Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x

July 2013

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

Text Part Number: OL-25541-01

Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x

CONTENTS

Preface

Revised: July 18, 2013, OL-25541-01

This guide describes how you can configure and maintain the Cisco Identity Services Engine (ISE), Release 1.1 and 1.1.x, by using the command-line interface (CLI). Each topic provides a high-level summary of the tasks required for using the CLI for the Cisco ISE in the Cisco Application Deployment Engine (ADE) OS Release 2.0, that runs on supported appliances for small, medium, and large Cisco ISE deployments.

This preface includes:

Note Use this guide in conjunction with the documentation listed in Related Documentation, page ix.

Who Should Read This Guide

The majority of the instructions in this guide are straightforward; however, a few are complex. Therefore, only experienced users should use these instructions.

Note Use this guide in conjunction with the documentation listed in Related Documentation, page ix.

How to Use This Guide

Cisco makes the following recommendations for using this document:

- Read the document in its entirety. Subsequent sections build on information and recommendations discussed in previous sections.
- Use this document for all-inclusive information about the Cisco ISE appliance.
- Do not vary the command-line conventions (see Document Conventions, page viii).

How This Guide Is Organized

This table lists the major sections of this guide.

Chapter	Title	Description
Chapter 1	Overview of the Cisco ISE Command-Line Interface	Provides an overview of the Cisco ISE CLI environment and command modes.
Chapter 2	Using the Cisco ISE Command-Line Interface	Describes how you can access and administer Cisco ISE from the CLI.
Appendix A	Cisco ISE Command Reference	Provides a complete description of all the CLI commands.

Document Conventions

This guide uses the following conventions to convey instructions and information.

Convention	Description
bold font	Commands and keywords.
italic font	Variables for which you supply values.
[ ]	Keywords or arguments that appear within square brackets are optional.
{x | y | z}	A choice of required keywords appears in braces separated by vertical bars. You must select one.
`courier` font	Examples of information displayed on the screen.
`bold courier` font	Examples of information you must enter.
< >	Nonprinting characters (for example, passwords) appear in angle brackets.
[ ]	Default responses to system prompts appear in square brackets.

Note Means *reader take note*. Notes identify important information that you should think about before continuing, contain helpful suggestions, or provide references to material not covered in the manual.

Tip Means *the following information will help you solve a problem*. A tip might not consist of an action or troubleshooting help, but could still contain useful information.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Documentation Updates

Table 1 Updates to the Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x

Date	Description
07/18/13	Resolved CSCui14464
01/31/13	Resolved CSCue27909
10/31/12	Cisco Identity Services Engine, Release 1.1.2
9/20/2012	Resolved CSCuc04825
7/10/12	Cisco Identity Services Engine, Release 1.1.1
3/19/12	Cisco Identity Services Engine, Release 1.1

Related Documentation

Release-Specific Documents

Table 2 lists the product documentation available for the Cisco ISE Release. General product information for Cisco ISE is available at http://www.cisco.com/go/ise. End-user documentation is available on Cisco.com at http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html.

Table 2 Product Documentation for Cisco Identity Services Engine

Document Title	Location
• *Release Notes for the Cisco Identity Services Engine, Release 1.1* • *Release Notes for the Cisco Identity Services Engine, Release 1.1.x*	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
• *Cisco Identity Services Engine Network Component Compatibility, Release 1.1* • *Cisco Identity Services Engine Network Component Compatibility, Release 1.1.x*	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html

Table 2 Product Documentation for Cisco Identity Services Engine (continued)

Document Title	Location
• *Cisco Identity Services Engine User Guide, Release 1.1* • *Cisco Identity Services Engine User Guide, Release 1.1.x*	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
• *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1* • *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x*	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Upgrade Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine API Reference Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine Troubleshooting Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html
Regulatory Compliance and Safety Information for Cisco Identity Services Engine, Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card	http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html

Platform-Specific Documents

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

- Cisco ISE
  http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
- Cisco Secure ACS
  http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html
- Cisco NAC Appliance
  http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html
- Cisco NAC Profiler
  http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html
- Cisco NAC Guest Server
  http://www.cisco.com/en/US/products/ps10160/tsd_products_support_series_home.html

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 1

Overview of the Cisco ISE Command-Line Interface

This chapter provides an overview of how to access the Cisco ISE command-line interface (CLI), the different command modes, and the commands that are available in each mode.

You can configure and monitor the Cisco ISE by using the web interface. You can also use the CLI to perform configuration and monitoring tasks that this guide describes.

The following sections describe the Cisco ISE CLI:

Accessing the Cisco ISE Command Environment

You can access the Cisco ISE CLI through a Secure Shell (SSH) client or the console port using one of the following machines:

- Windows PC running Windows XP/Vista
- Apple Computer running Mac OS X 10.4 or later
- PC running Linux

For detailed information on accessing the CLI, see Chapter 2, “Using the Cisco ISE Command-Line Interface”

User Accounts and Modes in the Cisco ISE CLI

Two different types of accounts are available on the Cisco ISE CLI:

- Admin (administrator)
- Operator (user)

When you power up the Cisco ISE appliances for the first time, you are prompted to run the **setup** utility to configure the appliances. During this setup process, an administrator user account, also known as an Admin account, is created. After you enter the initial configuration information, the appliances automatically reboot and prompt you to enter the username and the password that you specified for the Admin account. You must use this Admin account to log into the Cisco ISE CLI for the first time.

An Admin can create and manage Operator (user) accounts, which have limited privileges and access to the Cisco ISE server. An Admin account also provides the functionality that is needed to use the Cisco ISE CLI.

To create more users (with admin and operator privileges) with SSH access to the Cisco ISE CLI, you must run the **username** command in the Configuration mode (see Command Modes in the Cisco ISE CLI, page 1-4).

Table 1-1 lists the command privileges for each type of user account: Admin and Operator (user).

Table 1-1 Command Privileges

	User Account	
Command	**Admin**	**Operator (User)**
application commands	*	
backup	*	
backup-logs	*	
cdp run	*	
clock	*	
configure terminal	*	
copy commands	*	
debug	*	
delete	*	
dir	*	
end	*	
exit	*	*
forceout	*	
halt	*	
hostname	*	
icmp	*	
interface	*	
ip default-gateway	*	
ip domain-name	*	
ip name-server	*	
ip route	*	
kron	*	
logging commands	*	
mkdir	*	

Table 1-1 Command Privileges (continued)

Command	User Account	
	Admin	Operator (User)
nslookup	*	*
ntp	*	
ntp server	*	
password policy	*	
patch	*	
patch install	*	
patch remove	*	
pep	*	
ping	*	*
ping6	*	*
reload	*	
repository	*	
restore commands	*	
rmdir	*	
service	*	
show application	*	
show backup	*	
show cdp	*	*
show clock	*	*
show cpu	*	*
show disks	*	*
show icmp_status	*	*
show interface	*	*
show inventory	*	*
show ip route	*	
show logging	*	*
show logins	*	*
show memory	*	*
show ntp	*	*
show pep	*	*
show ports	*	*
show process	*	*
show repository	*	
show restore	*	

Table 1-1 Command Privileges (continued)

Command	User Account	
	Admin	Operator (User)
show running-config	*	
show startup-config	*	
show tech-support	*	
show terminal	*	*
show timezone	*	*
show timezones	*	
show udi	*	*
show uptime	*	*
show users	*	
show version	*	*
snmp-server commands	*	
ssh	*	*
tech	*	
telnet	*	*
terminal	*	*
traceroute	*	*
undebug	*	
username	*	
write	*	

Logging into the Cisco ISE node places you in the Operator (user) mode or the Admin (EXEC) mode, which always requires a username and password for authentication.

You can tell which mode you are in by looking at the prompt. A right angle bracket (>) appears at the end of the Operator (user) mode prompt; a pound sign (#) appears at the end of the Admin mode prompt, regardless of the submode.

Command Modes in the Cisco ISE CLI

Cisco ISE supports these command modes:

- EXEC—Use the commands in this mode to perform system-level configuration. See EXEC Commands, page 1-5. In addition, refer to the commands in the EXEC that generate operational logs as listed in Table 1-6.
- Configuration—Use the commands in this mode to perform configuration tasks in the Cisco ISE. See Configuration Commands, page 1-8. In addition, refer to the commands in the configuration mode that generate operational logs as listed in Table 1-5.

EXEC Commands

EXEC commands primarily include system-level commands such as **show** and **reload** (for example, application installation, application start and stop, copy files and installations, restore backups, and display information).

- Table 1-2 describes the EXEC commands
- Table 1-3 describes the show commands in the EXEC mode

For detailed information on EXEC commands, see Understanding Command Modes, page 2-5.

EXEC or System-Level Commands

Table 1-2 describes the EXEC mode commands.

Table 1-2 Summary of EXEC Commands

Command	Description
application configure	Configures a specific application.
application install	Installs a specific application bundle.
application remove	Removes a specific application.
application reset-config	Resets the Cisco ISE configuration to factory defaults.
application reset-passwd	Resets the application password for a specific user (admin) in the application.
application start	Starts or enables a specific application.
application stop	Stops or disables a specific application.
application upgrade	Upgrades a specific application bundle.
backup	Performs a backup and places the backup in a repository.
backup-logs	Performs a backup of all the logs on the Cisco ISE to a remote location.
clock	Sets the system clock on the Cisco ISE server.
configure	Enters the Configuration mode.
copy	Copies any file from a source to a destination.
debug	Displays any errors or events for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.
delete	Deletes a file in the Cisco ISE server.
dir	Lists the files in the Cisco ISE server.
exit	Disconnects the encrypted session with a remote system. Exits from the current command mode to the previous command mode.
forceout	Forces the logout of all the sessions of a specific Cisco ISE server system user.
halt	Disables or shuts down the Cisco ISE server.
help	Describes the help utility and how to use it in the Cisco ISE server.
mkdir	Creates a new directory.
nslookup	Queries the IPv4 address or hostname of a remote system.

Table 1-2 Summary of EXEC Commands (continued)

Command	Description
patch	Installs System or Application patch.
pep	Configures the Inline Posture node.
ping	Determines the IPv4 network connectivity to a remote system.
ping6	Determines the IPv6 network connectivity to a remote system.
reload	Reboots the Cisco ISE server.
restore	Restores a previous backup.
rmdir	Removes an existing directory.
show	Provides information about the Cisco ISE server.
ssh	Starts an encrypted session with a remote system.
tech	Provides Cisco Technical Assistance Center (TAC) commands.
telnet	Establishes a Telnet connection to a remote system.
terminal length	Sets terminal line parameters.
terminal session-timeout	Sets the inactivity timeout for all terminal sessions.
terminal session-welcome	Sets the welcome message on the system for all terminal sessions.
terminal terminal-type	Specifies the type of terminal connected to the current line of the current session.
traceroute	Traces the route of a remote IP address.
undebug	Disables the output (display of errors or events) of the **debug** command for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.
write	Erases the startup configuration that forces to run the setup utility and prompt the network configuration, copies the running configuration to the startup configuration, and displays the running configuration on the console.

Show Commands

The **show** commands are used to display the Cisco ISE settings and are among the most useful commands. See Table 1-3 for a summary of the **show** commands.

The commands in Table 1-3 require the **show** command to be followed by a keyword; for example, **show application status**. Some **show** commands require an argument or variable after the keyword to function; for example, **show application version**.

Table 1-3 Summary of show Commands

Command	Description
application (requires keyword)	Displays information about the installed application; for example, status information or version information.
backup (requires keyword)	Displays information about the backup.
cdp (requires keyword)	Displays information about the enabled Cisco Discovery Protocol interfaces.

Table 1-3 Summary of show Commands (continued)

Command	Description
clock	Displays the day, date, time, time zone, and year of the system clock.
cpu	Displays CPU information.
disks	Displays file-system information of the disks.
icmp-status	Displays the Internet Control Message Protocol (ICMP) echo response configuration information.
interface	Displays statistics for all the interfaces configured on the Cisco ISE.
inventory	Displays information about the hardware inventory, including the Cisco ISE appliance model and serial number.
ip route	Displays information in the IP routing table for a Cisco ISE server.
logging (requires keyword)	Displays the Cisco ISE server logging information.
logins (requires keyword)	Displays the login history of the Cisco ISE server.
memory	Displays memory usage by all running processes.
ntp	Displays the status of the Network Time Protocol (NTP) servers.
pep	Displays the Inline Posture node information.
ports	Displays all the processes listening on the active ports.
process	Displays information about the active processes of the Cisco ISE server.
repository (requires keyword)	Displays the file contents of a specific repository.
restore (requires keyword)	Displays the restore history in the Cisco ISE.
running-config	Displays the contents of the configuration file that currently runs in the Cisco ISE.
startup-config	Displays the contents of the startup configuration in the Cisco ISE.
tech-support	Displays system and configuration information that you can provide to the TAC when you report a problem.
terminal	Displays information about the terminal configuration parameter settings for the current terminal line.
timezone	Displays the current time zone in the Cisco ISE.
timezones	Displays all the time zones available for use in the Cisco ISE.
udi	Displays information about the unique device identifier (UDI) of the Cisco ISE.
uptime	Displays how long the system you are logged in to has been up and running.
users	Displays information about the system users.
version	Displays information about the currently loaded software version, along with hardware and device information.

Configuration Commands

Configuration commands include **interface** and **repository**. To access the Configuration mode, run the **configure** command in the EXEC mode.

Some of the configuration commands require that you enter the configuration submode to complete the configuration.

Table 1-4 describes the configuration commands.

Table 1-4 Summary of Configuration Commands

Command	Description
backup-staging-url	Specifies a Network File System (NFS) temporary space or staging area for the remote directory for backup and restore operations.
cdp holdtime	Specifies the amount of time the receiving device should hold a Cisco Discovery Protocol packet from the Cisco ISE server before discarding it.
cdp run	Enables Cisco Discovery Protocol.
cdp timer	Specifies how often the Cisco ISE server sends Cisco Discovery Protocol updates.
clock timezone	Sets the time zone for display purposes.
do	Executes an EXEC-level command from the configuration mode or any configuration submode. **Note** To initiate, the **do** command precedes the EXEC command.
end	Returns to the EXEC mode.
exit	Exits the Configuration mode.
hostname	Sets the hostname of the system.
icmp echo	Configures the ICMP echo requests.
interface	Configures an interface type and enters the interface configuration mode.
ipv6 address autoconfig	Enables IPv6 stateless autoconfiguration in the interface configuration mode.
ipv6 address dhcp	Enables IPv6 address DHCP in the interface configuration mode.
ip address	Sets the IP address and netmask for the Ethernet interface. **Note** This is an interface configuration command.
ip default-gateway	Defines or sets a default gateway with an IP address.
ip domain-name	Defines a default domain name that a Cisco ISE server uses to complete hostnames.
ip name-server	Sets the Domain Name System (DNS) servers for use during a DNS query.
ip route	Configures an IProute for an IP address.
kron occurrence	Schedule one or more Command Scheduler commands to run at a specific date and time or a recurring level.
kron policy-list	Specifies a name for a Command Scheduler policy.
logging	Enables the system to forward logs to a remote system.
logging loglevel	Configures the log level for the **logging** command.

Table 1-4 Summary of Configuration Commands (continued)

Command	Description
no	Disables or removes the function associated with the command.
ntp	Synchronizes the software clock through the NTP server for the system.
ntp authenticate	Enables authentication of all time sources.
ntp authentication-key	Adds Message Digest 5 (MD5)-type authentication keys for trusted time sources.
ntp server	Specifies an NTP server to use.
ntp trusted-key	Specifies the key numbers for trusted time sources.
password-policy	Enables and configures the password policy.
repository	Enters the repository submode.
service	Specifies the type of service to manage.
snmp-server community	Sets up the community access string to permit access to the Simple Network Management Protocol (SNMP).
snmp-server contact	Configures the SNMP contact the Management Information Base (MIB) value on the system.
snmp-server host	Sends SNMP traps to a remote system.
snmp-server location	Configures the SNMP location MIB value on the system.
username	Adds a user to the system with a password and a privilege level.

For detailed information on Configuration mode and submode commands, see Understanding Command Modes, page 2-5.

CLI Audit

You must have administrator access to execute the Cisco ISE configuration commands. Whenever an administrator logs in to the configuration mode and executes a command that causes configurational changes in the Cisco ISE server, the information related to those changes is logged in the Cisco ISE operational logs.

Table 1-5 describes the Configuration mode commands that generate operational logs.

Table 1-5 Configuration Mode Commands for the Operation Log

Command	Description
clock	Sets the system clock on the Cisco ISE server.
ip name-server	Sets the DNS servers for use during a DNS query.
hostname	Sets the hostname of the system.
ip address	Sets the IP address and netmask for the Ethernet interface.
ntp server	Allows synchronization of the software clock by the NTP server for the system.

In addition to the configuration mode commands, some commands in the EXEC generate operational logs.

Table 1-6 describes the EXEC mode commands that generate operational logs.

Table 1-6 EXEC Mode Commands for the Operation Log

Command	Description
backup	Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.
backup-logs	Backs up system logs.

CHAPTER 2

Using the Cisco ISE Command-Line Interface

This chapter provides helpful tips for understanding and configuring the Cisco Identity Services Engine (Cisco ISE) using the command-line interface (CLI). Cisco ISE can be deployed in small, medium, and large deployments and is available on different platforms and also as a software that can run on VMware. This chapter contains the following sections:

Before Accessing the Cisco ISE CLI

Before logging in to the Cisco ISE CLI, ensure that you have completed the installation tasks as specified in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.1*.

Running Setup to Configure the Cisco ISE

When you power up the Cisco ISE appliances for the first time, you are prompted to run the setup utility to configure the Cisco ISE appliances. Before you run the utility using the **setup** command, ensure that you have values for the following network configuration prompts:

- Hostname
- IP address—Ethernet interface address
- Netmask
- Default Gateway
- DNS domain name
- Primary nameserver
- Primary NTP server (optional)
- System time zone
- Username
- Password

This example shows sample output of the **setup** command.

```
*******************************************
Please type 'setup' to configure the appliance
*******************************************
localhost login:  setup
Press 'Ctrl-C' to abort setup
Enter hostname[]: ise
Enter IP address[]: 172.16.90.183
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 172.16.90.1
Enter default DNS domain[]: mydomain.com
Enter primary nameserver[]: 172.16.168.183
Add/Edit another nameserver? Y/N : n
Enter primary NTP server[time.nist.gov]:
Add/Edit secondary NTP server? Y/N : n
Enter system timezone[UTC]:
Enter username[admin]:
Enter password:
Enter password again:
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver...
Do not use 'Ctrl-C' from this point on...
Appliance is configured
```

After you enter the required information, the Cisco ISE appliance automatically reboots and the following login prompt appears:

```
machine_name login:
```

where *machine_name* identifies the hostname that you specified when you ran the **setup** command.

In this example, this prompt appears:

```
ise login:
```

To log in, use the administrator user account (and the corresponding password) that you created during the setup process. You must also use this Admin account to log into the Cisco ISE CLI for the first time. After accessing the CLI as an administrator, you can create more users (with admin and operator privileges) with SSH access to the CLI by running the username command in the Configuration mode.

Note The administrator user account and the corresponding password (a CLI user account) that you created during the initial setup wizard can be used to manage the Cisco ISE application using the CLI. The CLI user has privileges to 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 the system and the application logs, and reload or shutdown the Cisco ISE appliance. To protect the CLI user credentials, explicitly create users with access to the CLI.

See the "Accessing the Cisco ISE CLI" section on page 2-3.

Note Any users that you create from the Cisco ISE web interface cannot automatically log into the Cisco ISE CLI. You must explicitly create users with access to the CLI. To create these users, you must log in to the CLI using the Admin account that you created during setup; then, enter the Configuration mode, and run the **username** command.

Accessing the Cisco ISE CLI

Before logging in to the Cisco ISE CLI, ensure that you have completed the hardware installation and configuration process outlined in "Before Accessing the Cisco ISE CLI" section on page 2-1.

To log into the Cisco ISE server and access the CLI, use an SSH Secure Shell client or the console port.

Note To access the Cisco ISE CLI environment, use any SSH client that supports SSH v2.

You can log in from:

- A PC running Windows XP/Vista.
- A PC running Linux.
- An Apple computer running Mac OS X 10.4 or later.
- Any terminal device compatible with VT100 or ANSI characteristics. On the VT100-type and ANSI devices, you can use cursor-control and cursor-movement key. Keys include left arrow, up arrow, down arrow, right arrow, Delete, and Backspace. The CLI senses the use of the cursor-control keys and automatically uses the optimal device characteristics (see the "Supported Hardware and Software Platforms" section on page 2-3).

To exit the CLI, use the **exit** command from the EXEC mode. You are currently in one of the configuration modes and you want to exit the CLI, enter the **end, exit,** or **Ctrl-z** command to return to the EXEC mode, and then enter the **exit** command (see EXEC Mode, page 2-5).

Supported Hardware and Software Platforms

The following valid terminal types can access the Cisco ISE:

- 1178
- 2621
- 5051
- 6053
- 8510
- altos5
- amiga
- ansi
- apollo
- Apple_Terminal
- att5425
- ibm327x
- kaypro
- vt100

See the terminfo database for a complete listing.

Opening the CLI with Secure Shell

You can also access the Cisco ISE through an SSH client or the console port.

Note To access the Cisco ISE CLI environment, use any SSH client that supports SSH v2.

The following example shows you how to log in with a Secure Shell (SSH) client (connecting to a wired WAN) via a PC by using Windows XP. Assuming that Cisco ISE is preconfigured through the **setup** utility to accept an Admin (administrator) user, log in as Admin.

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

The SSH window appears.

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

The Connect to Remote Host window appears.

Step 3 Enter a hostname, username, port number, and authentication method.

In this example, you enter **ise** for the hostname, **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**.

The Enter Password window appears.

Step 5 Enter your assigned password for the administrator.

The SSH with the Add Profile window appears.

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

Step 7 Click **Close** on the Add Profile window.

The Cisco ISE prompt ise/admin# appears. You can now enter Cisco ISE CLI commands.

Opening the CLI Using a Local PC

If you need to configure Cisco ISE locally (without connecting to a wired LAN), you can connect a PC to the console port on the Cisco ISE appliance by using a null-modem cable.

The serial console connector (port) provides access to the CLI locally by connecting a terminal to the console port. The terminal is a PC running terminal-emulation software or an ASCII terminal. The console port (EIA/TIA-232 asynchronous) requires only a null-modem cable.

To connect a PC 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).

To connect to the console port and open the CLI, complete the following steps:

Step 1 Connect a null-modem cable to the console port on the Cisco ISE appliance and to the COM port on your PC.

Step 2 Set up a terminal emulator to communicate with the 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 At the window, enter your username, then press **Enter**.

Step 5 Enter the password, then press **Enter**.

When the CLI activates, you can enter CLI commands to configure the Cisco ISE.

Understanding Command Modes

This section describes the Cisco ISE command modes in detail. The primary modes of operation are:

- EXEC Mode, page 2-5
- Configuration Mode, page 2-6
- Configuration Submodes, page 2-7

EXEC Mode

When you start a session on the Cisco ISE, you begin in the Admin or EXEC mode. From the EXEC mode, you can enter the Configuration mode. Most of the EXEC commands (one-time commands), such as **show** commands, display the current configuration status. The Admin or EXEC mode prompt consists of the device name or hostname before a pound sign (#), as shown:

```
ise/admin# (Admin or EXEC mode)
```

Note Throughout this guide, the Cisco ISE server uses the name *ise* in place of the hostname and *admin* of the Cisco ISE server for the user account.

You can always tell when you are in the EXEC mode or the Configuration mode by looking at the prompt. In the:

- EXEC mode, a pound sign (#) appears after the Cisco ISE server hostname and your username.

  For example:

  ```
  ise/admin#
  ```

- Configuration mode, the 'config' keyword and a pound sign (#) appear after the hostname of the Cisco ISE server and your username.

  For example:

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

If you are familiar with UNIX, you can equate the EXEC mode to *root* access. You could also equate it to the administrator level in Windows NT or the supervisor in NetWare. In this mode, you have permission to access everything in the Cisco ISE server, including the configuration commands. However, you cannot enter configuration commands directly. Before you can change the actual configuration of the Cisco ISE server, you must enter the Configuration mode by running the **configure** or **configure terminal (conf t)** command. Enter this command only when in the EXEC mode.

For example:

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

The Configuration mode has several submodes; each has its own prompt. To enter these submodes, you must first enter the Configuration mode by entering the **configure terminal** command.

To exit the Configuration mode, enter the **end**, **exit**, or **Ctrl-z** command. To exit the EXEC mode, enter the **exit** command. To exit both Configuration and EXEC modes, enter this sequence of commands:

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

To obtain a listing of commands in the EXEC mode, enter a question mark (**?**):

```
ise/admin# ?
```

Configuration Mode

Use the Configuration mode to make changes to the existing configuration. When you save the configuration, these commands remain across Cisco ISE server reboots, but only if you run either of these commands:

- **copy running-config startup-config**
- **write memory**

To enter the Configuration mode, run the **configure** or **configure terminal (conf t)** command in the EXEC mode. When in the Configuration mode, the Cisco ISE expects configuration commands.

For example:

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

From this level, you can enter commands directly into the Cisco ISE configuration. To obtain a listing of commands in this mode, enter a question mark (**?**):

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

The Configuration mode has several configuration submodes. Each of these submodes places you deeper in the prompt hierarchy. When you enter **exit**, the Cisco ISE backs you out one level and returns you to the previous level. When you enter **exit** again, the Cisco ISE backs you out to the EXEC level.

Note In the Configuration mode, you can alternatively enter **Ctrl-z** instead of the **end** or **exit** command.

Configuration Submodes

In the configuration submodes, you can enter commands for specific configurations. For example:

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

To obtain a list of commands in this mode, enter a question mark (**?**):

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

Use the **exit** or **end** command to exit this prompt and return to the configuration prompt.

Table 2-1 lists the commands in the interface GigabitEthernet 0 configuration submode. Other configuration submodes exist including those specific to the **kron**, **repository**, and **password policy** commands.

Table 2-1 Command Options in the Interface GigabitEthernet 0 Configuration Submode

Command	Comment

`ise/admin(config)# interface GigabitEthernet 0`
`ise/admin(config-GigabitEthernet)# ?`
`Configure ethernet interface:`
`  do  EXEC command`
`  end  Exit from configure mode`
`  exit  Exit from this submode`
`  ip  Configure IP features`
`  ipv6  Configure IPv6 features`
`  no  Negate a command or set its defaults`
`  shutdown  Shutdown the interface`
`ise/admin(config-GigabitEthernet)#`
	Enter the command that you want to configure for the interface. This example uses the **interface GigabitEthernet** command.
	Enter **?** to display what you must enter next on the command line. This example shows the available **interface GigabitEthernet** configuration submode commands.

`ise/admin(config-GigabitEthernet)# ip ?`
`  address  Configure IP address`
`ise/admin(config-GigabitEthernet)# ip`
	Enter the command that you want to configure for the interface. This example uses the **ip** command.
	Enter **?** to display what you must enter next on the command line. This example shows the available **ip** configuration submode commands.

Table 2-1 Command Options in the Interface GigabitEthernet 0 Configuration Submode

Command	Comment

`ise/admin(config-GigabitEthernet)# ip address ?`
`  <A.B.C.D>  IPv4 address`
`ise/admin(config-GigabitEthernet) ip address`
	Enter the command that you want to configure for the interface. This example uses the **ip addresss** command.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter an IPv4 address.
	A carriage return <cr> does not appear; therefore, you must enter additional arguments to complete the command.

`ise/admin(config-GigabitEthernet)# ip address 172.16.0.1 ?`
`  <A.B.C.D>  Network mask`
`ise/admin(config-GigabitEthernet)# ip address 172.16.0.1`
	Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter a network mask.
	A carriage return <cr> does not display; therefore, you must enter additional arguments to complete the command.

`ise/admin(config-GigabitEthernet)# ip address 172.16.0.1 255.255.255.224 ?`
`  <cr>  Carriage Return`
`ise/admin(config-GigabitEthernet)# ip address 172.16.0.1 255.255.255.224`
	Enter the network mask. This example uses the 255.255.255.224 IP address.
	Enter **?** to display what you must enter next on the command line. In this example, you can press **Enter**.
	A carriage return <cr> displays; you can press **Enter** to complete the command.

Navigating the CLI Commands

This section describes how to navigate the commands and modes on the Cisco ISE.

Getting Help

Use the question mark (**?**) and the arrow keys to help you enter commands:

- For a list of available commands, enter a question mark (**?**):

  ```
  ise/admin# ?
  ```

- To complete a command, enter a few known characters before **?** (with no space):

  ```
  ise/admin# s?
  ```

- To display keywords and arguments for a command, enter **?** at the prompt or after entering part of a command followed by a space:

  ```
  ise/admin# show ?
  ```

  The Cisco ISE displays a list and brief description of available keywords and arguments.

  Note The <cr> symbol in command help stands for "carriage return", which means to press the **Return** or the **Enter** key). The <cr> at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available, and that you must press **Enter** to complete the command.

- To redisplay a command that you previously entered, press the **Up Arrow** key. Continue to press the **Up Arrow** key to see more commands.

Using the No and Default Forms of Commands

Some EXEC or configuration commands have a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to re-enable a disabled function or to enable a function disabled by default; for example, an IP address enabled by default. To disable the IP address, use the **no ip address** command; to re-enable the IP address, use the **ip address** command.

Configuration commands can also 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.

See Appendix A, "Cisco ISE Command Reference," for a description of the complete syntax of the configuration commands, and the **no** and **default** forms of a command.

Command Line Conventions

While reading this document, you might not understand some of the information if you do not know certain basic conventions of CLI usage.

Command Line Editing Key Conventions

Cisco ISE provides a number of keyboard shortcuts that you can use to edit an entered line.

Tab

Press **Tab** to try to finish the current command.

If you press the **Tab** key:

- At the beginning of a line, the system lists all the short-form options.

- When you enter a partial command, the system lists all the short form options beginning with those characters.
- When only one possible option is available, the system fills in the option automatically.

Ctrl-c

Press Ctrl-c to abort the sequence. Breaks out of any executing command and returns to the previous mode.

Ctrl-z

Press Ctrl-z to exit the Configuration mode and return to the previous configuration mode.

?

Enter a question mark (?) at the prompt to list the available commands (see Getting Help, page 2-8).

Command Line Completion

Command-line completion makes the Cisco ISE CLI more user-friendly. It saves you extra key strokes and helps out when you cannot remember the syntax of a command.

For example, in the **show running-config** command:

```
ise/admin# show running-config
```

You could have used:

```
ise/admin# sh run
```

The Cisco ISE expands the command **sh run** to **show running-config**.

Another shortcut is to press the **Tab** key after you type **sh**; the Cisco ISE CLI fills in the rest of the command completion, in this case **show**.

If the Cisco ISE CLI does not understand a command, it repeats the entire command line and places a caret symbol (^) under the point at which it could not parse the command.

For example:

```
ise/admin# show unning-configuration
               ^
% Invalid input detected at '^' marker.
```

The caret symbol (^) points to the first letter in the command line that the Cisco ISE does not understand. Usually, this means that you need to provide additional arguments to complete the command or you mispelled the command. In this case, you omitted the “r” in the “unning” command. To fix the error, retype the command.

In another form of command-line completion, you can start a command by entering the first few characters, then pressing the **Tab** key. As long as you can match one command, the Cisco ISE CLI will complete the command. For example, if you type **sh** and press **Tab**, the Cisco ISE completes the **sh** with **show**. If the Cisco ISE does not complete the command, you can enter a few more letters and press **Tab** again. For more information, see Tab, page 2-9.

Continuing Output at the --More-- Prompt

When working with the Cisco ISE CLI, output often extends beyond the visible screen length. For cases where output continues beyond the bottom of the screen, such as with the output of many **?** or **show** commands, the output pauses and a **--More--** prompt appears at the bottom of the screen. To resume output, press **Return** to scroll down one line, or press the **spacebar** to display the next full screen of output.

Tip If output pauses on your screen but you do not see the **--More--** prompt, try entering a smaller value for the screen length by using the **terminal length** EXEC command. Command output will not pause if you set the length value to zero (0).

Where to Go Next

Now that you are familiar with some of the Cisco ISE CLI basics, you can begin to configure the Cisco ISE by using the CLI.

Remember that:

- You can use the question mark (**?**) and arrow keys to help you enter commands.
- Each command mode restricts you to a set of commands. If you have difficulty entering a command, check the prompt and then enter the question mark (**?**) to see a list of available commands.
- To disable a feature, enter the keyword **no** before the command; for example, **no ip address**.
- You must save your configuration changes so that you preserve them during a system reload or power outage.

Proceed to Appendix A, "Cisco ISE Command Reference," for command listings, descriptions, syntax, usage guidelines, and sample output.

APPENDIX A

Cisco ISE Command Reference

This appendix contains an alphabetical listing of the commands specific to the Cisco Identity Services Engine (Cisco ISE).

The commands comprise these modes:

- EXEC
  - System-level
  - Show
- Configuration
  - Configuration submode

Note Use the EXEC mode system-level **config** or **configure** command to access the Configuration mode.

Each of the commands in this appendix is followed by a brief description of its use, command syntax, usage guidelines, and one or more examples. Throughout this appendix, the Cisco ISE server uses the name *ise* in place of the Cisco ISE server's hostname.

Note If an error occurs in any command usage, use the **debug** command to determine the cause of the error.

This appendix describes:

EXEC Commands

This section lists each EXEC command and includes a brief description of its use, command syntax, usage guidelines, and sample output.

Table A-1 lists the EXEC commands that this section describes.

Table A-1 List of EXEC Commands

• application configure	• delete	• restore
• application install	• dir	• rmdir
• application remove	• exit	• show (see Show Commands)
• application reset-config	• forceout	• ssh
• application reset-passwd	• halt	• tech
• application start	• help	• telnet
• application stop	• mkdir	• terminal length
• application upgrade	• nslookup	• terminal session-timeout
• backup	• patch install	• terminal session-welcome
• backup-logs	• patch remove	• terminal terminal-type
• clock	• pep	• traceroute
• configure	• ping	• undebug
• copy	• ping6	• write
• debug	• reload	

application configure

To configure Microsoft Windows Active Directory settings in the Cisco ISE, use the **application configure** command in the EXEC mode.

application configure *application-name*

Syntax Description

application	The application command for an application install and administration.
configure	Configures a specific application.
application-name	Application name. Supports up to 255 alphanumeric characters.
Parameter Name	Use dns.servers.
Parameter Value	Specifies the IPv4 address of a specific name-server.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

You can configure to use only a specific name-server that has the required Active Directory configuration when there are multiple IP name-servers that are configured in a Cisco ISE node.

Cisco ISE allows you to configure Active Directory settings by using the **application configure** command. It prompts you the following warning message for confirmation:

```
Active Directory internal setting modification should only be performed if approved by ISE
support. Please confirm this change has been approved y/n [n]:
```

Examples

```
ise/admin# application configure ise
Selection ISE configuration option
[1]Reset Active Directory settings to defaults
[2]Display Active Directory settings
[3]Configure Active Directory settings
[4]Restart/Apply Active Directory settings
[5]Clear Active Directory Trusts Cache and restart/apply Active Directory settings
[6]Exit

3 (option 3 from the menu)
You are about to configure Active Directory settings.
Are you sure you want to proceed? y/n [n]: y
Parameter Name: dns.servers
Parameter Value: 10.77.122.135
Active Directory internal setting modification should only be performed if approved by ISE
support. Please confirm this change has been approved y/n [n]: y
Active Directory settings were modified.
Settings will take effect after choosing apply option from menu.

Selection ISE configuration option
[1]Reset Active Directory settings to defaults
[2]Display Active Directory settings
[3]Configure Active Directory settings
[4]Restart/Apply Active Directory settings
[5]Clear Active Directory Trusts Cache and restart/apply Active Directory settings
[6]Exit

4 (option 4 from the menu)
You are about to Reset/Apply Active Directory settings.
Are you sure you want to proceed? y/n [n]: y
You are about to apply recent settings changes. This will require AD client to be
restarted which may take several minutes. Continue y/n [n]: y
Active Directory settings were applied

Selection ISE configuration option
[1]Reset Active Directory settings to defaults
[2]Display Active Directory settings
[3]Configure Active Directory settings
[4]Restart/Apply Active Directory settings
[5]Clear Active Directory Trusts Cache and restart/apply Active Directory settings
[6]Exit

2 (option 2 from the menu)
Parameter Name: dns.servers
dns.servers: 10.77.122.135

Selection ISE configuration option
[1]Reset Active Directory settings to defaults
[2]Display Active Directory settings
[3]Configure Active Directory settings
[4]Restart/Apply Active Directory settings
[5]Clear Active Directory Trusts Cache and restart/apply Active Directory settings
```

```
[6]Exit

5 (option from the menu)
You are about to clear the Active Directory Trusts Cache and reset/apply Active Directory
settings.
Are you sure you want to proceed? y/n [n]: y
log4j:WARN No appenders could be found for logger
(com.cisco.cpm.acs.nsf.config.handlers.ad.cli.ADAgentRestart).
log4j:WARN Please initialize the log4j system properly.
You are about to apply recent settings changes. This will require AD client to be
restarted which may take several minutes. Continue y/n [n]: y
Active Directory settings were applied

Selection ISE configuration option
[1]Reset Active Directory settings to defaults
[2]Display Active Directory settings
[3]Configure Active Directory settings
[4]Restart/Apply Active Directory settings
[5]Clear Active Directory Trusts Cache and restart/apply Active Directory settings
[6]Exit

6 (option from the menu)
ise/admin#
```

Related Commands

Command	Description
application install	Installs an application bundle.
application remove	Removes or uninstalls an application.
application reset-config	Resets an application configuration to factory defaults.
application reset-passwd	Resets an application password for a specified user.
application start	Starts or enables an application.
application stop	Stops or disables an application.
application upgrade	Upgrades an application bundle.
show application	Shows application information for the installed application packages on the system.

application install

Note You are not allowed to run the **application install** command from the CLI under normal operations because the Cisco ISE application is preinstalled with a Cisco IOS image on all supported appliances and VMware.

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

application install *application-bundle remote-repository-name*

Syntax Description

application	The application command for an application install and administration.
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.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

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

Examples

Example 1

```
ise/admin# application install ise-appbundle-1.1.0.362.i386.tar.gz myrepository
Do you want to save the current configuration? (yes/no) [yes]? y
Please enter yes or no
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#
```

Example 2

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

Application successfully installed
ise/admin#
```

Related Commands

Command	Description
application configure	Configures an application.
application remove	Removes or uninstalls an application.
application reset-config	Resets an application configuration to factory defaults.

Command	Description
application reset-passwd	Resets an application password for a specified user.
application start	Starts or enables an application.
application stop	Stops or disables an application.
application upgrade	Upgrades an application bundle.
show application	Shows application information for the installed application packages on the system.

application remove

Note You are not allowed to run the **application remove** command from the CLI to remove the Cisco ISE application unless you are explicitly instructed for an upgrade.

To remove a specific application other than the Cisco ISE, use the **application remove** command in the EXEC mode. To remove this function, use the **no** form of this command.

application remove *application-name*

Syntax Description

application	The application command for an application install and administration.
remove	Removes or uninstalls an application.
application-name	Application name. Supports up to 255 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Removes or uninstalls an application.

Examples

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

Application successfully uninstalled
ise/admin#
```

Related Commands

Command	Description
application configure	Configures an application.
application install	Installs an application bundle.
application reset-config	Resets an application configuration to factory defaults.

Command	Description
application reset-passwd	Resets an application password for a specified user.
application start	Starts or enables an application.
application stop	Stops or disables an application.
application upgrade	Upgrades an application bundle.
show application	Shows application information for the installed application packages on the system.

application reset-config

To reset the Cisco ISE application configuration and clear the Cisco ISE database, use the **application reset-config** command in the EXEC mode. (This command does not reset your initial chassis configuration settings like the IP address, netmask, administrator user interface password, and so on.) Part of this reset function requires you to enter new Cisco ISE database administrator and user passwords.

application reset-config *application-name*

Syntax Description

application	The application command for an application install and administration.
reset-config	Resets the Cisco ISE application configuration and clears the Cisco ISE database.
application-name	Name of the application configuration you want to reset. Supports up to 255 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

You can use the **application reset-config** command to reset the Cisco ISE configuration and clear the Cisco ISE database without reimaging the Cisco ISE appliance or VMware, and reset the 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.

Examples

Example 1

```
ise/admin# application reset-config ise
Initialize your identity policy database to factory defaults? (y/n): y
Reinitializing local policy database to factory default state...
```

```
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Please follow the prompts below to create the database administrator password.

Enter new database admin password:
Confirm new database admin password:
Successfully created database administrator password.

Please follow the prompts below to create the database user password.

Enter new database user password:
Confirm new database user password:
Successfully created database user password.
Extracting ISE database content...
Starting ISE database processes...
Restarting ISE database processes...
Creating ISE M&T session directory...
Performing ISE database priming...

Application successfully reset configuration
ise/admin#
```

Example 2

```
ise/admin# application reset-config ise
Initialize your identity policy database to factory defaults? (y/n): n
Existing policy database will be retained.

Application successfully reset configuration
ise/admin#
```

Related Commands

Command	Description
application configure	Configures an application.
application install	Installs an application bundle.
application remove	Removes or uninstalls an application.
application reset-passwd	Resets an application password for a specified user.
application start	Starts or enables an application.
application stop	Stops or disables an application.
application upgrade	Upgrades an application bundle.
show application	Shows application information for the installed application packages on the system.

application reset-passwd

Note This command was introduced in Cisco ISE Maintenance Release 1.0.4 and does not apply to regular Cisco ISE, Release 1.0. Use this command to reset the administrator user interface password. It does not affect the command-line interface password for the specified administrator ID.

To reset the administrator user interface 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 the EXEC mode. You can also use this command to reset the Cisco ISE database administrator and user passwords.

application reset-passwd *application-name administrator-ID* | **internal-database-admin** | **internal-database-user**

Syntax Description

application	The application command for an application install and administration.
reset-passwd	Resets the administrator account password.
application-name	Application name. Supports up to 255 alphanumeric characters.
administrator-ID	The name of an existing administrator account that has been disabled and for which you want to reset the password.
internal-database-admin	Identifies the Cisco ISE database system-level password. You must create this password (there is no default). The password must be a minimum of 11 characters in length and include at least one lowercase letter (a-z), at least one uppercase letter (A-Z), and at least one number (0-9).
internal-database-user	Identifies the Cisco ISE database access-level password. You must create this password (there is no default). The password must be a minimum of 11 characters in length and include at least one lowercase letter (a-z), at least one uppercase letter (A-Z), and at least one number (0-9). **Note** If you reset the internal database user password, Cisco ISE prompts you to restart the application. The internal database user password is reset after you restart the Cisco ISE application.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The following special characters are allowed when resetting Cisco ISE administrator user interface password:

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

If you enter an incorrect password for your administrator user ID more than the specified number of times necessary to disable the administrator account in Cisco ISE, then the user interface "locks you out" of the system. Cisco ISE suspends the credentials for that administrator ID until you have an opportunity to reset the password associated with that administrator ID. It is the Administration ISE node on which the password is being reset only from the CLI.

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

UTF-8 admin users can change passwords only through the Cisco ISE administrator user interface.

Examples

Example 1

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

Password reset successfully.
ise/admin#
```

Example 2

```
ise/admin# application reset-passwd ise internal-database-admin
Enter new database admin password: ***********
Confirm new database admin password: ***********

Password reset successfully.
ise/admin#
```

Related Commands

Command	Description
application configure	Configures an application.
application installs	Installs an application bundle.
application remove	Removes or uninstalls an application.
application reset-config	Resets an application configuration to factory defaults.
application start	Starts or enables an application.
application stop	Stops or disables an application.
application upgrade	Upgrades an application bundle.
show application	Shows application information for the installed application packages on the system.

application start

To enable a specific application, use the **application start** command in the EXEC mode. To remove this function, use the **no** form of this command.

application start *application-name*

application start *application-name safe*

Syntax Description

application	The application command for an application install and administration.
start	Enables an application bundle.
application-name	Name of the predefined application that you want to enable. Supports up to 255 alphanumeric characters.
safe	Starts an application in safe mode.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Enables an application.

You cannot use this command to start the Cisco ISE application. If you use this command to start the application, you can see that the Cisco ISE is already running.

You can use the **application start** *ise safe* command to start the Cisco ISE in a safe mode that allows you to disable access control temporarily to the admin user interface, 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 user interface. 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 in to the Cisco ISE admin user interface.

Examples

```
ise/admin# application start ise
ISE Database processes is already running, PID: 7585
ISE M&T Session Database is already running, PID: 7851
ISE Application Server process is already running, PID: 7935
ISE M&T Log Collector is already running, PID: 7955
ISE M&T Log Processor is already running, PID: 8005
ISE M&T Alert Processor is already running, PID: 8046
ise/admin#
ise/admin# application start ise safe

Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

Related Commands

Command	Description
application configure	Configures an application.
application install	Installs an application bundle.
application remove	Removes or uninstalls an application.

Command	Description
application reset-config	Resets an application configuration to factory defaults.
application reset-passwd	Resets an application password for a specified user.
application stop	Stops or disables an application.
application upgrade	Upgrades an application bundle.
show application	Shows application information for the installed application packages on the system.

application stop

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

application stop *application-name*

Syntax Description

application	The application command for application install and administration.
stop	Disables an application.
application-name	Name of the predefined application that you want to disable. Supports up to 255 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Disables an application.

Examples

```
ise/admin# application stop ise

Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...

ise/admin#
```

Related Commands

Command	Description
application configure	Configures an application.
application install	Installs an application bundle.

Command	Description
application remove	Removes or uninstalls an application.
application reset-config	Resets an application configuration to factory defaults.
application reset-passwd	Resets an application password for a specified user.
application start	Starts or enables an application.
application upgrade	Upgrades an application bundle.
show application	Shows application information for the installed application packages on the system.

application upgrade

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

application upgrade *application-bundle remote-repository-name*

Syntax Description

application	The application command for application install and administration.
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.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Upgrades an application bundle, and preserves any application configuration data.

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 the upgrade is in progress. This action might cause the database to be corrupted.

Note Before attempting to use this application upgrade command to upgrade to a newer release, you must read the upgrade instructions in the release notes supplied with that newer release. The release notes contains important instructions updated for upgrading to the newer release, which must be followed.

Examples

Example 1

```
ise/admin# application upgrade ise-appbundle-1.1.0.362.i386.tar.gz http
```

```
Save the current ADE-OS running configuration? (yes/no) [yes]? yes
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Initiating Application Upgrade...
Stopping ISE application before upgrade...
Running ISE Database upgrade...
Upgrading ISE Database schema...
ISE Database schema upgrade completed.
Running ISE Global data upgrade as this node is a STANDALONE...
Running ISE data upgrade for node specific data...

Application upgrade successful
ise/admin#
```

Example 2

```
ise/admin# application upgrade ise-appbundle-1.1.0.362.i386.tar.gz http
Save the current ADE-OS running configuration? (yes/no) [yes]? no
Initiating Application Upgrade...
Stopping ISE application before upgrade...
Running ISE Database upgrade...
Upgrading ISE Database schema...
ISE Database schema upgrade completed.
Running ISE Global data upgrade as this node is a STANDALONE...
Running ISE data upgrade for node specific data...

Application upgrade successful
ise/admin#
```

Related Commands

Command	Description
application configure	Configures an application.
application install	Installs an application bundle.
application remove	Removes or uninstalls an application.
application reset-config	Resets an application configuration to factory defaults.
application reset-passwd	Resets an application password for a specified user.
application start	Starts or enables an application.
application stop	Stops or disables an application.
show application	Shows application information for the installed application packages on the system.

backup

To perform a backup (including the Cisco ISE and Cisco ADE OS data) and place the backup in a repository, use the **backup** command in the EXEC mode. To perform a backup of only the Cisco ISE application data without the Cisco ADE OS data, use the **application** command.

Note Before attempting to use this **backup** command in the 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 your Cisco ISE application from the backup and system logs. For more information of copying the running configuration to the startup configuration, see the "copy" section on page A-19.

backup *backup-name* **repository** *repository-name* **application** *application-name* **encryption-key hash |plain** *encryption-key name*

Syntax Description

backup	The command to perform a backup the Cisco ISE and Cisco ADE OS and place the backup in a repository.
backup-name	Name of backup file. Supports up to 100 alphanumeric characters.
repository	Repository command.
repository-name	Location where the files should be backed up to. Supports up to 80 alphanumeric characters.
application	Application command (application-only backup, excludes the Cisco ODE OS system data).
application-name	Application name. Supports up to 255 alphanumeric characters.
encryption-key	Specifies user-defined encryption key to protect the backup.
hash	Hashed encryption key for protection of backup. Specifies an *encrypted* (hashed) encryption key that follows. Supports up to 40 characters.
plain	Plaintext encryption key for protection of backup. Specifies an *unencrypted* plaintext encryption key that follows. Supports up to 15 characters.
encryption-key name	Specifies encryption key in hash | plain format for backup.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Performs a backup of the Cisco ISE and Cisco ADE OS data and places the backup in a repository with an encrypted (hashed) or unencrypted plaintext password.

To perform a backup of only the Cisco ISE application data without the Cisco ADE OS data, use the **application** command.

You can encrypt and decrypt backups now by using user-defined encryption keys.

Examples

Example 1

```
ise/admin# backup mybackup repository myrepository encryption-key plain Lab12345
% Creating backup with timestamped filename: backup-111125-1252.tar.gpg
ise/admin#
```

Example 2

```
ise/admin# backup mybackup repository myrepository application ise encryption-key plain
Lab12345
% Creating backup with timestamped filename: backup-111125-1235.tar.gpg
ise/admin#
```

Related Commands

Command	Description
backup-logs	Backs up system logs.
delete	Deletes a file from the Cisco ISE server.
dir	Lists a file from the Cisco ISE server.
reload	Reboots the system.
repository	Enters the repository submode for configuration of backups.
restore	Restores from backup the file contents of a specific repository.
show backup history	Displays the backup history of the system.
show repository	Displays the available backup files located on a specific repository.

backup-logs

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

Note Before attempting to use this **backup-logs** command in the 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 your Cisco ISE application from the backup and system logs. For more information of copying the running configuration to the startup configuration, see the "copy" section on page A-19.

backup-logs *backup-name* **repository** *repository-name* **encryption-key** *hash* | *plain encryption-key name*

Syntax Description

backup-logs	The command to back up the system and application logs to a repository.
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.
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 | plain format.

Defaults

No default behavior or values.

Command Modes

EXEC

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

Examples

```
ise/admin# backup-logs mybackup repository myrepository encryption-key plain Lab12345
% Creating log backup with timestamped filename: mybackup-111125-1117.tar.gpg
ise/admin#
```

Related Commands

Command	Description
backup	Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.
repository	Enters the repository submode for configuration of backups.
show backup history	Shows the backup history of the system.
show repository	Shows the available backup files located on a specific repository.

clock

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

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

Syntax Description

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

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines Sets the system clock. You must restart the Cisco ISE server after you reset the clock for the change to take effect.

Warning **Changing the system time on a Cisco ISE appliance causes the Cisco ISE application to be unusable in the deployment.**

For more information on how changing system time impacts different Cisco ISE nodes types of your deployment and the steps to recover from the impact, see the "Standalone or Primary ISE Node" section on page A-18 and "Secondary ISE Node" section on page A-18.

Standalone or Primary ISE Node

Changing the system time after installation is not supported on a Standalone or Primary ISE node.

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

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

Secondary ISE Node

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

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

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

Note To ensure that you have the correct system time set at the time of installation, the setup wizard prompts for an NTP server and tries to sync with it. You must ensure that the configured NTP server 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 and this in turn can corrupt the ADE-OS system time during reboot. If you do not configure a NTP server during setup, then you have to ensure that the system BIOS time is set relative to UTC as described in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.1*.

Examples

```
ise/admin# clock set May 5 18:07:20 2010
ise/admin# show clock
Thu May 5 18:07:26 UTC 2010
ise/admin#
```

Related Commands

Command	Description
show clock	Displays the time and date set on the system software clock.

configure

To enter the Configuration mode, use the **configure** command in the EXEC mode. If the **replace** option is used with this command, copies a remote configuration to the system which overwrites the existing configuration.

configure terminal

Syntax Description

configure	The command that allows you to enter the Configuration mode.
terminal	Executes configuration commands from the terminal.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use this command to enter the Configuration mode. Note that commands in this mode write to the running configuration file as soon as you enter them (press **Enter**).

To exit the Configuration mode and return to the EXEC mode, enter **end**, **exit**, or **Ctrl-z**.

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

Examples

Example 1

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

Example 2

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

Related Commands

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration.
show startup-config	Displays the contents of the startup configuration file or the configuration.

copy

To copy any file from a source to a destination, use the **copy** command in the EXEC mode. The **copy** command in the Cisco ISE copies a configuration (running or startup).

Running Configuration

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

Startup Configuration

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

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

The following command lines show some of the **copy** command scenarios available:

copy running-config startup-config—Copies the running configuration to the startup configuration.

copy run start—Replaces the startup configuration with the running configuration.

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

copy startup-config running-config—Copies the startup configuration to the running configuration.

copy start run—Merges the startup configuration on top of the running configuration.

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

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

copy startup-config [*protocol***://***hostname***/***location*]—Copies the startup configuration to a remote system.

copy running-config [*protocol***://***hostname***/***location*]—Copies the running configuration to a remote system.

copy logs [*protocol***://***hostname***/***location*]—Copies log files from the system to another location.

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

Syntax Description

copy	The command that copies items.
running-config	Represents the current running configuration file.
startup-config	Represents the configuration file used during initialization (startup).
protocol	See Table A-2 for protocol keyword options.
hostname	Hostname of destination.
location	Location of destination.
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.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

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

You can enter on the command line all the 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.

Timesaver

Aliases reduce the amount of typing that you need to do. For example, type **copy run start** (the abbreviated form of the **copy running-config startup-config** command).

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 FTP error messages.

Table A-2 Protocol Prefix Keywords

Keyword	Source of Destination
ftp	Source or destination URL for FTP network server. The syntax for this alias: **ftp:**[[[*//username* [**:***password*]*@*]*location*]*/directory*]*/filename*

Table A-2 Protocol Prefix Keywords (continued)

Keyword	Source of Destination
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*

Examples

Example 1

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

Example 2

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

Example 3

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

Example 4

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

Example 5

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

Example 6

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

Related Commands

Command	Description
application install	Starts or stops a Cisco ISE instance.
backup	Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.
delete	Deletes a file from the Cisco ISE server.
dir	Lists a file from the Cisco ISE server.
reload	Reboots the system.
restore	Restores from backup the file contents of a specific repository.
show application	Shows application status and version information.
show version	Displays information about the software version of the system.

debug

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

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

Syntax Description

debug	The command to identify various failures with the Cisco ISE server.
all	Enables all debugging.
application	Application files. • *all*—Enables all application debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *install*—Enables application install debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *operation*—Enables application operation debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *uninstall*—Enables application uninstall debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
backup-restore	Backs up and restores files. • *all*—Enables all debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all. • *backup*—Enables backup debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all. • *backup-logs*—Enables backup-logs debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all. • *history*—Enables history debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all. • *restore*—Enables restore debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.
cdp	Cisco Discovery Protocol configuration files. • *all*—Enables all Cisco Discovery Protocol configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *config*—Enables configuration debug output for Cisco Discovery Protocol. Set level between 0 and 7, with 0 being severe and 7 being all. • *infra*—Enables infrastructure debug output for Cisco Discovery Protocol. Set level between 0 and 7, with 0 being severe and 7 being all.

config	Configuration files. • *all*—Enables all configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *backup*—Enables backup configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *clock*—Enables clock configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *infra*—Enables configuration infrastructure debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *kron*—Enables command scheduler configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *network*—Enables network configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *repository*—Enables repository configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *service*—Enables service configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
icmp	Internet Control Message Protocol (ICMP) echo response configuration. *all*—Enable all debug output for ICMP echo response configuration. Set level between 0 and 7, with 0 being severe and 7 being all.
copy	Copy commands. Set level between 0 and 7, with 0 being severe and 7 being all.
locks	Resource locking. • *all*—Enables all resource locking debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *file*—Enables file locking debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
logging	Logging configuration files. *all*—Enables all logging configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
snmp	SNMP configuration files. *all*—Enables all SNMP configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
system	System files. • *all*—Enables all system files debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *id*—Enables system ID debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *info*—Enables system info debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *init*—Enables system init debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
transfer	File transfer. Set level between 0 and 7, with 0 being severe and 7 being all.

user	User management. • *all*—Enables all user management debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *password-policy*—Enables user management debug output for password-policy. Set level between 0 and 7, with 0 being severe and 7 being all.
utils	Utilities configuration files. *all*—Enables all utilities configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use the **debug** command to identify various failures within the Cisco ISE server; for example, setup failures or configuration failures.

Examples

```
ise/admin# debug all
ise/admin# mkdir disk:/1
ise/admin# 6 [15347]: utils: vsh_root_stubs.c[2742] [admin]: mkdir operation success

ise/admin# rmdir disk:/1
6 [15351]: utils: vsh_root_stubs.c[2601] [admin]: Invoked Remove Directory disk:/1 command
6 [15351]: utils: vsh_root_stubs.c[2663] [admin]: Remove Directory operation success
ise/admin#

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

Related Commands

Command	Description
undebug	Disables the output (display of errors or events) of the **debug** command for various command situations.

delete

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

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

Syntax Description

delete	The command to delete a file from the Cisco ISE server.
filename	Filename. Supports up to 80 alphanumeric characters.
disk:/path	Location.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

If you attempt to delete the 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.

Examples

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

Related Commands

Command	Description
dir	Lists all the files on the Cisco ISE server.

dir

To list a file from the Cisco ISE server, use the **dir** command in the EXEC mode. To remove this function, use the **no** form of this command.

dir [*word*] [**recursive**]

Syntax Description

dir	The command to list files on a local system.
word	Directory name. Supports up to 80 alphanumeric characters. Requires **disk:/** preceding the directory name.
recursive	Lists a local directory or filename recursively.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

Example 1

```
ise/admin# dir

Directory of disk:/

    2034113 Aug 05 2010 19:58:39 ADElogs.tar.gz
       4096 Jun 10 2010 02:34:03 activemq-data/
       4096 Aug 04 2010 23:14:53 logs/
      16384 Jun 09 2010 02:59:34 lost+found/
    2996022 Aug 05 2010 19:11:16 mybackup-100805-1910.tar.gz
       4096 Aug 04 2010 23:15:20 target/
       4096 Aug 05 2010 12:25:55 temp/

           Usage for disk: filesystem
                 8076189696 bytes total used
                 6371618816 bytes free
                15234142208 bytes available
ise/admin#
```

Example 2

```
ise/admin# dir disk:/logs

0 Aug 05 2010 11:53:52 usermgmt.log

           Usage for disk: filesystem
                 8076189696 bytes total used
                 6371618816 bytes free
                15234142208 bytes available
ise/admin#
```

Example 3

```
ise/admin# dir recursive

Directory of disk:/

    2034113 Aug 05 2010 19:58:39 ADElogs.tar.gz
    2996022 Aug 05 2010 19:11:16 mybackup-100805-1910.tar.gz
       4096 Aug 04 2010 23:14:53 logs/
       4096 Aug 05 2010 12:25:55 temp/
       4096 Jun 10 2010 02:34:03 activemq-data/
       4096 Aug 04 2010 23:15:20 target/
      16384 Jun 09 2010 02:59:34 lost+found/

Directory of disk:/logs

          0 Aug 05 2010 11:53:52 usermgmt.log

Directory of disk:/temp

        281 Aug 05 2010 19:12:45 RoleBundles.xml
       6631 Aug 05 2010 19:12:34 PipDetails.xml
         69 Aug 05 2010 19:12:45 GroupRoles.xml
        231 Aug 05 2010 19:12:34 ApplicationGroupTypes.xml
     544145 Aug 05 2010 19:12:35 ResourceTypes.xml
      45231 Aug 05 2010 19:12:45 UserTypes.xml
        715 Aug 05 2010 19:12:34 ApplicationGroups.xml
        261 Aug 05 2010 19:12:34 ApplicationTypes.xml
       1010 Aug 05 2010 19:12:34 Pdps.xml
    1043657 Aug 05 2010 19:12:44 Groups.xml
     281003 Aug 05 2010 19:12:38 Resources.xml
         69 Aug 05 2010 19:12:45 GroupUsers.xml
```

```
       2662 Aug 05 2010 19:12:44 RoleTypes.xml
         79 Aug 05 2010 19:12:34 UserStores.xml
       4032 Aug 05 2010 19:12:38 GroupTypes.xml
       1043 Aug 05 2010 19:12:34 Organization.xml
      58377 Aug 05 2010 19:12:46 UserRoles.xml
        300 Aug 05 2010 19:12:45 Contexts.xml
        958 Aug 05 2010 19:12:34 Applications.xml
      28010 Aug 05 2010 19:12:45 Roles.xml
     122761 Aug 05 2010 19:12:45 Users.xml

Directory of disk:/activemq-data

       4096 Jun 10 2010 02:34:03 localhost/

Directory of disk:/activemq-data/localhost

          0 Jun 10 2010 02:34:03 lock
       4096 Jun 10 2010 02:34:03 journal/
       4096 Jun 10 2010 02:34:03 kr-store/
       4096 Jun 10 2010 02:34:03 tmp_storage/

Directory of disk:/activemq-data/localhost/journal

   33030144 Aug 06 2010 03:40:26 data-1
       2088 Aug 06 2010 03:40:26 data-control

Directory of disk:/activemq-data/localhost/kr-store

       4096 Aug 06 2010 03:40:27 data/
       4096 Aug 06 2010 03:40:26 state/

Directory of disk:/activemq-data/localhost/kr-store/data

        102 Aug 06 2010 03:40:27 index-container-roots
          0 Aug 06 2010 03:40:27 lock

Directory of disk:/activemq-data/localhost/kr-store/state

       3073 Aug 06 2010 03:40:26 hash-index-store-state_state
         51 Jul 20 2010 21:33:33 index-transactions-state
        204 Aug 06 2010 03:40:26 index-store-state
        306 Jun 10 2010 02:34:03 index-kaha
        290 Jun 10 2010 02:34:03 data-kaha-1
      71673 Aug 06 2010 03:40:26 data-store-state-1
          0 Jun 10 2010 02:34:03 lock

Directory of disk:/activemq-data/localhost/tmp_storage

No files in directory

Directory of disk:/target

       4096 Aug 04 2010 23:15:20 logs/

Directory of disk:/target/logs

          0 Aug 04 2010 23:15:20 ProfilerPDP.log
       2208 Aug 05 2010 11:54:26 ProfilerSensor.log

Directory of disk:/lost+found

No files in directory

           Usage for disk: filesystem
```

```
                 8076189696 bytes total used
                 6371618816 bytes free
                15234142208 bytes available

ise/admin#
```

Related Commands	Command	Description
	delete	Deletes a file from the Cisco ISE server.

exit

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

exit

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines Use the **exit** command in EXEC mode to exit an active session (log out of the Cisco ISE server) or to move up from the Configuration mode.

Examples

```
ise/admin# exit
ise/admin#
```

Related Commands	Command	Description
	end	Exits the Configuration mode.
	exit	Exits the Configuration mode or EXEC mode.
	Ctrl-z	Exits the Configuration mode.

forceout

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

forceout *username*

Syntax Description

forceout	The command that enforces logout of all the sessions of a specific system user.
username	The name of the user. Supports up to 31 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

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

Examples

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

halt

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

halt

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

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

```
WARNING: A backup or restore is currently in progress! Continue with halt?

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

If you get any of these warnings, enter **Yes** to halt the 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, the Cisco ISE asks you to respond to the following option:

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

Enter **Yes** to save the existing Cisco ISE configuration. The Cisco ISE displays the following message:

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

Examples

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

Related Commands

Command	Description
reload	Reboots the system.

help

To describe the interactive help system for the Cisco ISE server, use the **help** command in the EXEC mode.

help

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

All configuration modes.

Usage Guidelines

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

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

Examples

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

```
   (e.g. 'show pr?'.)

ise/admin#
```

mkdir

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

mkdir *directory-name* [*disk:/path*]

Syntax Description

mk dir	The command to create directory.
directory-name	The name of the directory to create. Supports up to 80 alphanumeric characters.
disk:/path	Use *disk:/path* with the directory name.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

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

Examples

```
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#
```

Related Commands

Command	Description
dir	Displays a list of files on the ISE server.
rmdir	Removes an existing directory.

nslookup

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

nslookup *word*

Syntax Description

nslookup	The command to search the IP address or hostname of a remote system.
word	IPv4 address or hostname of a remote system. Supports up to 64 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

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 209.165.200.225
Trying "225.200.165.209.in-addr.arpa"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65283
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;225.200.165.209.in-addr.arpa. IN      PTR

;; ANSWER SECTION:
225.200.165.209.in-addr.arpa. 86400 IN PTR     209-165-200-225.got.net.

;; AUTHORITY SECTION:
200.165.209.in-addr.arpa. 86400 IN      NS      ns1.got.net.
200.165.209.in-addr.arpa. 86400 IN      NS      ns2.got.net.

Received 119 bytes from 171.70.168.183#53 in 28 ms

ise/admin#
```

patch install

The **patch install** command installs a patch bundle of the application only on a specific node where you run the **patch install** command from the CLI.

Note In a Cisco ISE distributed deployment environment, install the patch bundle of the application from the primary Administration ISE node in the Cisco ISE Administration user interface so that the patch bundle automatically gets installed on all the secondary nodes.

To install a patch bundle of the application, use the **patch** command in the EXEC mode.

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

Syntax Description

patch	The command to install System or Application patch.
install	The command that installs a specific patch bundle of the application.
patch-bundle	The patch bundle file name. Supports up to 255 alphanumeric characters.
repository	Repository name. Supports up to 255 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Installs a specific patch bundle of the application.

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

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

Note Before attempting to use this patch install command to install a patch, you must read the patch installation instructions in the release notes supplied with that patch. The release notes contains important instructions updated for installing that patch, which must be followed. For more information, refer to the Managing ISE Backup and Restore Operations section in the *Cisco Identity Services Engine User Guide, Release 1.1.1* on patch installation and rollback.

Examples

Example 1

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

Patch successfully installed
ise/admin#
```

Example 2

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

Patch successfully installed
ise/admin#
```

Example 3

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

Related Commands

Command	Description
patch remove	The command that removes a specific patch bundle version of the application.
show version	Displays information about the currently loaded software version, along with hardware and device information.

patch remove

Note In a Cisco ISE distributed deployment environment, remove the patch bundle of the application from the primary Administration ISE node in the Cisco ISE Administration user interface so that the patch bundle automatically gets uninstalled from all the secondary nodes. For more information, refer to the Managing ISE Backup and Restore Operations section in the *Cisco Identity Services Engine User Guide, Release 1.1.1* on patch installation and rollback.

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

patch remove *word word*

Syntax Description

patch	The command to install System or Application patch.
remove	The command that removes a specific patch bundle version of the application.
word	The name of the application for which the patch is to be removed. Supports up to 255 alphanumeric characters.
word	The patch version number to be removed. Supports up to 255 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Removes a specific patch bundle of the application.

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

```
% Patch is not installed
```

Note Before attempting to use this patch remove command to rollback a patch, you must read the rollback instructions of the patch in the release notes supplied with that patch. The release notes contains important instructions updated for rolling back the previously installed patch, which must be followed.

Examples

Example 1

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

Example 2

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

Related Commands

Command	Description
patch install	The command that installs a specific patch bundle of the application.
show version	Displays information about the currently loaded software version, along with hardware and device information.

pep

You can use the **pep** command along with **certificate**, **set**, and **switch** command options in the EXEC mode to perform the following:

- **pep certificate**—To manipulate CA and server certificates for an Inline Posture node
- **pep set**—To log the Cisco ISE Inline Posture node information
- **pep switch into-pep**—To configure a secondary node into a Cisco ISE Inline Posture node in a Cisco ISE distributed deployment
- **pep switch outof-pep—**To configure the Cisco ISE Inline Posture node back to a Cisco ISE standalone node

The following command lines show the **pep** command scenarios available:

pep certificate {*certauthority*|*server*}—manipulates CA and server certificates for an Inline Posture node.

pep set loglevel {*0*|*1*|*2*|*3*}—sets the Inline Posture node log information.

pep switch {*into-pep*| *outof-pep*}—configures the Cisco ISE node into Inline Posture node or Inline Posture role to a Cisco ISE standalone node.

Syntax Description

pep	The command to configure a secondary node in the distributed deployment to the Inline Posture role.
certificate	The command that manipulates both CA and server certificates.
certauthority	The command that manipulates CA certificates.
add	Adds a certificate to the CA store of Inline Posture node.
delete	Deletes a certificate from the CA store of Inline Posture node.
server	The command that manipulates server certificates.
add	Adds a new server certificate with the different key and certificate to the server store.
delete	Deletes a server certificate from the server store.
set	The command that sets the Inline Posture loglevel configuration.
loglevel	The command that sets the Inline Posture log level.
0-3	0-info—Logs only information. 1-warn —Warning conditions. 2-debug—Debugging messages. 3-trace—Logs information for troubleshooting.
switch	The command that configures the Inline Posture node personna changes.

into-pep	Configures the secondary node into the Inline Posture role.
outof-pep	Configures the Inline Posture role to a standalone role enabled with the administration, monitoring and policy service roles.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

You cannot use this **pep** command in a VMware setup.

Use the **pep certificate** command options to manipulate CA and server certificates for an Inline Posture node. Any certificate change in the trust store results in an Inline Posture application restart. To view the certificates list in the trust store, use the **show pep certificate certauthority** command.

Use the **pep set** command options to log Inline Posture node information.

Use the **pep switch** command options to configure an ISE secondary node into an ISE Inline Posture node, or configure an ISE Inline Posture node into an ISE standalone node that will be enabled with the administration, monitoring, and policy services role. But, Cisco ISE recommends not to use the **pep switch into-pep** command to change a registered ISE policy service node into an ISE Inline Posture node. Registering the secondary node as an Inline Posture node from the Cisco ISE Administration node user interface is always recommended, and the conversion takes place automatically. Cisco ISE also recommends not to use the **pep switch outof-pep** command to change an ISE Inline Posture node back to an ISE standalone node. Deregistering the Inline Posture node from the ISE Administration node user interface is always recommended.

Examples

Example 1

The following command adds a CA certificate to the trust store of an Inline Posture node. The certificate file needs to be present in the local disk repository of the Inline Posture node. Create a local disk repository for copying certificate and server private key files into the Inline Posture node, so that the **add** command can use those files. Use the **copy** command to download certificate and key files into the local disk repository.

Use the **show pep certificate certauthority** command to view the certificates list in the trust store. You can see the CA certificate added to the trust store with its alias name.

Note Use the **show pep certificate certauthority** command to check whether a CA certificate is already present in the trust store. If you import the same certificate (by using the **add** command) that is already present in the trust store, the certificate may be unusable when you use a different alias name for that certificate at the prompt, and the Inline Posture node may not be accessible after restart. Either you use the same alias name when you import the same certificate, or delete the certificate from the trust srore and then import with a different alias name for that ceritficate.

```
ise/admin# pep certificate certauthority add
CA Certificate change will result in application restart. Proceed? (y/n):
y
Enter the name of the certificate to be added (.pem/.crt):
ise70ciscocom4f061e00d0afb.pem
```

```
Enter an alias name for the certificate to be added:
ca-1
IPEP Application Restarting
ise/admin#
```

The following command deletes a CA certificate from the trust store of an Inline Posture node. Use the **show pep certificate certauthority** command to view the certificates list in the trust store. You can see the CA certificate deleted from the trust store.

```
ise/admin# pep certificate certauthority delete
CA Certificate change will result in application restart. Proceed? (y/n):
y
Enter the alias name of the certificate to be removed:
ca-1
IPEP Application Restarting
ise/admin#
```

Example 2

The following command adds server private key and server certificate (for example, tomcat) to the key store of an Inline Posture node. Use the **show pep certificate certauthority** command to view the certificates list in the trust store. You can see tomcat added to the trust store. The server certificate details can be seen by using the **show pep certificate server** command.

```
ise/admin# pep certificate server add
Server Certificate change will result in application restart. Proceed? (y/n):
y
Enter the server key file name:
mykey.pem
Enter the server certificate file name:
mycert.pem
Enter server key pass phrase:
IPEP Application Restarting
ise/admin#
```

The following command deletes a server certificate (tomcat) from the key store of an Inline Posture node. Use the **show pep certificate certauthority** command to view the certificates list. You can see tomcat deleted from the trust store.

```
ise/admin# pep certificate server delete
Server Certificate change will result in application restart. Proceed? (y/n):
y
IPEP Application Restarting
ise/admin#
```

Example 3

```
ise/admin# pep set loglevel 0
ise/admin#
```

The **show pep loglevel** command displays the loglevel.

```
ise/admin# show pep loglevel
INFO
ise/admin#
```

Example 4

```
ise/admin# pep switch into-pep
Do you really want to switch into Inline PEP persona? (y/n): y
Switch into IPEP needs restart. Proceed? (y/n): y
Broadcast message from root (pts/2) (Thu Jan 19 09:20:57 2012):
```

```
ise/admin#
```

To check the configuration of the secondary node after reboot, run the **show application status ise** command and the secondary node now runs the Inline Posture services after reboot.

```
ise/admin# show application status ise
Inline PEP click kernel module is loaded.
Inline PEP runtime java application is running,PID=25364.
ise/admin#
```

Example 5

```
ise/admin# pep switch outof-pep
Broadcast message from root (pts/0) (Wed Oct 13 09:03:10 2010):
The system is going down for reboot NOW!
ise/admin#
```

To check the configuration of the Inline Posture node after reboot, run the **show application status ise** command and the node now runs the administration, monitoring and policy service roles as a Standalone node after reboot.

```
ise/admin# show application status ise

ISE Database listener is running, PID: 3057
ISE Database is running, number of processes: 27
ISE Application Server is running, PID: 3357
ISE M&T Session Database is running, PID: 2858
ISE M&T Log Collector is running, PID: 3378
ISE M&T Log Processor is running, PID: 3422
ISE M&T Alert Process is running, PID: 3467

ise/admin#
```

Related Commands

Command	Description
show pep	Shows the Inline Posture node information.

ping

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

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

Syntax Description

ping	The command to ping a remote IP address.
ip-address	IP address of the system to ping. Supports up to 32 alphanumeric characters.
hostname	Hostname of the system to ping. Supports up to 32 alphanumeric characters.
df	Specification for packet fragmentation.
df	Specify the value as **1** to prohibit packet fragmentation, or **2** to fragment the packets locally, or **3** to not set df.
packetsize	Size of the ping packet.
packetsize	Specify the size of the ping packet; the value can be between 0 and 65507.

pingcount	Number of ping echo requests.
pingcount	Specify the number of ping echo requests; the value can be between 1 and 10.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **ping** command sends an echo request packet to an address, then awaits a reply. The ping output can help you evaluate path-to-host reliability, delays over the path, and whether you can reach a host.

Examples

```
ise/admin# ping 172.16.0.1 df 2 packetsize 10 pingcount 2
PING 172.16.0.1 (172.16.0.1) 10(38) bytes of data.
18 bytes from 172.16.0.1: icmp_seq=0 ttl=40 time=306 ms
18 bytes from 172.16.0.1: icmp_seq=1 ttl=40 time=300 ms

--- 172.16.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 300.302/303.557/306.812/3.255 ms, pipe 2
ise/admin#
```

Related Commands

Command	Description
ping6	Ping a remote IPv6 address.

ping6

Similar to the IPv4 **ping,** use the IPv6 **ping6** command in the EXEC mode.

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

Syntax Description

ping	The command to ping a remote IPv6 address.
ip-address	IP address of the system to ping. Supports up to 64 alphanumeric characters.
hostname	Hostname of the system to ping. Supports up to 64 alphanumeric characters.
GigabitEthernet	Ethernet interface.
0-3	Select an Ethernet interface.
packetsize	Size of the ping packet.
packetsize	Specify the size of the ping packet; the value can be between 0 and 65507.
pingcount	Number of ping echo requests.
pingcount	Specify the number of ping echo requests; the value can be between 1 and 10.

Command Default No default behavior or values.

Command Modes EXEC

Usage Guidelines The IPv6 **ping6** command sends an echo request packet to an address, then awaits a reply. The ping output can help you evaluate path-to-host reliability, delays over the path, and whether you can reach a host.

The IPv6 **ping6** command is similar to the existing IPv4 ping command. The ping 6 command does not support the IPv4 ping fragmentation (df in IPv4) 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. The packetsize and pingcount options work the same as they do with the IPv4 command.

Examples

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
rtt min/avg/max/mdev = 0.065/0.221/0.599/0.220 ms, pipe 2

ise/admin#
```

Example 2

```
ise/admin# ping6 3ffe:302:11:2:20c:29ff:feaf:da05 GigabitEthernet 0 packetsize 10
pingcount 2
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
rtt min/avg/max/mdev = 0.073/0.073/0.073/0.000 ms, pipe 2

ise/admin#
```

Related Commands

Command	Description
ping	Ping a remote ip address.

reload

To reload the Cisco ISE operating system, use the **reload** command in the EXEC mode.

reload

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines The **reload** command reboots the system. Use the **reload** command after you enter configuration information into a file and save the running-configuration to the persistent startup-configuration on the CLI and save any settings in the web Administration user interface session.

Before you issue the **reload** command, ensure that the Cisco ISE is not performing any backup, restore, installation, upgrade, or remove operation. If the Cisco ISE performs any of these operations and you issue the **reload** command, you will notice any 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 halt the operation, or enter **No** to cancel the halt.

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

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

Enter **Yes** to save the existing Cisco ISE configuration. The Cisco ISE displays the following message:

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

Examples

```
ise/admin# reload
Do you want to save the current configuration? (yes/no) [yes]? yes
Generating configuration...
Saved the running configuration to startup successfully
Continue with reboot? [y/n] y

Broadcast message from root (pts/0) (Fri Aug 7 13:26:46 2010):

The system is going down for reboot NOW!

ise/admin#
```

Related Commands

Command	Description
halt	Disables the system.

restore

To perform a restore of a previous backup, use the **restore** command in the EXEC mode. A restore operation restores data related to the Cisco ISE as well as the Cisco ADE OS. To perform a restore of a previous backup of the application data of the Cisco ISE only, add the **application** command to the **restore** command in the EXEC mode. To remove this function, use the **no** form of this command.

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*

Use the following command to restore data related only to the Cisco ISE application:

restore *filename* **repository** *repository-name* **application** *application-name* **encryption-key hash | plain** *encryption-key name*

Syntax Description

restore	The command to restore the system.
filename	Name of the backed-up file that resides in the repository. Supports up to 120 alphanumeric characters. **Note** You must add the .tar.gpg extension after the filename (for example, myfile.tar.gpg).
repository	The repository command.
repository-name	Name of the repository you want to restore from backup.
application	The application command.
application name	The name of the application data to be restored. Supports up to 255 alphanumeric characters.
encryption-key	Optional. Specifies user-defined encryption key to restore backup.
hash	Hashed encryption key for restoring backup. Specifies an *encrypted* (hashed) encryption key that follows. Supports up to 40 characters.
plain	Plaintext encryption key for restoring backup. Specifies an *unencrypted* plaintext encryption key that follows. Supports up to 15 characters.
encryption-key name	Specifies encryption key in hash | plain format.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

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

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

Examples

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository application ise
encryption-key plain Lab12345
```

```
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore.  Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

Related Commands

Command	Description
backup	Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
repository	Enters the repository submode for configuration of backups.
show repository	Displays the available backup files located on a specific repository.
show backup history	Displays the backup history of the system.

rmdir

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

rmdir *word*

Syntax Description

rmdir	The command to remove an existing directory.
word	Directory name. Supports up to 80 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

```
ise/admin# mkdir disk:/test
ise/admin# dir

Directory of disk:/

       4096 May 06 2010 13:34:49 activemq-data/
       4096 May 06 2010 13:40:59 logs/
      16384 Mar 01 2010 16:07:27 lost+found/
       4096 May 06 2010 13:42:53 target/
       4096 May 07 2010 12:26:04 test/

           Usage for disk: filesystem
                  181067776 bytes total used
                19084521472 bytes free
                20314165248 bytes available
ise/admin#

ise/admin# rmdir disk:/test
ise/admin# dir

Directory of disk:/

       4096 May 06 2010 13:34:49 activemq-data/
       4096 May 06 2010 13:40:59 logs/
      16384 Mar 01 2010 16:07:27 lost+found/
       4096 May 06 2010 13:42:53 target/

           Usage for disk: filesystem
                  181063680 bytes total used
                19084525568 bytes free
                20314165248 bytes available
ise/admin#
```

Related Commands

Command	Description
dir	Displays a list of files on the Cisco ISE server.
mkdir	Creates a new directory.

show

To show the running system information, use the **show** command in the EXEC mode. The **show** commands are used to display the Cisco ISE settings and are among the most useful commands.

The commands in Table A-3 require the **show** command to be followed by a keyword; for example, **show application status**. Some **show** commands require an argument or variable after the keyword to function; for example, **show application version**.

For detailed information on all the Cisco ISE **show** commands, see Show Commands, page A-58.

show *keyword*

Syntax Description

Table A-3 provides a summary of the **show** commands.

Table A-3 Summary of show Commands

Command[1]	Description
application (requires keyword)[2]	Displays information about the installed application; for example, status or version.
backup (requires keyword)	Displays information about the backup.
cdp (requires keyword)	Displays information about the enabled Cisco Discovery Protocol interfaces.
clock	Displays the day, date, time, time zone, and year of the system clock.
cpu	Displays CPU information.
disks	Displays file-system information of the disks.
interface	Displays statistics for all the interfaces configured on the Cisco ADE OS.
logging (requires keyword)	Displays system logging information.
logins (requires keyword)	Displays login history.
memory	Displays memory usage by all running processes.
ntp	Displays the status of the Network Time Protocol (NTP).
ports	Displays all the processes listening on the active ports.
process	Displays information about the active processes of the Cisco ISE server.
repository (requires keyword)	Displays the file contents of a specific repository.
restore (requires keyword)	Displays restore history on the Cisco ISE server.
running-config	Displays the contents of the currently running configuration file on the Cisco ISE server.
startup-config	Displays the contents of the startup configuration on the Cisco ISE server.
tech-support	Displays system and configuration information that you can provide to the TAC when you report a problem.
terminal	Displays information about the terminal configuration parameter settings for the current terminal line.
timezone	Displays the time zone of the Cisco ISE server.
timezones	Displays all the time zones available for use on the Cisco ISE server.
udi	Displays information about the unique device identifier (UDI) of the Cisco ISE.
uptime	Displays how long the system you are logged in to has been up and running.
users	Displays information for currently logged in users.
version	Displays information about the installed application version.

1. The commands in this table require that the **show** command precedes a keyword; for example, **show application**.

2. Some **show** commands require an argument or variable after the keyword to function; for example, **show application version**. This **show** command displays the version of the application installed on the system (see show application, page A-58).

Defaults No default behavior or values.

Command Modes EXEC

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

Examples

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

ssh

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

Note An Admin or Operator (user) can use this command (see Table 1-1).

ssh [*ip-address* | *hostname*] *username* **port** [*number*] **version [1 | 2] delete hostkey** *word*

Syntax Description

ssh	The command to start an encrypted session with a remote system.
ip-address	IP address of the remote system. Supports up to 64 alphanumeric characters.
hostname	Hostname of the remote system. Supports up to 64 alphanumeric characters.
username	Username of the user logging in through SSH.
port [*number*]	(Optional) Indicates the port number of the remote host. From 0 to 65,535. Default 22.
version [1 | 2]	(Optional) Indicates the version number. Default 2.
delete hostkey	Deletes the SSH fingerprint of a specific host.
word	IPv4 address or hostname of a remote system. Supports up to 64 alphanumeric characters.

Defaults Disabled.

Command Modes EXEC (Admin or Operator)

Usage Guidelines

The **ssh** command enables a system to make a secure, encrypted connection to another remote system or server. This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for secure communication over an insecure network.

Examples

Example 1

```
ise/admin# ssh ise1 admin
admin@ise1's password:
Last login: Wed Jul 11 05:53:20 2008 from ise.cisco.com

ise1/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 the EXEC mode.

tech dumptcp <*0-3*> *count* <*package count*>

Syntax Description

tech	TAC commands.
dumptcp	The command to dump a TCP package to the console.
0-3	Gigabit Ethernet interface number (0 to 3).
count	Specifies a maximum package count, and default is continuous (no limit).
package count	Supports 1–10000.

Defaults

Disabled.

Command Modes

EXEC

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.

Examples

```
ise-201/admin# tech dumptcp 0 count 30
Invoking tcpdump. Press Control-C to interrupt.
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
```

```
10:27:32.923319 IP (tos 0x10, ttl  64, id 1377, offset 0, flags [DF], proto: TCP (6),
length: 92) 10.77.122.201.22 > 10.77.204.132.3142: P 165
9025089:1659025141(52) ack 793752673 win 12144
10:27:32.923613 IP (tos 0x10, ttl  64, id 1378, offset 0, flags [DF], proto: TCP (6),
length: 156) 10.77.122.201.22 > 10.77.204.132.3142: P 52
:168(116) ack 1 win 12144
10:27:32.940203 IP (tos 0x0, ttl  55, id 12075, offset 0, flags [none], proto: UDP (17),
length: 123) 72.163.128.140.53 > 10.77.122.201.43876:
  13150 NXDomain* q: AAAA? ise-201.cisco.com. 0/1/0 ns: cisco.com. SOA[|domain]
10:27:32.952693 IP (tos 0x0, ttl 119, id 52324, offset 0, flags [DF], proto: TCP (6),
length: 40) 10.77.204.132.3142 > 10.77.122.201.22: ., ck
sum 0x4ed3 (correct), 1:1(0) ack 168 win 64192
10:27:33.201646 IP (tos 0x0, ttl  64, id 39209, offset 0, flags [DF], proto: UDP (17),
length: 63) 10.77.122.201.50340 > 72.163.128.140.53: [b
ad udp cksum b8a2!]  49140+ AAAA? ise-201.cisco.com. (35)
10:27:33.226571 IP (tos 0x0, ttl  55, id 26568, offset 0, flags [none], proto: UDP (17),
length: 123) 72.163.128.140.53 > 10.77.122.201.50340:
  49140 NXDomain* q: AAAA? ise-201.cisco.com. 0/1/0 ns: cisco.com. SOA[|domain]
10:27:33.415173 IP (tos 0x0, ttl  64, id 39423, offset 0, flags [DF], proto: UDP (17),
length: 63) 10.77.122.201.56578 > 72.163.128.140.53: [b
ad udp cksum 8854!]  62918+ AAAA? ise-201.cisco.com. (35)
10:27:33.453429 IP (tos 0x0, ttl  55, id 12076, offset 0, flags [none], proto: UDP (17),
length: 123) 72.163.128.140.53 > 10.77.122.201.56578:
  62918 NXDomain* q: AAAA? ise-201.cisco.com. 0/1/0 ns: cisco.com. SOA[|domain]
10:27:33.579551 arp who-has 10.77.122.120 tell 10.77.122.250
10:27:33.741303 IP (tos 0x0, ttl 128, id 21433, offset 0, flags [DF], proto: UDP (17),
length: 306) 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHC
P, Request from e4:1f:13:77:13:34, length: 278, xid:0x1377f72b, flags: [Broadcast]
(0x8000)
          Client Ethernet Address: e4:1f:13:77:13:34 [|bootp]
10:27:33.788119 IP (tos 0x0, ttl  64, id 39796, offset 0, flags [DF], proto: UDP (17),
length: 63) 10.77.122.201.43779 > 72.163.128.140.53: [b
ad udp cksum 2ffc!]  32798+ AAAA? ise-201.cisco.com. (35)
10:27:33.812961 IP (tos 0x0, ttl  55, id 26569, offset 0, flags [none], proto: UDP (17),
length: 123) 72.163.128.140.53 > 10.77.122.201.43779:
  32798 NXDomain* q: AAAA? ise-201.cisco.com. 0/1/0 ns: cisco.com. SOA[|domain]
10:27:34.003769 IP (tos 0x0, ttl  64, id 40011, offset 0, flags [DF], proto: UDP (17),
length: 63) 10.77.122.201.23267 > 72.163.128.140.53: [b
ad udp cksum 2e85!]  18240+ AAAA? ise-201.cisco.com. (35)
10:27:34.038636 IP (tos 0x0, ttl  55, id 26570, offset 0, flags [none], proto: UDP (17),
length: 123) 72.163.128.140.53 > 10.77.122.201.23267:
  18240 NXDomain* q: AAAA? ise-201.cisco.com. 0/1/0 ns: cisco.com. SOA[|domain]
10:27:34.579054 arp who-has 10.77.122.120 tell 10.77.122.250
10:27:34.927369 arp who-has 10.77.122.42 tell 10.77.122.40
10:27:35.727151 IP (tos 0x0, ttl 255, id 64860, offset 0, flags [none], proto: UDP (17),
length: 317) 0.0.0.0.68 > 255.255.255.255.67: BOOTP/D
HCP, Request from 3c:df:1e:58:0f:c0, length: 289, xid:0x161504, flags: [Broadcast]
(0x8000)
          Client Ethernet Address: 3c:df:1e:58:0f:c0 [|bootp]
10:27:36.190658 CDPv2, ttl: 180s, checksum: 692 (unverified), length 384
        Device-ID (0x01), length: 12 bytes: 'hyd04-lab-SW'[|cdp]
30 packets captured
30 packets received by filter
0 packets dropped by kernel
ise-201/admin#
```

telnet

To log in to a host that supports Telnet, use the **telnet** command in Operator (user) or EXEC mode.

telnet [*ip-address* | *hostname*] **port** *number*

Syntax Description

telnet	The command to log in to a host that supports Telnet.
ip-address	IP address of the remote system. Supports up to 64 alphanumeric characters.
hostname	Hostname of the remote system. Supports up to 64 alphanumeric characters.
port *number*	(Optional) Indicates the port number of the remote host. From 0 to 65,535.

Defaults

No default behavior or values.

Command Modes

Operator

EXEC

Usage Guidelines

None.

Examples

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

terminal length

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

terminal length *integer*

Syntax Description

terminal	The command to set the terminal line parameters.
length	The command that sets the number of lines on the current terminal screen for the current session.
integer	Number of lines on the screen. Contains between 0 to 511 lines, inclusive. A value of zero (0) disables pausing between screens of output.

Defaults

24 lines

Command Modes

EXEC

Usage Guidelines

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

Examples

```
ise/admin# terminal length 0
ise/admin#
```

terminal session-timeout

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

terminal session-timeout *minutes*

Syntax Description

terminal	The command to set the terminal line parameters.
session-timeout	The command that sets the inactivity time out of all the sessions.
minutes	Sets the number of minutes for the inactivity timeout. From 0 to 525,600. Zero (0) disables the timeout.

Defaults

30 minutes

Command Modes

EXEC

Usage Guidelines

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

Examples

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

Related Commands

Command	Description
terminal session-welcome	Sets a welcome message on the system for all users who log in to the system.

terminal session-welcome

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

terminal session-welcome *string*

Syntax Description

terminal	The command to set the terminal line parameters.

session-welcome	The command that sets a welcome message on the system for all users who log in to the system.
string	Welcome message. Supports up to 2,048 alphanumeric characters.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines Specify a message using up to 2,048 characters.

Examples

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

Related Commands

Command	Description
terminal session-timeout	Sets the inactivity timeout for all sessions.

terminal terminal-type

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

terminal terminal-type *type*

Syntax Description

terminal	The command to set the terminal line parameters.
terminal-type	The command that specifies the type of terminal connected. The default terminal type is VT100.
type	Defines the terminal name and type, and permits terminal negotiation by hosts that provide that type of service. Supports up to 80 alphanumeric characters.

Defaults VT100

Command Modes EXEC

Usage Guidelines Indicate the terminal type if it is different from the default of VT100.

Examples

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

traceroute

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

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

Syntax Description

traceroute	The command to discover the routes of the packets to their destination address.
ip-address	IP address of the remote system. Supports up to 32 alphanumeric characters.
hostname	Hostname of the remote system. Supports up to 32 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

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

ise/admin#
```

undebug

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

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

Syntax Description

undebug	The command to disable identifying various failures with the Cisco ISE server.
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 output. • *config*—Disables configuration debug output for Cisco Discovery Protocol. • *infra*—Disables infrastructure debug output for Cisco Discovery Protocol.
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.
icmp	ICMP echo response configuration. *all*—Disable all debug output for ICMP echo response configuration. Set level between 0 and 7, with 0 being severe and 7 being all.
locks	Resource locking. • *all*—Disables all resource locking debug output. • *file*—Disables file locking debug output.
logging	Logging configuration files. *all*—Disables all debug output for logging configuration.
snmp	SNMP configuration files. *all*—Disables all debug output for SNMP configuration.

system	System files. • *all*—Disables all system files debug output. • *id*—Disables system ID debug output. • *info*—Disables system info debug output. • *init*—Disables system init debug output.
transfer	File transfer.
user	User management. • *all*—Disables all user management debug output. • *password-policy*—Disables user management debug output for password-policy.
utils	Utilities configuration files. *all*—Disables all utilities configuration debug output.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

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

Related Commands

Command	Description
debug	Displays errors or events for command situations.

write

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

write {**erase** | **memory** | **terminal**}

Syntax Description

write	The command to write running system information.
erase	Erases the startup configuration. This option is disabled in Cisco ISE.
memory	Copies the running configuration to the startup configuration.
terminal	Copies the running configuration to console.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines Using this write command with the erase option is disabled in Cisco ISE.

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

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

Examples

Example 1

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

Example 2

```
ise/admin# write terminal

Generating configuration...
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 10.201.2.121 255.255.255.0
  ipv6 address autoconfig
!
interface GigabitEthernet 1
  shutdown
!
interface GigabitEthernet 2
  shutdown
!
interface GigabitEthernet 3
  shutdown
!
ip name-server 171.68.226.120
!
ip default-gateway 10.201.2.1
!
clock timezone UTC
!
ntp server clock.cisco.com
!
username admin password hash $1$6yQQaFXM$UBgbp7ggD1bG3kpExywwZ0 role admin
!
service sshd
!
repository myrepository
  url disk:
  user admin password hash 2b50ca94445f240f491e077b5f49fa0375942f38
!
password-policy
  lower-case-required
  upper-case-required
```

```
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
cdp timer 60
cdp holdtime 180
cdp run GigabitEthernet 0
!
icmp echo on
!

ise/admin#
```

Show Commands

This section lists each **show** command and includes a brief description of its use, command syntax, usage guidelines, and sample output.

Table A-4 lists the show commands in the EXEC mode that this section describes.

Table A-4 List of EXEC show Commands

• show application	• show logins	• show tech-support
• show backup history	• show memory	• show terminal
• show cdp	• show ntp	• show timezone
• show clock	• show pep	• show timezones
• show cpu	• show ports	• show udi
• show disks	• show process	• show uptime
• show icmp-status	• show repository	• show users
• show interface	• show restore	• show version
• show inventory	• show running-config	
• show logging	• show startup-config	

show application

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

show application [**status** | **version** [*app_name*]]

Syntax Description

show application	The command to display the Cisco ISE application information.
status	Displays the status of the installed application.
version	Displays the application version for an installed application—the Cisco ISE.

app_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 word *count*. |—Output modifier variables (see Table A-5). • *end*—End with line that matches. Supports up to 80 alphanumeric characters. • *exclude*—Exclude lines that match. Supports up to 80 alphanumeric characters. • *include*—Include lines that match. Supports up to 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. Supports up to 80 lines to display. Default 10. |—Output modifier variables (see Table A-5).

Table A-5 Output Modifier Variables for Count or Last

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

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

Example 1

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

Example 2

```
ise/admin# show application version ise

Cisco Identity Services Engine
------------------------------------------
Version      : 1.0.2.051
Build Date   : Mon Aug 2 00:34:25 2010
Install Date : Thu Aug 5 17:48:49 2010

ise/admin#
```

Example 3

```
ise/admin# show application status ise

ISE Database listener is running, PID: 21096
ISE Database is running, number of processes: 27
ISE Application Server is running, PID: 21432
ISE M&T Session Database is running, PID: 21365
ISE M&T Log Collector is running, PID: 21468
ISE M&T Log Processor is running, PID: 21494
ISE M&T Alert Process is running, PID: 21524
ise/admin#
```

Related Commands

Command	Description
application configure	Configures an application.
application install	Installs an application bundle.
application reset-config	Resets an application configuration to factory defaults.
application reset-passwd	Resets an application password for a specified user.
application remove	Removes or uninstalls an application.
application start	Starts or enables an application.
application stop	Stops or disables an application.
application upgrade	Upgrades an application bundle.

show backup history

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

show backup history

Syntax Description

show backup	The command to display the Cisco ISE backup information.
history	Displays history information about any backups on the system.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

Example 1

```
ise/admin# show backup history
Wed Aug 18 12:55:21 UTC 2010: backup logs logs-0718.tar.gz to repository fileserver007:
success
Wed Aug 18 12:55:53 UTC 2010: backup full-0718.tar.gpg to repository fileserver007:
success
ise/admin#
```

Example 2

```
ise/admin# show backup history
backup history is empty
ise/admin#
```

Related Commands

Command	Description
backup	Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.
repository	Enters the repository submode for configuration of backups.
show repository	Displays the available backup files located on a specific repository.

show cdp

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

show cdp {**all** | **neighbors**}

Syntax Description

show cdp	The command to display Cisco Discovery Protocol show commands.
all	Shows all the enabled Cisco Discovery Protocol interfaces.
neighbors	Shows the Cisco Discovery Protocol neighbors.

Defaults No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

Example 1

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

        CDP is enabled on port GigabitEthernet0.
ise/admin#
```

Example 2

```
ise/admin# show cdp neighbors
CDP Neighbor: 000c297840e5
        Local Interface : GigabitEthernet0
        Device Type     : ISE-1141VM-K9
        Port            : eth0
        Address         : 172.23.90.114

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

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

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

ise/admin#
```

Related Commands

Command	Description
cdp holdtime	Specifies the length of time that the receiving device should hold a Cisco Discovery Protocol packet from your router before discarding it.
cdp run	Enables the Cisco Discovery Protocol.
cdp timer	Specifies how often the Cisco ISE server sends Cisco Discovery Protocol updates.

show clock

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

show clock

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

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

Note The **show clock** output in the previous example includes Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), Great Britain, or Zulu time (see Tables A-14, A-15, and A-16 on pages A-84 and A-85 for sample time zones).

Related Commands

Command	Description
clock	Sets the system clock for display purposes.

show cpu

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

show cpu [*statistics*] [|] [|]

Syntax Description

show cpu	The command to display CPU information.
statistics	Displays CPU statistics.

|	Output modifier variables: • *begin*—Matched pattern. Supports up to 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. |—Output modifier variables (see Table A-6). • *end*—End with line that matches. Supports up to 80 alphanumeric characters. • *exclude*—Exclude lines that match. Supports up to 80 alphanumeric characters. • *include*—Include lines that match. Supports up to 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. Supports up to 80 lines to display. Default 10. |—Output modifier variables (see Table A-6).

Table A-6 Output Modifier Variables for Count or Last

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

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

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#
```

Related Commands

Command	Description
show disks	Displays the system information of all disks.
show memory	Displays the amount of system memory that each system process uses.

show disks

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

show disks [|] [|]

Syntax Description

show disks	The command to display the disks and the file-system information
|	Output modifier variables: • *begin*—Matched pattern. Supports up to 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. |—Output modifier variables (see Table A-7). • *end*—End with line that matches. Supports up to 80 alphanumeric characters. • *exclude*—Exclude lines that match. Supports up to 80 alphanumeric characters. • *include*—Include lines that match. Supports up to 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. Supports up to 80 lines to display. Default 10. |—Output modifier variables (see Table A-7).

Table A-7 Output Modifier Variables for Count or Last

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

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

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

Examples

```
ise/admin# show disks

temp. space 2% used (17828 of 988116)
disk: 3% used (143280 of 5944440)

Internal filesystems:
 all internal filesystems have sufficient free space

ise/admin#
```

Related Commands

Command	Description
show cpu	Displays CPU information.
show memory	Displays the amount of system memory that each system process uses.

show icmp-status

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

show icmp_status {**>** *file* | **|**}

Syntax Description

show icmp_status	The command to display the Internet Control Message Protocol echo response configuration information.
>	Output direction.
file	Name of file to redirect standard output (stdout).
|	Output modifier commands: • *begin*—Matched pattern. Supports up to 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word count. – |—Output modifier commands (see Table A-8). • *end*—End with line that matches. Supports up to 80 alphanumeric characters. • *exclude*—Exclude lines that match. Supports up to 80 alphanumeric characters. • *include*—Include lines that match. Supports up to 80 alphanumeric characters. • last—Display last few lines of output. Add number after the word last. Supports up to 80 lines to display. Default 10. – |—Output modifier commands (see Table A-8).

Table A-8 Output Modifier Variables for Count or Last

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

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

Example 1

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

Example 2

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

Related Commands

Command	Description
icmp echo	Configures the Internet Control Message Protocol (ICMP) echo requests.

show interface

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

show interface [*GigabitEthernet*] |

Syntax Description

show interface	The command to display interface information.
GigabitEthernet	Shows the Gigabit Ethernet interface. Enter <0-3>.
|	Output modifier variables: • *begin*—Matched pattern. Supports up to 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. • *end*—End with line that matches. Supports up to 80 alphanumeric characters. • *exclude*—Exclude lines that match. Supports up to 80 alphanumeric characters. • *include*—Include lines that match. Supports up to 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. Supports up to 80 lines to display. Default 10.

Defaults No default behavior or values.

Command Modes EXEC

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

Examples

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#
```

Related Commands

Command	Description
interface	Configures an interface type and enters the interface configuration submode.
ipv6 address autoconfig	Enables IPv6 stateless autoconfiguration on an interface.
ipv6 address dhcp	Enables IPv6 address DHCP on an interface.

show inventory

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

show inventory |

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

```
ise/admin# show inventory

NAME: "ISE-VM-K9      chassis", DESCR: "ISE-VM-K9      chassis"
PID: ISE-VM-K9     , VID: V01 , SN: H8JESGOFHGG
Total RAM Memory: 1035164 kB
CPU Core Count: 1
CPU 0: Model Info: Intel(R) Xeon(R) CPU           E5320  @ 1.86GHz
Hard Disk Count(*): 1
Disk 0: Device Name: /dev/sda
```

```
Disk 0: Capacity: 64.40 GB
Disk 0: Geometry: 255 heads 63 sectors/track 7832 cylinders
NIC Count: 1
NIC 0: Device Name: eth0
NIC 0: HW Address: 00:0C:29:6A:88:C4
NIC 0: Driver Descr: eth0: registered as PCnet/PCI II 79C970A

(*) Hard Disk Count may be Logical.

ise/admin#
```

show logging

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

show logging {**application** [*application-name*]} {**internal**} {**system**} |

Syntax Description

show logging	The command to display system logging information.
application	Displays application logs. *application-name*—Application name. Supports up to 255 alphanumeric characters. – *tail*—Tail system syslog messages. – *count*—Tail last count messages. From 0 to 4,294,967,295. |—Output modifier variables (see below).
internal	Displays the syslogs configuration.
system	Displays the system syslogs.
|	Output modifier variables: • *begin*—Matched pattern. Supports up to 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. • *end*—End with line that matches. Supports up to 80 alphanumeric characters. • *exclude*—Exclude lines that match. Supports up to 80 alphanumeric characters. • *include*—Include lines that match. Supports up to 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. Supports up to 80 lines to display. Default 10.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

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

Examples

Example 1

```
ise/admin# show logging system
ADEOS Platform log:
-----------------

Aug 5 10:44:32 localhost debugd[1943]: [16618]: config:network: main.c[252] [setup]: Setup
is complete
Aug 5 10:45:02 localhost debugd[1943]: [17291]: application:install cars_install.c[242]
[setup]: Install initiated with bundle - ise.tar.gz,
repo - SystemDefaultPkgRepos
Aug 5 10:45:02 localhost debugd[1943]: [17291]: application:install cars_install.c[256]
[setup]: Stage area - /storeddata/Installing/.1281030
302
Aug 5 10:45:02 localhost debugd[1943]: [17291]: application:install cars_install.c[260]
[setup]: Getting bundle to local machine
Aug 5 10:45:03 localhost debugd[1943]: [17291]: transfer: cars_xfer.c[58] [setup]: local
copy in of ise.tar.gz requested
Aug  5 10:45:46 localhost debugd[1943]: [17291]: application:install cars_install.c[269]
[setup]: Got bundle at - /storeddata/Installing/.1281
030302/ise.tar.gz
Aug 5 10:45:46 localhost debugd[1943]: [17291]: application:install cars_install.c[279]
[setup]: Unbundling package ise.tar.gz
Aug 5 10:47:06 localhost debugd[1943]: [17291]: application:install cars_install.c[291]
[setup]: Unbundling done. Verifying input parameters.
..
Aug 5 10:47:06 localhost debugd[1943]: [17291]: application:install cars_install.c[313]
[setup]: Manifest file is at - /storeddata/Installing
/.1281030302/manifest.xml
Aug 5 10:47:07 localhost debugd[1943]: [17291]: application:install cars_install.c[323]
[setup]: Manifest file appname - ise
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[386]
[setup]: Manifest file pkgtype - CARS
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[398]
[setup]: Verify dependency list -
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[410]
[setup]: Verify app license -
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[420]
[setup]: Verify app RPM's
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[428]
[setup]: No of RPM's - 9
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[439]
[setup]: Disk - 50
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[325]
[setup]: Disk requested = 51200 KB
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[345]
[setup]: More disk found Free = 40550400, req_disk = 51200
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[450]
[setup]: Mem requested by app - 100
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[369]
[setup]: Mem requested = 102400
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[384]
[setup]: Found MemFree = MemFree:         13028 kB
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[390]
[setup]: Found MemFree value = 13028
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[393]
[setup]: Found Inactive = Inactive:       948148 kB
```

```
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[399]
[setup]: Found Inactive MemFree value = 948148
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[409]
[setup]: Sufficient mem found
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[415]
[setup]: Done checking memory...
Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[461]
[setup]: Verifying RPM's...
--More--
(press Spacebar to continue)

ise/admin#
```

Example 2

```
ise/admin# show logging internal

log server:          localhost
Global loglevel:     6
Status:              Enabled
ise/admin#
```

Example 3

```
ise/admin# show logging internal

log server:          localhost
Global loglevel:     6
Status:              Disabled
ise/admin#
```

show logins

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

show logins cli

Syntax Description

show logins	The command to display system login history.
cli	Lists the cli login history.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

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

Examples

```
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 the running processes, use the **show memory** command in the EXEC mode.

show memory

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

```
ise/admin# show memory
total memory:    1035164 kB
free memory:       27128 kB
cached:           358888 kB
swap-cached:      142164 kB

ise/admin#
```

show ntp

To show the status of the NTP associations, use the **show ntp** command in the EXEC mode.

show ntp

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

Example:1

```
ise/admin# show ntp
Primary NTP   : ntp.esl.cisco.com
Secondary NTP : 171.68.10.150
Tertiary NTP : 171.68.10.80

synchronised to local net at stratum 11
   time correct to within 11 ms
   polling server every 128 s

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.          10 l    9   64  377    0.000    0.000   0.001
 171.68.10.80    .RMOT.          16 u   11   64    0    0.000    0.000   0.000
 171.68.10.150   .INIT.          16 u   11   64    0    0.000    0.000   0.000
Warning: Output results may conflict during periods of changing synchronization.
ise/admin#
```

Example:2

```
ise/admin# show ntp
% no NTP servers configured
ise/admin#
```

Related Commands

Command	Description
ntp	Allows you to configure NTP configuration up to three NTP servers.
ntp server	Allows synchronization of the software clock by the NTP server for the system.

show pep

To show the Inline Posture node information, use the **show pep** command in the EXEC mode.

show pep [**certificate** {**certauthority**} {**server**}] [**deploymentmode**] [**log**] [**Loglevel**] [**status**] [**summary**] [**table** {**accesslist**(**normal** | **raw**)} {**arp**} {**ipfilters**} {**macfilters**} {**managedsubnets**} {**radius**} {**route**} {**session**} {**vlan**}]

Syntax Description

show pep	The command to display Inline Posture node information.
certificate	Displays certificate stores.
certauthority	Lists Inline Posture node CA certificates in the trust store.
server	Displays Inline Posture node in its own server certificate.
deploymentmode	Displays Inline Posture node Deployment Mode.
log	Displays Inline Posture node Logfile.

Loglevel	Displays Inline Posture node loglevel.
status	Displays Inline Posture node Status.
highavailability	Displays Inline Posture node High Availability Status.
summary	Displays Inline Posture node Summary.
table	Displays Inline Posture node Tables.
accesslist	Displays Inline Posture node Downloadable Access Control Lists (dACLs).
normal	Displays Inline Posture node Downloadable ACLs in normal format.
raw	Displays Inline Posture node Downloadable ACLs in raw format.
arp	Displays Inline Posture node ARP Table.
ipfilters	Displays Inline Posture node IP Filters.
macfilters	Displays Inline Posture node MAC Filters.
managedsubnets	Displays Inline Posture node Managed Subnets.
radius	Displays Inline Posture node Radius Configuration.
route	Displays Inline Posture node Routing Table.
session	Displays Inline Posture node Session Table.
vlan	Displays Inline Posture node VLANs.
>	Output direction.
file	Name of file to redirect standard output (stdout).
|	Output modifier variables: • *begin*—Matched pattern. Supports up to 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. |—Output modifier variables (see Table A-9). • *end*—End with line that matches. Supports up to 80 alphanumeric characters. • *exclude*—Exclude lines that match. Supports up to 80 alphanumeric characters. • *include*—Include lines that match. Supports up to 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. Supports up to 80 lines to display. Default 10. |—Output modifier variables (see Table A-9).

Table A-9 Output Modifier Variables for Count or Last

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

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

Example 1

```
ise/admin# show pep certificate certauthority
Certificate Nickname                                      Trust Attributes
                                                          SSL,S/MIME,JAR/XPI

cise.cisco.com.pem                                        CT,C,C
ca-2                                                      CT,C,C
www.cisco.com.pem                                         CT,C,C
www.perfigo.com.pem                                       CT,C,C
tomcat                                                    u,u,u
ise/admin#
```

Example 2

```
ise/admin# show pep certificate server
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            00:8f:fd:cf:8f:fd:b7:55:c7
        Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
        Issuer: "E=192.30.30.71@email.com,CN=192.30.30.71,OU=snsbu,O=cisco,L=
            san jose,ST=ca,C=us"
        Validity:
```

```
            Not Before: Thu Jan 19 01:35:53 2012
            Not After : Fri Jan 18 01:35:53 2013
        Subject: "E=192.30.30.71@email.com,CN=192.30.30.71,OU=snsbu,O=cisco,L
            =san jose,ST=ca,C=us"
        Subject Public Key Info:
            Public Key Algorithm: PKCS #1 RSA Encryption
            RSA Public Key:
                Modulus:
                    dd:f1:79:b6:2b:2f:66:92:e9:0d:9a:06:1e:53:a4:19:
                    38:e0:08:4d:28:83:24:a6:98:99:39:cb:28:d8:9c:e1:
                    30:7c:90:a6:ac:e0:e6:d2:75:78:5b:a0:10:a0:fb:dd:
                    68:73:04:1d:a6:9e:31:5c:25:d4:bf:b1:8e:8c:a0:79:
                    b4:1e:8e:67:07:8d:5d:2a:e7:72:4d:08:88:93:6c:a9:
                    35:4f:df:97:6c:8e:f2:2c:d5:a1:84:b5:5b:ca:00:ed:
                    1d:cd:09:8a:18:14:b9:21:df:f6:15:1a:05:77:ea:fc:
                    20:b8:c3:c1:ca:bc:a8:33:b3:2c:55:70:41:28:3d:6d
                Exponent: 65537 (0x10001)
        Signed Extensions:
            Name: Certificate Subject Key ID
            Data:
                50:75:2b:4c:72:54:0c:03:ee:ed:e7:e0:44:f0:71:28:
                10:ab:3f:ef

            Name: Certificate Authority Key Identifier
            Key ID:
                50:75:2b:4c:72:54:0c:03:ee:ed:e7:e0:44:f0:71:28:
                10:ab:3f:ef
            Issuer:
                Directory Name: "E=192.30.30.71@email.com,CN=192.30.30.71,OU=
                    snsbu,O=cisco,L=san jose,ST=ca,C=us"
            Serial Number:
                00:8f:fd:cf:8f:fd:b7:55:c7

            Name: Certificate Basic Constraints
            Data: Is a CA with no maximum path length.

    Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
    Signature:
        2a:c9:c1:50:fb:2a:9a:ff:65:42:1a:bb:9e:f1:6b:6f:
        92:e4:bb:1f:64:4c:1c:f8:e9:75:3c:de:1e:9b:0a:df:
        76:96:d2:33:9b:06:cd:88:9b:f7:f3:e7:06:e5:cc:94:
        21:8e:70:9f:b1:5a:cf:19:35:2d:a0:9b:a7:ba:bc:ee:
        c0:34:4d:ee:f7:2f:4e:96:d3:39:c9:0d:48:26:ed:1a:
        63:51:fa:31:1a:c4:12:76:46:2d:57:28:8e:72:ff:e7:
        c2:7c:85:87:5d:c6:68:e4:d0:e9:b6:ad:e0:d1:0d:a2:
        23:88:9a:73:39:59:20:ce:7c:fb:61:8d:96:e2:bd:87
    Fingerprint (MD5):
        05:19:7D:45:3F:A7:42:9A:69:B5:F0:5A:A6:60:39:6C
    Fingerprint (SHA1):
        A0:91:6E:57:81:BA:29:AF:55:DE:58:64:A2:BD:6A:00:2A:56:33:D5

    Certificate Trust Flags:
        SSL Flags:
            User
        Email Flags:
            User
        Object Signing Flags:
            User

ise/admin#
```

Example 3

```
ise/admin# show pep deploymentmode
```

```
Bridge

ise/admin#
```

Example 4

```
ise/admin# show pep log

IPEP Logs:
Fri Oct 8 13:24:50 UTC 2010
ipep setloglevel 0
Mon Oct 11 12:40:00 UTC 2010
ipep setloglevel 0
Mon Oct 11 12:41:24 UTC 2010
ipep switch-into-ipep
Mon Oct 11 12:44:20 UTC 2010
ipep start

=======================
ipep runtime start: Mon Oct 11 12:44:33 UTC 2010
Flushing firewall rules: [  OK  ]
Setting chains to policy ACCEPT: filter [ OK  ]
Unloading iptables modules: [ OK  ]
12:44:39 main       INFO  Controller               - Starting services...
12:44:39 main       INFO  Controller               - Starting System Service...
=================
Mon Oct 11 12:44:40 UTC 2010
ipepconfig ha-config standalone
=================
Mon Oct 11 12:44:40 UTC 2010
ipep sysrestart
12:44:56 main       INFO  Controller               - System Service started
12:44:56 main       INFO  Controller               - Starting Radius Service...
rpm: /opt/CSCOcpm/prrt/lib/libnss3.so: version `NSS_3.10' not found (required by
/usr/lib/librpmio-4.4.so)
Adding URL: file:/opt/CSCOcpm/prrt//lib/rtpolicy.jar
Adding URL: file:/opt/CSCOcpm/prrt//lib/prrt-flowapi.jar
Adding URL: file:/opt/CSCOcpm/prrt//lib/rteventhandlers.jar
Adding URL: file:/opt/CSCOcpm/prrt//lib/rtidstores.jar
Adding URL: file:/opt/CSCOcpm/prrt//lib/prrt-interface.jar
Adding URL: file:/opt/CSCOcpm/prrt//lib/
Loading com.cisco.cpm.prrt.policy.PolicyEngine
IllegalAccessException:  The class 'com.cisco.cpm.prrt.policy.PolicyEngine' wasn't loaded
by the EventHandlerClassLoader but by sun.misc.Launc
--More--
ise/admin#
```

Example 5

```
ise/admin# show pep loglevel
INFO
ise/admin#
```

Example 6

```
ise/admin# show pep status
Inline PEP click kernel module is loaded.
Inline PEP runtime java application is running,PID=3208.
ise/admin#
```

Example 7

```
ise/admin# show pep status highavailability
HA Status:
System configured for standalone operation.
```

```
ise/admin#
```

Example 8

```
ise/admin# show pep table accesslist ?
  normal  Display PEP Downloadable ACL (dACLs) in normal format
  raw     Display PEP Downloadable ACL (dACLs) in raw format

ise/admin# show pep table accesslist normal
#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f0d890d:
permit ip any any

#ACSACL#-IP-PRE-POSTURE-iPEP-4f0f75e5:
deny tcp any any eq 80
deny tcp any any eq 443
permit ip any host 10.35.48.241
permit ip any host 10.35.48.242
permit udp any any eq 53

ise/admin#
```

Example 9

```
ise/admin# show pep table accesslist raw
Current Downloaded ACLs
3
0
0 all
1
0 tcp and (dst port 80)
0 tcp and (dst port 443)
1 (dst host 10.35.48.241)
1 (dst host 10.35.48.242)
1 udp and (dst port 53)
0 all
2
1 all
0 all

ACLs in Queue
3
0
empty
1
empty
2
empty

ise/admin#
```

Example 9

```
ise/admin# show pep table arp
Untrusted Side ARP Table:
ip              ok      mac                     vtag    vtci    login   svtag
svtci   subnet          mask            idle(secs)
10.203.108.37   1       00:25:9C:A3:7D:4F       1       32       1      0
0       0.0.0.0         0.0.0.0         0

ise/admin#
```

Related Commands

Command	Description
pep	Inline Posture configuration.

show ports

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

show ports [|] [|]

Syntax Description

show ports	The command to display all the processes listening on open ports in the Cisco ISE.
|	Output modifier variables: • *begin*—Matched pattern. Supports up to 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. |—Output modifier variables (see Table A-10). • *end*—End with line that matches. Supports up to 80 alphanumeric characters. • *exclude*—Exclude lines that match. Supports up to 80 alphanumeric characters. • *include*—Include lines that match. Supports up to 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. Supports up to 80 lines to display. Default 10. |—Output modifier variables (see Table A-10).

Table A-10 Output Modifier Variables for Count or Last

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

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

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

Examples

```
ise/admin# show ports
Process : timestensubd (21372)
     tcp: 127.0.0.1:11298
Process : timestenorad (21609)
     tcp: 127.0.0.1:51715
     udp: ::1:28314, ::1:59055, ::1:45113, ::1:49082, ::1:64737, ::1:62570, ::1:19577,
::1:29821
Process : ttcserver (21382)
     tcp: 127.0.0.1:16612, 0.0.0.0:53385
Process : timestenrepd (21579)
     tcp: 127.0.0.1:62504, 0.0.0.0:18047
     udp: ::1:51436
Process : timestend (21365)
     tcp: 0.0.0.0:53384
Process : rpc.statd (2387)
     tcp: 0.0.0.0:873
     udp: 0.0.0.0:867, 0.0.0.0:870
Process : timestensubd (21373)
     tcp: 127.0.0.1:43407
Process : portmap (2350)
     tcp: 0.0.0.0:111
     udp: 0.0.0.0:111
Process : Decap_main (21468)
     tcp: 0.0.0.0:2000
     udp: 0.0.0.0:9993
Process : timestensubd (21369)
     tcp: 127.0.0.1:37648
Process : timestensubd (21374)
     tcp: 127.0.0.1:64211
Process : sshd (2734)
     tcp: 172.23.90.113:22
Process : java (21432)
     tcp: 127.0.0.1:8888, :::2080, :::2020, ::ffff:127.0.0.1:8005, :::8009, :::8905,
:::8010, :::2090, :::1099, :::9999, :::61616, :::8080, ::
:80, :::60628, :::8443, :::443
     udp: 0.0.0.0:1812, 0.0.0.0:1813, 0.0.0.0:1700, 0.0.0.0:10414, 0.0.0.0:3799,
0.0.0.0:1645, 0.0.0.0:1646, :::8905, :::8906
Process : monit (21531)
     tcp: 127.0.0.1:2812
Process : java (21524)
     tcp: :::62627
Process : java (21494)
     tcp: ::ffff:127.0.0.1:20515
     udp: 0.0.0.0:20514
Process : tnslsnr (21096)
     tcp: :::1521
Process : ora_d000_ise1 (21222)
     tcp: :::26456
     udp: ::1:63198
Process : ntpd (2715)
    udp: 172.23.90.113:123, 127.0.0.1:123, 0.0.0.0:123, ::1:123, fe80::20c:29ff:fe6a:123,
:::123
Process : ora_pmon_ise1 (21190)
     udp: ::1:51994
Process : ora_mmon_ise1 (21218)
     udp: :::38941
Process : ora_s000_ise1 (21224)
     udp: ::1:49864
ise/admin#
```

show process

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

show process |

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

See Table A-11 for process field descriptions.

```
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#
```

Table A-11 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

show repository

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

show repository *repository-name*

Syntax Description

show repository	The command to display the repository contents.
repository-name	Name of the repository whose contents you want to view. Supports up to 30 alphanumeric characters.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

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

Related Commands

Command	Description
backup	Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.
repository	Enters the repository submode for configuration of backups.
show backup history	Displays the backup history of the system.

show restore

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

show restore {**history**}

Syntax Description

show restore	The command to display the restore information.
history	Displays the restore history.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

Example 1

```
ise/admin# show restore history

ise/admin#
```

Example 2

```
ise/admin# show restore history
restore history is empty
ise/admin#
```

Related Commands

Command	Description
backup	Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.
repository	Enters the repository submode for configuration of backups.
show backup history	Displays the backup history of the system.

show running-config

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

show running-config

Syntax Description No arguments or keywords.

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

Command Modes EXEC

Usage Guidelines None.

Examples

```
ise/admin# show running-config
Generating configuration...
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 171.70.168.183
!
ip default-gateway 172.23.90.1
!
clock timezone UTC
!
```

```
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. role admin
!
service sshd
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
cdp timer 60
cdp holdtime 180
cdp run GigabitEthernet 0
!
icmp echo on
!

ise/admin#
```

Related Commands

Command	Description
configure	Enters the Configuration mode.
show startup-config	Displays the contents of the startup configuration file or the configuration.

show startup-config

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

show startup-config

Syntax Description No arguments or keywords.

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

Command Modes EXEC

Usage Guidelines None.

Examples

```
ise/admin# show startup-config
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 171.70.168.183
!
ip default-gateway 172.23.90.1
!
clock timezone UTC
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. role admin
!
service sshd
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
cdp timer 60
cdp holdtime 180
cdp run GigabitEthernet 0
!
icmp echo on
!
ise/admin#
```

Related Commands

Command	Description
configure	Enters the Configuration mode.
show running-config	Displays the contents of the currently running configuration file or the configuration.

show tech-support

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

show tech-support file [*word*]

Syntax Description

show tech-support	The command to display the technical support information.
file	Save any technical support data as a file in the local disk.
word	Filename to save. Supports up to 80 alphanumeric characters.

Defaults

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

Command Modes

EXEC

Usage Guidelines

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

Examples

```
ise/admin# show tech-support
################################################
Application Deployment Engine(ADE) - 2.0.0.568
Technical Support Debug Info follows...
################################################


****************************************
Checking dmidecode Serial Number(s)
****************************************
  None
 VMware-56 4d 14 cb 54 3d 44 5d-49 ee c4 ad a5 6a 88 c4

****************************************
Displaying System Uptime...
****************************************
 12:54:34 up 18:37,  1 user,  load average: 0.14, 0.13, 0.12

****************************************
Display Memory Usage(KB)
****************************************
             total       used       free     shared    buffers     cached
Mem:       1035164    1006180      28984          0      10784     345464
-/+ buffers/cache:     649932     385232
Swap:      2040244     572700    1467544

****************************************
Displaying Processes(ax --forest)...
****************************************
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:02 init [3]
    2 ?        S<     0:00 [migration/0]
    3 ?        SN     0:00 [ksoftirqd/0]
    4 ?        S<     0:00 [watchdog/0]
    5 ?        S<     0:00 [events/0]
--More--
(press Spacebar to continue)

ise/admin#
```

Related Commands

Command	Description
show interface	Displays the usability status of the interfaces.
show process	Displays information about active processes.
show running-config	Displays the contents of the current running configuration.

show terminal

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

show terminal

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

None.

Examples

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

Table A-12 describes the fields of the **show terminal** output.

Table A-12 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: 24 lines	Length of the terminal display.
Width: 80 columns	Width of the terminal display, in character columns.
Session Timeout: 30 minutes	Length of time, in minutes, for a session, after which the connection closes.

show timezone

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

show timezone

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

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

Related Commands

Command	Description
clock timezone	Sets the time zone on the system.
show timezones	Displays the time zones available on the system.

show timezones

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

show timezones

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines

See the "clock timezone" section on page A-100, for examples of the time zones available for the ISE server.

Examples

```
ise/admin# show timezones
Africa/Blantyre
Africa/Dar_es_Salaam
Africa/Dakar
Africa/Asmara
Africa/Timbuktu
Africa/Maputo
Africa/Accra
Africa/Kigali
Africa/Tunis
Africa/Nouakchott
Africa/Ouagadougou
Africa/Windhoek
Africa/Douala
Africa/Johannesburg
Africa/Luanda
Africa/Lagos
Africa/Djibouti
Africa/Khartoum
Africa/Monrovia
Africa/Bujumbura
Africa/Porto-Novo
Africa/Malabo
Africa/Ceuta
Africa/Banjul
Africa/Cairo
Africa/Mogadishu
Africa/Brazzaville
Africa/Kampala
Africa/Sao_Tome
Africa/Algiers
Africa/Addis_Ababa
Africa/Ndjamena
Africa/Gaborone
Africa/Bamako
Africa/Freetown
--More--
(press Spacebar to continue)

ise/admin#
```

Related Commands

Command	Description
show timezone	Displays the time zone set on the system.
clock timezone	Sets the time zone on the system.

show udi

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

show udi

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

Example 1

```
ise/admin# show udi
SPID: ISE-3315-K9
VPID: V01
Serial: LAB12345678

ise/admin#
```

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

Example 2

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

ise/admin#
```

show uptime

To display the length of time that you have been logged in to the Cisco ISE server, use the **show uptime** command in the EXEC mode.

show uptime |

Syntax Description

show uptime	The command to display the period that you have been logged into the Cisco ISE server.
|	Output modifier variables: • *begin*—Matched pattern. Supports up to 80 alphanumeric characters. • *count*—Count the number of lines in the output. Add number after the word *count*. • *end*—End with line that matches. Supports up to 80 alphanumeric characters. • *exclude*—Exclude lines that match. Supports up to 80 alphanumeric characters. • *include*—Include lines that match. Supports up to 80 alphanumeric characters. • *last*—Display last few lines of output. Add number after the word *last*. Supports up to 80 lines to display. Default 10.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

```
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 the EXEC mode.

show users

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines None.

Examples

```
ise/admin# show users
USERNAME         ROLE   HOST                      TTY      LOGIN DATETIME

admin            Admin  10.77.137.60              pts/0    Fri Aug  6 09:45:47 2010

ise/admin#
```

show version

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

show version

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Usage Guidelines This command displays version information about the Cisco ADE-OS software running on the Cisco ISE server, and displays the Cisco ISE version.

Examples

```
ise/admin# show version
Cisco Application Deployment Engine OS Release: 2.0
ADE-OS Build Version: 2.0.0.568
ADE-OS System Architecture: i386

Copyright (c) 2005-2010 by Cisco Systems, Inc.
All rights reserved.
Hostname: pmbudev-vm3


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

Cisco Identity Services Engine
----------------------------------------------
Version      : 1.0.2.051
Build Date   : Mon Aug  2 00:34:25 2010
Install Date : Thu Aug  5 17:48:49 2010
ise/admin#
```

Configuration Commands

This section list each Configuration command and includes a brief description of its use, command syntax, usage guidelines, and sample output.

Configuration commands include **interface** and **repository**.

Note Some of the Configuration commands require you to enter the configuration submode to complete the command configuration.

To access the Configuration mode, you must use the **configure** command in the EXEC mode.

Table A-13 lists the Configuration commands that this section describes.

Table A-13 List of Configuration Commands

• backup-staging-url	• kron occurrence
• cdp holdtime	• kron policy-list
• cdp run	• logging
• cdp timer	• ntp
• clock timezone	• ntp authenticate
• do	• ntp authentication-key
• end	• ntp server
• exit	• ntp trusted-key
• hostname	• password-policy
• icmp echo	• repository
• interface	• service
• ipv6 address autoconfig	• shutdown
• ipv6 address dhcp	• snmp-server community
• ip address	• snmp-server contact
• ip default-gateway	• snmp-server host
• ip domain-name	• snmp-server location
• ip name-server	• username
• ip route	

backup-staging-url

To allow you to configure a Network File System (NFS) location that the backup and restore operations will use as a staging area to package and unpackage backup files, use the **backup-staging-url** command in Configuration mode.

backup-staging-url *word*

Syntax Description

backup-staging-url	The command to configure a Network File System (NFS) location as a staging area that the backup and restore operations use.
word	NFS URL for staging area. Supports up to 2048 alphanumeric characters. Use **nfs://***server***:***path*[1].

1. Server is the server name and path refers to /subdir/subsubdir. Remember that a colon (:) is required after the server.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

The URL is NFS only. The format of the command is **backup-staging-url nfs:**//*server:path*.

Warning **Ensure that you secure your NFS server in such a way that the directory can be accessed only by the IP address of the Cisco ISE server.**

Examples

```
ise/admin(config)# backup-staging-url nfs://loc-filer02a:/vol/local1/private1/jdoe
ise/admin(config)#
```

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

cdp holdtime *seconds*

Syntax Description

cdp	The command to configure the Cisco Discovery Protocol parameters.
holdtime	The Cisco Discovery Protocol hold time specified.
seconds	Specifies the hold time, in seconds. Value from 10 to 255 seconds.

Defaults

180 seconds

Command Modes Configuration

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.

Examples

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

Related Commands

Command	Description
cdp timer	Specifies how often the Cisco ISE server sends Cisco Discovery Protocol updates.
cdp run	Enables the Cisco Discovery Protocol.

cdp run

To enable the Cisco Discovery Protocol, use the **cdp run** command in Configuration mode. To disable the Cisco Discovery Protocol, use the **no** form of this command.

cdp run [*GigabitEthernet*]

Syntax Description

cdp	The command to configure the Cisco Discovery Protocol parameters.
run	The command to enable or disable the Cisco Discovery Protocol.
GigabitEthernet	Specifies the GigabitEthernet interface on which to enable the Cisco Discovery Protocol.

Defaults No default behavior or values.

Command Modes Configuration

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.

Examples

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

Related Commands

Command	Description
cdp holdtime	Specifies the length of time that the receiving device should hold a Cisco Discovery Protocol packet from the Cisco ISE server before discarding it.
cdp timer	Specifies how often the Cisco ISE server sends Cisco Discovery Protocol updates.

cdp timer

To specify how often the Cisco ISE server sends Cisco Discovery Protocol updates, use the **cdp timer** command in Configuration mode. To revert to the default setting, use the **no** form of this command.

cdp timer *seconds*

Syntax Description

cdp	The command to configure the Cisco Discovery Protocol parameters.
timer	The command that refreshes the time interval of the Cisco Discovery Protocol.
seconds	Specifies how often, in seconds, the Cisco ISE server sends Cisco Discovery Protocol updates. Value from 5 to 254 seconds.

Defaults

60 seconds

Command Modes

Configuration

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.

Examples

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

Related Commands

Command	Description
cdp holdtime	Specifies the amount of time that the receiving device should hold a Cisco Discovery Protocol packet from the Cisco ISE server before discarding it.
cdp run	Enables the Cisco Discovery Protocol.

clock timezone

To set the time zone, use the **clock timezone** command in Configuration mode. To disable this function, use the **no** form of this command.

clock timezone *timezone*

Syntax Description

clock	The command to configure time zone.
timezone	The command to configure system timezone.
timezone	Name of the time zone visible when in standard time. Supports up to 64 alphanumeric characters.

Defaults

UTC

Command Modes

Configuration

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 A-14, A-15, and A-16 for sample time zones to enter on your system).

Table A-14 Common Time Zones

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

Table A-14 Common Time Zones (continued)

Acronym or name	Time Zone Name
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

Table A-15 Australia Time Zones

Australia[1]			
ACT[2]	Adelaide	Brisbane	Broken_Hill
Canberra	Currie	Darwin	Hobart
Lord_Howe	Lindeman	LHI[3]	Melbourne
North	NSW[4]	Perth	Queensland
South	Sydney	Tasmania	Victoria
West	Yancowinna		

1. Enter the country and city together with a forward slash (/) between them; for example, Australia/Currie.
2. ACT = Australian Capital Territory
3. LHI = Lord Howe Island
4. NSW = New South Wales

Table A-16 Asia Time Zones

Asia[1]			
Aden[2]	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		

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

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

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

For more information on how changing time zone impacts different Cisco ISE nodes types of your deployment and the steps to recover from the impact, see the "Standalone or Primary ISE Node" section on page A-102 and "Secondary ISE Node" section on page A-102.

Standalone or Primary ISE Node

Changing the time zone after installation is not supported on a Standalone or Primary ISE node.

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

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

Secondary ISE Node

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

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

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

Examples

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

Related Commands

Command	Description
show timezones	Displays a list of available time zones on the system.
show timezone	Displays the current time zone set on the system.

do

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

do *arguments*

Syntax Description

do	The EXEC command to execute an EXEC-level command from Configuration mode or any configuration submode
arguments	The EXEC command to execute an EXEC-level command (see Table A-17).

Table A-17 Command Options for Do Command

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

Table A-17 Command Options for Do Command (continued)

Command	Description
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.
telnet	Establishes a Telnet connection to a remote system.
terminal length	Sets terminal line parameters.
terminal session-timeout	Sets the inactivity timeout for all terminal sessions.
terminal session-welcome	Sets the welcome message on the system for all terminal sessions.
terminal terminal-type	Specifies the type of terminal connected to the current line of the current session.
traceroute	Traces the route of a remote IP address.
undebug	Disables the output (display of errors or events) of the **debug** command for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.
write	Erases the startup configuration that forces to run the setup utility and prompt the network configuration, copies the running configuration to the startup configuration, displays the running configuration on the console.

Command Default

No default behavior or values.

Command Modes

Configuration or any configuration submode

Usage Guidelines

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

Examples

```
ise/admin(config)# do show run
Generating configuration...
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 171.70.168.183
!
ip default-gateway 172.23.90.1
```

```
!
clock timezone EST
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. role admin
!
service sshd
!
backup-staging-url nfs://loc-filer02a:/vol/local1/private1/jdoe
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
--More--

ise/admin(config)#
```

end

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

end

Syntax Description

No arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Configuration

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.

Examples

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

Related Commands

Command	Description
exit	Exits Configuration mode.
exit (EXEC)	Closes the active terminal session by logging out of the Cisco ISE server.

exit

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

exit

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes Configuration

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 the 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 the EXEC mode and disconnects from the Cisco ISE server (see the "exit" section on page A-29, for a description of the **exit** (EXEC) command).

Examples

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

Related Commands

Command	Description
end	Exits Configuration mode.
exit (EXEC)	Closes the active terminal session by logging out of the Cisco ISE server.

hostname

To set the hostname of the system, use the **hostname** command in Configuration mode. To delete the hostname from the system, use the **no** form of this command, which resets the system to localhost.

hostname *word*

Syntax Description

hostname	The command to configure the hostname.
word	Name of the host. Contains at least 2 to 64 alphanumeric characters and an underscore (_). The hostname must begin with a character that is not a space.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

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.

Examples

```
ise/admin(config)# hostname ise-1
Changing the hostname or IP may result in undesired side effects,
such as installed application(s) being restarted.
Are you sure you want to proceed? [y/n] y
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Alert Process...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.

ise-1/admin(config)#

ise-1/admin# show application status ise

ISE Database listener is running, PID: 11142
ISE Database is running, number of processes: 29
ISE Application Server is still initializing.
ISE M&T Session Database is running, PID: 11410
ISE M&T Log Collector is running, PID: 11532
ISE M&T Log Processor is running, PID: 11555
ISE M&T Alert Process is running, PID: 11623

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

icmp	The command to configure Internet Control Message Protocol echo requests.
echo	Configures ICMP echo response.
off	Disables ICMP echo response
on	Enables ICMP echo response.

Defaults

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

Command Modes

Configuration

Usage Guidelines

None.

Examples

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

Related Commands

Command	Description
show icmp-status	Display ICMP echo response configuration information.

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

interface	The command to configure an interface.
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).

do	EXEC command. Allows you to perform any EXEC commands in this mode (see the "do" section on page A-103).
end	Exits the config-GigabitEthernet submode and returns you to the EXEC mode.
exit	Exits the config-GigabitEthernet configuration submode.
ip	Sets the IP address and netmask for the Ethernet interface (see the "ip address" section on page A-113).
ipv6	Configures IPv6 autoconfiguration address and IPv6 address from DHCPv6 server. (see the "ipv6 address autoconfig" section on page A-109 and the "ipv6 address dhcp" section on page A-111)
no	Negates the command in this mode. Two keywords are available: • ip—Sets the IP address and netmask for the interface. • shutdown—Shuts down the interface.
shutdown	Shuts down the interface (see the "shutdown" section on page A-132).

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

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

Examples

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

Related Commands

Command	Description
show interface	Displays information about the system interfaces.
ip address (interface configuration mode)	Sets the IP address and netmask for the interface.
shutdown (interface configuration mode)	Shuts down the interface (see "shutdown" section on page A-132).

ipv6 address autoconfig

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

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

interface GigabitEthernet *0*

Syntax Description

interface	The command to configure an interface.
GigabitEthernet	Configures the Gigabit Ethernet interface.
<0 - 3>	Number of the Gigabit Ethernet port to configure.

Defaults

No default behavior or values.

Command Modes

Configuration

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 using the **show** command.

Example 1

```
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 example 2, 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.

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#
```

The following RFC provides the IPv6 stateless autoconfiguration privacy extensions:

http://www.ietf.org/rfc/rfc3041.txt

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 3 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:

Example 3

```
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#
```

Related Commands

Command	Description
show interface	Displays information about the system interfaces.
ip address (interface configuration mode)	Sets the IP address and netmask for the interface.
shutdown (interface configuration mode)	Shuts down the interface (see "shutdown" section on page A-132).
ipv6 address dhcp	Enables IPv6 address DHCP on an interface.
show running-config	Displays the contents of the currently running configuration file or the configuration.

ipv6 address dhcp

To enable IPv6 address DHCP, use the **interface GigabitEthernet 0** command in Configuration mode. This command does not have a **no** form.

interface GigabitEthernet *0*

Syntax Description

interface	The command to configure an interface.
GigabitEthernet	Configures the Gigabit Ethernet interface.
0	Gigabit Ethernet port number to be configured.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

None.

Examples

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

When IPv6 DHCPv6 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 dhcp
!
```

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** 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 0
  ip address 172.23.90.116 255.255.255.0
  ipv6 address dhcp
!
```

Related Commands

Command	Description
show interface	Displays information about the system interfaces.
ip address (interface configuration mode)	Sets the IP address and netmask for the interface.
shutdown (interface configuration mode)	Shuts down the interface (see "shutdown" section on page A-132).
ipv6 address autoconfig	Enables IPv6 stateless autoconfiguration on an interface.
show running-config	Displays the contents of the currently running configuration file or the configuration.

ip address

To set the IP address and netmask for the Ethernet interface, use the **ip address** command in interface Configuration mode. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address *ip-address network mask*

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

Syntax Description

ip address	The command to configure IP address and netmask for the GigabitEthernet interface.
ip-address	IPv4 version IP address.
network mask	Mask of the associated IP subnet.

Defaults

Enabled.

Command Modes

Interface configuration

Usage Guidelines

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

Examples

```
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ip address 209.165.200.227 255.255.255.224
Changing the hostname or IP may result in undesired side effects,
such as installed application(s) being restarted.
........
To verify that ISE processes are running, use the
'show application status ise' command.
ise/admin(config-GigabitEthernet)#
```

Related Commands

Command	Description
shutdown (interface configuration mode)	Disables an interface (see "shutdown" section on page A-132).
ip default-gateway	Sets the IP address of the default gateway of an interface.
show interface	Displays information about the system IP interfaces.
interface	Configures an interface type and enters the interface mode.

ip default-gateway

To define or set a default gateway with an IP address, use the **ip default-gateway** command in Configuration mode. To disable this function, use the **no** form of this command.

ip default-gateway *ip-address*

Syntax Description

ip default-gateway	The command to define a default gateway with an IP address.
ip-address	IP address of the default gateway.

Defaults

Disabled.

Command Modes

Configuration

Usage Guidelines

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

Examples

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

Related Commands

Command	Description
ip address (interface configuration mode)	Sets the IP address and netmask for the Ethernet interface.

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

ip domain-name *word*

Syntax Description

ip domain-name	The command to define a default domain name.
word	Default domain name used to complete the hostnames. Contains at least 2 to 64 alphanumeric characters.

Defaults

Enabled.

Command Modes Configuration

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

Examples

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

Related Commands

Command	Description
ip name-server	Sets the DNS servers for use during a DNS query.

ip name-server

To set the Domain Name Server (DNS) servers for use during a DNS query, use the **ip name-server** command in Configuration mode. You can configure one to three DNS servers. To disable this function, use the **no** form of this command.

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

ip name-server *ip-address* [*ip-address**]

Syntax Description

ip name-server	The command to configure IP addresses of name server(s) to use.
ip-address	Address of a name server.
*ip-address**	(Optional) IP addresses of additional name servers. **Note** You can configure a maximum of three name servers.

Defaults No default behavior or values.

Command Modes Configuration

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 one at a time or all at once, until you reach the maximum (3). If you already configured the system with three 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.

Examples

```
ise/admin(config)# ip name-server 209.165.201.1


To verify that ISE processes are running, use the
'show application status ise' command.
ise/admin(config)#
```

You can choose not to restart the Cisco ISE server; nevertheless, the changes will take effect.

Related Commands

Command	Description
ip domain-name	Defines a default domain name that the server uses to complete hostnames.

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.

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.

ip route *prefix mask* **gateway** *ip-address*

no ip route *prefix mask*

Syntax Description

ip route	The command to configure IP routes.
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.

Defaults

No default behavior or values.

Command Modes

Configuration

Examples

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

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

kron	The command to schedule the Command Scheduler commands.
occurrence	Schedules Command Scheduler commands.
occurrence-name	Name of the occurrence. Supports up to 80 alphanumeric characters. (See the following note and Syntax Description.)

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

at	Identifies that the occurrence is to run at a specified calendar date and time. Usage: at [*hh:mm*] [*day-of-week* | *day-of-month* | *month day-of-month*].
do	EXEC command. Allows you to perform any EXEC commands in this mode (see the "do" section on page A-103).
end	Exits the kron-occurrence configuration submode and returns you to the EXEC mode.
exit	Exits the kron-occurrence configuration mode.
no	Negates the command in this mode. Three keywords are available: • at—Usage: at [*hh:mm*] [*day-of-week* | *day-of-month* | *month day-of-month*]. • policy-list—Specifies a policy list to be run by the occurrence. Supports up to 80 alphanumeric characters. • recurring—Execution of the policy lists should be repeated.
policy-list	Specifies a Command Scheduler policy list to be run by the occurrence.
recurring	Identifies that the occurrences run on a recurring basis. **Note** If kron occurrence is not recurring, then the kron occurrence configuration for the scheduled backup is removed after it has run.

Defaults

No default behavior or values.

Command Modes

Configuration

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 on the Cisco ISE server at a specified time. See the "kron policy-list" section on page A-118.

Examples

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.

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)#
```

Related Commands

Command	Description
kron policy-list	Specifies a name for a Command Scheduler policy.

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

kron	The command to schedule the Command Scheduler commands.
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).

cli	Command to be executed by the scheduler. Supports up to 80 alphanumeric characters.
do	EXEC command. Allows you to perform any EXEC commands in this mode (see "do" section on page A-103).
end	Exits from the config-Policy List configuration submode and returns you to the EXEC mode.
exit	Exits this submode.
no	Negates the command in this mode. One keyword is available: • cli—Command to be executed by the scheduler.

Defaults No default behavior or values.

Command Modes Configuration

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. See the "ip route" section on page A-116.

Examples

```
ise/admin(config)# kron policy-list SchedBackupMonday
ise/admin(config-Policy List)# cli backup SchedBackupMonday repository SchedBackupRepo
ise/admin(config-Policy List)# exit
ise/admin(config)#
```

Related Commands

Command	Description
ip route	Specifies schedule parameters for a Command Scheduler occurrence and enters the config-Occurrence configuration mode.

logging

To enable the system to forward logs to a remote system or to configure the log level, use the **logging** command in Configuration mode. To disable this function, use the **no** form of this command.

logging {*ip-address* | *hostname*} {**loglevel** *level*}

Syntax Description

logging	The command to configure system logging.
ip-address	IP address of remote system to which you forward logs. Supports up to 32 alphanumeric characters.
hostname	Hostname of remote system to which you forward logs. Supports up to 32 alphanumeric characters.
loglevel	The command to configure the log level for the **logging** command.
level	Number of the desired priority level at which you set the log messages. Priority levels are (enter the number for the keyword): • 0-emerg—Emergencies: System unusable. • 1-alert—Alerts: Immediate action needed. • 2-crit—Critical: Critical conditions. • 3-err—Error: Error conditions. • 4-warn—Warning: Warning conditions. • 5-notif—Notifications: Normal but significant conditions. • 6-inform—(Default) Informational messages. • 7-debug—Debugging messages.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

This command requires an IP address or hostname or the **loglevel** keyword; an error occurs if you enter two or more of these arguments.

Examples

Example 1

```
ise/admin(config)# logging 209.165.200.225
ise/admin(config)#
```

Example 2

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

Related Commands

Command	Description
show logging	Displays list of logs for the system.

ntp

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

ntp authenticate

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

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

ntp trusted-key <*key*>

Syntax Description

ntp	The command to specify an NTP configuration.

Defaults

None

Command Modes

Configuration.

Usage Guidelines

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

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

For more information on how to configure an NTP server, see ntp server, page A-124.

Examples

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

Related Commands

Command	Description
ntp authenticate	Enables authentication of all time sources.
ntp authentication-key	Configures authentication keys for trusted time sources.
ntp server	Allows synchronization of the software clock by the NTP server for the system.

Command	Description
ntp trusted-key	Specifies key numbers for trusted time sources that needs to be defined as NTP authentication keys.
show ntp	Displays the status information about the NTP associations.

ntp authenticate

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

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

ntp authenticate

Syntax Description

ntp	The command to specify NTP configuration.
authenticate	Enables authentication of all time sources.

Defaults

None

Command Modes

Configuration.

Usage Guidelines

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

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

Examples

```
ise/admin(config)# ntp ?
  authenticate        Authenticate time sources
  authentication-key  Authentication key for trusted time sources
  server              Specify NTP server to use
  trusted-key         Key numbers for trusted time sources
ise/admin(config)#

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

Related Commands

Command	Description
ntp	The command to specify NTP configuration.
ntp authentication-key	Configures authentication keys for trusted time sources.
ntp server	Allows synchronization of the software clock by the NTP server for the system.

Command	Description
ntp trusted-key	Specifies key numbers for trusted time sources that needs to be defined as NTP authentication keys.
show ntp	Displays the status information about the NTP associations.

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.

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

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

Syntax Description

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

Defaults

None

Command Modes

Configuration.

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.

Examples

```
ise/admin# configure
ise/admin(config)#
ise/admin(config)# ntp authentication-key 1 md5 plain SharedWithServe
ise/admin(config)# ntp authentication-key 2 md5 plain SharedWithServ
ise/admin(config)# ntp authentication-key 3 md5 plain SharedWithSer
```

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.

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

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

Related Commands

Command	Description
ntp	The command to specify NTP configuration.
ntp authenticate	Enables authentication of all time sources.
ntp server	Allows synchronization of the software clock by the NTP server for the system.
ntp trusted-key	Specifies key numbers for trusted time sources that needs to be defined as NTP authentication keys.
show ntp	Displays the status information about the NTP associations.

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*} *key* <*peer key number*>

Syntax Description

ntp	The command to specify NTP configuration.
server	Allows the system to synchronize with a specified server.
ip-address | *hostname*	IP address or hostname of the server providing the clock synchronization. Arguments are limited to 255 alphanumeric characters.
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, and also needs to be added as a trusted-key by using the **ntp trusted-key** command. For authentication to work, the key and the key value should be the same as that which is defined on the actual NTP server.

Defaults

No servers are configured by default.

Command Modes

Configuration.

Usage Guidelines

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

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

The **show ntp** command displays the status of synchronization. If none of the configured NTP servers are reachable or not authenticated (if NTP authentication is configured), then this command displays synchronization to local with the least stratum. If an NTP server is not reachable or is not properly authenticated, then its reach as per this command statistics will be 0.

To define an NTP server configuration and authentication in the Cisco ISE admin user interface, see the System Time and NTP Server Settings section in the *Cisco Identity Services Engine User Guide, Release 1.1.1.*

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

Examples

Example 1

```
ise/admin(config)# ntp server ntp.esl.cisco.com key 1
% WARNING: Key 1 needs to be defined as a ntp trusted-key.
ise/admin(config)#
ise/admin(config)# ntp trusted-key 1
% WARNING: Key 1 needs to be defined as a ntp authentication-key.
ise/admin(config)#
ise/admin(config)# ntp authentication-key 1 md5 plain SharedWithServe
ise/admin(config)#

ise/admin(config)# ntp server ntp.esl.cisco.com 1
ise/admin(config)# ntp server 171.68.10.80 2
ise/admin(config)# ntp server 171.68.10.150 3
ise/admin(config)#
ise/admin(config)# do show running-config
Generating configuration...
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.21.79.246 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 171.70.168.183
!
ip default-gateway 172.21.79.1
!
clock timezone UTC
!
ntp authentication-key 1 md5 hash ee18afc7608ac7ecdbeefc5351ad118bc9ce1ef3
ntp authentication-key 2 md5 hash f1ef7b05c0d1cd4c18c8b70e8c76f37f33c33b59
ntp authentication-key 3 md5 hash ee18afc7608ac7ec2d7ac6d09226111dce07da37
ntp trusted-key 1
```

```
ntp trusted-key 2
ntp trusted-key 3
ntp authenticate
ntp server ntp.esl.cisco.com key 1
ntp server 171.68.10.80 key 2
ntp server 171.68.10.150 key 3
!
--More--
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#
```

Related Commands

Command	Description
ntp	The command to specify NTP configuration.
ntp authenticate	Enables authentication of all time sources.
ntp authentication-key	Configures authentication keys for trusted time sources.
ntp trusted-key	Specifies key numbers for trusted time sources that needs to be defined as NTP authentication keys.
show ntp	Displays the status information about the NTP associations.

ntp trusted-key

To add a time source to the trusted list, use the **ntp trusted-key** command with a unique identifier. To disable this capability, use the **no** form of this command.

ntp trusted-key <*key*>

Syntax Description

ntp	The command to specify NTP configuration.
trusted-key	The identifier that you want to assign to this key.
key	Specifies key numbers for trusted time sources that needs to be defined as NTP authentication keys. Supports up to 65535 numeric characters.

Defaults

None

Command Modes

Configuration.

Usage Guidelines

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

Examples

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

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

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

Related Commands

Command	Description
ntp	The command to specify NTP configuration.
ntp authenticate	Enables authentication of all time sources.
ntp authentication-key	Configures authentication keys for trusted time sources.
ntp server	Allows synchronization of the software clock by the NTP server for the system.
show ntp	Displays the status information about the NTP associations.

password-policy

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

password-policy *option*

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.

Syntax Description

password-policy	The command to configure the password policy.

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

digit-required	Requires a digit in user passwords.
disable-cisco-password	Disables the ability to use the word Cisco or any combination as the password.
disable-repeat-chars	Disables the ability of the password to contain more than four identical characters.
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 upto 40 characters.
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-expiration-days	Number of days until a password expires. Supports an integer upto 3600.
password-expiration-enabled	Enables password expiration. **Note** You must enter the **password-expiration-enabled** command before the other password-expiration commands.
password-expiration-warning	Number of days before expiration that warnings of impending expiration begin. Supports an integer upto 3600.
password-lock-enabled	Locks a password after several failures.
password-lock-retry-count	Number of failed attempts before user password locks. Supports an integer upto 20.
special-required	Requires a special character in user passwords.
upper-case-required	Requires an uppercase letter in user passwords.

Defaults No default behavior or values.

Command Modes Configuration

Usage Guidelines None.

Examples

```
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	The command to configure the repository.
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).

do	EXEC command. Allows you to perform any of the EXEC commands in this mode (see the "do" section on page A-103).
end	Exits the config-Repository submode and returns you to the 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 80 alphanumeric characters (see Table A-18).
user	Configure the username and password for access. Supports up to 30 alphanumeric characters.

Table A-18 URL Keywords

Keyword	Source of Destination
word	Enter the repository URL, including server and path information. Supports up to 80 alphanumeric characters.
cdrom:	Local CD-ROM drive (read only).
disk:	Local storage. You can run the **show repository** *repository_name* to view all the files in the local repository. **Note** All local repositories are created on the /localdisk partition. When you specify disk:// in the repository URL, the system creates directories in a path that is relative to /localdisk. For example, if you entered **disk://backup,** the directory is created at /localdisk/backup.
ftp:	Source or destination URL for an FTP network server. Use url ftp://*server*/*path*[1].
nfs:	Source or destination URL for an NFS network server. Use url nfs://*server*:*path*[1].
sftp:	Source or destination URL for an SFTP network server. Use url sftp://*server*/*path*[1].
tftp:	Source or destination URL for a TFTP network server. Use url tftp://*server*/*path*[1]. **Note** You cannot use a TFTP repository for performing a Cisco ISE upgrade.

1. 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.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

When configuring **url sftp:** in the submode, you must provide the host-key under repository configuration through CLI and the RSA fingerprint is added to the list of SSH known hosts.

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

Cisco ISE displays the following warning when you configure a secure ftp repository in the administration user interface 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.

Example 1

```
ise/admin# configure termainal
ise/admin(config)# repository myrepository
ise/admin(config-Repository)# url sftp://ise-pap
ise/admin(config-Repository)# host-key host ise-pap
host key fingerprint added
```

```
# Host ise-pap found: line 1 type RSA
2048 f2:e0:95:d7:58:f2:02:ba:d0:b8:cf:d5:42:76:1f:c6 ise-pap (RSA)

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

Example 2

```
ise/admin# configure termainal
ise/admin(config)# repository myrepository
ise/admin(config-Repository)# url sftp://ise-pap
ise/admin(config-Repository)# no host-key host ise-pap
ise/admin(config-Repository)# exit
ise/admin(config)# exit
ise/admin#
```

Related Commands

Command	Description
backup	Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.
restore	Performs a restore and takes the backup out of a repository.
show backup history	Displays the backup history of the system.
show repository	Displays the available backup files located on a specific repository.

service

To specify a service to manage, use the **service** command in Configuration mode. To disable this function, use the **no** form of this command.

service *sshd*

Syntax Description

service	The command to specify a service to be managed.
sshd	Secure Shell Daemon. The daemon program for SSH.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

None.

Examples

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

shutdown

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

Syntax Description No arguments or keywords.

Defaults No default behavior or values.

Command Modes Interface Configuration

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.

Examples

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

Related Commands

Command	Description
interface	Configures an interface type and enters the interface mode.
ip address (interface configuration mode)	Sets the IP address and netmask for the Ethernet interface.
show interface	Displays information about the system IP interfaces.
ip default-gateway	Sets the IP address of the default gateway of an interface.

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

snmp-server community *word* **ro**

Syntax Description

snmp-server community	The command to configure the SNMP server.
word	Accessing string that functions much like a password and allows access to SNMP. No blank spaces allowed. Supports up to 255 alphanumeric characters.
ro	Specifies read-only access.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

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

The SNMP Agent on the Cisco ISE provides read-only SNMP v1 and SNMP v2c access to the following MIBs:

- SNMPv2-MIB
- RFC1213-MIB
- IF-MIB
- IP-MIB
- IP-FORWARD-MIB
- TCP-MIB
- UDP-MIB
- HOST-RESOURCES-MIB
- ENTITY-MIB—Only 3 MIB variables are supported on the ENTITY-MIB:
  - Product ID: entPhysicalModelName
  - Version ID: entPhysicalHardwareRev
  - Serial Number: entPhysicalSerialNumber
- DISMAN-EVENT-MIB
- NOTIFICATION-LOG-MIB
- CISCO-CDP-MIB

Examples

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

Related Commands

Command	Description
snmp-server host	Sends traps to a remote system.
snmp-server location	Configures the SNMP location MIB value on the system.
snmp-server contact	Configures the SNMP contact MIB value on the system.

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 *word*

Syntax Description

snmp-server contact	The command to identify the contact person for this managed node. Supports up to 255 alphanumeric characters.
word	String that describes the system contact information of the node. Supports up to 255 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

None.

Examples

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

Related Commands

Command	Description
snmp-server host	Sends traps to a remote system.
snmp-server community	Sets up the community access string to permit access to the SNMP.
snmp-server location	Configures the SNMP location MIB value on the system.

snmp-server host

To send SNMP traps to a remote user, use the **snmp-server host** command in Configuration mode. To remove trap forwarding, use the **no** form of this command.

snmp-server host {*ip-address* | *hostname*} **version** {*1* | *2c*} *community*

Syntax Description

snmp-server host	The command to configure hosts to receive SNMP notifications.
ip-address	IP address of the SNMP notification host. Supports up to 32 alphanumeric characters.
hostname	Name of the SNMP notification host. Supports up to 32 alphanumeric characters.

version {1 | 2c}	(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.
community	Password-like community string that is sent with the notification operation.

Defaults

Disabled.

Command Modes

Configuration

Usage Guidelines

The command takes arguments as listed; otherwise, an error occurs. SNMP traps are not supported.

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)#
```

Related Commands

Command	Description
snmp-server community	Sets up the community access string to permit access to SNMP.
snmp-server location	Configures the SNMP location MIB value on the system.
snmp-server contact	Configures the SNMP contact MIB value on the system.

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 *word*

Syntax Description

snmp-server location	The command to configure the physical location of this managed node. Supports up to 255 alphanumeric characters.
word	String that describes the physical location information of the system. Supports up to 255 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

Configuration

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 (“).

Examples

Example 1

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

Example 2

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

Related Commands

Command	Description
snmp-server host	Sends traps to a remote system.
snmp-server community	Sets up the community access string to permit access to SNMP.
snmp-server contact	Configures the SNMP location MIB value on the system.

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**] [**disabled** [**email** *email-address*]] [**email** *email-address*]

For an existing user, use the following command option:

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

Syntax Description

username	The command to create a user to access the Cisco ISE appliance using SSH.
username	Only one word for the username argument. Blank spaces and quotation marks (“) are not allowed. Supports up to 31 alphanumeric characters.
password	The command to use specify password and user role.
password	Password character length up to 40 alphanumeric characters. You must specify the password for all new users.
hash | plain	Type of password. Supports up to 34 alphanumeric characters.
role admin | user	Sets the privilege level for the user.
disabled	Disables the user according to the user’s email address.
email *email-address*	The user’s email address. For example, *user1@mydomain.com*.

Defaults

The initial user during setup.

Command Modes

Configuration

Usage Guidelines

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

Examples

Example 1

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

Example 2

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

Example 3

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

Related Commands

Command	Description
password-policy	Enables and configures the password policy.
show users	Displays a list of users and their privilege level. It also displays a list of logged-in users.

GLOSSARY

A

ADE Application Deployment Engine.

C

CDP Cisco Discovery Protocol. A proprietary tool that network administrators use to access a summary of protocol and address information about other devices that are directly connected to the device initiating the command.

Cisco Discovery Protocol runs over the data-link layer that connects the physical media to the upper-layer protocols. Because Cisco Discovery Protocol operates at this level, two or more Cisco Discovery Protocol devices that support different network layer protocols (for example, IP and Novell IPX) can learn about each other.

Physical media that supports the Subnetwork Access Protocol (SNAP) encapsulation connect Cisco Discovery Protocol devices. These can include all LANs, Frame Relay, and other WANs, and ATM networks.

Cisco Discovery Protocol *See* CDP.

CLI command-line interface. An interface through which the user can interact with the software operating system by entering commands and optional arguments.

client Node or software program that requests services from a server. For example, the Secure Shell (SSH) client. *See also* server.

command-line interface *See* CLI.

community string A text string that acts as a password, which is used to authenticate messages sent between a management station and an IP Transfer Point (ITP) that contains an SNMP agent. The community string sends in every packet between the manager and the agent.

D

DNS Domain Name System. DNS associates various sorts of information with so-called domain names; most importantly, it serves as the "phone book" for the Internet: it translates human-readable computer hostnames (for example, *en.wikipedia.org*) into the IP addresses that networking equipment needs for delivering information. It also stores other information, such as the list of mail exchange servers that accept email for a given domain. By providing a worldwide keyword-based redirection service, the DNS is an essential component of contemporary Internet use.

DNS name Initial name of a node.

domain name The style of identifier—a sequence of case-insensitive ASCII labels separated by dots (.) (for example, *bbn.com.*)—defined for subtrees in the Internet DNS [R1034] and used in other Internet identifiers, such as hostnames, mailbox names, and URLs.

Domain Name System *See* DNS.

F

FTP File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.

H

host Computer system on a network. Similar to the term node; except that host usually implies a computer system, whereas node generally applies to any network system, including access servers and ITPs.

hostname The name of the operating system's server or computer that contains the major program files.

I

IP Internet Protocol. Network layer protocol in the TCP/IP stack that offers a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Documented in RFC 791.

IP address A 32-bit address assigned to hosts by using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and written as 4 octets separated by periods (.) (dotted-decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. For routing, the network and subnetwork numbers stay together, while the host number addresses an individual host within the network or subnetwork. A subnet mask extracts network and subnetwork information from the IP address.

M

MIB Management Information Base. A directory listing information that is used and maintained by the network's management protocol of a network, such as SNMP.

N

name server A name server is a computer server that implements a name-service protocol. It normally maps a computer-usable identifier of a host to a human-usable identifier for that host. For example, a DNS server might translate the domain name *en.wikipedia.org* to the IP address 145.97.39.155.

Network Time Protocol *See* NTP.

NTP Network Time Protocol. A protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses User Datagram Protocol (UDP) port 123 as its transport layer. NTP is designed particularly to resist the effects of variable latency (jitter).

NTP is one of the oldest Internet protocols still in use (since before 1985). NTP was originally designed by Dave Mills of the University of Delaware, who still maintains it, along with a team of volunteers.

NTP is not related to the much simpler DAYTIME (RFC 867) and TIME (RFC 868) protocols.

P

port In IP terminology, an upper-layer process that receives information from lower layers. Each numbered port associates with a specific process. For example, SMTP associates with port 25.

S

Secure Shell *See* SSH.

server An application or device that performs services for connected clients as part of a client-server architecture. A server application, as defined by RFC 2616 (HTTP/1.1), is "an application program that accepts connections in order to service requests by sending back responses." Server computers are devices designed to run such an application or applications, often for extended periods of time, with minimal human direction. Examples of servers include web servers, email servers, and file servers.

See also client.

Simple Network Management Protocol *See* SNMP.

SSH Secure Shell. A network protocol in which data is exchanged over a secure channel between two computers. Encryption provides confidentiality and integrity of data. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user.

SSH is typically used to log in to a remote machine and execute commands; but, it also supports tunneling, forwarding arbitrary TCP ports, and X Window System (X11) connections. It can transfer files by using the associated SSH File Transfer Protocol (SFTP).

An SSH server, by default, listens on the standard TCP port 22. An SSH client program is typically used for establishing connections to an sshd daemon accepting remote connections. Both are commonly present on most modern operating systems. Proprietary, freeware, and open-source versions of various levels of complexity and completeness exist.

SNMP Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMPv1 SNMPv1 is a simple request/response protocol. In the SNMPv1 framework, the network-management system issues a request, and managed devices return responses.

SNMPv2C The second release of SNMP, described in RFC 1902. It provides additions to data types, counter size, and protocol operations. SNMPv2C support includes a bulk-retrieval mechanism and more detailed error message reporting to management stations. The bulk-retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trip transmissions required. SNMPv2C improved error-handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type. Three kinds of exceptions are also reported: No such object, No such instance, and End of MIB view.

SNMPv3 SNMPv3 is an interoperable standards-based protocol for network management, which provides secure access to devices by a combination of authenticating and encrypting packets over the network. It has primarily added security and remote configuration enhancements to SNMP. SNMPv3 provides important security features such as message integrity that ensures packets are not tampered with in-transit, authentication that verifies messages are from a valid source, and encryption of packets that prevents snooping by an unauthorized source.

T

TCP Transmission Control Protocol. Connection-oriented transport-layer protocol that provides reliable full-duplex data transmission. Part of the TCP/IP protocol stack.

Telnet

Telnet (TELetype NETwork). A network protocol used on the Internet or LAN connections. It was developed in 1969 beginning with RFC 0015 and standardized as IETF STD 8, one of the first Internet standards.

The term Telnet also refers to software that implements the client part of the protocol. Telnet clients have been available on most UNIX systems for many years and are available for virtually all platforms. Most network equipment and operating systems with a TCP/IP stack support some kind of Telnet service server for their remote configuration (including those based on Windows NT). Recently, Secure Shell has begun to dominate remote access for UNIX-based machines.

Most often, a user establishes a telnet connection to a UNIX-like server system or a simple network device such as a switch. For example, you might "telnet in from home to check your email at work." In doing so, you would be using a Telnet client to connect from your computer to one of your servers. When the connection is established, you would then log in with your account information and execute the operating system commands remotely on that computer, such as **ls** or **cd**.

TFTP

Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network.

Transmission Control Protocol

See TCP.

Trivial File Transfer Protocol

See TFTP.

U

UDI

Unique Device Identifier. Each identifiable product is an entity, as defined by the Entity MIB (RFC 2737) and its supporting documents. Some entities, such as a chassis, will have subentities like slots. An Ethernet switch might be a member of a super entity like a stack. Most Cisco entities that are orderable products leave the factory with an assigned UDI. The UDI information is printed on a label that is affixed to the physical hardware device, and it is also stored electronically on the device in order to facilitate remote retrieval.

A UDI consists of the following elements: product identifier (PID), version identifier (VID), and serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the "Product Name" or "Part Number." You use this identifier to order an exact replacement part.

The VID is the version of the product. Whenever a product is revised, the VID is incremented, according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product carries a unique serial number assigned at the factory, which cannot be changed in the field. This number identifies an individual, specific instance of a product.

Unique Device Identifier

See UDI.

INDEX

A

C

D

E

H

M

N

O

R

S

T

U