

Revised: May 13, 2026

Upgrade and login to Cisco ISE on cloud instances

Upgrade Cisco ISE hybrid deployments

Cisco ISE upgrade workflow is not available in Cisco ISE on AWS, Microsoft Azure, or OCI. Only fresh installs of Cisco ISE are supported. However, you can carry out backup and restore of configuration data. You can upgrade Cisco ISE hybrid deployments where the Primary Administration Node (PAN) is installed either on cloud or on premises.

- [Upgrade hybrid deployments with PAN installed on premises, on page 1.](#)
- [Upgrade hybrid deployments with PAN installed on cloud, on page 1.](#)

Upgrade hybrid deployments with PAN installed on premises

Follow these steps to upgrade a hybrid deployment in which the PAN is installed on premises, and any or some of the secondary nodes are installed on the cloud.

- Step 1** Deregister the secondary nodes that are installed on the cloud from the Cisco ISE deployment.
If all the secondary nodes are installed on the cloud, this could cause a downtime.
- Step 2** Upgrade the on-prem deployment to a higher release.
For more information on this, refer to the section "Perform the Upgrade" in the [Cisco Identity Services Engine Upgrade Journey](#) for your release.
- Step 3** Install the required number of standalone Cisco ISE nodes on the cloud with the higher release.
You must install and configure the nodes with the same IP addresses to avoid configuration changes on the NADs. For more information on the installation process, refer to the [Cisco Identity Services Engine Installation Guide](#) for your release.
- Step 4** Register these standalone nodes to the upgraded on premises deployment.
You need to import the system certificates to the newly deployed nodes in Cisco ISE. For more information about how to import system certificates to a Cisco ISE node, refer to the "Import a System Certificate" section in the "Basic Setup" chapter of the [Cisco Identity Services Engine Administrator Guide](#) for your release.

The upgrade of a hybrid Cisco ISE deployment in which the PAN is installed on premises is complete.

Upgrade hybrid deployments with PAN installed on cloud

Follow these steps to upgrade a hybrid deployment in which the PAN is installed on cloud.

- Step 1** Backup Cisco ISE configuration settings and operational logs from the existing deployment.
- Step 2** Shut down all the nodes in the deployment.
- Step 3** Install the required number of standalone Cisco ISE nodes on cloud and on premises with the higher release.
You must install and configure the nodes with the same IP addresses to avoid configuration changes on the NADs. For more information on the installation process, refer to the [Cisco Identity Services Engine Installation Guide](#) for your release.

Step 4 Restore Cisco ISE configuration from the backup data. For more information, refer to the "Backup and Restore Upgrade Process" section in the [Cisco Identity Services Engine Upgrade Journey](#) for your release.

Step 5 Register all the nodes to the upgraded cloud deployment.

The upgrade of a hybrid Cisco ISE deployment in which the PAN is installed on cloud is complete.

Login credentials for Cisco ISE instances launched through cloud platforms

The username and password for any Cisco ISE instance launched using cloud-native images or hosted on supported cloud platforms must be secure.

Username for Cisco ISE on cloud

The default username for Cisco ISE instances that are launched through cloud platforms is iseadmin. Even if you enter a different username in the user data, the Cisco ISE instance is created with the username iseadmin.

Remember

For Cisco ISE release 3.1 instances that are launched through AWS, the default username is admin.

Passwords for Cisco ISE on cloud

In all cloud platforms, the password that you configure when setting up an instance is stored as plaintext. However, a plaintext password can present a security risk. So, for any Cisco ISE instance launched from a cloud platform, you must reset the login password when you first access the Cisco ISE GUI. Then, you must also update your API-based automation scripts with the updated password to avoid any errors.

The username and password for any Cisco ISE instance launched using cloud-native images or hosted on supported cloud platforms must be secure.