Upgrade Methods for Different Types of Deployments

Review the following sections in this chapter for information on how to perform an upgrade on the following different types of deployments:

- Upgrade a Standalone Node, page 1
- Upgrade a Two-Node Deployment, page 3
- Upgrade a Distributed Deployment, page 4
- Verify the Upgrade Process, page 9

Upgrade a Standalone Node

You can use the `application upgrade` command directly, or the application upgrade `prepare` and `proceed` commands in sequence to upgrade a standalone node.

You can run the `application upgrade` 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 `application upgrade` command to save time during upgrade.

Alternatively, you can use the `application upgrade prepare` and `application upgrade proceed` commands. The `application upgrade prepare` 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` and `proceed` commands described below.

**Before You Begin**

Ensure that you have read the instructions in the Before You Upgrade chapter.

**Procedure**

**Step 1**

Create a repository on the local disk. For example, you can create a repository called "upgrade."
Example:
ise/admin# conf
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 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 ise-upgradebundle-1.4.0.253.x86_64.tar.gz upgrade
Getting bundle to local machine...
  md5: 35a159416afd0900c9da7b3dc6c72043
  sha256: e3358ca42d977af67f8bb2bb3574b3e559ce9578d2f36c44cd8ba9e6dddfedf
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y] ?

Step 3
Enter Y to continue.
The upgrade package is extracted. The following message appears.

Example:
Getting bundle to local machine...
  md5: 35a159416afd0900c9da7b3dc6c72043
  sha256: e3358ca42d977af67f8bb2bb3574b3e559ce9578d2f36c44cd8ba9e6dddfedf
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y] ?

Step 4
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.
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: Registering this node to primary of new deployment...
STEP 6: Downloading configuration data from primary of new deployment...
STEP 7: Importing configuration data...
STEP 8: Running ISE configuration data upgrade for node specific data...
STEP 9: Running ISE M&T DB upgrade...
ISE Database Mnt schema upgrade completed.

Gathering Config schema(CEPM) stats ......
Gathering Operational schema(MNT) stats ..........
% NOTICE: Upgrading ADEOS. Appliance will be rebooted after upgrade completes successfully.

% This application Install or Upgrade requires reboot, rebooting now...
The upgrade is now complete.
Upgrade a Two-Node Deployment

Use the application upgrade prepare 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 (node A). If you have a deployment set up as shown in the following figure, you can proceed with this upgrade procedure.

Figure 1: Cisco ISE Two-Node Administrative Deployment

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 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.

**Step 3** Promote node A 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 those nodes.

---

**What to Do Next**

Verify the Upgrade Process, on page 9

---

**Upgrade a Distributed Deployment**

You must first upgrade the Secondary Administration Node to the new release. For example, if you have a deployment setup as shown in the following figure, with one Primary Administration Node (node A), one Secondary Administration Node (node B), one Inline Posture Node (IPN) (node C), and four Policy Service Nodes (PSNs) (node D, node E, node F, and node G), one Primary Monitoring Node (node H), and one Secondary Monitoring Node (node I), you can proceed with the following upgrade procedure.

![Figure 2: Cisco ISE Deployment Before Upgrade](image)

---

**Note**

Do not manually deregister the node before an upgrade. Use the `application upgrade prepare` 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 (if your license was installed by a Cisco partner vendor, for example), contact the Cisco Technical Assistance Center for assistance.
To upgrade your deployment with minimum possible downtime while providing maximum resiliency and ability to roll back, the upgrade order should be as follows:

1. **Secondary Administration Node** (the Primary Administration Node at this point remains at the previous version and can be used for rollback, if upgrade fails.

2. **Primary Monitoring Node**

3. **Policy Service Nodes**

   At this point, verify if the upgrade is successful and also run the network tests to ensure that the new deployment functions as expected. See **Verify the Upgrade Process, on page 9** for more information. If the upgrade is successful, proceed to upgrade the following nodes:

4. **Secondary Monitoring Node**

5. **Primary Administration Node**

   Re-run the upgrade verification and network tests after you upgrade the Primary Administration Node.

**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 Before You Upgrade chapter.

- 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 Secondary Administration Node (node B) from the CLI.

The upgrade process automatically deregisters node B from the deployment and upgrades it. Node B 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 node B even if it was not enabled on this node in the old deployment. If the Policy Service persona was enabled on node B in the old deployment, this configuration is retained after upgrading to the new deployment.

**Step 2** Upgrade one of your Monitoring nodes (node H) 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 node A, which is the Primary Administration Node in the old deployment. Node persona changes result in a Cisco ISE application restart. Wait for node A 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 (nodes D, E, F, and G) next. You can upgrade several PSNs in parallel, but if you upgrade all the PSNs concurrently, your network will experience a downtime. If your PSN is part of a node group cluster, you must deregister the PSN from the PAN, upgrade it as a standalone node, and register it with the PAN in the new deployment.

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

Step 4 Deregister the IPN node (node C) from the Primary Administration Node.

Step 5 Register the IPN node (node C) to the Primary Administration Node (node B) of the new deployment.

Step 6 If you have a second Monitoring node (node I) in your old deployment, you must do the following:

   a) Enable the Monitoring persona on node A, 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 (node I) from the old deployment to the new deployment. Except for the Primary Administration Node (node A), you must have upgraded all the other nodes to the new deployment.

Step 7 Finally, upgrade the Primary Administration Node (node A). This node is upgraded and added to the new deployment as a Secondary Administration Node. You can promote the Secondary Administration Node (node A) 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.

Figure 3: Cisco ISE Deployment After Upgrade
CLI Transcripts of Successful Upgrades

Here is an example CLI transcript of a successful secondary Administration node upgrade.

```bash
ise74/admin# application upgrade proceed
Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
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: De-registering node from current deployment.
STEP 5: Taking backup of the configuration data...
STEP 6: Running ISE configuration DB schema upgrade...
- Running db sanity check to fix index corruption, if any...
ISE Database schema upgrade completed.
STEP 7: Running ISE configuration data upgrade...
- Data upgrade step 1/77, NSFUpgradeService(1.3.0.100) ... Done in 0 seconds.
- Data upgrade step 2/77, RegisterPostureTypes(1.3.0.170) ... Done in 0 seconds.
- Data upgrade step 3/77, ProfilerUpgradeService(1.3.0.187) ... Done in 4 seconds.
- Data upgrade step 4/77, GuestUpgradeService(1.3.0.194) ... Done in 0 seconds.
- Data upgrade step 5/77, NetworkAccessUpgrade(1.3.0.220) ... Done in 1 seconds.
- Data upgrade step 6/77, GuestUpgradeService(1.3.0.208) ... Done in 1 seconds.
- Data upgrade step 7/77, GuestUpgradeService(1.3.0.220) ... Done in 0 seconds.
- Data upgrade step 8/77, RBACUpgradeService(1.3.0.228) ... Done in 9 seconds.
- Data upgrade step 9/77, NetworkAccessUpgrade(1.3.0.230) ... Done in 2 seconds.
- Data upgrade step 10/77, NSFUpgradeService(1.3.0.230) ... Done in 0 seconds.
- Data upgrade step 11/77, NetworkAccessUpgrade(1.3.0.250) ... Done in 0 seconds.
- Data upgrade step 12/77, RBACUpgradeService(1.3.0.334) ... Done in 5 seconds.
- Data upgrade step 13/77, RBACUpgradeService(1.3.0.335) ... Done in 5 seconds.
- Data upgrade step 14/77, ProfilerUpgradeService(1.3.0.360) ... Done in 73 seconds.
- Data upgrade step 15/77, ProfilerUpgradeService(1.3.0.410) ... Done in 0 seconds.
- Data upgrade step 16/77, NSFUpgradeService(1.3.0.410) ... Done in 0 seconds.
- Data upgrade step 17/77, NSFUpgradeService(1.3.0.406) ... Done in 0 seconds.
- Data upgrade step 18/77, NSFUpgradeService(1.3.0.410) ... Done in 0 seconds.
- Data upgrade step 19/77, RBAC UpgradeService(1.3.0.423) ... Done in 0 seconds.
- Data upgrade step 20/77, NetworkAccessUpgrade(1.3.0.423) ... Done in 0 seconds.
- Data upgrade step 21/77, RBAC UpgradeService(1.3.0.433) ... Done in 0 seconds.
- Data upgrade step 22/77, EgressUpgradeService(1.3.0.437) ... Done in 0 seconds.
- Data upgrade step 23/77, NSFUpgradeService(1.3.0.438) ... Done in 0 seconds.
- Data upgrade step 24/77, NSFUpgradeService(1.3.0.439) ... Done in 0 seconds.
- Data upgrade step 25/77, CdaRegistration(1.3.0.446) ... Done in 1 seconds.
- Data upgrade step 26/77, RBAC UpgradeService(1.3.0.452) ... Done in 8 seconds.
- Data upgrade step 27/77, NetworkAccessUpgrade(1.3.0.458) ... Done in 0 seconds.
- Data upgrade step 28/77, NSF UpgradeService(1.3.0.461) ... Done in 0 seconds.
- Data upgrade step 29/77, Cert Mgmt UpgradeService(1.3.0.462) ... Done in 3 seconds.
- Data upgrade step 30/77, NetworkAccessUpgrade(1.3.0.476) ... Done in 0 seconds.
- Data upgrade step 31/77, Token UpgradeService(1.3.0.500) ... Done in 0 seconds.
- Data upgrade step 32/77, NSF UpgradeService(1.3.0.508) ... Done in 0 seconds.
- Data upgrade step 33/77, RBAC UpgradeService(1.3.0.509) ... Done in 8 seconds.
- Data upgrade step 34/77, NSF UpgradeService(1.3.0.526) ... Done in 0 seconds.
- Data upgrade step 35/77, NSF UpgradeService(1.3.0.531) ... Done in 0 seconds.
- Data upgrade step 36/77, MDM UpgradeService(1.3.0.536) ... Done in 0 seconds.
- Data upgrade step 37/77, NSF UpgradeService(1.3.0.554) ... Done in 0 seconds.
- Data upgrade step 38/77, NetworkAccessUpgrade(1.3.0.561) ... Done in 0 seconds.
- Data upgrade step 39/77, Cert Mgmt UpgradeService(1.3.0.615) ... Done in 1 seconds.
- Data upgrade step 40/77, Cert Mgmt UpgradeService(1.3.0.616) ... Done in 2 seconds.
- Data upgrade step 41/77, Cert Mgmt UpgradeService(1.3.0.617) ... Done in 0 seconds.
- Data upgrade step 42/77, Opcap UpgradeRegistration(1.3.0.617) ... Done in 0 seconds.
- Data upgrade step 43/77, NSF UpgradeService(1.3.0.630) ... Done in 0 seconds.
- Data upgrade step 44/77, NSF UpgradeService(1.3.0.631) ... Done in 0 seconds.
- Data upgrade step 45/77, Cert Mgmt UpgradeService(1.3.0.634) ... Done in 0 seconds.
- Data upgrade step 46/77, RBAC UpgradeService(1.3.0.650) ... Done in 3 seconds.
- Data upgrade step 47/77, Cert Mgmt UpgradeService(1.3.0.653) ... Done in 0 seconds.
- Data upgrade step 48/77, Node Group UpgradeService(1.3.0.655) ... Done in 0 seconds.
- Data upgrade step 49/77, RBAC UpgradeService(1.3.0.670) ... Done in 2 seconds.
- Data upgrade step 50/77, Profiler UpgradeService(1.3.0.670) ... Done in 71 seconds.
- Data upgrade step 51/77, NSF UpgradeService(1.3.0.676) ... Done in 0 seconds.
- Data upgrade step 52/77, Authz UpgradeService(1.3.0.676) ... Done in 0 seconds.
- Data upgrade step 53/77, Guest Access UpgradeService(1.3.0.676) ... Done in 119 seconds.
- Data upgrade step 54/77, NSF UpgradeService(1.3.0.694) ... Done in 0 seconds.
- Data upgrade step 55/77, Provisioning Registration(1.3.0.700) ... Done in 0 seconds.
- Data upgrade step 56/77, Register Posture Types(1.3.0.705) ... Done in 0 seconds.
```

Cisco Identity Services Engine Upgrade Guide, Release 1.4

Upgrade a Distributed Deployment
**Data upgrade step 57/77, CertMgmtUpgradeService(1.3.0.727)... Done in 0 seconds.**
**Data upgrade step 58/77, CertMgmtUpgradeService(1.3.0.808)... Done in 0 seconds.**
**Data upgrade step 59/77, NSFUpgradeService(1.3.0.810)... Done in 9 seconds.**
**Data upgrade step 61/77, ProfilerUpgradeService(1.3.0.844)... Done in 44 seconds.**
**Data upgrade step 62/77, GuestAccessUpgradeService(1.3.0.855)... Done in 0 seconds.**
**Data upgrade step 63/77, NSFUpgradeService(1.3.0.858)... Done in 0 seconds.**
**Data upgrade step 64/77, NSFUpgradeService(1.3.0.861)... Done in 0 seconds.**
**Data upgrade step 65/77, ProvisioningUpgradeService(1.3.0.876)... Done in 0 seconds.**
**Data upgrade step 66/77, CertReqMgmtBootstrapService(1.4.0.0)... Done in 0 seconds.**
**Data upgrade step 67/77, NSFUpgradeService(1.4.0.110)... Done in 0 seconds.**
**Data upgrade step 68/77, NSFUpgradeService(1.4.0.119)... Done in 0 seconds.**
**Data upgrade step 69/77, NSFUpgradeService(1.4.0.125)... Done in 0 seconds.**
**Data upgrade step 70/77, NSFUpgradeService(1.4.0.157)... Done in 0 seconds.**
**Data upgrade step 71/77, GuestAccessUpgradeService(1.4.0.157)... Done in 3 seconds.**
**Data upgrade step 72/77, NSFUpgradeService(1.4.0.164)... Done in 0 seconds.**
**Data upgrade step 73/77, MEMPartnerUpgradeService(1.4.0.166)... Done in 0 seconds.**
**Data upgrade step 74/77, MEMPartnerUpgradeService(1.4.0.167)... Done in 0 seconds.**
**Data upgrade step 75/77, ProfilerUpgradeService(1.4.0.175)... Done in 1 second.**
**Data upgrade step 76/77, CertMgmtUpgradeService(1.4.0.217)... Done in 0 seconds.**
**Data upgrade step 77/77, GuestAccessUpgradeService(1.4.0.253)... Done in 0 seconds.**

**STEP 8:** Running ISE configuration data upgrade for node specific data...

**STEP 9:** Making this node PRIMARY of the new deployment. When other nodes are upgraded it will be added to this deployment.

**STEP 10:** Running ISE M&T DB upgrade...

ISE Database Mnt schema upgrade completed.

**Gathering Config schema(CEPM) stats ....
Gathering Operational schema(MNT) stats .......
Stopping ISE Database processes...

% 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...

---

Here is an example CLI transcript of a successful PSN node upgrade.

```
ise/admin# application upgrade ise-upgradebundle=1.4.0.253.x86_64.tar.gz sftp
Save the current ADE-OS running configuration? (yes/no) [yes] ?
Please enter yes or no
Save the current ADE-OS running configuration? (yes/no) [yes] ?
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Getting bundle to local machine...
md5: 35a159416afd0900c9da7b3dc6c72043
sha256: 8b3b43057067b0995ecabf5673c69565c0d0dfae790defe58d1e998aa9f8c7427a
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y] ?
Unbundling Application Package...
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: De-registering node from current deployment.
STEP 5: Taking backup of the configuration data...
STEP 6: Registering this node to primary of new deployment...
STEP 7: Downloading configuration data from primary of new deployment...
STEP 8: Importing configuration data...
STEP 9: Running ISE configuration data upgrade for node specific data...
STEP 10: Running ISE M&T DB upgrade...
ISE Database Mnt schema upgrade completed.
No gather stats needed as this is not PAP or MNT node

% NOTICE: Upgrading ADEOS. Appliance will be rebooted after upgrade completes successfully.
% This application Install or Upgrade requires reboot, rebooting now...
```

---

**What to Do Next**

Verify the Upgrade Process, on page 9
Verify the Upgrade Process

To verify if an upgrade is successful, do one of the following:

- 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.

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 upgrade fails because of configuration database issues, the changes are rolled back automatically. Refer to Chapter 4, "Recovering from Cisco ISE Upgrade Failures" for more information.