# Upgrade a Cisco ISE Deployment from the CLI



# Upgrade Process

## Upgrade a Standalone Node

You can use the **application upgrade** command directly, or the application upgrade **prepare** and **proceed** commands in the specified 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 as described below.

### Before you begin

Ensure that you have read the instructions in the Prepare for Upgrade chapter.

**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** 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 application upgrade prepare
ise-upgradebundle-2.2.0.452.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 check to fix index corruption, if any...
- Auto Upgrading Schema for UPS Model...
- Upgrading Schema completed for UPS Model.

ISE database schema upgrade completed.
STEP 6: Running ISE configuration data upgrade...
- Data upgrade step 1/48, NSFUpgradeService(2.1.101.145)... Done in 21 seconds.
- Data upgrade step 2/48, ProfilerUpgradeService(2.1.101.145)... Done in 1 seconds.
- Data upgrade step 3/48, UPSUpgradeHandler(2.1.101.188)... Done in 10 seconds.
- Data upgrade step 4/48, NetworkAccessUpgrade(2.2.0.007)... Done in 1 seconds.
- Data upgrade step 5/48, UPSUpgradeHandler(2.2.0.118)... Done in 2 seconds.
- Data upgrade step 6/48, UPSUpgradeHandler(2.2.0.119)... Done in 0 seconds.
- Data upgrade step 7/48, GuestAccessUpgradeService(2.2.0.124)... Done in 14 seconds.
- Data upgrade step 8/48, NSFUpgradeService(2.2.0.135)... Done in 0 seconds.
- Data upgrade step 9/48, NSFUpgradeService(2.2.0.136)... Done in 0 seconds.
- Data upgrade step 10/48, NetworkAccessUpgrade(2.2.0.137)... Done in 0 seconds.
- Data upgrade step 11/48, NetworkAccessUpgrade(2.2.0.143)... Done in 4 seconds.
- Data upgrade step 12/48, NSFUpgradeService(2.2.0.145)... Done in 1 seconds.
- Data upgrade step 13/48, NSFUpgradeService(2.2.0.146)... Done in 0 seconds.
- Data upgrade step 14/48, NetworkAccessUpgrade(2.2.0.155)... Done in 0 seconds.
- Data upgrade step 15/48, CdaRegistration(2.2.0.156)... Done in 1 seconds.
- Data upgrade step 16/48, NetworkAccessUpgrade(2.2.0.161)... Done in 0 seconds.
- Data upgrade step 17/48, UPSUpgradeHandler(2.2.0.166)... Done in 0 seconds.
- Data upgrade step 18/48, NetworkAccessUpgrade(2.2.0.169)... Done in 0 seconds.
```

```
- Data upgrade step 19/48, UPSUpgradeHandler(2.2.0.169)... Done in 0 seconds.
- Data upgrade step 20/48, CertMgmtUpgradeService(2.2.0.200)... Done in 0 seconds.
- Data upgrade step 21/48, NetworkAccessUpgrade(2.2.0.208)... Done in 0 seconds.
- Data upgrade step 22/48, RegisterPostureTypes(2.2.0.218)... Done in 1 seconds.
- Data upgrade step 23/48, NetworkAccessUpgrade(2.2.0.218)... Done in 1 seconds.
- Data upgrade step 24/48, NetworkAccessUpgrade(2.2.0.222)... Done in 0 seconds.
- Data upgrade step 25/48, NetworkAccessUpgrade(2.2.0.223)... Done in 0 seconds.
- Data upgrade step 26/48, NetworkAccessUpgrade(2.2.0.224)... Done in 0 seconds.
- Data upgrade step 27/48, SyslogTemplatesRegistration(2.2.0.224)... Done in 0 seconds.
- Data upgrade step 28/48, ReportUpgradeHandler(2.2.0.242)... Done in 0 seconds.
- Data upgrade step 29/48, IRFUpgradeService(2.2.0.242)... Done in 0 seconds.
- Data upgrade step 30/48, LocalHostNADRegistrationService(2.2.0.261)... Done in 0 seconds.
- Data upgrade step 31/48, DomainControllerUpgrade(2.2.0.299)... Done in 0 seconds.
- Data upgrade step 32/48, NetworkAccessUpgrade(2.2.0.300)... Done in 0 seconds.
- Data upgrade step 33/48, CertMgmtUpgradeService(2.2.0.300)... Done in 1 seconds.
- Data upgrade step 34/48, PolicyUpgradeService(2.2.0.306)... Done in 0 seconds.
- Data upgrade step 35/48, NSFUpgradeService(2.2.0.323)... Done in 0 seconds.
- Data upgrade step 36/48, NetworkAccessUpgrade(2.2.0.330)... Done in 0 seconds.
- Data upgrade step 37/48, NSFUpgradeService(2.2.0.340)... Done in 0 seconds.
- Data upgrade step 38/48, NetworkAccessUpgrade(2.2.0.340)... Done in 0 seconds.
- Data upgrade step 39/48, NetworkAccessUpgrade(2.2.0.342)... Done in 0 seconds.
- Data upgrade step 40/48, AuthzUpgradeService(2.2.0.344)... Done in 0 seconds.
- Data upgrade step 41/48, RegisterPostureTypes(2.2.0.350)... Done in 19 seconds.
- Data upgrade step 42/48, ProfilerUpgradeService(2.2.0.359)... Done in 28 seconds.
- Data upgrade step 43/48, DictionaryUpgradeRegistration(2.2.0.374)... Done in 10 seconds.
- Data upgrade step 44/48, UPSUpgradeHandler(2.2.0.403)... Done in 0 seconds.
- Data upgrade step 45/48, DictionaryUpgradeRegistration(2.2.0.410)... Done in 0 seconds.
- Data upgrade step 46/48, NSFUpgradeService(2.2.0.452)... Done in 0 seconds.
- Data upgrade step 47/48, ProfilerUpgradeService(2.2.0.452)... Done in 0 seconds.
- Data upgrade step 48/48, GuestAccessUpgradeService(2.2.0.452)... Done in 4 seconds.
STEP 7: Running ISE configuration data upgrade for node specific data...
STEP 8: Running ISE M&T database upgrade...
ISE M&T Log Processor is not running
ISE database M&T schema upgrade completed.
% Warning: Some warnings encountered during MNT sanity check

Gathering Config schema(CEPM) stats ....
Gathering Operational schema(MNT) stats ....
% NOTICE: Upgrading ADEOS. Appliance will be rebooted after upgrade completes successfully.
warning: file /opt/xgrid/install/xcp-1.3-iteration-1.21-x86_64.zip: remove failed: No such file or
directory
warning: file /opt/xgrid/gc/pxgrid-controller-1.0.3.32-dist.tar.gz: remove failed: No such file or
directory

% This application Install or Upgrade requires reboot, rebooting now...

Broadcast message from root@ise165 (pts/1) (Thu Jan 12 14:04:50 2017):

The system is going down for reboot NOW

Broadcast message from root@ise165 (pts/1) (Thu Jan 12 14:04:50 2017):

The system is going down for reboot NOW

Connection closed by foreign host.
```

The upgrade is now complete.

### What to do next

Verify the Upgrade Process, on page 9

# 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 thereafter(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.

**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.

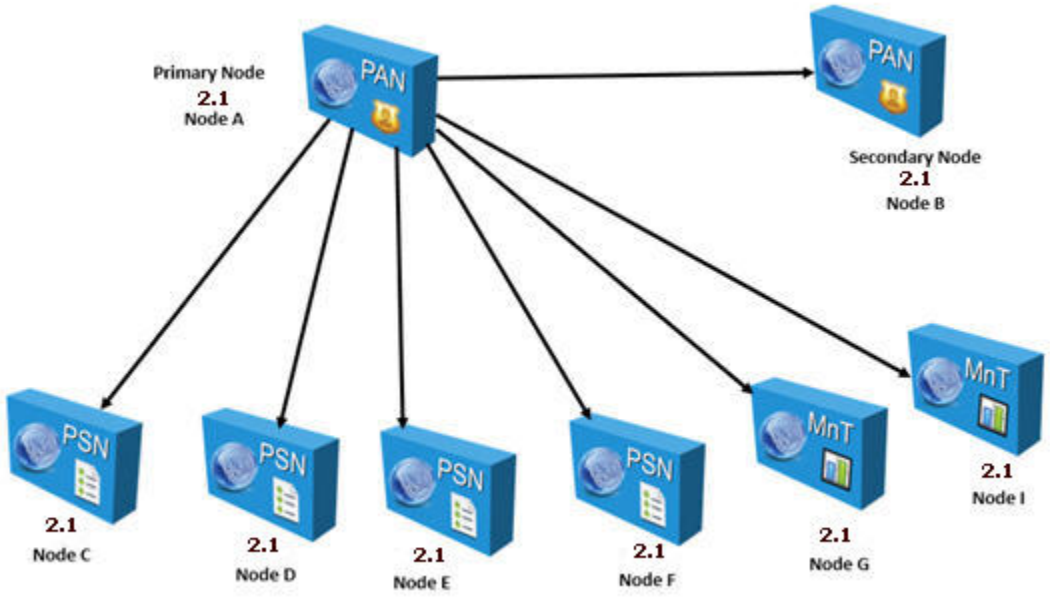
### What to do next

Verify the Upgrade Process, on page 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), and four Policy Service Nodes (PSNs) (node C, node D, node E, and node F), one Primary Monitoring Node (node G), and one Secondary Monitoring Node (node I), you can proceed with the following upgrade procedure.

***Figure 2: Cisco ISE Deployment Before Upgrade***




**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 (for example, if your license was installed by a Cisco partner vendor), 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 the 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.

**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 G) 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 C, D, E, and F) 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** (If you have an IPN node in your deployment) Deregister the IPN node from the Primary Administration Node.

Cisco ISE, Release 2.0 and later, does not support IPN nodes.

**Step 5** 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.

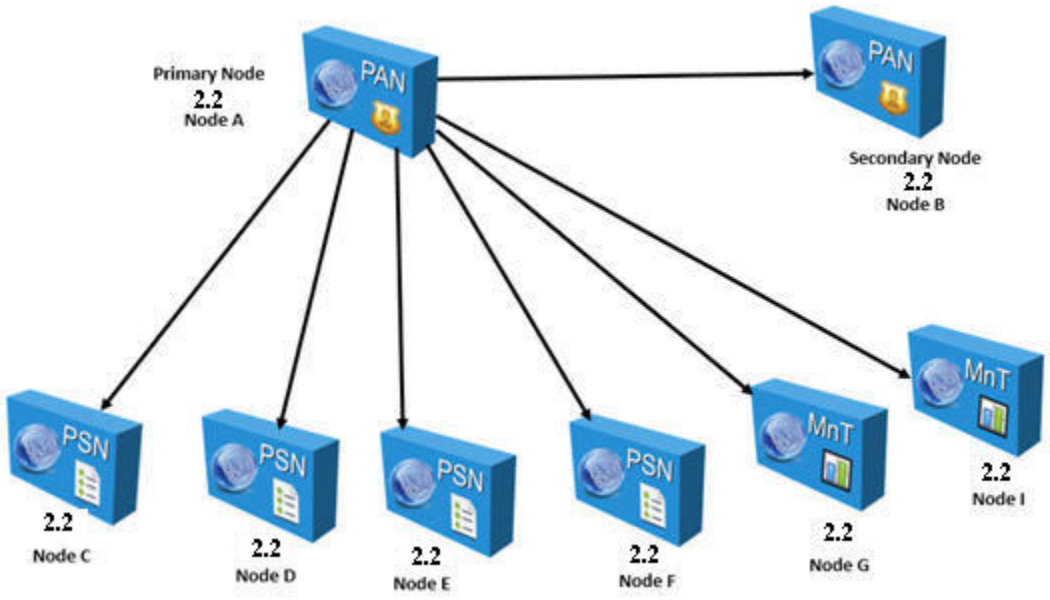
**Step 6** Finally, upgrade the Primary Administration Node (node A).

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.

### Example

***Figure 3: Cisco ISE Deployment After Upgrade***




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

```
ise74/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: 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 1/12, CertReqMgmtBootstrapService(1.4.0.0)... Done in 2 seconds.
- Data upgrade step 2/12, NSFUpgradeService(1.4.0.110)... Done in 0 seconds.
- Data upgrade step 3/12, NSFUpgradeService(1.4.0.119)... Done in 0 seconds.
- Data upgrade step 4/12, NSFUpgradeService(1.4.0.125)... Done in 0 seconds.
- Data upgrade step 5/12, NSFUpgradeService(1.4.0.157)... Done in 0 seconds.
- Data upgrade step 6/12, GuestAccessUpgradeService(1.4.0.157)... Done in 27 seconds.
- Data upgrade step 7/12, NSFUpgradeService(1.4.0.164)... Done in 1 seconds.
- Data upgrade step 8/12, MDMPartnerUpgradeService(1.4.0.166)... Done in 0 seconds.
- Data upgrade step 9/12, MDMPartnerUpgradeService(1.4.0.167)... Done in 44 seconds.
- Data upgrade step 10/12, ProfilerUpgradeService(1.4.0.175)... ..............Done in 878
seconds.
- Data upgrade step 11/12, CertMgmtUpgradeService(1.4.0.217)... Done in 6 seconds.
- Data upgrade step 12/12, GuestAccessUpgradeService(1.4.0.244)... Done in 17 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: Upgrading ADEOS. Appliance will be rebooted after upgrade completes successfully.

% This application Install or Upgrade requires reboot, rebooting now...
```

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

```
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: 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 database upgrade...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE database M&T schema upgrade completed.
% 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...
```

### What to do next

Verify the Upgrade Process, on page 9

# 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.

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.

# Recover from Upgrade Failures

This section describes what you need to do in order to recover if the upgrade fails.

Sometimes, upgrade fails because of not following the order in which the nodes have to be upgraded, such as upgrading the secondary Administration node first. If you encounter this error, you can upgrade the deployment again following the order of upgrade specified in this guide.

In rare cases, you might have to reimage, perform a fresh install, and restore data. So it is important that you have a backup of Cisco ISE configuration and monitoring data before you start the upgrade. It is important that you back up the configuration and monitoring data although we automatically try to roll back the changes in case of configuration database failures.

**Note** Upgrade failures that happen because of issues in the monitoring database are not rolled back automatically. You have to manually reimage your system, install Cisco ISE, Release 1.2, and restore the configuration and monitoring data on it.

Upgrade failures that happen because of issues in the monitoring database are not rolled back automatically. You have to manually reimage your system, install Cisco ISE, Release 1.3, and restore the configuration and monitoring data on it.

Upgrade failures that happen because of issues in the monitoring database are not rolled back automatically. You have to manually reimage your system, install Cisco ISE, and restore the configuration and monitoring data on it.

## Upgrade Failures

This section describes some of the known upgrade errors and what you must do to recover from them.

**Note** 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 upgrade progress. You can use the **show logging application** command from the Cisco ISE CLI to view the following logs (example filenames are given in parenthesis):

- DB Data Upgrade Log (*dbupgrade-data-global-20160308-154724.log*)
- DB Schema Log (*dbupgrade-schema-20160308-151626.log*)
- Post OS Upgrade Log (*upgrade-postosupgrade-20160308-170605.log*)

### Configuration and Data Upgrade Errors

During upgrade, the configuration database schema and data upgrade failures are rolled back automatically. Your system returns to the last known good state. If this is encountered, the following message appears on the console and in the logs:

```
% Warning: The node has been reverted back to its pre-upgrade state.
error: %post(CSCOcpm-os-1.4.0-205.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
 Assistance Center for support.
```

### Remediation Errors

If you need to remediate an upgrade failure to get the node back to the original state, the following message appears on the console. Check the logs for more information.

```
% Warning: Do the following steps to revert node to its pre-upgrade state."
error: %post(CSCOcpm-os-1.4.0-205.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
 Assistance Center for support.
```

### Validation Errors

Validation errors are not an actual upgrade failure. Validations errors may occur. For example, you might see this error if you attempt to upgrade a PSN before the secondary PAN is upgraded or if the system does not meet the specified requirements. The system returns to the last known good state. If you encounter this error, ensure that you perform the upgrade as described in this document.

```
STEP 1: Stopping ISE application...
% Warning: Cannot upgrade this node until the standby PAP node is upgraded and running. If
 standbyPAP is already upgraded
and reachable ensure that this node is in SYNC from current Primary UI.
Starting application after rollback...

% Warning: The node has been reverted back to its pre-upgrade state.
error: %post(CSCOcpm-os-1.4.0-205.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
 Assistance Center for support.
```

### Application Binary Upgrade Errors

If the ADE-OS or application binary upgrade fails, the following message appears when you run the **show application status ise** command from the CLI following a reboot. You should reimage and restore the configuration and operational backups.

```
% WARNING: An Identity Services Engine upgrade had failed. Please consult logs. You have
to reimage and restore to previous version.
```

### Other Types of Errors

For any other types of failures (including cancellation of the upgrade, disconnection of the console session, power failure, and so on), you must reimage and restore the configuration and operational backup depending on the personas enabled on the node originally.

### Reimage

The term, reimage, refers to a fresh installation of Cisco ISE. For Monitoring database upgrade (schema + data) errors, you must reimage and restore the configuration and operational backups. Before you reimage, ensure that you generate a support bundle by running the **backup-logs** CLI command and place the support bundle in a remote repository in order to help ascertain the cause of failure. You must reimage to the old or new version based on the node personas, as follows:

- Secondary Administration Node—Reimage to the old version and restore the configuration and operational backup.
- Monitoring Nodes—If the nodes are deregistered from the existing deployment, reimage to the new version, register with the new deployment, and enable the Monitoring persona.
- All Other NodesPrimary Administration Node—If there are upgrade failures on the other nodes, the system usually returns to the last known good state. If the system does not roll back to the old version, you can reimage to the new version, and register with the new deployment, and enable the personas as done in the old deployment.

### Upgrade after Failure

In case of upgrade failures, before you try to upgrade again:

- Analyze the logs. Check the support bundle for errors.
- Identify and resolve the problem by submitting the support bundle that you generated to the Cisco Technical Assistance Center (TAC).

**Note** 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...

### Upgrade Progress

**Note** Upgrade from Cisco ISE, Release 1.1.*x*, to 1.2 is a 32-bit to 64-bit upgrade. This process involves an ADE-OS upgrade and application binary upgrade to 64-bit and the node is rebooted twice during this time.

# Upgrade Failures during Binary Install

**Problem** An application binary upgrade occurs after the database upgrade. If a binary upgrade failure happens, the following message appears on the console and ADE.log:

```
% Application install/upgrade failed with system removing the corrupted install
```

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

To roll back, reimage the Cisco ISE appliance by using the previous ISO image and restore the data from the backup file. You need a new upgrade bundle each time you retry an upgrade.

- Analyze the logs. Check the support bundle for errors.
- Identify and resolve the problem by submitting the support bundle that you generated to the Cisco Technical Assistance Center (TAC).