx
NIC 0: Driver Descr: VMware vmxnet3 virtual NIC driver

(*) Hard Disk Count may be Logical.
```

show ip

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

show ip route

Syntax Description

route	Displays IP route information.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

This command displays the IP routing table.

Example

```
ise/iseadmin#show ip route

Destination          Gateway             Iface
-----------          -------             -----
default              10.1.100.1          eth0
10.1.100.0/24        0.0.0.0             eth0
169.254.2.0/24       0.0.0.0             cni-podman1
169.254.4.0/24       0.0.0.0             cni-podman2
```

show ipv6 route

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

show ipv6 route

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

This command displays the IPv6 routing table.

Example 1

```
ise/admin# show ipv6 route
Destination             Gateway                 Iface
-----------             -------                 ------

2001:DB8:cc00:1::/64    2001:DB8:cc00:1::1      eth0
ff02::1:2/128           ff02::1:2               eth0
ise/admin#
```

Example 2

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

show logging

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

show logging | save *file_name*

show logging application *application-logfile-name*

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

show logging internal

show logging system *system-logfile-name*

Syntax Description

| save	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 adapt
container-name *container-name*	Displays the log files related to the specified container (TC-NAC adapt
internal	Displays the syslog configuration.
system	Displays system syslogs.
system-logfile-name	Name of the system log file.
system-file-name	Name of the system log file name.
|	Output modifier variables: • begin—Matched pattern. Supports up to 80 alphanumeric characte • count—Count the number of lines in the output. Add number after t count. • end—End with line that matches. Supports up to 80 alphanumeric ch • exclude—Exclude lines that match. Supports up to 80 alphanumer characters. • include—Include lines that match. Supports up to 80 alphanumeric characters. • last—Display last few lines of output. Add number after the word Supports up to 80 lines to display. Default 10.

Command Default No default behavior or values.

Command Modes EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.
2.7	The display environment changed to the Unix less command.
3.2	To redirect the command output to a file, you must use **| save *file_name*** instead of **> *file-name***.

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. When you run this command, the content is opened in the Unix less evironment. Typing "H" displays the search and movement commands.

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
     129371 Feb 26 2013 02:40:22  secure
      27521 Feb 25 2013 16:10:02  anaconda.syslog
     345031 Feb 25 2013 16:10:02  anaconda.log
          0 Jul 28 2011 00:56:37  mail/statistics
    1272479 Feb 26 2013 02:42:52  ade/ADE.log
     567306 Feb 26 2013 02:40:22  audit/audit.log
      24928 Feb 26 2013 02:40:01  sa/sa26
          0 Feb 25 2013 16:01:40  pm/suspend.log
ise/admin#
```

Example 2

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

```
ise/admin# show logging application
       61 Oct 07 2016 03:02:43  dbalert.log
       4569 Oct 07 2016 03:21:18  ad_agent.log
          0 Oct 07 2016 03:13:18  ise-elasticsearch_index_indexing_slowlog.log
          0 Oct 07 2016 03:02:59  edf.log
        124 Oct 07 2016 03:21:59  diagnostics.log
       8182 Oct 07 2016 03:26:45  caservice.log
        426 Oct 07 2016 03:19:17  redis.log
       1056 Oct 07 2016 03:13:07  caservice_bootstrap.log
      49637 Oct 07 2016 03:27:40  passiveid-mgmt.log
          0 Oct 07 2016 03:02:59  passiveid.log
```

```
           0 Oct 07 2016 03:13:18  ise-elasticsearch_index_search_slowlog.log
       14152 Oct 07 2016 03:26:03  collector.log
           0 Oct 07 2016 03:02:59  idc-endpoint.log
         134 Oct 07 2016 03:22:34  ocsp.log
           0 Oct 07 2016 03:02:59  dbconn.log
           0 Oct 07 2016 03:02:59  idc-kerberos.log
      100958 Oct 07 2016 03:24:43  crypto.log
           0 Oct 07 2016 03:02:59  idc-syslog.log
           0 Oct 07 2016 03:02:59  replication.log.2016-10-04.1
       10394 Oct 07 2016 03:24:01  guest.log
           0 Oct 07 2016 03:02:59  guest.log.2016-10-07.1
           0 Oct 07 2016 03:02:59  vcs.log.2016-10-04.1
      288624 Oct 07 2016 03:27:25  ise-psc.log
ise/admin#
```

show logins

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

show logins cli

Syntax Description

cli	Lists the cli login history.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

show memory

To display the memory usage of all running processes, use the **show memory** command in EXEC mode.

This command has no keywords and arguments.

show memory

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

To view used memory, use the **show memory** command.

Example

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

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

show ntp

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

This command has no keywords and arguments.

show ntp

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

```
ise-az2/iseadmin#show ntp
Configured NTP Servers:
  xx.x.xxx.x
  0.north-america.pool.ntp.org
  1.north-america.pool.ntp.org
Reference ID    : 62BFD502 (mail.example.com)
Stratum         : 2
Ref time (UTC)  : Thu May 19 15:49:40 2022
System time     : 0.000000384 seconds fast of NTP time
Last offset     : -0.000422698 seconds
RMS offset      : 0.000422698 seconds
Frequency       : 7.323 ppm slow
Residual freq   : +2.728 ppm
Skew            : 0.352 ppm
Root delay      : 0.090078361 seconds
Root dispersion : 0.002209879 seconds
Update interval : 2.1 seconds
Leap status     : Normal

210 Number of sources = 3
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^? ns-dmz.demo.local             0   7     0     -     +0ns[   +0ns] +/-    0ns
^+ lofn.fancube.com              2   6    17    45  +5381us[+4959us] +/-   67ms
^* mail.intrax.com               1   6    17    44  -3730us[-4153us] +/-   47ms

M indicates the mode of the source.
^ server, = peer, # local reference clock.

S indicates the state of the sources.
* Current time source, + Candidate, x False ticker, ? Connectivity lost, ~ Too much
variability

Warning: Output results may conflict during periods of changing synchronization.
```

show ports

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

show ports | save *file_name*

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	To redirect the command output to a file, you must use **| save *file_name*** instead of **> *file-name***.

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, 127.0.0.1:8
005, 0.0.0.0:9990, 0.0.0.0:8009, 0.0.0.0:8905, 0.0.0.0:5514, 0.0.0.0:1099, 0.0.0
.0:61616, 0.0.0.0:80, 127.0.0.1:8888, 0.0.0.0:9080, 0.0.0.0:62424, 0.0.0.0:8443,
 0.0.0.0:443, 0.0.0.0:8444
     udp: 172.21.79.91:1812, 172.21.79.91:1813, 172.21.79.91:1700, 0.0.0.0:48425
, 172.21.79.91:8905, 172.21.79.91:3799, 0.0.0.0:54104, 172.21.79.91:57696, 172.2
```

```
1.79.91:1645, 172.21.79.91:1646
Process : timestenrepd (21516)
     tcp: 127.0.0.1:56513, 0.0.0.0:51312
Process : timestensubd (21421)
     tcp: 127.0.0.1:50598
Process : rpc.statd (3042)
     tcp: 0.0.0.0:680
     udp: 0.0.0.0:674, 0.0.0.0:677
Process : ttcserver (21425)
     tcp: 0.0.0.0:53385, 127.0.0.1:49293
Process : timestensubd (21420)
     tcp: 127.0.0.1:51370
Process : redis-server (21535)
     tcp: 0.0.0.0:6379
Process : portmap (2999)
     tcp: 0.0.0.0:111
     udp: 0.0.0.0:111
Process : Decap_main (22728)
--More--
```

show process

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

show process | save *file_name*

Syntax Description

| save	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 characte • count—Count the number of lines in the output. Add number after t count. • end—End with line that matches. Supports up to 80 alphanumeric ch • exclude—Exclude lines that match. Supports up to 80 alphanumer characters. • include—Include lines that match. Supports up to 80 alphanumeric characters. • last—Display last few lines of output. Add number after the word Supports up to 80 lines to display. Default 10.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	To redirect the command output to a file, you must use **| save *file_name*** instead of **> *file-name***.

Usage Guidelines

Table 1: Show Process Field Descriptions

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

Example

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

show repository

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

show repository *repository-name*

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

Note If you have enabled PKI authentication for an SFTP repository, you must generate the public key for the repository from the ISE CLI in addition to generating it from the ISE GUI. When the SFTP repository is configured from the ISE GUI, the public key on Cisco ISE is generated only for the root user and not for the admin user (user with which all commands can be run from the CLI). Follow these steps to verify and configure the public key from the ISE CLI:

1. Verify whether the crypto key is yet generated or not. If the output for the following command is empty it means that the crypto key is not generated.

```
ise24/admin# show crypto key
```

2. Hence from the CLI EXEC mode generate the key using the command: **crypto key generate rsa passphrase <secretkey>**.
3. From the following we can now confirm that the crypto key is generated successfully:

```
ise24/admin# show crypto key
admin public key: ssh-rsa SHA256:eEziR/ARPyFo1WptgI+y5WNjGIrgfPmEpEswVY7Qjb0 admin@ise24
```

4. After this, the admin needs to export the public key for 'admin' user using the command:**crypto key export <sample-name> repository <another-repository-name>**.
5. Now open the file saved to the **<another-repository-name>** and add it to **/home/<username>/.ssh/authorized_keys** folder in the SFTP server.

show restore

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

show restore {**history** | **status**}

Syntax Description

history	Displays the restore history on the system.
status	Displays the status of restore on the system.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Example

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

show running-config

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

This command has no keywords and arguments.

show running-config

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

```
ise/iseadmin#show running-config ?
Possible completions:
  cdp               CDP Configuration parameters
  clock             Configure timezone
  conn-limit        Configure a TCP connection limit from source IP
  hostname          Configure hostname
  icmp              Configure icmp echo requests
  identity-store    Configure identity store for CLI users
  interface         Configure interface
  ip                Configure IP features
  ipv6              Configure IPv6 features
  kron              Configure command scheduler
  logging           Configure system logging
  ntp               Specify NTP configuration
  password-policy   Password Policy Configuration
  rate-limit        Configure a TCP/UDP/ICMP packet rate limit from source IP
  repository        Configure Repository
  service
  snmp-server       Configure snmp server
  synflood-limit    Average number of TCP SYN packets per second allowed
  username          User creation
  |                 Output modifiers
  <cr>
ise/iseadmin#show running-config
```

show snmp-server engineid

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

show snmp-server engineid

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.1	The command was updated from **show snmp engineid** to **show snmp-server engineid**.

Example

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

ise/admin#
```

show snmp-server user

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

show snmp-server user

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.1	The command was updated from **show snmp user** to **show snmp-server user**.

Example

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

ise/admin#
```

show tech-support

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

show tech-support > *file-name*

show tech-support file *file-name*

Syntax Description

>	Redirects output to a file.
file	Saves any technical support data as a file in the local disk.
file-name	Filename to save technical support data. Supports up to 80 alphanumeri characters.

Command Default

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

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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


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

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

*************************************
Displaying ISE application status ....
*************************************
```

```
ISE PROCESS NAME                       STATE            PROCESS ID
--More--
(press Spacebar to continue)
ise/admin#
```

Example

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


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

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

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

show terminal

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

This command has no keywords and arguments.

show terminal

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Table 2: Show Terminal Field Descriptions

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

Example

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

show timezone

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

This command has no keywords and arguments.

show timezone

This command has no keywords and arguments.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Example

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

show timezones

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

This command has no keywords and arguments.

show timezones

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

show udi

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

This command has no keywords and arguments.

show udi

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Example 1

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

Example 2

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

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

show uptime

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

show uptime > *file-name*

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

show users

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

show users > *file-name*

Syntax Description

>	Redirects output to a file.
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 w count. • end—End with line that matches. Supports up to 80 alphanumeric charac • exclude—Exclude lines that match. Supports up to 80 alphanumeric characters. • include—Include lines that match. Supports up to 80 alphanumeric characters. • last—Display last few lines of output. Add number after the word last Supports up to 80 lines to display. Default 10.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

```
ise/admin# show users
USERNAME         ROLE   HOST                    TTY      LOGIN DATETIME
admin            Admin  10.77.202.52            pts/0    Tue Feb 26 20:36:41 2013
-------------------
DETACHED SESSIONS:
-------------------
USERNAME             ROLE                STARTDATE
% No disonnected user sessions present
ise/admin#
```

show version

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

show version > *file-name*

show version history

Note You must type the **show version history** command fully. Short form is not supported for this command.

Syntax Description

>	Redirects output to a file.
file-name	Name of the file to redirect.
history	Shows software version history information.
|	Output modifier variables: • begin—Matched pattern. Supports up to 80 alphanumeric characte • count—Count the number of lines in the output. Add number after t count. • end—End with line that matches. Supports up to 80 alphanumeric ch • exclude—Exclude lines that match. Supports up to 80 alphanumer characters. • include—Include lines that match. Supports up to 80 alphanumeric characters. • last—Display last few lines of output. Add number after the word Supports up to 80 lines to display. Default 10.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example 1

```
ise/admin# show version
```

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

Copyright (c) 2005-2014 by Cisco Systems, Inc.
All rights reserved.
Hostname: docs-ise-23-lnx


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

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

ise/admin#
```

Example 2

```
ise/admin# show version history
---------------------------------------------
Install Date: Wed Jul 26 19:02:13 UTC 2017
Application: ise
Version: 2.3.0.297
Install type: Application Install
Bundle filename: ise.tar.gz
Repository: SystemDefaultPkgRepos
ise/admin#
```

Cisco ISE CLI Commands in Configuration Mode

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

- Switch to Configuration Mode in EXEC Mode, on page 157
- Configuring Cisco ISE in the Configuration Mode, on page 158
- Configuring Cisco ISE in the Configuration Submode, on page 160
- CLI Configuration Command Default Settings, on page 161
- backup interface, on page 162
- cdp holdtime, on page 166
- cdp run, on page 167
- cdp timer, on page 168
- clock timezone, on page 169
- cls, on page 172
- conn-limit, on page 173
- service cache, on page 174
- do, on page 175
- end, on page 178
- exit, on page 179
- hostname, on page 180
- icmp echo, on page 182
- identity-store, on page 183
- interface, on page 184
- ip address, on page 186
- ip default-gateway, on page 188
- ip domain-name, on page 189
- ip host, on page 191
- ip mtu, on page 193
- ip name-server, on page 194
- ip route, on page 196
- ipv6 address, on page 198
- ipv6 address autoconfig, on page 200
- ipv6 address dhcp, on page 202
- ipv6 enable, on page 203

- ipv6 route, on page 205
- kron occurrence, on page 207
- kron policy-list, on page 209
- logging, on page 211
- ntp, on page 212
- ntp authentication-key, on page 214
- ntp maxdistance, on page 216
- ntp server, on page 217
- rate-limit, on page 220
- password-policy, on page 222
- repository, on page 224
- service, on page 227
- shutdown, on page 229
- snmp-server enable, on page 230
- snmp-server user, on page 232
- snmp-server host, on page 235
- snmp-server community, on page 238
- snmp-server contact, on page 239
- snmp-server location, on page 240
- snmp-server trap dskThresholdLimit, on page 241
- snmp engineid, on page 242
- synflood-limit, on page 243
- username, on page 245
- Additional References, on page 247

Switch to Configuration Mode in EXEC Mode

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

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

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

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

You can perform configuration tasks in configuration mode. Configuration changes are saved by default to preserve them during a system reload or power outage.

Configuring Cisco ISE in the Configuration Mode

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

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

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

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

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

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

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

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

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

Configuring Cisco ISE in the Configuration Submode

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

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

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

Step 2 Enter into the configuration submode.

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

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

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

CLI Configuration Command Default Settings

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

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

backup interface

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

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

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

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

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

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

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

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

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

Syntax Description

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

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

Command Default

No default behavior or values.

Command Modes

Interface configuration submode (config-GigabitEthernet)#

Command History

Release	Modification
2.1.0.474	This command was introduced.

Usage Guidelines

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

Example 1 - Configure NIC Bonding

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

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

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

Example 2 - Verify NIC Bonding Configuration

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

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

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

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

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

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

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

cdp holdtime

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

cdp holdtime *seconds*

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

no cdp holdtime

Syntax Description

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

Command Default

The default CDP holdtime, in seconds is 180.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

Example

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

cdp run

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

cdp run *GigabitEthernet*

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

no cdp run

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

Example

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

cdp timer

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

cdp timer *seconds*

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

no cdp timer

Syntax Description

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

Command Default

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

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

Example

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

clock timezone

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

clock timezone *timezone*

Syntax Description

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

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

Command Default

Coordinated Universal Time (UTC)

Command Modes

Configuration (config)#

Command History

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

Usage Guidelines

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

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

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

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

Example

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

Changing the Time Zone on Cisco ISE Nodes

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

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

Common Time Zones

Table 3: Table 4-1 Common Time Zones (Continued)

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

Australia Time Zones

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

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

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

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

Asia Time Zones

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

Table 5: Table 4-3 Asia Time Zones (Continued)

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

cls

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

cls

Syntax Description

This command has no keywords and arguments.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

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

conn-limit

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

Syntax Description

name	Enter a name for the conn-limit you are configuring.
<1-2147483647>	Number of TCP connections.
ip	(Optional). Source IP address to apply the TCP connection limit.
mask	(Optional). Source IP mask to apply the TCP connection limit.
port	(Optional). Destination port number to apply the TCP connection limit.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.
3.2	This command is updated to include assigning a name for the conn-limit configure.

Usage Guidelines

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

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

Example

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

service cache

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

service cache enable hosts ttl *ttl*

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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Usage Guidelines

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

Example

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

do

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

do *EXEC commands*

Syntax Description

EXEC commands	Specifies to execute an EXEC-system level command (see Table 6: Tab Command Options for Do Command (Continued)).

Table 6: Table 4-4 Command Options for Do Command (Continued)

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

Command	Description
mkdir	Creates a new directory.
nslookup	Queries the IPv4 or IPv6 address or hostname of a remote system.
password	Updates the CLI account password.
patch	Installs a Patch Bundle or uninstalls an Application patch.
ping	Determines the IPv4 address or hostname of a remote system.
ping6	Determines the IPv6 address of a remote system.
reload	Reboots the Cisco ISE server.
restore	Performs a restore and retrieves the backup out of a repository.
rmdir	Removes an existing directory.
show	Provides information about the Cisco ISE server.
ssh	Starts an encrypted session with a remote system.
tech	Provides Technical Assistance Center (TAC) commands.
terminal length	Sets terminal line parameters.
terminal session-timeout	Sets the inactivity timeout for all terminal sessions.
terminal session-welcome	Sets the welcome message on the system for all terminal sessions.
terminal terminal-type	Specifies the type of terminal connected to the current line of the current ses
traceroute	Traces the route of a remote IP address.
undebug	Disables the output (display of errors or events) of the debug command for va command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.
write	Erases the startup configuration that forces to run the setup utility and pron the network configuration, copies the running configuration to the startup configuration, displays the running configuration on the console. **Note** Cisco ISE Release 3.2 onwards, this command is modified to n longer support running-config and startup-config functions.

Command Default

No default behavior or values.

Command Modes

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

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

```
ise/admin(config)# do show run
Generating configuration...
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 10.0.0.1
ip default-gateway 172.23.90.1
!
clock timezone EST
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. role admin
!
service sshd
!
backup-staging-url nfs://loc-filer02a:/vol/local1/private1/jdoe
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
--More--
ise/admin(config)#
```

end

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

This command has no keywords and arguments.

end

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

Example

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

exit

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

exit

This command has no keywords and arguments.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

Example

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

hostname

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

hostname *hostname*

Syntax Description

hostname	Name of the host. Supports up to 19 alphanumeric characters and a hyphen The hostname must begin with a character that is not a space.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

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

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

Example

```
ise/admin(config)# hostname new-hostname
% Changing the hostname will cause ISE services to restart
```

```
Continue with hostname change?  Y/N [N]: y

Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE Identity Mapping Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
ISE Database processes already running, PID: 9651
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise-1/admin#
```

icmp echo

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

icmp echo {*off* | *on*}

Syntax Description

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

Command Default

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

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

identity-store

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

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

Command History

Release	Modification
2.6.0.156	This command was introduced.

Example

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

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

interface

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

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

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

Syntax Description

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

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

Syntax Description

backup	Configures the NIC bonding feature to provide high availability for the phy interfaces.
do	EXEC command. Allows you to perform any EXEC commands in this mo
end	Exits the config-GigabitEthernet submode and returns you to EXEC mode.
exit	Exits the config-GigabitEthernet configuration submode.
ip	Sets the IP address and netmask for the Gigabit Ethernet interface.
ipv6	Configures IPv6 autoconfiguration address and IPv6 address from DHCPv server.
no	Negates the command in this mode. Two keywords are available: • ip—Sets the IP address and netmask for the interface. • ipv6—Sets the IPv6 address for the interface. • shutdown—Shuts down the interface.
shutdown	Shuts down the interface.

Command Default No default behavior or values.

Command Modes Interface configuration (config-GigabitEthernet)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

ip address

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

ip address *ip-address network mask*

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

no ip address

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

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

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

Syntax Description

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

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

Command Default

Enabled.

Command Modes

Interface configuration (config-GigabitEthernet)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

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

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

Example

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

ip default-gateway

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

ip default-gateway *ip-address*

Note Deleting the default gateway is not recommended since it is mandatory for packet traffic to go out of the system. You can enable the default gateway function on another interface instead. If you want to have a quad zero static route, it is recommended that you add that on an interface that is not configured as the default gateway.

Syntax Description

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

Command Default

Disabled.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

```
ise/admin(config)# ip default-gateway 209.165.202.129
Adding/Changing gateway may cause ise services to restart.
Are you sure you want to proceed? Y/N [N]:
```

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

ip domain-name

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

ip domain-name *domain-name*

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

no ip domain-name

Syntax Description

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

Command Default

Enabled.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

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

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

Example

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

ip host

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

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

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

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

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

Syntax Description

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

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

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

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

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Supported IPv6 address formats include:

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

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

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

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

Example 1

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

Example 2

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

Stopping ISE Application Server...
Stopping ISE Profiler DB...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler DB...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config)#
```

ip mtu

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

ip mtu *bytes*

no ip mtu *bytes*

Syntax Description

mtu	Configures the MTU on a Cisco ISE interface.

Command Default

The MTU is set as 1500.

Command Modes

Interface configuration (config-GigabitEthernet)#

Command History

Release	Modification
2.4.0.357	This command was introduced.

Usage Guidelines

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

Example

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

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

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

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

ip name-server

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

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

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

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

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

Syntax Description

name-server	Configures the IP addresses of the name server(s).
ip-address	Address of a name server.
*ip-address**	(Optional). IP addresses of additional name servers. **Note** You can configure any combination of IPv4 and/or IPv6 addres Ensure that the ISE eth0 interface is statically configured with IPv6 address if you want to add a name-server with an IPv6 addr

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

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

Example 1

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

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

Example 2

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

```
ise/admin# show run | in name-server
ip name-server 10.0.0.1 10.0.1.1
3201:db8:0:20:f41d:eee:7e66:4eba
ise/admin#
```

Example 3

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

ip route

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

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

no ip route *prefix mask*

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

The following example describes how to configure multiple default routes:

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

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

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

```
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.114.1
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.115.1
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.116.1
```

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

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

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

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

Example 2

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

ipv6 address

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

ipv6 address *ipv6-address/prefix-length*

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

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

Syntax Description

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

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

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

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

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-GigabitEthernet)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Supported IPv6 address formats include:

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

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

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

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

Example 1

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

Example 2

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

ipv6 address autoconfig

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

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

ipv6 address autoconfig

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

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-GigabitEthernet)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

Configuring IPv6 Auto Configuration

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

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

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

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

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

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

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

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

Verifying the Privacy Extensions Feature

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

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

The output appears similar to the following:

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

ipv6 address dhcp

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

ipv6 address dhcp

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-GigabitEthernet)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Example

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

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

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

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

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

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

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

ipv6 enable

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

ipv6 enable

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

no ipv6 enable

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-GigabitEthernet)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example 1

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

Example 2

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

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


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

ipv6 route

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

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

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

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

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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Global configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

Supported IPv6 address formats include:

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

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

Example 1

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

Example 2

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

where ::/0 indicates a default route prefix.

kron occurrence

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

kron occurrence *occurrence-name*

Syntax Description

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

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

Syntax Description

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

Command Default No default behavior or values.

Command Modes Configuration (config-Occurance)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

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

Example 1: Weekly Backup

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

Example 2: Daily Backup

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

Example 3: Weekly Backup

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

kron policy-list

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

kron policy-list *list-name*

Syntax Description

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

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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Configuration (config-Policy List)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

Example

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

logging

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

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

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

no logging

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

This command requires the **loglevel** keyword.

Example

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

ntp

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

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

ntp maxdistance <*maximum distance*>

ntp reselectdistance <*reselect distance*>

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

no ntp server

Syntax Description

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

Command Default

None

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

Example

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


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

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

ntp authentication-key

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

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

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

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

ntp authentication-key <*key id*> **sha512 hash | plain** *key value*

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

no ntp authentication-key

Syntax Description

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

Command Default

None

Command Modes

Configuration (config)#.

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

Example 1

```
ise/admin# configure
ise/admin(config)#
ise/admin(config)# ntp authentication-key 1 ?
  md5     MD5 authentication
  sha1    SHA1 authentication
  sha256  SHA256 authentication
  sha512  SHA512 authentication
```

Example 2

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

Example 3

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

Example 4

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

ntp maxdistance

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

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

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

ntp maxdistance

Syntax Description

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

Command Default

None

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

ntp server

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

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

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

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

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

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

Syntax Description

server	Allows the system to synchronize with a specified server.
ip-address | *hostname*	IPv4 or IPv6 address or hostname of the server providing the clock synchronization. Arguments are limited to 255 alphanumeric characters that the ISE eth0 interface is statically configured with an IPv6 address want to add an NTP server with an IPv6 address.
key	(Optional). Peer key number. Supports up to 65535 numeric characters. This key needs to be defined with a key value, by using the **ntp authentication-key** command. For authentication to work, the key and the key value should be the sam which is defined on the actual NTP server.
minpoll	Minimum interval between requests sent to the server as a power of 2 in s For example, **minpoll 5** would mean that the polling interval should no below 32 seconds. The default is 6 (64 seconds), the minimum is -6 (1/6 second), and the maximum is 24 (6 months).
trust	Assume time from this source is always true.

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

Command Default

No servers are configured by default.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

Example

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


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

ntp server 209.165.200.228 key nn
ntp server 209.165.200.229
!


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

Verifying the Status of Synchronization

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

Example 1

```
ise/admin# show ntp
Primary NTP   : ntp.esl.cisco.com
Secondary NTP : 171.68.10.80
```

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

Example 2

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

rate-limit

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

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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

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

Usage Guidelines

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

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

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

See netfilter documentation for more details on how hashlimits work.

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

Example

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

password-policy

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

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

password-policy *options*

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

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

Syntax Description

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

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

Command Default

No default behavior or values.

Command Modes

Configuration (config-password-policy)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

None.

Example

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

repository

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

repository *repository-name*

Syntax Description

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

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

Syntax Description

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

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

Table 7: Table 4-5 URL Keywords (Continued)

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

Command Default

No default behavior or values.

Command Modes

Configuration (config-Repository)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

service

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

service sshd

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

no service

Syntax Description

sshd	Secure Shell Daemon. The daemon program for SSH.
enable	Enables sshd service.
encryption-algorithm	Configures SSH encryption algorithms. The supported algorithms are a aes128-cbc, aes128-ctr, aes256-cbc, and aes256-ctr.
encryption-mode	Configures SSH encryption mode on system. The supported modes are ctr.
key-exchange-algorithm	Specifies allowable key exchange algorithms for sshd service.
diffie-hellman-group14-sha1	Restricts key exchange algorithm to diffie-hellman-group14-sha1
Loglevel	Specifies the log level of messages from sshd to secure system log. • 1—QUIET • 2—FATAL • 3— ERROR • 4—INFO (default) • 5—VERBOSE • 6—DEBUG • 7—DEBUG1 • 8 —DEBUG2 • 9—DEBUG3
PubkeyAuthentication	Specifies that user authentication should take place using private key of **Note** Do not execute the command **service sshd PubkeyAuthent** if you haven't included the public key in the ZTP configura image file before installation. This disables password-base authentication and Cisco ISE will expect you to login using a key. If you do run into this issue, you need to use the conso to login into Cisco ISE and revert the configuration.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

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

Usage Guidelines

None.

Example

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

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

To enable public key authentication:

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

To disable public key authentication:

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

shutdown

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

This command has no keywords and arguments.

Command Default

No default behavior or values.

Command Modes

Configuration (config-GigabitEthernet)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

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

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

Example

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

snmp-server enable

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

snmp-server enable

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

Command Default

The SNMP server is enabled.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Example

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

MIBs

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

- SNMPv2-MIB
- RFC1213-MIB
- IF-MIB
- IP-MIB
- IP-FORWARD-MIB
- TCP-MIB
- UDP-MIB
- HOST-RESOURCES-MIB
- ENTITY-MIB-Only 3 MIB variables are supported on the ENTITY-MIB:

  Product ID: entPhysicalModelName

  Version ID: entPhysicalHardwareRev

  Serial Number: entPhysicalSerialNumber
- DISMAN-EVENT-MIB
- NOTIFICATION-LOG-MIB
- CISCO-CDP-MIB

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

For example:

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


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

snmp-server user

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

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

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

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

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

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

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

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

Syntax Description

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

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

Command Default

Disabled.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

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

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

snmp-server host

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

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

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

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

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

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

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

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

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

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

Syntax Description

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

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

Command Default

Enabled.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

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


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


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


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

snmp-server community

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

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

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

no snmp-server

Syntax Description

community	Sets SNMP community string.
community-string	Accessing string that functions much like a password and allows access to SN No blank spaces allowed. Supports up to 255 alphanumeric characters. To c a community string with the exclamation symbol (!), you must first enter th backslash symbol (\), for example, **abc\!23**.
ro	Specifies read-only access.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example

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

snmp-server contact

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

snmp-server contact *contact-name*

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

None.

Example

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

snmp-server location

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

snmp-server location *location*

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

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

Example 1

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

Example 2

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

snmp-server trap dskThresholdLimit

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

snmp-server trap dskThresholdLimit *value*

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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.1.0.474	This command was introduced.

Usage Guidelines

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

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

Example

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

snmp engineid

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

snmp engineid *engine_ID_string*

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

Syntax Description

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

Command Default

No command defaults.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Example

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

synflood-limit

To configure a TCP SYN packet rate limit.

synflood-limit ?

Syntax Description

synflood-limit	Average number of TCP SYN packets allowed per second.
?	The valid range is from 1 to 2147483647.

Command Default

No default behavior or values.

Command Modes

Configuration (config)#

Command History

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

Usage Guidelines

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

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

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

Example

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

username

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

username *username* **password hash** | **plain** {*password*} **role admin** | **user email** {*email-address*}

For an existing user, use the following command option:

username *username* **password role admin** | **user** {*password*}

Syntax Description

username	Only one word for the username argument. Blank spaces and quotation (“) are not allowed. Supports up to 31 alphanumeric characters.
password	Specifies password.
password	Password character length up to 40 alphanumeric characters. You must the password for all new users.
hash | **plain**	Type of password. Supports up to 34 alphanumeric characters.
role admin | **user**	Sets the user role and the privilege level for the user.
disabled	Disables the user according to the user’s email address.
email	Sets user’s email address.
email-address	Specifies the user’s email address. For example, user1@mydomain.com

Command Default

The initial user during setup.

Command Modes

Configuration (config)#

Command History

Release	Modification
2.0.0.306	This command was introduced.

Usage Guidelines

The **username** command requires that the username and password keywords precede the hash | plain and the admin | user options.

Example 1

```
ise/admin(config)# username admin password hash ###### role admin
ise/admin(config)#
```

Example 2

```
ise/admin(config)# username admin password plain Secr3tp@swd role admin
ise/admin(config)#
```

Example 3

```
ise/admin(config)# username admin password plain Secr3tp@swd role admin email
admin123@mydomain.com
ise/admin(config)#
```

Additional References

See Cisco ISE End-User Resources for additional resources that you can use when working with Cisco ISE.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.