Cisco ISE 2.4 Upgrade Guide: Upgrade Method

First Published: 2022-04-01

Upgrade Sequence of the Nodes

You can upgrade Cisco ISE using GUI, Backup and Restore, or CLI. In case you are using GUI to upgrade you can choose the order of nodes to be upgraded. However, we recommend that you follow the below provided order of the nodes for upgarding your deployment. This will help you to reduce downtime while providing maximum resiliency and ability to roll back.

1. Backup all configuration and monitoring data. This task should be done before initiating upgrade in order to ensure that you can easily roll back manually, if necessary.
2. Secondary Administration Node

   At this point, the Primary Administration Node remains at the previous version and can be used for rollback if the upgrade fails.
3. Primary Monitoring Node or Secondary Monitoring Node

   If you have a distributed deployment, upgrade all the nodes that are available in the site that has Secondary Administration Node of your existing Cisco ISE deployment.
4. Policy Service Nodes

   After you upgrade a set of Policy Service nodes, verify whether the upgrade is successful (see Verify the Upgrade Process, on page 18) and run the necessary network tests to ensure that the new deployment is functioning as expected. If the upgrade is successful, you can upgrade the next set of Policy Service nodes.
5. Secondary Monitoring Node or Primary Monitoring Node
6. Primary Administration Node

   Rerun the upgrade verification and network tests after you upgrade the Primary Administration Node.

Note If upgrade fails during the registration of the Primary Administration node (the last node from the old deployment that has to be upgraded), the upgrade is rolled back and the node becomes a standalone node. From the CLI, upgrade the node as a standalone node. Register the node to the new deployment as a Secondary Administration node.

After the upgrade, the Secondary Administration Node becomes the Primary Administration Node, and the original Primary Administration Node becomes the Secondary Administration Node. In the Edit Node window, click Promote to Primary to promote the Secondary Administration Node as the Primary Administration Node (as in your old deployment), if necessary.

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	**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	**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	**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	**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	**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	**1.** Secondary Administration/Secondary Monitoring Node **2.** Policy Service Nodes **3.** Primary Monitoring Node **4.** Primary Administration Node

You will get a error message **No Secondary Administration Node in the Deployment** under the following circumstances:

- 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. Typically, this occurs when you use the **Refresh Deployment Details** option after the Secondary Administration node is upgraded.

To resolve this issue, perform one of the tasks, as applicable:

- If the deployment does not have a Secondary Administration node, configure a Secondary Administration node 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, use the CLI to manually upgrade the other nodes in the deployment.

Choose your Upgrade Method

This release of Cisco ISE supports the following upgrade processes. You can choose from the below upgrade processes depending on your technical expertise and time availability for the upgrade.

- Upgrade Cisco ISE using Backup and Restore Procedure (Recommended)
- Upgrade a Cisco ISE deployment from GUI
- Upgrade a Cisco ISE deployment from CLI

Table 1: Cisco ISE Upgrade Method Comparison

Comparison Factors	Backup and Restore (Recommended)	Upgrade using the GUI	Upgrade using CLI
Comparison Synopsis	Fast but more administration required	Long but less administration required	Longer and more administration required
Difficulty	Hard	Easy	Moderate
Minimum Version	Cisco ISE 2.0 or later	Cisco ISE 2.0 or later	Cisco ISE 2.0 or later
VMs	If you have enough capacity, you can pre-stage the new VMs and join them immediately to the new PAN	Each PSN is upgraded sequentially which increases the total upgrade time linearly	Each PSN is upgraded however they can be done in parallel to decrease total upgrade time
Time	Least upgrade downtime because PSNs are imaged with new version and not upgraded	Each PSN is upgraded sequentially which increases the total upgrade time linearly	Each PSN is upgraded however they can be done in parallel to decrease total upgrade time

Comparison Factors	Backup and Restore (Recommended)	Upgrade using the GUI	Upgrade using CLI
Personnel	Involvement of multiple stakeholders across business units to transit the configurational settings and operational logs.	Automated upgrade process with fewer manual interventions	Technical expertise on Cisco ISE.
Rollback	Requires reimaging of the nodes.	Easy rollback option.	Easy rollback option.

A detailed comparison of the upgrade methods is as follows:

Upgrade Cisco ISE using Backup and Restore Method

Re-imaging of the Cisco ISE node is done as a part the initial deployment and during troubleshooting, however you can also re-image Cisco ISE node to upgrade a deployment while providing for restoration of the policy onto the new deployment once the new version is deployed.

In case the resources are limited, and new deployment is unable to spin up a parallel ISE node, Secondary PAN & MnT is removed from production deployment to be upgraded before upgrading the other nodes. Nodes are moved into the new deployment; a configuration & operational backup is restored from the previous deployment on respective nodes creating a parallel deployment. This allows to restore the policy sets, custom profiles, network access devices, and endpoints into the new deployment without need for manual intervention.

The advantages of upgrading Cisco ISE using Backup and Restore process are as follows:

- You can restore the configuration setting and the operational logs from the previous ISE deployment. Thus, preventing from data loss.
- You can manually choose the nodes that should be reused for the new deployment.
- You can upgrade multiple PSNs parallelly thus reducing the upgrade downtime.
- You can stage the nodes outside of maintenance windows, reducing the time of the upgrade during the production.

Things to consider before upgrading Cisco ISE using Backup and Restore

Resources Required: The backup and restore upgrade process requires additional resources which can be reserved for the ISE deployment before being released. In the case of reusing existing hardware, additional load will need to be balanced to nodes which remain online. Hence, you need to evaluate the current load and latency limits before the deployment begins in order to ensure that the deployment can handle an increase in number of users per node.

Personnel Required: You will require involvement from multiple business units including network administration, security administration, data centre, and virtualization resources to perform upgrade. In addition, you will need to re-join the node to the new deployment, restore certificates, re-join to active directory, and wait for policy synchronization. This can lead to multiple reloads and requires timeframe that of a net-new deployment.

Rollback Mechanism: Due to the re-imaging of the nodes, all information and configuration setting are erased from the previous deployment. Thus, the rollback mechanism for a backup and restore upgrade is the same procedure as re-imaging of the nodes for the second time.

Best Practice for the Backup and Restore Upgrade Process:

- Create an standalone environment or dedicate load balancers to switch Virtual IP address for RADIUS requests.
- You can start the deployment process well before the maintenance window and point the user load balancer to the new deployment.

Upgrade a Cisco ISE deployment from GUI

You can also upgrade Cisco ISE from the GUI in a single click with some customizable options. A GUI upgrade is executed from the **ISE Administration** > **Upgrade** menu and requires a new repository to download the ISO image.

During the upgrade the Secondary PAN is moved into an upgraded deployment automatically and is upgraded first, followed by Primary MnT. As a result, if either of these upgrades fail, it is mandatory that the node will be rolled back to the previous version and re-join to the previous ISE deployment. Later PSN's are moved one by one to the new deployment and upgraded. In case of an upgrade failure, you can also choose to continue or cease the upgrade. This will result in a dual-version of same Cisco ISE deployment, allowing for troubleshooting to occur before the upgrade continues. Once all PSN's are upgraded, the Secondary MnT and Primary PAN is upgraded and joined to the new Cisco ISE deployment.

Given that this upgarde process requires limited technical expertise, a single administrator start the upgrade and assign NOC or SOC engineers to monitor and report the upgrade status or open a TAC case.

The advantages of upgrading Cisco ISE from the GUI are as follows:

- The upgrade is automated with minimal intervention.
- You can choose the upgrade order of the PSNs to ensure continuity whenever possible, especially when redundancy available between data centres.
- A single administrator can execute the upgrade without any additional personnel, third party hypervisors or network access devices.

Things to consider before upgrading Cisco ISE from GUI

Continuation in Failure Scenarios: In case of an upgrade failure, you can also choose to continue or cease the upgrade. This will result in a dual-version of same Cisco ISE deployment, allowing for troubleshooting to occur before the upgrade continues. While the Cisco Upgrade Readiness Tool should indicate any incompatibilities or misconfigurations, if the Proceed field is checked, additional errors may be encountered if due diligence was not acted upon before the upgrade.

Rollback Mechanism: If an upgrade fails on a PAN or MnT node, the nodes are automatically rolled back. However, if a PSN fails to upgrade, the nodes remain on the same Cisco ISE version and can be fixed while impairing redundancy. Cisco ISE is still operational during this time, and therefore rollback abilities are limited without re-imaging.

Time Required: Each PSN takes around 90-120 minutes to upgrade, hence if you have a large number PSNs it takes time to upgrade all of them.

Best Practice for the Upgrade from GUI: If you have a larger number of PSNs, group the PSNs in batches and perform the upgrade.

Upgrade a Cisco ISE deployment from CLI

Upgrading Cisco ISE from the CLI is an elaborate process and requires the administrator to download the upgrade image to the local node, execute the upgrade, and monitor each node individually throughout the upgrade process. While the upgrade sequence is similar in nature to that of the GUI upgrade, this approach operationally intensive from a monitoring and actions point of view.

Upgrading from CLI is recommended for troubleshooting purposes only due to the level of effort required.

The advantages of upgrading Cisco ISE from the CLI are as follows:

- CLI presents additional logging messages to the administrator while the upgrade is performed.
- The nodes which are upgraded can be chosen with more control and upgraded in parallel. Nodes that are not being upgraded can handle additional load as endpoints are rebalanced across the deployment.
- Rolling back at the CLI is much easier due to the ability to instruct scripts to undo previous changes.
- As the image resides on the node locally, copy errors between PAN and PSNs, if any, can be eliminated.

Things to consider before upgrading Cisco ISE from CLI

You need technical expertise and longer time to upgrade your Cisco ISE using CLI.

Upgrade Cisco ISE Deployment Using Backup and Restore Method (Recommended)

Overview of the Backup and Restore Upgrade Method

We recommend backup and restore upgrade process over the other upgrade processes as it helps to reinstate your current Cisco ISE deployment node settings and prevent data loss, in case of any breakage during the upgrade process. This procedure starts by creating configuration and operational backups of the existing Cisco ISE deployment and then apply them to the new deployment.

Best Practice for the Backup and Restore Upgrade Process:

- Create a standalone environment or dedicate load balancers to switch Virtual IP address for RADIUS requests.
- You can start the deployment process well before the maintenance window and point the user load balancer to the new deployment.
- If you use RSA-based authentication to back up and restore, you must generate RSA configuration for all the PSNs in the deployment whenever you add a new PSN.

Note To avoid generating a new RSA configuration every time you add a new PSN, you must know the IP address of all the nodes that you are going to add to the deployment before starting the backup and restore process. Then, you must generate the RSA configuration file using all the IP addresses and upload it to the PAN UI.

Procedure:

1. Create a configuration file in an RSA console with all the IP address of all the nodes including the nodes that are not in the deployment.

2. Import the new configuration file to the PAN UI.

Note You must clear the node secret on the RSA server before uploading the new RSA configuration file. This helps to create a new node secret and share it between ISE and RSA server.

Now you can add a new node to the deployment without generating a new configuration file as it is replicated as part of the configuration using the IP addresses that are already present in the imported configuration file.

The following is a broad overview of the steps involved in the Backup and Restore Upgrade method:

1. Deregister a Node

In order to remove a node from the deployment, you need to derigister the node. For more information about node deregistration or removal, see the "Remove a Node from Deployment" section in Cisco Identity Services Engine Administrator Guide.

2. Reimage a Node

In order to reimage a node, you need to freshly install the node in the Cisco ISE deployment. For more information about Cisco ISE installation, see the "Install Cisco ISE " chapter in the Cisco Identity Services Engine Installation Guide.

We recommend that you apply the latest patch of newly installed Cisco ISE Release.

3. Backup and Restore the Configuration or Operational Database

For more information about the backup and restore operations, see the "Backup and Restore Operations" section in Cisco Identity Services Engine Administrator Guide.

4. Assign Primary or Secondary Roles to a Node.

You can assign primary or secondary role to a node as per your requirement.

For more information about how to assign a role to a Policy Administartion Node (PAN), see the "Manually Promote Secondary PAN To Primary" section in the Cisco Identity Services Engine Administrator Guide.

For more information about how to assign a role to a Monitoring and Troubleshooting (MnT) node, see the "Manually Modify MnT Role" section in Cisco Identity Services Engine Administrator Guide.

5. Join the Policy Service Nodes

In order to join a Policy Service Node (PSN) to the new deployment, you need to register the node as PSN. For more information about registering or joining a PSN, see the "Register a Secondary Cisco ISE Node" in Cisco Identity Services Engine Administrator Guide.

6. Import Certificates

You need to import the system certificates to the newly deployed nodes in the Cisco ISE. For more information about how to import system certficates to a Cisco ISE node, see the "Import a System Certificate" section in Cisco Identity Services Engine Administrator Guide .

Backup and Restore Upgrade Process

This section describes the upgrade process using the recommended Backup and Restore Upgrade method.

If you are currently using Cisco ISE, Release 2.0 or later, you can directly upgrade to Cisco ISE, Release 2.4.

- Upgrade Secondary PAN and MnT Nodes to Cisco ISE, Release 2.4
- Join Policy Service Nodes to Cisco ISE, Release 2.4
- Upgrade Primary PAN and MnT to Cisco ISE, Release 2.4

In case you are using a Cisco ISE version that is not compatible to Cisco ISE Release 2.4, you need to first upgrade to an intermediate version, compatible to Cisco ISE, Release 2.4. And then you can upgrade from the intermediate version to Cisco ISE, Release 2.4. Follow the below steps to upgrade to an intermediate Cisco ISE version.

Upgrade Secondary PAN and Secondary MnT Nodes to Cisco ISE, Release 2.0, 2.1, 2.2 or 2.3

Before you begin

Restore backup from your existing Cisco ISE to intermediate Cisco ISE Release.

Procedure

Step 1 De-register Secondary PAN node.

Step 2 Re-image the deregistered Secondary PAN node to the intermediate Cisco ISE Release, as a standalone node. After the upgrade, make this node the Primary Administration Node in the new deployment.

Step 3 Restore Cisco ISE configuration from the backup data.

Step 4 De-register Secondary MnT node.

Step 5 Re-image the deregistered Secondary MnT node to the intermediate Cisco ISE Release, as a standalone node.

Step 6 Assign Primary role to this Mnt node and restore the operational backup from the backup repository. This is an optional step and needs to performed only if you need to report of the older logs

Step 7 Import ise-https-admin CA certificates from your original Cisco ISE backup repository.

Upgrade Secondary PAN and MnT Nodes to Cisco ISE, Release 2.4

Procedure

Step 1 Take a backup of Cisco ISE configuration settings and operational logs.

Step 2 De-register Secondary PAN node.

Step 3 Re-image the deregistered secondary PAN node to Cisco ISE, Release 2.4.

Step 4 Restore ISE configuration from the backup data and make this node as the Primary Node for your new deployment.

Step 5 Import ise-https-admin CA certificates from Secondary PAN unless you are using wild card certificates.

Step 6 De-register Secondary MnT node.

Step 7 Re-Image the deregistered Secondary MnT node to Cisco ISE, Release 2.4.

Step 8 Restore your current ISE operational backup and join node as Primary MnT for new deployment. This is an optional step and needs to performed only if you need to report of the older logs.

Join Policy Service Nodes to Cisco ISE, Release 2.4

In case you have Cisco ISE nodes deployed in multiple sites, join the PSNs available in the site (that has Secondary PAN and MnT nodes) first and then join the PSNs available in the other sites followed by the PSNs available at the site (that has Primary PAN and MnT nodes of your existing Cisco ISE).

Procedure

Step 1 De-register PSNs.

Step 2 Reimage PSN to Cisco ISE, Release 2.4 latest patch and join PSN to new Cisco ISE, Release 2.4 deployment.

What to do next

We recommend that you test your partially upgraded deployment at this point. You can do so by checking if logs are present and the upgraded nodes funtion as expected.

Upgrade Primary PAN and MnT to Cisco ISE, Release 2.4

Procedure

Step 1 Reimage Primary MnT node and join as Secondary MnT to new deployment.

In case you want to preserve the data for reporting, restore a copy of the operational backup to the Secondary MnT node.

Step 2 Reimage Primary PAN node and join as Secondary PAN to new deployment.

Upgrade a Cisco ISE Deployment from the GUI

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.

Choose **Adminstration** > **System** > **Upgrade** > **Overview** menu option 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.

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.

Upgrade From Release 2.0 , 2.0.1, 2.1, 2.2 or 2.3 to Release 2.4

You can upgrade all the nodes in a Cisco ISE deployment using the Admin portal from Release 2.0 onwards, you can also upgrade a Limited Availability Release of Cisco ISE 2.0 or later to the General Availability Release.

Before you begin

Ensure that you have read the instructions in the section.

Note If you are upgrading a Cisco ISE STANDALONE node or have de-registered a node from an existing deployment and wish to run a STANDALONE upgrade, then prior to starting the upgrade, there is a need to remove all the upgradedb_*.properties files located in the path : "/opt/oracle/base/admin/cpm10/dpdump".

Please contact Cisco TAC for deleting the above mentioned files, as root privilege is required to remove them. See CSCvi87302 for details.

The above workaround is required only if the upgrade file (ise-upgradebundle-2.0.x-2.3.x-to-2.4.0.357.SPA.x86_64.tar.gz) is downloaded before April 13, 2018.

Procedure

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

Step 2

Step 3 Click **Proceed**.

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

Step 4 Check the **I have reviewed the checklist** check box, and click **Continue**.

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

Step 5 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.

d) Check the check box next to the bundle that you want to use for the upgrade.

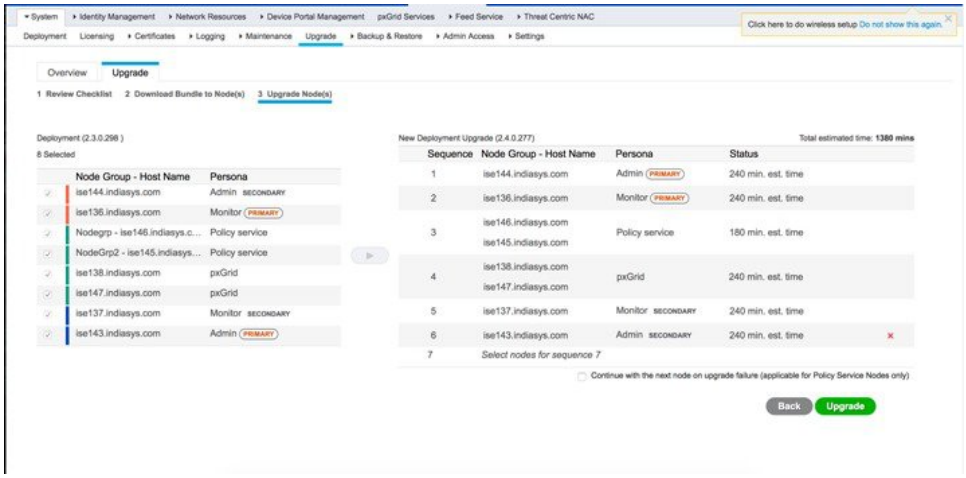
e) Click **Confirm**.

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

Step 6 Click **Continue**.

The **Upgrade Nodes** window appears.

Figure 1: Upgrade Window Showing the Current Deployment and the New Deployment



Step 7 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.

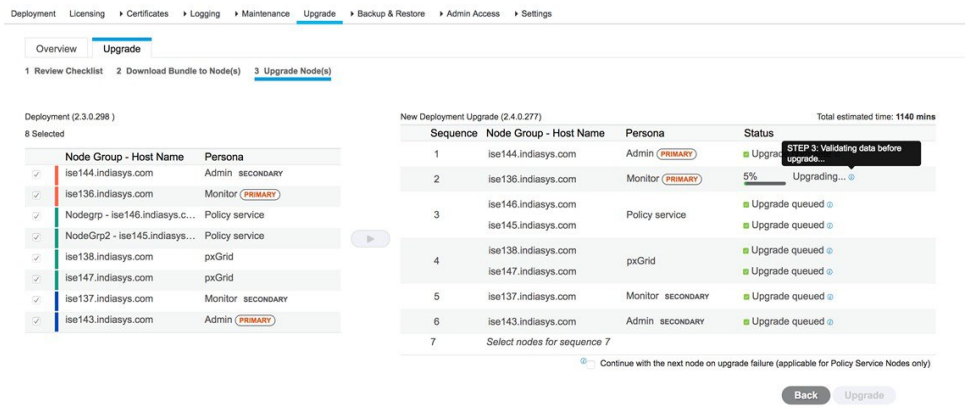
d) Select the Secondary Monitoring Node and move it to the new deployment.
e) Finally, select the Primary Administration Node and move it to the new deployment.

Step 8 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 9 Click **Upgrade** to begin the deployment upgrade.

Figure 2: Upgrade Window Showing the Upgrade Progress



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-yyyymmdd-xxxxxx.log*.

You can view the following upgrade logs from the CLI using the show logging application command:

- DB Data Upgrade Log
- DB Schema Log
- Post OS Upgrade Log

In case you get a warning message: **The node has been reverted back to its pre-upgrade state**, go to the **Upgrade** window, click the **Details** link. Address the issues that are listed in the **Upgrade Failure Details** window. After you fix all the issues, click **Upgrade** to reinitiate the upgrade.

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 **Updates** window while upgrading or registering a node to the new deployment. The navigation path for this window is **Administration** > **System** > **Settings** > **Posture** > **Updates**.

Upgrade a Cisco ISE Deployment from the CLI

The upgrade process using CLI depends on the deployment type.

Note If you are upgrading a Cisco ISE standalone node or have de-registered a node from an existing deployment and wish to run a standalone upgrade, then before starting the upgrade, you must first remove all the upgradedb_*.properties files located in the path: "/opt/oracle/base/admin/cpm10/dpdump".

Because root privileges are required to remove these files, you should contact Cisco TAC in order to delete them. See CSCvi87302 for details.

This workaround is required only if the upgrade file (ise-upgradebundle-2.0.x-2.3.x-to-2.4.0.357.SPA.x86_64.tar.gz) is downloaded before April 13, 2018.

Upgrade a Standalone Node

You can use the **application upgrade <upgrade bundle name> <repository name>** command directly, or the **application upgrade prepare <upgrade bundle name> <repository name>** and **application upgrade proceed** commands in the specified sequence to upgrade a standalone node.

You can run the **application upgrade <upgrade bundle name> <repository name>** command from the CLI on a standalone node that assumes the Administration, Policy Service, pxGrid, and Monitoring personas. If you choose to run this command directly, we recommend that you copy the upgrade bundle from the remote repository to the Cisco ISE node's local disk before you run the command to save time during upgrade.

Alternatively, you can use the **application upgrade prepare <upgrade bundle name> <repository name>** and **application upgrade proceed** commands. The **application upgrade prepare <upgrade bundle name> <repository name>** command downloads the upgrade bundle and extracts it locally. This command copies the upgrade bundle from the remote repository to the Cisco ISE node's local disk. After you have prepared a node for upgrade, run the **application upgrade proceed** command to complete the upgrade successfully.

We recommend that you run the **application upgrade prepare <upgrade bundle name> <repository name>** and **application upgrade proceed** commands as described below.

Before you begin

Ensure that you have read the instructions in the section.

Procedure

Step 1 Create a repository on the local disk. For example, you can create a repository called "upgrade."

Example:

```
ise/admin# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# repository upgrade
ise/admin(config-Repository)# url disk:
% Warning: Repositories configured from CLI cannot be used from the ISE web UI and are not
 replicated to other ISE nodes.
If this repository is not created in the ISE web UI, it will be deleted when ISE services
restart.
ise/admin(config-Repository)# exit
ise/admin(config)# exit
```

Step 2 From the Cisco ISE command line interface (CLI), enter **application upgrade prepare <upgrade bundle name> <repository name>** command.

This command copies the upgrade bundle to the local repository "upgrade" that you created in the previous step and lists the MD5 and SHA256 checksum.

Example:

```
ise/admin# application upgrade prepare <upgrade bundle name> <repository
name>application upgrade prepare
ise-upgradebundle-2.0.x-2.1.x-2.2.x-2.3.x-to-2.4.0.x.SPA.x86_64.tar.gz upgrade

Getting bundle to local machine...
Unbundling Application Package...
Verifying Application Signature...

Application upgrade preparation successful
```

Step 3

Note After beginning the upgrade, you can view the progress of the upgrade by logging in via SSH and using the **show application status ise** command. The following message appears: % NOTICE: Identity Services Engine upgrade is in progress...

From the Cisco ISE CLI, enter the **application upgrade proceed** command.

Example:

```
ise/admin# application upgrade proceed
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
-Checking VM for minimum hardware requirements
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
-Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: Taking backup of the configuration data...
STEP 5: Running ISE configuration database schema upgrade...
- Running db sanity to check and fix if any index corruption
- Auto Upgrading Schema for UPS Model
- Upgrading Schema completed for UPS Model
ISE database schema upgrade completed.
% Warning: Sanity test found some indexes missing in CEPM schema. Please recreate missing
indexes after upgrade using app configure ise cli
STEP 6: Running ISE configuration data upgrade...
- Data upgrade step 1/30, UPSUpgradeHandler(2.4.0.101)... Done in 50 seconds.
- Data upgrade step 2/30, UPSUpgradeHandler(2.4.0.116)... Done in 0 seconds.
- Data upgrade step 3/30, MachineAuthenticationSettingsRegistration(2.4.0.120)... Done in
0 seconds.
- Data upgrade step 4/30, GuestAccessUpgradeService(2.4.0.126)... Done in 15 seconds.
- Data upgrade step 5/30, RegisterPostureTypes(2.4.0.127)... Done in 1 seconds.
- Data upgrade step 6/30, UPSUpgradeHandler(2.4.0.127)... Done in 0 seconds.
- Data upgrade step 7/30, UPSUpgradeHandler(2.4.0.134)... Done in 0 seconds.
- Data upgrade step 8/30, NSFUpgradeService(2.4.0.140)... Done in 0 seconds.
- Data upgrade step 9/30, NSFUpgradeService(2.4.0.155)... Done in 1 seconds.
- Data upgrade step 10/30, UPSUpgradeHandler(2.4.0.158)... Done in 1 seconds.
- Data upgrade step 11/30, NSFUpgradeService(2.4.0.160)... Done in 0 seconds.
- Data upgrade step 12/30, NSFUpgradeService(2.4.0.161)... Done in 0 seconds.
- Data upgrade step 13/30, NSFUpgradeService(2.4.0.179)... Done in 0 seconds.
- Data upgrade step 14/30, NetworkAccessUpgrade(2.4.0.182)... Done in 1 seconds.
- Data upgrade step 15/30, StorageUpgradeService(2.4.0.183)... Done in 0 seconds.
- Data upgrade step 16/30, DnsHostnameResolutionRegistration(2.4.0.190)... Done in 0 seconds.
- Data upgrade step 17/30, ProfilerUpgradeService(2.4.0.194)... ..Done in 131 seconds.
- Data upgrade step 18/30, CertMgmtUpgradeService(2.4.0.200)... ..Done in 167 seconds.
- Data upgrade step 19/30, NSFUpgradeService(2.4.0.214)... Done in 0 seconds.
- Data upgrade step 20/30, ERSDictionaryRegistration(2.4.0.215)... Done in 0 seconds.
- Data upgrade step 21/30, NetworkAccessUpgrade(2.4.0.216)... Done in 0 seconds.
- Data upgrade step 22/30, ProfilerUpgradeService(2.4.0.227)... Done in 0 seconds.
- Data upgrade step 23/30, ProfilerUpgradeService(2.4.0.228)... Done in 6 seconds.
```

```
- Data upgrade step 24/30, ProfilerUpgradeService(2.4.0.229)... Done in 0 seconds.
- Data upgrade step 25/30, NetworkAccessUpgrade(2.4.0.240)... Done in 0 seconds.
- Data upgrade step 26/30, CertMgmtUpgradeService(2.4.0.293)... Done in 7 seconds.
- Data upgrade step 27/30, ProvisioningUpgradeService(2.4.0.299)... Done in 0 seconds.
- Data upgrade step 28/30, NSFUpgradeService(2.4.0.336)... Done in 2 seconds.
- Data upgrade step 29/30, ProfilerUpgradeService(2.4.0.336)... Done in 0 seconds.
- Data upgrade step 30/30, GuestAccessUpgradeService(2.4.0.336)... Done in 26 seconds.
STEP 7: Running ISE configuration data upgrade for node specific data...
STEP 8: Running ISE M&T database upgrade...
M&T Log Processor is not running
ISE database M&T schema upgrade completed.
cat: /opt/oracle/base/admin/cpm10/dpdump/upgradedb*.properties: No such file or directory

Gathering Config schema(CEPM) stats .....
Gathering Operational schema(MNT) stats ....
% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS. During this time
 progress of the upgrade is visible on console. It could take up to 30 minutes for this to
 complete.
Rebooting to do Identity Service Engine upgrade...
```

The upgrade is now complete.

What to do next

Verify the Upgrade Process, on page 18

Upgrade a Two-Node Deployment

Use the **application upgrade prepare <upgrade bundle name> <repository name>** and **proceed** commands to upgrade a two-node deployment. You do not have to manually deregister the node and register it again. The upgrade software automatically deregisters the node and moves it to the new deployment. When you upgrade a two-node deployment, you should initially upgrade only the Secondary Administration Node(node B). When the secondary node upgrade is complete, you upgrade the primary node thereafter(node A). If you have a deployment set up as shown in the following figure, you can proceed with this upgrade procedure.

Before you begin

- Perform an on-demand backup (manually) of the configuration and operational data from the Primary Administration Node.
- Ensure that the Administration and Monitoring personas are enabled on both the nodes in the deployment.

  If the Administration persona is enabled only on the Primary Administration Node, enable the Administration persona on the secondary node because the upgrade process requires the Secondary Administration Node to be upgraded first.

  Alternatively, if there is only one Administration node in your two-node deployment, then deregister the secondary node. Both the nodes become standalone nodes. Upgrade both the nodes as standalone nodes and set up the deployment after the upgrade.
- If the Monitoring persona is enabled only on one of the nodes, ensure that you enable the Monitoring persona on the other node before you proceed.

Procedure

Step 1 Upgrade the secondary node (node B) from the CLI.

The upgrade process automatically removes Node B from the deployment and upgrades it. Node B becomes the upgraded primary node when it restarts.

Step 2 Upgrade node A.

The upgrade process automatically registers node A to the deployment and makes it the secondary node in the upgraded environment.

Step 3 Promote node A, now to be the primary node in the new deployment.

After the upgrade is complete, if the nodes contain old Monitoring logs, ensure that you run the **application configure ise** command and choose 5 (Refresh Database Statistics) on the nodes.

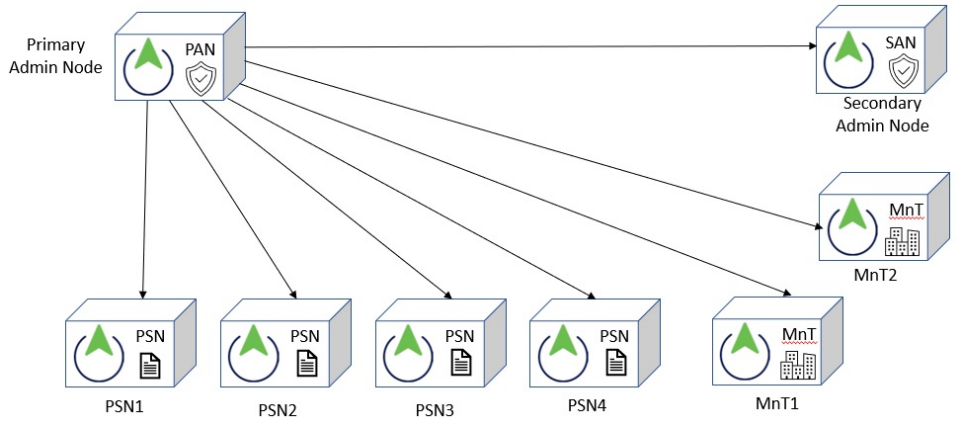
What to do next

Verify the Upgrade Process, on page 18

Upgrade a Distributed Deployment

You must first upgrade the Secondary Administration Node (SAN)to the new release. For example, if you have a deployment setup as shown in the following figure, with one Primary Administration Node (PAN), one Secondary Administration Node, four Policy Service Nodes (PSNs) , one Primary Monitoring Node (MnT1), and one Secondary Monitoring Node (MnT2), you can proceed with the following upgrade procedure.

Figure 3: Cisco ISE Deployment Before Upgrade



Note Do not manually deregister the node before an upgrade. Use the **application upgrade prepare <upgrade bundle name> <repository name>** and **proceed** commands to upgrade to the new release. The upgrade process deregisters the node automatically and moves it to the new deployment. If you manually deregister the node before an upgrade, ensure that you have the license file for the Primary Administration Node before beginning the upgrade process. If you do not have the file on hand (for example, if your license was installed by a Cisco partner vendor), contact the Cisco Technical Assistance Center for assistance.

Before you begin

- If you do not have a Secondary Administration Node in the deployment, configure a Policy Service Node to be the Secondary Administration Node before beginning the upgrade process.
- Ensure that you have read and complied with the instructions given in the section.
- When you upgrade a complete Cisco ISE deployment, Domain Name System (DNS) server resolution (both forward and reverse lookups) is mandatory; otherwise, the upgrade fails.

Procedure

Step 1 Upgrade the SAN from the CLI.

The upgrade process automatically deregisters SAN from the deployment and upgrades it. SAN becomes the primary node of the new deployment when it restarts. Because each deployment requires at least one Monitoring node, the upgrade process enables the Monitoring persona on SAN even if it was not enabled on this node in the old deployment. If the Policy Service persona was enabled on SAN in the old deployment, this configuration is retained after upgrading to the new deployment.

Step 2 Upgrade one of your Monitoring nodes (MnT1 and MnT2) to the new deployment.

We recommend that you upgrade your Primary Monitoring Node before the Secondary Monitoring Node (this is not possible if your Primary Administration Node in the old deployment functions as your Primary Monitoring Node as well). Your primary Monitoring node starts to collect the logs from the new deployment and you can view the details from the Primary Administration Node dashboard.

If you have only one Monitoring node in your old deployment, before you upgrade it, ensure that you enable the Monitoring persona on PAN, which is the Primary Administration Node in the old deployment. Node persona changes result in a Cisco ISE application restart. Wait for PAN to come up before you proceed. Upgrading the Monitoring node to the new deployment takes longer than the other nodes because operational data has to be moved to the new deployment.

If node B, the Primary Administration Node in the new deployment, did not have the Monitoring persona enabled in the old deployment, disable the Monitoring persona on it. Node persona changes result in a Cisco ISE application restart. Wait for the Primary Administration Node to come up before you proceed.

Step 3 Upgrade the Policy Service Nodes (PSNs) next. You can upgrade several PSNs in parallel, but if you upgrade all the PSNs concurrently, your network will experience a downtime.

After the upgrade, the PSNs are registered with the primary node of the new deployment SAN, and the data from the primary node is replicated to all the PSNs. The PSNs retain their personas, node group information, and profiling probe configurations.

Step 4 If you have a second Monitoring node in your old deployment, you must do the following:

a) Enable the Monitoring persona on PAN, which is the primary node in your old deployment.

A deployment requires at least one Monitoring node. Before you upgrade the second Monitoring node from the old deployment, enable this persona on the primary node itself. Node persona changes result in a Cisco ISE application restart. Wait for the primary ISE node to come up again.

b) Upgrade the Secondary Monitoring Node from the old deployment to the new deployment.

Except for the Primary Administration Node, you must have upgraded all the other nodes to the new deployment.

Step 5 Finally, upgrade the Primary Administration Node.

This node is upgraded and added to the new deployment as a Secondary Administration Node. You can promote the Secondary Administration Node to be the primary node in the new deployment.

After the upgrade is complete, if the Monitoring nodes that were upgraded contain old logs, ensure that you run the **application configure ise** command and choose 5 (Refresh Database Statistics) on the Monitoring nodes.

What to do next

Verify the Upgrade Process, on page 18

Verify the Upgrade Process

We recommend that you run some network tests to ensure that the deployment functions as expected and that users are able to authenticate and access resources on your network.

If an upgrade fails because of configuration database issues, the changes are rolled back automatically.

Procedure

Perform any of the following options in order to verify whether the upgrade was successful.

- Check the ade.log file for the upgrade process. To display the ade.log file, enter the following command from the Cisco ISE CLI: **show logging system ade/ADE.log**
- Enter the **show version** command to verify the build version.
- Enter the **show application status ise** command to verify that all the services are running.

Roll Back to the Previous Version of ISO Image

In rare cases, you might have to reimage the Cisco ISE appliance by using the previous version of ISO image and restoring the data from the backup file. After restoring the data, you can register with the old deployment, and enable the personas as done in the old deployment. Hence, we recommend that you back up the Cisco ISE configuration and monitoring data before you start the upgrade process.

Sometimes, upgrade failures that occur because of issues in the configuration and monitoring database are not rolled back automatically. When this occurs, you get a notification stating that the database is not rolled

back, along with an upgrade failure message. In such scenarios, you should manually reimage your system, install Cisco ISE, and restore the configuration data and monitoring data (if the Monitoring persona is enabled).

Before you attempt to rollback or recovery, generate a support bundle by using the **backup-logs** command, and place the support bundle in a remote repository.