

Revised: May 13, 2026

Installation Verification and Post-Installation Tasks

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 use the preinstalled Evaluation license.

- Step 1** After the Cisco ISE appliance finishes rebooting, launch one of the supported web browsers.
For information about validated browsers, refer to the “Validated Browsers” section in the [Cisco ISE Release Notes](#).
- Step 2** In the **Address** field, enter the IP address or hostname of the Cisco ISE appliance in this format, then press **Enter**.
`https://<IP address or host name>/admin/`
- Step 3** Enter your username and password.
- Step 4** Click **Login**.



Note

- For security, log out when you complete your administrative session. If you do not log out, Cisco ISE logs you out after 30 minutes of inactivity and does not save any unsubmitted configuration data.
- 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.

Differences between CLI admin and web-based admin user tasks

Use the username and password you set during Cisco ISE setup for administrative access to the CLI and the web interface.

The administrator with access to the Cisco ISE CLI is called the CLI-admin user. By default, the CLI-admin username is admin. The administrator must create the password during the setup process, as Cisco ISE does not provide a default password.

You can initially access the Cisco ISE web interface by using the CLI-admin username and password that you defined during setup. A web-based admin user does not have a default username or password.

Cisco ISE copies the CLI-admin user to the web-based admin user database. Only the first CLI-admin user is copied as the web-based admin user. Ensure that the CLI and web-based administrator user stores remain synchronized. Using the same username and password for both roles simplifies administration.

The CLI-admin user has different rights and capabilities than the web-based admin user and can perform additional 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	• Back up 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	• Start and stop Cisco ISE application software • Reload or shut down the Cisco ISE appliance • Reset the web-based admin user in case of a lockout • Access Cisco ISE CLI

Create a CLI admin

You can create additional CLI-admin user accounts after you complete the setup process. To keep your account secure, create only the number of CLI-admin users you need for Cisco ISE CLI access. This method helps you protect your credentials.

You can add a CLI-admin user with this command in configuration mode:

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

Create a web-based admin

To access Cisco ISE through the web interface initially, use the administrator username and password configured during CLI setup.

To add an administrator user, perform these steps:

1. In the Cisco ISE GUI, click the **Menu** icon () and choose **Administration > System > Admin Access > Administrators > Admin Users**.
2. Choose **Add > Create an Admin User**.
3. Add web-based administrator users using the user interface.
4. Click **Submit**.

Reset a disabled password due to administrator lockout

If you enter an incorrect password five times, your account becomes disabled.

Use these instructions to reset the administrator user interface password with the **application reset-passwd ise** command in the Cisco ISE CLI. Resetting the administrator password activates new credentials immediately and allows you to log in without rebooting the system. This process does not affect the administrator's CLI password.

Cisco ISE adds a log entry in the **Administrator Logins** window. Navigate to **Operations > Reports > Reports > Audit > Administrator Logins**. Reset your administrator ID password to regain access to your credentials.

This procedure helps you re-enable your credentials so you can resume system management tasks.

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 passwords that were used most recently for this administrator ID.

```
Enter new password:
Confirm new password:

Password reset successfully
```

Cisco ISE configuration verification

You can verify the Cisco ISE configuration using a web browser or the CLI. Each method requires a different set of username and password credentials.



Note

The CLI administrator user credentials and the web-based administrator user credentials are different in Cisco ISE.

Verify configuration using a web browser

Follow these steps to verify the configuration using a web browser:

Step 1 After the Cisco ISE appliance reboots, open a supported web browser.

Step 2 In the **Address** field, enter the IP address or host name of the Cisco ISE appliance using this format, and press **Enter**.

Step 3 On the Cisco ISE Login page, enter the username and password you created during setup. Click **Login**.

For example, enter `https://192.0.2.10/admin/`. The Cisco ISE Login page appears.

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



Note

For first-time access to the Cisco ISE system using a web browser, the administrator username and password are the same as the credentials you configured for command-line interface access during setup.

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

What's next

Use the Cisco ISE web-based interface menus and options to configure the system to suit your needs. For details on configuring Cisco ISE, refer to [Cisco Identity Services Engine Administrator Guide](#).

Verify configuration using the CLI

Follow these steps to verify the configuration using the CLI:

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

Step 1 After your Cisco ISE appliance reboots, open a supported application, such as PuTTY, to connect to your Cisco ISE appliance using Secure Shell (SSH).

- Step 2** In the **Host Name or IP Address** field, enter the hostname or IP address (in dotted decimal format) for your Cisco ISE appliance, and click **Open**.
- Step 3** At the login prompt, enter the CLI-admin username you created during setup. The default user name is admin. Press **Enter**.
- Step 4** At the password prompt, enter the CLI-admin password you created during setup. Press **Enter**.
- Step 5** At the system prompt, enter **show application version ise** and press **Enter**.
- 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:

```
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 (dhcpcd)	disabled	
DNS Server (named)	disabled	

List of post-installation tasks

After you install Cisco ISE, you must perform these mandatory tasks:

Table 2: Mandatory post-installation tasks

Task	Link in the Administration Guide
Apply the latest patches, if any	Refer to the "Software Patch Installation Guidelines" in the "Maintain and Monitor" chapter of the Cisco ISE Administrator Guide for your release.
Install licenses	Refer to the Cisco ISE Licensing Guide for more information. See the chapter "Licensing" in the Cisco ISE Administrator Guide for your release.

Task	Link in the Administration Guide
Install certificates	Refer to the section "Certificate Management in Cisco ISE" in the chapter "Basic Setup" in the Cisco ISE Administrator Guide for your release.
Create repository for backups	Refer to "Create Repositories" in the "Maintain and Monitor" chapter of the Cisco ISE Administrator Guide for your release
Configure backup schedules	Refer to "Schedule a Backup" in the "Maintain and Monitor" chapter of the Cisco ISE Administrator Guide for your release.
Deploy Cisco ISE personas	Refer to the section "Cisco ISE Distributed Deployment" in the chapter "Deployment" in the Cisco ISE Administrator Guide for your release.