# Cisco ISE CLI Commands in EXEC Mode

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

# Cisco ISE CLI Session Begins in EXEC Mode

When you start a session in the Cisco ISE CLI, you begin in EXEC mode. In EXEC mode, you have permissions to access everything in the Cisco ISE server and perform system-level configuration and generate operational logs.

# application install

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

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

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

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

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

**Command Modes** EXEC

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

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

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

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

**Example**

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

# application configure ise

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

- perform M&T operations

- refresh and display statistics related to the profiler

- export and import options to backup and restore Cisco ISE CA certificates and keys

- generate Key Performance Metrics (KPM) statistics

- enable or disable the ISE counter attribute data collection

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

| Syntax Description | configure | Configures a specific application. |
|---|---|---|
| | *application-name* | Application name. Supports up to 255 alphanumeric characters. |

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

**Command Modes**  EXEC

| Command History | Release | Modification |
|---|---|---|
| | 2.0.0.306 | This command was introduced. |
| | 3.0 | Wireless setup support was removed. |

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

**Example**

```
ise/admin# application configure ise

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

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

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

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

# Monitoring Database Settings

### Before You begin

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

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

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

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

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

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

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

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

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

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

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

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

**Example**

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

```
ise/admin# application configure ise

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



1
You are about to reset the M&T session database. Following this operation, an application
restart will be required.
Are you sure you want to proceed? y/n [n]: y
TimesTen Daemon stopped.
TimesTen Daemon startup OK.
Restarting application
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE Identity Mapping Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
```

```
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.

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

3
Enter number of days to be retained in purging MnT Operational data [between 1 to 90 days]
For instance, Entering 20 will purge MnT Operational data older than 20 days
Enter 'exit' to return to the main menu without purging
Enter days to be retained: 20
You are about to purge M&T data older than 20 from your database.
Are you sure you want to proceed? y/n [n]: y
M&T Operational data older than 20 is getting removed from database
4
You are about to reset the M&T database. Following this operation, application will be
restarted.
Are you sure you want to proceed? y/n [n]: y
Stopping application
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE Identity Mapping Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting Database only
Creating ISE M&T database tables...
Restarting application
ISE M&T Log Processor is not running
ISE Identity Mapping Service is disabled
ISE pxGrid processes are disabled
ISE Application Server process is not running
ISE Certificate Authority Service is not running
ISE Profiler Database is not running
ISE M&T Session Database is not running
ISE AD Connector is not running
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.

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

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

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

# Live Statistics of Profiling Events

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

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

### Example

```
ise/admin# application configure ise

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


6


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

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

# Export and Import Internal CA Store

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

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

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

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

### Example 1

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

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


7
Export Repository Name: sftp
Enter encryption-key for export: Test1234
Export on progress...............

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

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

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

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

ISE CA keys export completed successfully
```

**Example 2**

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

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


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


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

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

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

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

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

# Create Missing Indexes

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

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

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

### Example 1

To create the CEPM database index, use option 9.

```
ise/admin# application configure ise

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



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

### Example 2

To create missing Monitoring database indexes, use option 10.

```
ise/admin# application configure ise

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

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




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

# Key Performance Metrics Statistical Data

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

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

### Example

```
ise/admin# application configure ise

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

```
                                   .
                                [xx]Exit



                                12


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

# Counter Attribute Collection

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

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

### Example

To disable counter attribute collection, use option 14.

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

14
```

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

# Localized ISE Installation

While reinstalling Cisco ISE, you can use the **Localized ISE Install** option (option 38) in the **application configure ise** command to reduce the installation time. Though this option can be used for both Cisco Secure Network Server and virtual appliances, it significantly reduces the reinstallation time for Cisco Secure Network Servers.

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

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

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

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

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

    The following options are displayed:

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

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

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

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

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

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

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

   ```
   Error in mounting ISO
   ```

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

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

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

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

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

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

   Proceed with Installation? [y/n] y

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

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

# application remove

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

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

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

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

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

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

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

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

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

| **Usage Guidelines** | Removes or uninstalls an application. |
|---|---|

### Example

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

# application reset-config

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

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

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

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

**Command Modes**   EXEC

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

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

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

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

### Example

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

```
iseadmin#application reset-config ise
Initialize your Application configuration to factory defaults? (y/n): y
Leaving currently connected AD domains if any...
Please rejoin to AD domains from the administrative GUI
Retain existing Application server certificates? (y/n): n
Reinitializing local configuration to factory defaults...
Stopping ISE Monitoring & Troubleshooting Log Processor...
PassiveID WMI Service is disabled
PassiveID Syslog Service is disabled
```

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

# application reset-passwd

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

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

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

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

**Command Modes**  EXEC

**Command History**

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

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

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

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

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

### Example

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

# application start

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

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

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

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

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

**Command Modes** EXEC

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

**Usage Guidelines** Enables an application.

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

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

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

**Example 1**

```
ise/iseadmin#application start ise

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

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

### Starting Cisco ISE Application in Safe Mode

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

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

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

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

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

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

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

**Note** These changes are temporary and only relevant for that instance of the Cisco ISE application. If the Cisco ISE services are restarted again without the 'safe' option, all of the default functionality is restored.

```
ise/iseadmin#application stop ise

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

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


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

# application stop

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

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

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

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

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

**Command Modes**    EXEC

**Command History**

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

**Usage Guidelines**    Disables an application.

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

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

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

### Example

```
iseadmin#application stop ise

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

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

# application upgrade

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

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

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

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

**Command Modes**  EXEC

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

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

- Use the **cleanup** option, if you want to try another upgrade bundle in case of a failure or use a different version.

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

- Use the **proceed** option to upgrade Cisco ISE using the upgrade bundle you extracted with the prepare option. You can use this option after preparing an upgrade bundle instead of using the **application upgrade** command directly.

  - If upgrade is successful, this option removes the upgrade bundle.

  - If upgrade fails for any reason, this option retains the upgrade bundle.

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

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

⚠

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

✎

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

### Example 1

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

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

Application upgrade preparation successful
```

### Example 2

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

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

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

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

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

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

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

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

The system is going down for reboot NOW

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

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

# backup

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

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

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

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

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

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

**Command Modes** EXEC

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

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

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

☞

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

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

- **Option 1:**

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

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

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

- **Option 2:**

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

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

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

# Backing up Cisco ISE Configuration Data

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

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

### Example

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

# Backing up Cisco ISE Operational Data

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

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

**Example**

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

# backup-logs

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

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

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

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

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

**Command Modes**  EXEC

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

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

### Example 1

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

### Example 2

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

# clock

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

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

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

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

**Command Modes**  EXEC

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

**Usage Guidelines**

⚠️

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

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

To recover from the impact, use the following steps:

### Standalone or Primary ISE Node

✎

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

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

- Revert to the original system time (the time before it was changed).

- Run the **application reset-config** *ise* command from the CLI of that node.

- Restore from the last known good backup before the time change on that node.

**Secondary ISE Node**

✎

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

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

- Deregister the secondary ISE node.

- Correct the system time to be in sync with the primary ISE node.

- Run the **application reset-config** *ise* command from the CLI of the primary ISE node.

- Reregister the ISE node as a secondary ISE node to the primary ISE node.

✎

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

**Example**

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

# cls

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

**cls**

| Syntax Description | This command has no keywords and arguments. |
| --- | --- |

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

**Command Modes**  EXEC

**Command History**

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

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

### Example

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

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

# configure

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

**configure terminal**

| **Syntax Description** | **terminal** | Executes configuration commands from the terminal. |
| --- | --- | --- |

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

**Command Modes**  EXEC

**Command History**

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

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

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

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

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

### Example

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

# copy

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

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

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

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

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

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

| Syntax Description | *protocol* | |
|---|---|---|
| | **ftp** | Source or destination URL for FTP network server. The syntax for this alias: **ftp**:[[[//*username* [:*password*]@]*location*]/*directory*]/*filename* |
| | **sftp** | Source or destination URL for an SFTP network server. The syntax for this alias: **sftp**:[[//*location*]/*directory*]/*filename* |
| | **tftp** | Source or destination URL for a TFTP network server. The syntax for this alias: **tftp**:[[//*location*]/*directory*]/*filename* |
| | *location* | Location of destination. Represents the current running configuration file. |
| | **logs** | The system log files. |
| | **all** | Copies all Cisco ISE log files from the system to another location. All logs are packaged as iselogs.tar.gz and transferred to the specified directory on the remote host. |
| | **filename** | Allows you to copy a single Cisco ISE log file and transfer it to the specified directory on the remote host, with its original name. |
| | *log_filename* | Name of the Cisco ISE log file, as displayed by the **show logs** command (up to 255 characters). |
| | **mgmt** | Copies the Cisco ISE management debug logs and Tomcat logs from the system, bundles them as mgmtlogs.tar.gz, and transfers them to the specified directory on the remote host. |
| | **runtime** | Copies the Cisco ISE runtime debug logs from the system, bundles them as runtimelogs.tar.gz, and transfers them to the specified directory on the remote host. |
| | **disk** | The localdisk from where files can be downloaded or uploaded. |
| | **repository** | The repository from where files can be downloaded or uploaded. |

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

**Command Modes**   EXEC

**Command History**

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

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

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

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

Use the filename relative to the directory for file transfers.

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

# Copying Log files

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

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

### Example 1

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

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

### Example 2

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

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

### Example 3

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

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

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

Directory of disk:/

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

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

# crypto

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

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

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

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

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

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

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

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

**Command Modes**   EXEC

**Command History**

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

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

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

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

### Example 1

The following example shows the key management for SFTP repositories.

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

### Example 2

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

```
ise/admin# show crypto authorized_keys
Authorized keys for admin
ise/admin# crypto key delete authorized_keys
ise/admin# show crypto authorized_keys
ise/admin#
ise/admin# crypto key import mykey_rsa repository myrepository
ise/admin# show crypto key
admin public key: ssh-rsa f8:7f:8a:79:44:b8:5d:5f:af:e1:63:b2:be:7a:fd:d4 admin@ise
ise/admin#
```

**Example 3**

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

# debug

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

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

| Syntax Description | | |
| --- | --- |
| **all** | Enables all debugging. |
| **application** | Enables debugging application related errors or events.<br><br>• all—Enables all application debug output. Set level between 0 and 7, with 0 being severe and 7 being all.<br><br>• install—Enables application install debug output. Set level between 0 and 7, with 0 being severe and 7 being all.<br><br>• operation—Enables application operation debug output. Set level between 0 and 7, with 0 being severe and 7 being all.<br><br>• uninstall—Enables application uninstall debug output. Set level between 0 and 7, with 0 being severe and 7 being all. |
| **backup-restore** | Enables debugging back up and restore related errors or events.<br><br>• all—Enables all debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.<br><br>• backup—Enables backup debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.<br><br>• backup-logs—Enables backup-logs debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.<br><br>• history—Enables history debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.<br><br>• restore—Enables restore debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all. |
| **cdp** | Enables debugging Cisco Discovery Protocol configuration related errors or events.<br><br>• all—Enables all Cisco Discovery Protocol configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.<br><br>• config—Enables configuration debug output for Cisco Discovery Protocol. Set level between 0 and 7, with 0 being severe and 7 being all.<br><br>• infra—Enables infrastructure debug output for Cisco Discovery Protocol. Set level between 0 and 7, with 0 being severe and 7 being all. |

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

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

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

**Command Modes**    EXEC

**Command History**

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

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

**Example**

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

# delete

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

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

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

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

**Command Modes**   EXEC

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

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

**Example**

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

# dir

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

**dir**

**dir** *disk:/logs*

**dir recursive**

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

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

**Command Modes**    EXEC

**Command History**

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

**Usage Guidelines**    None.

### Example 1

```
iseadmin#dir

Directory of disk:/

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

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

### Example 2

```
iseadmin#dir disk:/corefiles

Directory of disk:/

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

**Example 3**

```
iseadmin#dir recursive

Directory of disk:/

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

./corefileanalysis:

./corefiles:

./CSD-config-backup:

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

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

# esr

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

**esr**

| **Syntax Description** | This command has no keywords and arguments. |

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

| **Command Modes** | EXEC |

**Command History**

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

**Usage Guidelines**

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

# exit

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

This command has no keywords and arguments.

**exit**

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

**Command Modes**    EXEC

**Command History**

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

**Example**

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

# forceout

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

**forceout** *username*

| Syntax Description | *username* | Name of the user. Supports up to 31 alphanumeric characters. |
|---|---|---|

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

**Command Modes**   EXEC

**Command History**

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

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

### Example

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

# generate-password

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

**Syntax Description**

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

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

**Command Modes**  EXEC

**Command History**

| Release | Modification |
|---|---|
| 3.1 | This command was introduced. |

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

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

### Example

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

# halt

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

This command has no keywords and arguments.

**halt**

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Command History**

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

**Usage Guidelines**

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

If you issue the **halt** command while the Cisco ISE is performing any of these operations, you will get one of the following warning messages:

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

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

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

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

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

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

**Example**

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

# idle-timeout

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

**idle-timeout** *seconds*

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

**Command Default**   None.

**Command Modes**   EXEC

| Command History | Release | Modification |
| --- | --- | --- |
| | 3.2 | This command was introduced. |

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

**Example**

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

# licence esr

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

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

| Syntax Description | | |
|---|---|
| **classic** | Enables ESR classic licensing. |
| **smart** | Enables ESR smart licensing. |

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

**Command Modes**     EXEC

**Command History**

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

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

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

# mkdir

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

**mkdir** *directory-name*

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

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Command History**

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

**Usage Guidelines**

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

**Example**

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

# nslookup

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

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

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

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

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

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

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

**Command History**

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

### Example 1

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

### Example 2

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

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

# password

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

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

> ✎
>
> **Note** When you create a password for the administrator during installation or after installation in the CLI, do not use the $ character, except when it is the last character of the password. If that character is first or inside the other characters, the password is accepted, but you cannot use it to log on to the CLI.
>
> You can fix this by logging into the console and using the CLI command, or by getting an ISE CD or ISO file. Instructions for using an ISO to reset the password are explained in the following document: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200568-ISE-Password-Recovery-Mechanisms.html

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

**Command Modes** EXEC

**Command History**

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

**Example**

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

# patch install

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

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

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

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

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

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

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

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

**Command Modes**   EXEC

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

**Usage Guidelines**   Installs a specific patch bundle of the application.

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

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

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

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

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

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

### Example

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

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

Patch successfully installed
ise/admin#
```

# patch remove

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

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

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

![note icon]

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

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

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

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

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

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

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

```
% Patch is not installed
```

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

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

**Example 1**

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

**Example 2**

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

# permit rootaccess

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

**permit rootaccess**

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

| Syntax Description | This command has no keywords and arguments. |
|---|---|

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

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

**Command History**

| Release | Modification |
|---|---|
| 2.7.0.349 | This command was introduced. |

**Example**

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

```
ise/admin##
ise/admin# permit rootaccess
1.  Generate Challenge Token Request
2.  Enter Challenge Response for Root Access
3.  Show History
4.  Exit
Enter CLI Option:
1
Generating Challenge.......................................
Challenge String (Please copy everything between the asterisk lines exclusively):
***********************************************************************************
GLOX7gAAXQEBAQAAAABAgFAAAAAACmdkgbDhitBAQLUw+XeD3mJ4HnJy3XQJABAAADAGANLUHAYZJUVfQJQJAANLUUJAGcJLDLANQNjgwLIFAUuEOWLlZSlwZjYLIFdIZD1M1QLMZUNQo=
***********************************************************************************
Starting background timer of 15mins
1.  Generate Challenge Token Request
2.  Enter Challenge Response for Root Access
3.  Show History
4.  Exit
Enter CLI Option:
2
Please input the response when you are ready ..........................
vQgogwewwUUdt9dbUrmMtiobQUorttd4lvMbtitzkPxbxdpEsQpd7malsrYnt3kstzaphsXG3jxsdsfrghgygj5D7rtkoltqwstshgd6JtMjbSuparrhyy0AMR2i5JdfpxSxZmpdRg
Response Signature Verified successfully !
Granting shell access
sh-4.2# ls
2.4backup                                     config         CT_Deme_Test_Rpm
ct_rolling.txt     lost+found                 threadHeapDumpGntr.sh
backup_anc-2.7.0-115.jar                       corefiles      CT_engine-2.7.0-1.0.x86_64.rpm
```

```
err.out              prrt-server.log          tomcat-process-log.txt
backup_guestaccess-upgrade-2.7.0-115.jar  corestacks.txt  ct_persistent.txt
Heap_dump20190705  libciscosafec.so.4.0.1  Thread_dump_2019-07-05-19:07:30
sh-4.2# exit
exit
Root shell exited
1.   Generate Challenge Token Request
2.   Enter Challenge Response for Root Access
3.   Show History
4.   Exit
Enter CLI Option:
3
***********************************
              SN No : 1
***********************************
Challenge
3/WcyAYYAQEBAQAYYBAgFEAYYYAYACM89hCTWWBAQwo9lyianffO4C5.i1+v8AQAJABAWDAGAANJ.0JHAYZJ.OJV.FQJQJAANJ.0JJACcJID.ZNGQNjgvJJ.FzPzHE.OW.OZS0wZjYJJIcJJZD.JJMGQJM.JJNQo=
  generated at 2019-06-12 15:40:01.000
***********************************
              SN No : 2
***********************************
Challenge
exNwkAYYAQEBAQAYYBAgFEAYYYAYACEb3bsKGBAQ04JKV7kfKQ7udE7qPGAJABAWDAGAANJ.0JHAYZJ.OJV.FQJQJAANJ.0JJACcJID.ZNGQNjgvJJ.FzPzHE.OW.OZS0wZjYJJIcJJZD.JJMGQJM.JJNQo=
  generated at 2019-06-12 15:43:31.000
1.   Generate Challenge Token Request
2.   Enter Challenge Response for Root Access
3.   Show History
4.   Exit
Enter CLI Option:
4
Exiting..............
ise/admin#
```

# ping

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

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

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

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

**Command Modes**  EXEC

**Command History**

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

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

### Example

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

# ping6

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

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

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

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

**Command Modes**   EXEC

**Command History**

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

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

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

### Example 1

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

### Example 2

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

# reload

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

**reload** [**cli**]

| **Syntax Description** | *cli* | Restart the underlying Confd processes and generate the CLI again with upd values. |
|---|---|---|

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

**Command Modes**  EXEC

**Command History**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

### Example 1

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

### Example 2

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

# reset-config

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

**reset-config**

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

| **Command Modes** | EXEC |

**Command History**

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

**Usage Guidelines**     All services will be restarted upon completion.

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

# restore

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

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

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

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

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

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

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

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

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

**Usage Guidelines**

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

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

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

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

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

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

# Restoring Cisco ISE Configuration Data from the Backup

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

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

### Example

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

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

```
 - Data upgrade step 20/67, ProfilerUpgradeService(1.3.0.360)... ...Done in 236 seconds.
 - Data upgrade step 21/67, ProfilerUpgradeService(1.3.0.380)... Done in 4 seconds.
 - Data upgrade step 22/67, NSFUpgradeService(1.3.0.401)... Done in 0 seconds.
 - Data upgrade step 23/67, NSFUpgradeService(1.3.0.406)... Done in 0 seconds.
 - Data upgrade step 24/67, NSFUpgradeService(1.3.0.410)... Done in 2 seconds.
 - Data upgrade step 25/67, RBACUpgradeService(1.3.0.423)... Done in 0 seconds.
 - Data upgrade step 26/67, NetworkAccessUpgrade(1.3.0.424)... Done in 0 seconds.
 - Data upgrade step 27/67, RBACUpgradeService(1.3.0.433)... Done in 1 seconds.
 - Data upgrade step 28/67, EgressUpgradeService(1.3.0.437)... Done in 1 seconds.
 - Data upgrade step 29/67, NSFUpgradeService(1.3.0.438)... Done in 0 seconds.
 - Data upgrade step 30/67, NSFUpgradeService(1.3.0.439)... Done in 0 seconds.
 - Data upgrade step 31/67, CdaRegistration(1.3.0.446)... Done in 2 seconds.
 - Data upgrade step 32/67, RBACUpgradeService(1.3.0.452)... Done in 16 seconds.
 - Data upgrade step 33/67, NetworkAccessUpgrade(1.3.0.458)... Done in 0 seconds.
 - Data upgrade step 34/67, NSFUpgradeService(1.3.0.461)... Done in 0 seconds.
 - Data upgrade step 35/67, CertMgmtUpgradeService(1.3.0.462)... Done in 2 seconds.
 - Data upgrade step 36/67, NetworkAccessUpgrade(1.3.0.476)... Done in 0 seconds.
 - Data upgrade step 37/67, TokenUpgradeService(1.3.0.500)... Done in 1 seconds.
 - Data upgrade step 38/67, NSFUpgradeService(1.3.0.508)... Done in 0 seconds.
 - Data upgrade step 39/67, RBACUpgradeService(1.3.0.509)... Done in 17 seconds.
 - Data upgrade step 40/67, NSFUpgradeService(1.3.0.526)... Done in 0 seconds.
 - Data upgrade step 41/67, NSFUpgradeService(1.3.0.531)... Done in 0 seconds.
 - Data upgrade step 42/67, MDMUpgradeService(1.3.0.536)... Done in 0 seconds.
 - Data upgrade step 43/67, NSFUpgradeService(1.3.0.554)... Done in 0 seconds.
 - Data upgrade step 44/67, NetworkAccessUpgrade(1.3.0.561)... Done in 3 seconds.
 - Data upgrade step 45/67, RBACUpgradeService(1.3.0.563)... Done in 19 seconds.
 - Data upgrade step 46/67, CertMgmtUpgradeService(1.3.0.615)... Done in 0 seconds.
 - Data upgrade step 47/67, CertMgmtUpgradeService(1.3.0.616)... Done in 15 seconds.
 - Data upgrade step 48/67, CertMgmtUpgradeService(1.3.0.617)... Done in 2 seconds.
 - Data upgrade step 49/67, OcspServiceUpgradeRegistration(1.3.0.617)... Done in 0 seconds.
 - Data upgrade step 50/67, NSFUpgradeService(1.3.0.630)... Done in 0 seconds.
 - Data upgrade step 51/67, NSFUpgradeService(1.3.0.631)... Done in 0 seconds.
 - Data upgrade step 52/67, CertMgmtUpgradeService(1.3.0.634)... Done in 0 seconds.
 - Data upgrade step 53/67, RBACUpgradeService(1.3.0.650)... Done in 8 seconds.
 - Data upgrade step 54/67, CertMgmtUpgradeService(1.3.0.653)... Done in 0 seconds.
 - Data upgrade step 55/67, NodeGroupUpgradeService(1.3.0.655)... Done in 1 seconds.
 - Data upgrade step 56/67, RBACUpgradeService(1.3.0.670)... Done in 4 seconds.
 - Data upgrade step 57/67, ProfilerUpgradeService(1.3.0.670)... Done in 0 seconds.
 - Data upgrade step 58/67, ProfilerUpgradeService(1.3.0.671)... Done in 0 seconds.
 - Data upgrade step 59/67, ProfilerUpgradeService(1.3.0.675)...
..................................Done in 2118 seconds.
 - Data upgrade step 60/67, NSFUpgradeService(1.3.0.676)... Done in 1 seconds.
 - Data upgrade step 61/67, AuthzUpgradeService(1.3.0.676)... Done in 20 seconds.
 - Data upgrade step 62/67, GuestAccessUpgradeService(1.3.0.676)... .......Done in 454
seconds.
 - Data upgrade step 63/67, NSFUpgradeService(1.3.0.694)... Done in 0 seconds.
 - Data upgrade step 64/67, ProvisioningRegistration(1.3.0.700)... Done in 0 seconds.
 - Data upgrade step 65/67, RegisterPostureTypes(1.3.0.705)... Done in 0 seconds.
 - Data upgrade step 66/67, CertMgmtUpgradeService(1.3.0.727)... Done in 0 seconds.
 - Data upgrade step 67/67, ProvisioningUpgradeService(1.3.105.181)... .Done in 103 seconds.
UPGRADE STEP 3: Running ISE configuration data upgrade for node specific data...
% restore in progress: Restoring logs...75% completed
% restore in progress: Restarting ISE Services...90% completed
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE Identity Mapping Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
```

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

# Restoring Cisco ISE Operational Data from the Backup

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

**restore** *mybackup-OPS-130103-0019.tar.gpg* **repository** *myrepository* **encryption-key  plain** *lablab12*

### Example

```
ise/admin# restore mybackup-OPS-130103-0019.tar.gpg repository myrepository
encryption-key plain lablab12
% Warning: Do not use Ctrl-C or close this terminal window until the restore completes.
Initiating restore.  Please wait...
% restore in progress: Starting Restore...10% completed
% restore in progress: Retrieving backup file from Repository...20% completed
% restore in progress: Decrypting backup data...40% completed
% restore in progress: Extracting backup data...50% completed
Stopping ISE Monitoring & Troubleshooting Log Processor...

Stopping ISE Application Server...
Stopping ISE Profiler DB...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
% restore in progress: starting dbrestore.......55% completed
% restore in progress: ending dbrestore.......75% completed
 checking for upgrade
Starting M&T DB upgrade
ISE Database processes already running, PID: 30124
ISE M&T Session Database is already running, PID: 484
Starting ISE Profiler DB...
Starting ISE Application Server...
ISE M&T Log Processor is already running, PID: 837
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
% restore in progress: Completing Restore...100% completed
ise/admin#
```

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

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

**restore** *mybackup-CFG-130405-0044.tar.gpg* **repository** *myrepository* **encryption-key  plain** *Mykey123*
**include-adeos**

### Example

```
ise/admin# restore mybackup-CFG-130405-0044.tar.gpg repository myrepository encryption-key
 plain Mykey123 include-adeos
% Warning: Do not use Ctrl-C or close this terminal window until the restore completes.
Initiating restore.  Please wait...
```

```
% restore in progress: Starting Restore...10% completed
% restore in progress: Retrieving backup file from Repository...20% completed
% restore in progress: Decrypting backup data...25% completed
% restore in progress: Extracting backup data...30% completed
% restore in progress: Stopping ISE processes required for restore...35% completed
% restore in progress: Restoring ISE configuration database...40% completed
% restore in progress: Updating Database metadata...70% completed
% restore in progress: Restoring logs...75% completed
% restore in progress: Performing ISE Database synchup...80% completed
% restore in progress: Completing Restore...100% completed
Broadcast message from root (pts/2) (Fri Apr  5 01:40:04 2013):
The system is going down for reboot NOW!
Broadcast message from root (pts/2) (Fri Apr  5 01:40:04 2013):
The system is going down for reboot NOW!
ise/admin#
```

# rmdir

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

**rmdir** *directory-name*

| Syntax Description | *directory-name* | Directory name. Supports up to 80 alphanumeric characters. |
| --- | --- | --- |

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

**Command Modes**  EXEC

**Command History**

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

**Example**

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

# screen-length

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

**screen-length** *integer*

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

**Command Default**

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

**Command Modes**

EXEC

**Command History**

| Release | Modification |
|---|---|
| 3.2 | This command was introduced. |

**Usage Guidelines**

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

**Example**

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

# screen-width

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

**screen-width** *integer*

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

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

**Command Modes**  EXEC

**Command History**

| Release | Modification |
|---|---|
| 3.2 | This command was introduced. |

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

**Example**

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

# ssh

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

✎

| **Note** | An administrator or user can use this command |

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

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

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

| **Command Default** | Disabled. |
|---|---|

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

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

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

> **Note** Cisco ISE initiates outbound SSH or SFTP connections in FIPS mode even if FIPS mode is not enabled on ISE. Ensure that the remote SSH or SFTP servers that communicate with ISE allow FIPS 140-2 approved cryptographic algorithms.
>
> Cisco ISE uses embedded FIPS 140-2 validated cryptographic modules. For details of the FIPS compliance claims, see the FIPS Compliance Letter.

### Example 1

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

### Example 2

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

# tech

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

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

**Command Default**  Disabled.

**Command Modes**  EXEC

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

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

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

- br-<...>

- docker0

- GigabitEthernet0 (and other GigabitEthernet interfaces if available)

• lo

• veth<...>

### Example 1

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

### Example 2

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

### Example 3

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

# Interpreting CPU and Memory Usage Data

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

• top shows uptime information

• Tasks shows process status information.

• %Cpu(s) shows various processor values.

- MiB Mem displays physical memory utilization. This value is based on the total amount of physical RAM installed on the system and provides the following information:

    - total shows total installed memory.

    - free shows available memory.

    - Used shows consumed memory.

    - buff/cache shows the amount of information cached to be written later.

- MiB Swap displays virtual memory utilization. OS can take advantage of virtual memory when physical memory space is used by borrowing storage space from storage disks. The process of swapping data back and forth between physical RAM and storage drives is time-consuming and uses system resources, so it is best to minimize the use of virtual memory. MiB Swap output provides the following information:

    - total shows total swap space.

    - free shows available swap space.

    - used shows consumed swap space.

    - buff/cache shows the amount of information cached for future reads.

- Load Average: The load average is broken down into three time increments. The first value displays the load for the last one minute, the second value for the last five minutes, and the final value for the last fifteen-minutes. For Cisco ISE high load average, use the five-minute interval. If the five-minute interval value goes beyond the cores allocated to the node, the load average alarm is triggered.

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

**Example:**

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

# terminal

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

**terminal**

| | | |
|---|---|---|
| **Syntax Description** | *type* | Defines the terminal name and type, and permits terminal negotiation by h[...] that provide that type of service. Supports up to 80 alphanumeric character[...] |

| | |
|---|---|
| **Command Default** | VT100 |

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

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

**Usage Guidelines**  Indicates the terminal type if it is different from VT100.

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

### Example

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

# traceroute

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

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

| Syntax Description | | |
|---|---|---|
| | *ip-address* | IPv4 address of the remote system. Supports up to 64 alphanumeric cha |
| | *hostname* | Hostname of the remote system. Supports up to 64 alphanumeric chara |

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

**Command Modes** EXEC

**Command History**

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

**Example**

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

# undebug

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

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

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

| copy | Copy commands. |
|------|----------------|
| locks | Resource locking.<br><br>• all—Disables all resource locking debug output.<br><br>• file—Disables file locking debug output. |
| logging | Logging configuration files.<br><br>all—Disables all debug output for logging configuration. |
| snmp | SNMP configuration files.<br><br>all—Disables all debug output for SNMP configuration. |
| system | System files.<br><br>• all—Disables all system files debug output.<br><br>• id—Disables system ID debug output.<br><br>• info—Disables system info debug output.<br><br>• init—Disables system init debug output. |
| transfer | File transfer. |
| user | User management.<br><br>• all—Disables all user management debug output.<br><br>• password-policy—Disables user management debug output for password-policy. |
| utils | Utilities configuration files.<br><br>all—Disables all utilities configuration debug output. |

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

**Command Modes**  EXEC

**Command History**

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

**Example**

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

# who

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

**who**

**Syntax Description**

This command has no keywords and arguments.

**Command Default**

No default behavior or values.

**Command Modes**

EXEC

**Command History**

| Release | Modification |
|---------|--------------|
| 3.2 | This command was introduced. |

**Usage Guidelines**

None.

**Example**

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

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