



Upgrade a Cisco ISE Deployment from the GUI

- [Upgrade a Cisco ISE Deployment from the GUI, on page 1](#)

Upgrade a Cisco ISE Deployment from the GUI

Cisco ISE offers a GUI-based centralized upgrade from the Admin portal. The upgrade process is much simplified, and the progress of the upgrade and the status of the nodes are displayed on the screen.

The Upgrade Overview page lists all the nodes in your deployment, the personas that are enabled on them, the version of ISE installed, and the status (indicates whether a node is active or inactive) of the node. You can begin upgrade only if the nodes are in the Active state.



Note The GUI-based upgrade from the Admin portal is supported only if you are currently on Release 2.0 or later and want to upgrade to Release 2.0.1 or later. If you want to upgrade directly from Release 1.4 to Release 2.2, you can do so from the Cisco ISE CLI. See [Upgrade a Cisco ISE Deployment from the CLI](#) for more information.

Different Types of Deployment

- Standalone Node—A single Cisco ISE node assuming the Administration, Policy Service, and Monitoring persona.
- Multi-Node Deployment—A distributed deployment with several ISE nodes. The procedure to upgrade a distributed deployment is discussed in the following listed references.

[ISE Community Resource](#)

For information on how to assess the network for ISE deployment readiness, see [ISE Deployment Assistant \(IDA\)](#).

Upgrade From Release 2.0 , 2.0.1 or 2.1 to Release 2.2

You can upgrade all the nodes in a Cisco ISE deployment from the Admin portal.



Note The GUI-based upgrade is applicable only if you are upgrading from Release 2.0 or later to a higher release or if you are upgrading a Limited Availability Release of Cisco ISE 2.0 or later to the General Availability Release.

Before you begin

Ensure that you have performed the following tasks before you upgrade:

- Obtain a backup of the ISE configuration and operational data.
- Obtain a backup of the system logs.
- Disable scheduled backups. Reconfigure the backup schedules after deployment upgrade is complete.
- Export the certificates and private keys.
- Configure a repository. Download the upgrade bundle and place it in the repository.
- Make a note of Active Directory join credentials and RSA SecurID node secret, if applicable. You need this information to connect to Active Directory or RSA SecurID server after upgrade.
- Purge the operational data to improve upgrade performance.

Step 1 Click the **Upgrade** tab in the Admin portal.

Step 2 Click **Proceed**.

The **Review Checklist** window appears. Read the given instructions carefully.

Step 3 Check the **I have reviewed the checklist** check box, and click **Continue**.

The **Download Bundle to Nodes** window appears.

Step 4 Download the upgrade bundle from the repository to the nodes:

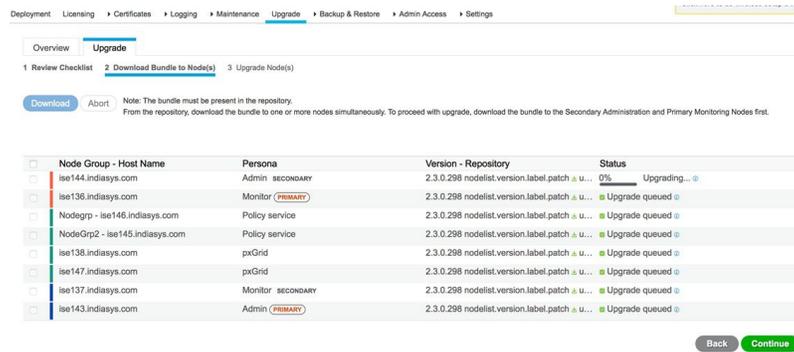
- a) Check the check box next to the nodes to which you want to download the upgrade bundle.
- b) Click **Download**.

The **Select Repository and Bundle** window appears.

- c) Select the repository.

You can select the same repository or different repositories on different nodes, but you must select the same upgrade bundle on all the nodes.

Figure 1: Upgrade Window Showing the Repositories Selected for Each Node



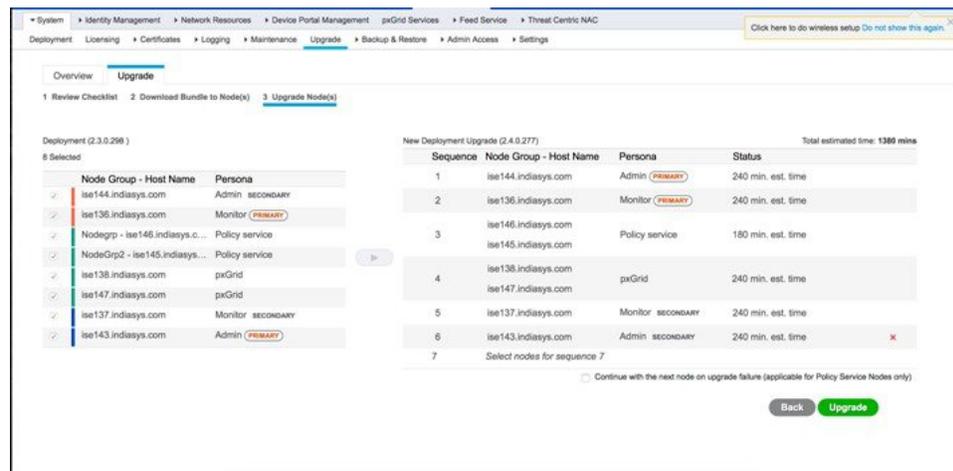
- d) Check the check box next to the bundle that you want to use for the upgrade.
- e) Click **Confirm**.

Once the bundle is downloaded to the node, the node status changes to **Ready for Upgrade**.

Step 5 Click **Continue**.

The **Upgrade Nodes** window appears.

Figure 2: Upgrade Window Showing the Current Deployment and the New Deployment



Step 6 Choose the upgrade sequence.

When you move a node to the new deployment, a time estimate for the upgrade is displayed on the **Upgrade Nodes** window. You can use this information to plan for upgrade and minimize downtime. Use the sequence given below if you have a pair of Administration and Monitoring Nodes, and several Policy Service Nodes.

- a) By default, the Secondary Administration Node is listed first in the upgrade sequence. After upgrade, this node becomes the Primary Administration Node in the new deployment.
- b) The Primary Monitoring Node is the next one in the sequence to be upgraded to the new deployment.
- c) Select the Policy Service Nodes and move them to the new deployment. You can alter the sequence in which the Policy Service Nodes are upgraded.

You can upgrade the Policy Service Nodes in sequence or in parallel. You can select a set of Policy Service Nodes and upgrade them in parallel.

- d) Select the Secondary Monitoring Node and move it to the new deployment.
- e) Finally, select the Primary Administration Node and move it to the new deployment.

If the Administration Nodes also assume the Monitoring persona, then follow the sequence given in the table below:

Node Personas In The Current Deployment	Upgrade Sequence
Secondary Administration/Primary Monitoring Node, Policy Service Nodes, Primary Administration/Secondary Monitoring Node	<ol style="list-style-type: none"> 1. Secondary Administration/Primary Monitoring Node 2. Policy Service Nodes 3. Primary Administration/Secondary Monitoring Node
Secondary Administration/Secondary Monitoring Node, Policy Service Nodes, Primary Administration/Primary Monitoring Node	<ol style="list-style-type: none"> 1. Secondary Administration/Secondary Monitoring Node 2. Policy Service Nodes 3. Primary Administration/Primary Monitoring Node
Secondary Administration Node, Primary Monitoring Node, Policy Service Nodes, Primary Administration/Secondary Monitoring Node	<ol style="list-style-type: none"> 1. Secondary Administration Node 2. Primary Monitoring Node 3. Policy Service Nodes 4. Primary Administration/Secondary Monitoring Node
Secondary Administration Node, Secondary Monitoring Node, Policy Service Nodes, Primary Administration/Primary Monitoring Node	<ol style="list-style-type: none"> 1. Secondary Administration Node 2. Secondary Monitoring Node 3. Policy Service Nodes 4. Primary Administration/Primary Monitoring Node
Secondary Administration/Primary Monitoring Node, Policy Service Nodes, Secondary Monitoring Node, Primary Administration Node	<ol style="list-style-type: none"> 1. Secondary Administration/Primary Monitoring Node 2. Policy Service Nodes 3. Secondary Monitoring Node 4. Primary Administration Node
Secondary Administration/Secondary Monitoring Node, Policy Service Nodes, Primary Monitoring Node, Primary Administration Node	<ol style="list-style-type: none"> 1. Secondary Administration/Secondary Monitoring Node 2. Policy Service Nodes 3. Primary Monitoring Node 4. Primary Administration Node

Step 7 Check the **Continue with upgrade on failure** check box if you want to continue with the upgrade even if the upgrade fails on any of the Policy Service Nodes in the upgrade sequence.

This option is not applicable for the Secondary Administration Node and the Primary Monitoring Node. If any one of these nodes fail, the upgrade process is rolled back. If any of the Policy Service Nodes fail, the Secondary Monitoring Node and the Primary Administration Node are not upgraded and remain in the old deployment.

Step 8 Click **Upgrade** to begin the deployment upgrade.

Figure 3: Upgrade Window Showing the Upgrade Progress

The screenshot shows the 'Upgrade' window in the Cisco ISE GUI. The navigation path is: Deployment > Licensing > Certificates > Logging > Maintenance > Upgrade > Backup & Restore > Admin Access > Settings. The current step is '3 Upgrade Node(s)'. There are 8 selected nodes for deployment (2.3.0.298). The nodes are listed in a table with columns for Node Group, Host Name, Persona, and Status. The status for the first node is 'Upgrading...' at 5%. A tooltip for the first node shows 'STEP 3: Validating data before upgrade...'. The total estimated time is 1140 mins. The table below shows the details of the nodes being upgraded.

Sequence	Node Group - Host Name	Persona	Status
1	ise144.indiasys.com	Admin (PRIMARY)	Upgrading... 5%
2	ise136.indiasys.com	Monitor (PRIMARY)	Upgrade queued
3	ise146.indiasys.com ise145.indiasys.com	Policy service	Upgrade queued
4	ise138.indiasys.com ise147.indiasys.com	pxGrid	Upgrade queued
5	ise137.indiasys.com	Monitor (SECONDARY)	Upgrade queued
6	ise143.indiasys.com	Admin (SECONDARY)	Upgrade queued
7	Select nodes for sequence 7		

The upgrade progress is displayed for each node. On successful completion, the node status changes to **Upgrade Complete**.

Note When you upgrade a node from the Admin portal, if the status does not change for a long time (and remains at 80%), you can check the upgrade logs from the CLI or the status of the upgrade from the console. Log in to the CLI or view the console of the Cisco ISE node to view the progress of upgrade. You can use the **show logging application** command to view the *upgrade-uibackend-cliconsole.log* and *upgrade-postosupgrade-yyyyymmdd-xxxxxx.log*.

Note If the posture data update process is running on the Primary Administration Node in the new deployment, you cannot register a node to the Primary Administration Node. You can either wait till the posture update process is over (which might take approximately 20 minutes) or disable the posture auto-update feature from the **Administration > System > Settings > Posture > Updates** page while upgrading or registering a node to the new deployment.

Troubleshoot Upgrade Failures

Upgrade Bundle Download Via the GUI Times Out

Before the upgrade, when you download the upgrade bundle from the repository to the node, the download times out if it takes more than 35 minutes to complete. This issue occurs because of poor bandwidth connection.

Workaround: Ensure that you have a good bandwidth connection with the repository.

Generic Upgrade Error

The following generic upgrade error appears:

```
error: % Warning: The node has been reverted back to its pre-upgrade
state.
```

Workaround: Click the **Details** link. Address the issues that are listed in the Upgrade Failure Details. After you fix all the issues, click **Upgrade** to reinitiate the upgrade.

Upgrade is in Blocked State

When the node status says that “Upgrade cannot begin...,” the upgrade is in a blocked state. This issue might occur when all the nodes in the deployment are not on the same Cisco ISE version and patch version.

Workaround: Bring all the nodes in the deployment to the same Cisco ISE version and patch version (upgrade or downgrade, or install or roll back a patch) before you begin your upgrade.

No Secondary Administration Node in the Deployment

Cisco ISE upgrade requires a Secondary Administration Node in the deployment. You cannot proceed with upgrade unless you have a Secondary Administration persona enabled on any of the nodes in your deployment. This error occurs when:

- There is no Secondary Administration Node in the deployment.
- The Secondary Administration Node is down.
- The Secondary Administration Node is upgraded and moved to the upgraded deployment. You might encounter this issue when you click the Refresh Deployment Details button after the Secondary Administration Node is upgraded.

Workaround:

- If the deployment does not have a Secondary Administration Node, enable the Secondary Administration persona on one of nodes in the deployment and retry upgrade.
- If the Secondary Administration Node is down, bring up the node and retry upgrade.
- If the Secondary Administration Node is upgraded and moved to the upgraded deployment, then manually upgrade the other nodes in the deployment from the Command-Line Interface (CLI).

Upgrade Times Out

The ISE node upgrade times out with the following message:

```
Upgrade timed out after minutes: x
```

Workaround: If you see this error message in the GUI, log in to the CLI of the Cisco ISE node and verify the status of the upgrade. This error message could either indicate a real issue with the upgrade process or could be a false alarm.

- If the upgrade was successful and:
 - The node on which you see this error message is the Secondary Administration Node from the old deployment, then you must upgrade the rest of the nodes from the CLI.



Note If you remove the Secondary Administration Node from the Upgrade page in the Admin portal, you cannot continue with the upgrade from the GUI. Hence, we recommend that you continue the upgrade from the CLI for the rest of the nodes.

- The node on which you see this error message is a non-Secondary Administration Node, remove that node from the Upgrade page in the Admin portal and continue to upgrade the rest of the nodes from the GUI.

- If the upgrade process fails, follow the instructions on the screen to proceed with your upgrade.

Upgrade Fails During Registration on the Primary Administration Node in the Old Deployment

If upgrade fails during registration on the Primary Administration Node (the last node from the old deployment to be upgraded), the upgrade is rolled back and the node becomes a standalone node.

Workaround: From the CLI, upgrade the node as a standalone node to Release 2.2. Register the node to the new deployment as a Secondary Administration Node.

