

Revised: June 2, 2026

Cisco ISE Software Patch

Software patch upgrade

You can upgrade to a new Cisco ISE release with or without a patch for that release. If you have already installed a patch for your Cisco ISE release, you can use the **Patch** option to upgrade only the patch in your current release.

You can choose one of these two options:

- Full Upgrade
- Split Upgrade



Note

Mutual exclusivity in Cisco ISE deployments ensures that only one upgrade method is active at a time. This prevents conflicts during patch installation or upgrade processes.

- The **Install** in the **Administration > System > Maintenance > Installed Patches** page is **disabled** when you use the **Full Upgrade** or **Split Upgrade** option in the **Upgrade & Rollback** page.
- Conversely, if you select the **Install** option in the **Installed Patches** page, the **Full Upgrade** and **Split Upgrade** options become disabled in the **Upgrade & Rollback** page.

Upgrade patch using full upgrade option

Full upgrade is a process that

- performs a complete upgrade of your Cisco ISE deployment
- provides a complete patch upgrade
- upgrades the deployment in less time than the split upgrade process
- makes application services to be unavailable as all nodes are upgraded at the same time.

To perform a patch upgrade using the Full upgrade option, complete these steps:

Step 1 In the Cisco ISE GUI, navigate to **Administration > System > Upgrade & Rollback**.

Step 2 In the **Upgrade & Rollback** page,

- a. click **Upgrade**
- b. click **Patch**
- c. click **Full**, and then
- d. click **Initialize**.

Step 3 Click **Let's Do It** in the **Welcome** page to start the upgrade workflow.

The **Prerequisite Checks** page is displayed.

Step 4 Under **How do you want to fetch Patch Bundle?**, choose one of these options:

- **Choose from Repository:** Allows you to upload a patch upgrade file from a repository or your local disk. From the **Patch** drop-down list, choose the patch upgrade bundle.
- **Upload Now:** Allows you to choose or drag and drop a file from your local disk. You can upload only .tar files, and the maximum file size allowed is 4 GB.

Step 5 Click **Start Preparation**.

Cisco ISE validates all prerequisites for your selected workflow and generates a deployment report.

Cisco ISE checks these items during your patch upgrade process:

Precheck list	Description
Repository Validation	Checks whether repositories are configured for all nodes.
Patch Bundle Download	Checks whether the patch bundle is downloaded.
Deployment Validation	Checks whether the deployment node is in sync or in progress.
System Certificate Validation	Validates the system certificate for each node.
Admin Certificate Check in Trust Store	Checks whether the admin certificate is present in the trust store.
Services or Process Failures	Checks whether the service or application is running or in a failed state.
PAN Failover Validation	Checks whether high availability (HA) for PAN is disabled for your deployment.

If any check fails, resolve the issue and click **Refresh Failed Checks** to rerun it.

The report remains valid for three hours. Install your patch within this time.

Step 6 Click **Next** to proceed to the **Upgrade Nodes** page.

Step 7 Click **Start** in the **Upgrade Nodes** page.

In the **Upgrade Nodes** page, review the progress and status for each node.

You can monitor the upgrade progress of the primary node from the secondary node, and the upgrade progress of the secondary node from the primary node.

If you are using the CLI to install the patch, you cannot use this upgrade wizard to initiate or track the upgrade process.

Step 8 Click **Next** on the **Upgrade Nodes** page to check whether all the nodes are upgraded successfully.

After completing the upgrade, view and download the diagnostic upgrade reports for your deployment in the **Summary** page.

Step 9 Click **Finish** to close the wizard.

You can view and download upgrade summary reports with relevant details.

Patch upgrade using split upgrade option

Split upgrade is a multistep process that

- enables you to upgrade patches in your Cisco ISE deployment
- allows you to choose which Cisco ISE nodes to upgrade
- allows other services to remain available during the upgrade
- allows you to limit downtime by dividing nodes into batches and upgrading each batch sequentially
- supports a reliable upgrade, however, might take longer than a full upgrade.

Follow these steps to upgrade a patch using the Split upgrade option.

Step 1 In the Cisco ISE GUI, navigate to **Administration > System > Upgrade & Rollback**.

Step 2 In the **Upgrade & Rollback** page,

- click **Upgrade**
- click **Patch**
- click **Split**, and then
- click **Initialize**.

Step 3 Click **Let's Do It** in the **Welcome** page to start the upgrade workflow.

Step 4 In the **Select Nodes** page, check the check boxes next to the nodes to be upgraded in the current iteration.



Note

- The system selects Primary PAN by default in the first iteration of the patch upgrade. You can also select multiple PSN nodes and either the primary or secondary MnT node along with the Primary PAN. However, you cannot include the secondary PAN and both MnT nodes in the first iteration.
- If you select nodes other than the primary PAN in the first iteration, the process occurs in two batches. The system upgrades the primary PAN in the first batch, then upgrades the remaining selected nodes simultaneously.
- Select a maximum of 16 nodes per iteration during the split upgrade process.

Click **Next**.

Step 5 Under **How do you want to fetch Patch Bundle?**, choose one of these options:

- **Choose from Repository:** Allows you to upload a patch upgrade file from a repository or your local disk. From the **Patch** drop-down list, choose the patch upgrade bundle.
- **Upload Now:** Allows you to choose or drag and drop a file from your local disk. You can upload only .tar files and the maximum file size allowed is 4 GB.

Step 6 Click **Start Preparation**.

Cisco ISE validates all the prerequisites and generates a report for your deployment.

Cisco ISE checks these during the upgrade process:

Precheck List	Description
Repository Validation	Checks whether a repository is configured for all the nodes.
Patch Bundle Download	Checks whether the patch bundle is downloaded.

Precheck List	Description
Deployment Validation	Checks the state of the deployment node—whether it is in sync or in progress.
Admin Certificate Check in Trust Store	Checks whether the admin certificate is present in the trust store.
System Certificate Validation	Checks the system certificate validation for each node.
Services or Process Failures	Checks the state of the service or application (whether it is running or in failed state).
PAN Failover Validation	Checks whether PAN HA is disabled or not for the deployment.

Click the **Expand to Show** icon to check additional information about each node and its status.

Click the **Information** icon to check more information about each component.

The generated report is valid for three hours. You must install your patch within that period.

During the first iteration, the system runs local prechecks (**Repository Validation**, **Bundle Download**, **System Certificate Validation**, and **Services or Process Failures**) on all the nodes. In later iterations, these checks run only on the selected nodes.

Step 7 If any of the checks failed, resolve the issues, and click **Refresh Failed Checks** to rerun the checks. Click **Next**.

Step 8 Click **Start** in the **Upgrade Nodes** page.

In the **Upgrade Nodes** page, you can check the overall upgrade progress and the status for each node in your deployment.

You can monitor the upgrade progress of the primary PAN from the secondary PAN, or monitor the secondary PAN from the primary PAN.

If you install the patch using the CLI, you cannot initiate or track the upgrade process with this wizard.

Step 9 Click **Next** in the **Upgrade Nodes** page to check whether all the nodes are upgraded successfully. Click **Finish**.

The system redirects you to the **Node Selection** page, where you can select nodes for the next iteration.

After completing the upgrade process, you can view and download diagnostic upgrade reports for your deployment on the **Summary** page.

Verify patch installation

It is mandatory to ensure that the patch is installed on all nodes within your deployment. Inconsistent patch levels across nodes can cause severe system instability, including replication failures and service disruptions. The upgrade process is not considered complete until every node reflects the correct patch version.

To verify that the patch is correctly installed on all nodes, follow these steps:

Step 1 In the Cisco ISE GUI, navigate to **Administration > System > Maintenance > Patch Management**.

Step 2 Locate the patch in the list and click the radio button next to it.

Step 3 Click **Show Node Status**.

Step 4 A dialog box will appear displaying the status of each node. Confirm that every node is listed as **Installed**.

If a node does not have the patch installed and shows the status as **Uninstalled**, follow the CLI patch installation process to install the patch on that node.

Roll back software patches

To roll back a patch, perform these steps:

- Step 1** In the Cisco ISE GUI, navigate to **Administration > System > Upgrade & Rollback**.
- Step 2** Click **Patch Rollback** to view the patch rollback version.
- Step 3** Click **Initialize**.
- Step 4** Click **Let's Do It** in the **Welcome** page to start the rollback workflow.
- Step 5** In the **Prerequisite Checks** page, click **Start Preparation**.
Cisco ISE validates all the prerequisites and generates a report for your deployment.
- Step 6** (Optional) Click **Download Report** to download the prerequisite checklist for your reference.
- Step 7** If any of the checks fail, rectify the issue, and click **Refresh Failed Checks** to rerun them. Click **Next**.
- Step 8** In the **Rollback Nodes** page, click **Start Rollback**.
The system rolls back all nodes in the deployment simultaneously, except the primary PAN. The primary PAN is rolled back after the other nodes finish.
You can view the overall rollback progress and the status of each node in the **Rollback Nodes** page.
Monitor the rollback progress from the secondary PAN while the primary PAN is rolling back. Then, monitor from the primary PAN while the secondary PAN is rolling back.
- Step 9** Click **Next**.
After the rollback process completes, view and download the diagnostic reports for your deployment from the **Summary** page.
Click **Finish** to exit the wizard.



Note

- If you have used the **Install** option in the **Administration > System > Maintenance > Patch Management** page for a Cisco ISE release 3.4 patch 1 upgrade, it is recommended to use **Rollback** option in the **Patch Management** page for rollback operations.
- Avoid using the **Patch Rollback** option in the **Upgrade & Rollback** page if the patch was installed using the **Install** option in **Patch Management**.
- If you have used either the **Full Upgrade** or **Split Upgrade** option in the **Upgrade & Rollback** page, you should use the **Patch Rollback** in the same **Upgrade & Rollback** page for rolling back patches.
- This distinction ensures proper rollback procedures depending on the method used for the patch upgrade, maintaining deployment stability and consistency.