



Installation Verification and Post-Installation Tasks

- [Log in to the Cisco ISE Web-Based Interface, on page 1](#)
- [Cisco ISE Configuration Verification, on page 3](#)
- [List of Post-Installation Tasks, on page 5](#)

Log in to the Cisco ISE Web-Based Interface

When you log in to the Cisco ISE web-based interface for the first time, you will be using the preinstalled Evaluation license.



Note We recommend that you use the Cisco ISE user interface to periodically reset your administrator login password.



Caution For security reasons, we recommend that you log out when you complete your administrative session. If you do not log out, the Cisco ISE web-based web interface logs you out after 30 minutes of inactivity, and does not save any unsubmitted configuration data.

For information about the validated browsers, see "Validated Browsers" section in the [Cisco ISE Release Notes](#).



Note If Cisco ISE is installed in the cloud or using the ZTP process, you will be prompted to change the web-based admin user password during the first login.

Step 1 After the Cisco ISE appliance reboot has completed, launch one of the supported web browsers.

Step 2 In the Address field, enter the IP address (or hostname) of the Cisco ISE appliance by using the following format and press **Enter**.

`https://<IP address or host name>/admin/`

Step 3 Enter a username and password that you defined during setup.

Step 4 Click **Login**.

Differences Between CLI Admin and Web-Based Admin Users Tasks

The username and password that you configure when using the Cisco ISE setup program are intended to be used for administrative access to the Cisco ISE CLI and the Cisco ISE web interface. The administrator that has access to the Cisco ISE CLI is called the CLI-admin user. By default, the username for the CLI-admin user is admin and the password is user-defined during the setup process. There is no default password.

You can initially access the Cisco ISE web interface by using the CLI-admin user's username and password that you defined during the setup process. There is no default username and password for a web-based admin.

The CLI-admin user is *copied* to the Cisco ISE web-based admin user database. Only the first CLI-admin user is copied as the web-based admin user. You should keep the CLI- and web-based admin user stores synchronized, so that you can use the same username and password for both admin roles.

The Cisco ISE CLI-admin user has different rights and capabilities than the Cisco ISE web-based admin user and can perform other administrative tasks.

Table 1: Tasks Performed by CLI-Admin and Web-Based Admin Users

Admin User Type	Tasks
Both CLI-Admin and Web-Based Admin	<ul style="list-style-type: none"> • Back up the Cisco ISE application data. • Display any system, application, or diagnostic logs on the Cisco ISE appliance. • Apply Cisco ISE software patches, maintenance releases, and upgrades. • Set the NTP server configuration.
CLI-Admin only	<ul style="list-style-type: none"> • Start and stop the Cisco ISE application software. • Reload or shut down the Cisco ISE appliance. • Reset the web-based admin user in case of a lockout. • Access the ISE CLI.

Create a CLI Admin

Cisco ISE allows you to create additional CLI-admin user accounts other than the one you created during the setup process. To protect the CLI-admin user credentials, create the minimum number of CLI-admin users needed to access the Cisco ISE CLI.

You can add the CLI-admin user by using the following command in the configuration mode:

```
username <username> password [plain/hash] <password> role admin
```

Create a Web-Based Admin

For first-time web-based access to Cisco ISE system, the administrator username and password is the same as the CLI-based access that you configured during setup.

To add an admin user:

1. Choose **Administration > System > Admin Access > Administrators > Admin Users**.
2. Choose **Add > Create an Admin User**.
3. Enter the name, password, admin group, and the other required details.
4. Click **Submit**.

Reset a Disabled Password Due to Administrator Lockout

An administrator can enter an incorrect password enough times to disable the account. The minimum and default number of attempts is five.

Use these instructions to reset the administrator user interface password with the **application reset-passwd ise** command in the Cisco ISE CLI. It does not affect the CLI password of the administrator. After you successfully reset the administrator password, the credentials are immediately active and you can log in without having to reboot the system. .

Cisco ISE adds a log entry in the **Administrator Logins** window. The navigation path for this window is **Operations > Reports > Reports > Audit > Administrator Logins**. The credentials for that administrator ID is suspended until you reset the password associated with that administrator ID.

Step 1 Access the direct-console CLI and enter:

```
application reset-passwd ise administrator_ID
```

Step 2 Specify and confirm a new password that is different from the previous two passwords that were used for this administrator ID:

```
Enter new password:
```

```
Confirm new password:
```

```
Password reset successfully
```

Cisco ISE Configuration Verification

There are two methods that each use a different set of username and password credentials for verifying Cisco ISE configuration by using a web browser and CLI.



Note A CLI-admin user and a web-based admin user credentials are different in Cisco ISE.

Verify Configuration Using a Web Browser

- Step 1** After the Cisco ISE appliance reboot has completed, launch one of the supported web browsers.
- Step 2** In the **Address** field, enter the IP address (or host name) of the Cisco ISE appliance using the following format and press **Enter**.
- Step 3** In the Cisco ISE Login page, enter the username and password that you have defined during setup and click **Login**.
For example, entering `https://10.10.10.10/admin/` displays the Cisco ISE Login page.

```
https://<IP address or host name>/admin/
```

Note For first-time web-based access to Cisco ISE system, the administrator username and password is the same as the CLI-based access that you configured during setup.

- Step 4** Use the Cisco ISE dashboard to verify that the appliance is working correctly.
-

What to do next

By using the Cisco ISE web-based user interface menus and options, you can configure the Cisco ISE system to suit your needs. For details on configuring Cisco ISE, see *Cisco Identity Services Engine Administrator Guide*.

Verify Configuration Using the CLI

Before you begin

Download and install the latest [Cisco ISE patch](#) to keep Cisco ISE up-to-date.

- Step 1** After the Cisco ISE appliance reboot has completed, launch a supported product, such as PuTTY, for establishing a Secure Shell (SSH) connection to a Cisco ISE appliance.
- Step 2** In the Host Name (or IP Address) field, enter the hostname (or the IP address in dotted decimal format of the Cisco ISE appliance) and click **Open**.
- Step 3** At the login prompt, enter the CLI-admin username (admin is the default) that you configured during setup and press **Enter**.
- Step 4** At the password prompt, enter the CLI-admin password that you configured during setup (this is user-defined and there is no default) and press **Enter**.
- Step 5** At the system prompt, enter **show application version ise** and press **Enter**.

Note The Version field lists the currently installed version of Cisco ISE software.

The console output appears as shown below:

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

```

Cisco Identity Services Engine
-----
Version       : 2.4.0.226
Build Date    : Fri Nov 24 17:36:37 2017
Install Date  : Thu Nov 30 21:40:54 2017

```

Step 6 To check the status of the Cisco ISE processes, enter **show application status ise** and press **Enter**.

The console output appears as shown below:

```

ise-server/admin# show application status ise

ISE PROCESS NAME                STATE          PROCESS ID
-----
Database Listener               running       4930
Database Server                 running       66 PROCESSES
Application Server              running       8231
Profiler Database              running       6022
ISE Indexing Engine             running       8634
AD Connector                    running       9485
M&T Session Database            running       3059
M&T Log Collector               running       9271
M&T Log Processor               running       9129
Certificate Authority Service    running       8968
EST Service                     running       18887
SXP Engine Service              disabled
TC-NAC Docker Service           disabled
TC-NAC MongoDB Container        disabled
TC-NAC RabbitMQ Container       disabled
TC-NAC Core Engine Container    disabled
VA Database                     disabled
VA Service                      disabled
pxGrid Infrastructure Service     disabled
pxGrid Publisher Subscriber Service disabled
pxGrid Connection Manager        disabled
pxGrid Controller               disabled
PassiveID Service               disabled
DHCP Server (dhcpd)             disabled
DNS Server (named)              disabled

```

List of Post-Installation Tasks

After you install Cisco ISE, you must perform the following mandatory tasks:

Table 2: Mandatory Post-Installation Tasks

Task	Link in the Administration Guide
Apply the latest patches, if any	Install a Software Patch
Install Licenses	See the Cisco ISE Ordering Guide for more information. See the Administration Guide for information on how to Register Licenses.

Task	Link in the Administration Guide
Install Certificates	See the Manage Certificates chapter of the Cisco ISE Administration Guide for more details.
Create Repository for Backups	See the Create Repositories section of the Cisco ISE Administration Guide for more details.
Configure Backup Schedules	See the Schedule a Backup section of the Cisco ISE Administration Guide for more details.
Deploy Cisco ISE personas	See the Set Up Cisco ISE in a Distributed Environment chapter of the Cisco ISE Administration Guide.