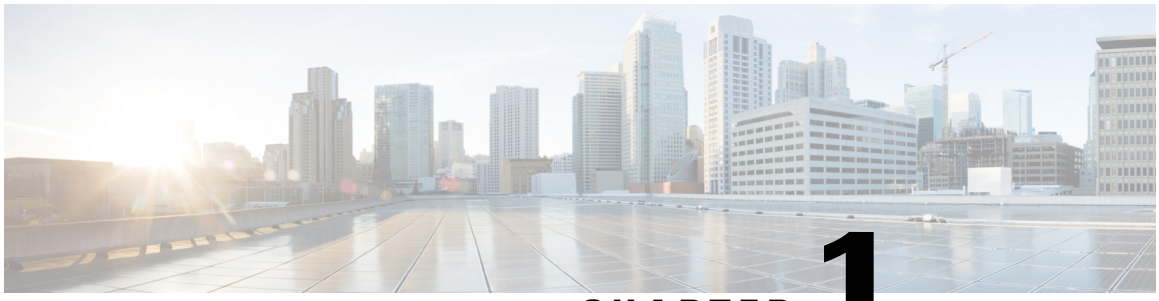
Cisco Identity Services Engine Upgrade Guide, Release 2.2

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco ISE Upgrade Overview

Cisco ISE Upgrade Overview

This document describes how to upgrade Cisco Identity Services Engine (ISE) software on Cisco ISE appliances and virtual machines to Release 2.2.

Upgrading a Cisco ISE deployment is a multi-step process and must be performed in the order specified in this document. Use the time estimates provided in this document to plan for upgrade with minimum downtime. For a deployment with multiple PSNs that are part of a PSN group, there would be no downtime. If there are endpoints authenticating through a PSN that is being upgraded, the request is processed by another PSN in the node group. The endpoint is re-authenticated and granted network access after successful authentication.

If you have a standalone deployment or a deployment with a single PSN, you might experience a downtime for all authentications when the PSN is being upgraded.

You can directly upgrade to Release 2.2, from any of the following releases:

- Cisco ISE, Release 1.4
- Cisco ISE, Release 2.0
- Cisco ISE, Release 2.0.1
- Cisco ISE, Release 2.1

Note Due to the following known issues, we recommend that you apply the latest patch to your current Cisco ISE version before upgrade:

- CSCvc38488
- CSCvc34766

If you are on a version earlier than Cisco ISE, Release 1.4, you must first upgrade to one of the releases listed above and then upgrade to Release 2.2.

You can download the upgrade bundle from Cisco.com. The following upgrade bundles are available for Release 2.2:

- ise-upgradebundle-1.4.x-to-2.2.0.x.x86_64.tar.gz—Use this bundle to upgrade from Release 1.4 to 2.2
- ise-upgradebundle-2.0.x-to-2.2.0.x.x86_64.tar.gz—Use this bundle to upgrade from Release 2.0 or Release 2.0.1 to 2.2
- ise-upgradebundle-2.2.0.x.x86_64.tar.gz—Use this bundle to upgrade from Release 2.1 to 2.2

This release of Cisco ISE supports both GUI-based as well as CLI-based upgrade.

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 2.2. See Upgrade a Cisco ISE Deployment from the GUI, on page 11 for more information.

From the Cisco ISE CLI, you can upgrade from Release 1.4, 2.0, 2.0.1, or 2.1 directly to Release 2.2. See Upgrade a Cisco ISE Deployment from the CLI, on page 19 for more information.

Supported Operating System for Virtual Machines

Release 2.2 supports Red Hat Enterprise Linux (RHEL) 7.0.

If you are upgrading Cisco ISE nodes on VMware virtual machines, after upgrade is complete, ensure that you change the Guest Operating System to Red Hat Enterprise Linux (RHEL) 7. To do this, you must power down the VM, change the Guest Operating System to RHEL 7, and power on the VM after the change.

Time Taken for Upgrade

Upgrade Time Estimation

The following table provides an estimate of the amount of time it might take to upgrade Cisco ISE nodes. Actual time taken for upgrade varies depending on a number of factors. Your production network continues to function without any downtime during the upgrade process if you have multiple PSNs as part of a node group.

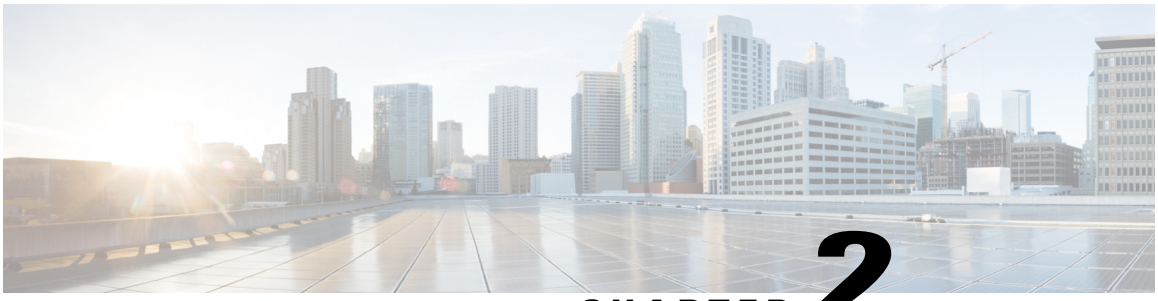
Type of Deployment	Node Persona	Time Taken for Upgrade
Standalone	Administration, Policy Service, Monitoring	240 minutes + 60 minutes for every 15 GB of data
Distributed	Secondary Administration Node	240 minutes
	Policy Service Node	180 minutes
	Monitoring	240 minutes + 60 minutes for every 15 GB of data

Upgrade to Release 2.2 involves upgrading the Guest operating system on a virtual machine and changing the type of network adapter. The Guest OS change requires you to power down the system, change the RHEL version, and power it back again. Apart from the time estimates given in the table above, you must factor in time for the pre-upgrade tasks. For a distributed deployment with multiple PSNs, you would need about 2 hours to prepare the system for upgrade.

Factors That Affect Upgrade Time

- Number of endpoints in your network
- Number of users and guest users in your network
- Amount of logs in a Monitoring or Standalone node
- Profiling service, if enabled

Note Cisco ISE nodes on virtual machines might take a longer time to upgrade than physical appliances.



CHAPTER 2

Prepare for Upgrade

Prepare for Upgrade

Before you start the upgrade process, ensure that you perform the following tasks:

Note In a multinode deployment with Primary and Secondary PANs, monitoring dashboards and reports might fail after upgrade because of a caveat in data replication. See CSCvd79546 for details. As a workaround, perform a manual synchronization from the Primary PAN to the Secondary PAN before initiating upgrade.

Note If you are currently on Release 2.0.1 on an SNS-3415 appliance, you cannot upgrade to Release 2.1 because of an exception. See CSCva96507 for details. As a workaround, reimage the SNS-3415 appliance, perform a fresh installation of Cisco ISE, Release 2.1, and restore backup from Release 2.0.1.

- Record Profiler Configuration, on page 8
- Obtain Active Directory and Internal Administrator Account Credentials, on page 9
- Activate MDM Vendor Before Upgrade, on page 9
- Create Repository and Copy the Upgrade Bundle, on page 9
- Check Load Balancer Configuration, on page 10

Apply Latest Patch to Your Current Cisco ISE Version Before Upgrade

Due to the following known issues, we recommend that you apply the latest patch to your current Cisco ISE version before upgrade:

- CSCvc38488
- CSCvc34766

Change VMware Virtual Machine Guest Operating System and Settings

If you are upgrading Cisco ISE nodes on virtual machines, ensure that you change the Guest Operating System to Red Hat Enterprise Linux (RHEL) 7. To do this, you must power down the VM, change the Guest Operating System to RHEL 7, and power on the VM after the change. RHEL 7 supports only E1000 and VMXNET3 network adapters. Be sure to change the network adapter type before you upgrade.

Remove Non-English Characters From Sponsor Group Names

Prior to release 2.2, if you have created sponsor groups with non-English characters, before upgrade, be sure to rename the sponsor groups and use only English characters.

Cisco ISE, Release 2.2 and later does not support non-English characters in sponsor group names.

Firewall Ports That Must be Open for Communication

If you have a firewall deployed between your primary Administration node and any other node, the following ports must be open before you upgrade:

- TCP 1521—For communication between the primary administration node and monitoring nodes.
- TCP 443—For communication between the primary administration node and all other secondary nodes.
- TCP 12001—For global cluster replication.
- TCP 7800 and 7802—(Applicable only if the policy service nodes are part of a node group) For PSN group clustering.

For a full list of ports that Cisco ISE uses, see the Cisco ISE Ports Reference.

Back Up Cisco ISE Configuration and Operational Data from the Primary Administration Node

Obtain a back up of the Cisco ISE configuration and operational data from the Command Line Interface (CLI) or the GUI. The CLI command is:

backup *backup-name* **repository** *repository-name* {**ise-config | ise-operational**} **encryption-key** {**hash | plain**} *encryption-keyname*

Note When Cisco ISE is run on VMware, Vmware snapshots are not supported for backing up ISE data.

VMware snapshot saves the status of a VM at a given point of time. In a multi-node Cisco ISE deployment, data in all the nodes are continuously synchronized with current database information. Restoring a snapshot might cause database replication and synchronization issues. Cisco recommends that you use the backup functionality included in Cisco ISE for archival and restoration of data.

Using VMware snapshots to back up ISE data results in stopping Cisco ISE services. A reboot is required to bring up the ISE node.

You can also obtain the configuration and operational data backup from the Cisco ISE Admin Portal. Ensure that you have created repositories for storing the backup file. Do not back up using a local repository. You cannot back up the monitoring data in the local repository of a remote Monitoring node. The following repository types are not supported: CD-ROM, HTTP, HTTPS, or TFTP. This is because, either these repository types are read-only or the protocol does not support file listing.

1. Choose **Administration > System > Backup and Restore**.
2. Click **Backup Now**.
3. Enter the values as required to perform a backup.
4. Click **OK**.
5. Verify that the backup completed successfully.

   Cisco ISE appends the backup filename with a timestamp and stores the file in the specified repository. In addition to the timestamp, Cisco ISE adds a CFG tag for configuration backups and OPS tag for operational backups. Ensure that the backup file exists in the specified repository.

   In a distributed deployment, do not change the role of a node or promote a node when the backup is running. Changing node roles will shut down all the processes and might cause some inconsistency in data if a backup is running concurrently. Wait for the backup to complete before you make any node role changes.

Back Up System Logs from the Primary Administration Node

Obtain a backup of the system logs from the Primary Administration Node from the Command Line Interface (CLI). The CLI command is:

backup-logs *backup-name* **repository** *repository-name* **encryption-key** { **hash | plain**} *encryption-key name*

Check the Validity of Certificates

The upgrade process fails if any certificate in the Cisco ISE Trusted Certificates or System Certificates store has expired. Ensure that you check the validity of the certificates in the Trusted Certificate and System Certificates store, and renew them, if necessary before upgrade.

Export Certificates and Private Keys

We recommend that you export:

- All local certificates (from all the nodes in your deployment) along with their private keys to a secure location. Record the certificate configuration (what service the certificate was used for).
- All certificates from the Trusted Certificates Store of the Primary Administration Node. Record the certificate configuration (what service the certificate was used for).

Disable PAN Automatic Failover and Scheduled Backups Before Upgrade

Cisco ISE does not support deployment changes when a backup is in progress. Ensure that you disable the following configurations before upgrade:

- Primary Administration Node Automatic Failover—If you have configured the Primary Administration Node for automatic failover, be sure to disable the automatic failover option before upgrade.
- Scheduled Backups—Plan your deployment upgrade in such a way that you reschedule the backups after the upgrade. You can choose to disable the backup schedules and recreate them after upgrade.

  Backups with a schedule frequency of once get triggered every time the Cisco ISE application is restarted. Hence, if you have a backup schedule that was configured to run just once, be sure to disable it before upgrade.

NTP Server Should Be Configured Correctly and Reachable

During upgrade, the Cisco ISE nodes reboot, migrate and replicate data from the primary administration node to the secondary administration node. For these operations, it is important that the NTP server in your network is configured correctly and is reachable. If the NTP server is not set up correctly or is unreachable, the upgrade process fails.

Ensure that the NTP servers in your network are reachable, responsive, and synchronized during upgrade.

Record Profiler Configuration

If you use the Profiler service, ensure that you record the profiler configuration for each of your Policy Service nodes from the Admin portal (Administration > System > Deployment > <*node*> > Profiling Configuration). You can make a note of the configuration or obtain screen shots.

Obtain Active Directory and Internal Administrator Account Credentials

If you use Active Directory as your external identity source, ensure that you have the Active Directory credentials and a valid internal administrator account credentials on hand. After upgrade, you might lose Active Directory connections. If this happens, you need the ISE internal administrator account to log in to the Admin portal and Active Directory credentials to rejoin Cisco ISE with Active Directory.

Activate MDM Vendor Before Upgrade

If you use the MDM feature, then before upgrade, ensure that the MDM vendor status is active.

Otherwise, the existing authorization profiles for MDM redirect are not updated with the MDM vendor details. After upgrade, you must manually update these profiles with an active vendor and the users will go through the onboarding flow again.

Create Repository and Copy the Upgrade Bundle

Create a repository to obtain backups and copy the upgrade bundle. We recommend that you use FTP for better performance and reliability. Do not use repositories that are located across slow WAN links. We recommend that you use a local repository that is closer to the nodes.

Download the upgrade bundle from Cisco.com.

To upgrade to Release 2.2, there are three upgrade bundles available:

- ise-upgradebundle-1.4.x-to-2.2.0.x.x86_64.tar.gz—Use this bundle to upgrade from Release 1.4 to 2.2
- ise-upgradebundle-2.0.x-to-2.2.0.x.x86_64.tar.gz—Use this bundle to upgrade from Release 2.0 or 2.0.1 to 2.2
- ise-upgradebundle-2.2.0.x.x86_64.tar.gz—Use this bundle to upgrade from Release 2.1 to 2.2

For upgrade, you can copy the upgrade bundle to the Cisco ISE node's local disk using the following command:

copy *repository_url/path/ise-upgradebundle-1.4.x-to-2.2.0.x.x86_64.tar.gz* **disk:/**

For example, if you want to use SFTP to copy the upgrade bundle, you can do the following:

1. (Add the host key if it does not exist) **crypto host_key add host** *mySftpserver*
2. **copy sftp:**//*aaa.bbb.ccc.ddd/ise-upgradebundle-1.4.x-to-2.2.0.x.x86_64.tar.gz* **disk:/**

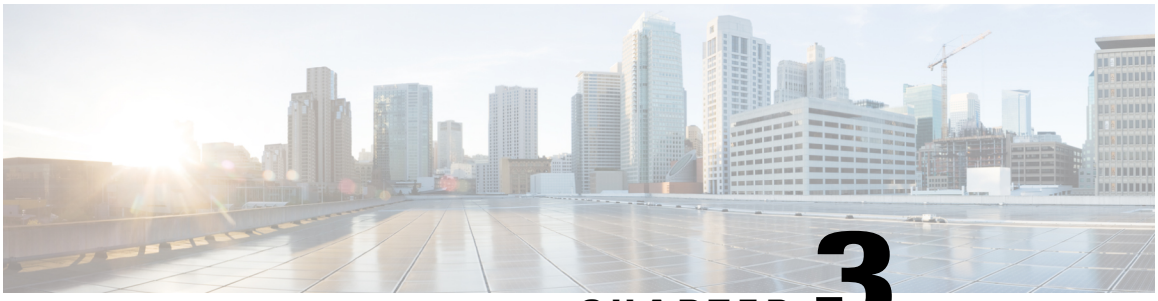
   where *aaa.bbb.ccc.ddd* is the IP address or hostname of the SFTP server and *ise-upgradebundle-1.4.x-to-2.2.0.x.x86_64.tar.gz* is the name of the upgrade bundle.

Having the upgrade bundle in the local disk saves time during upgrade. Alternatively, you can use the **application upgrade prepare** command to copy the upgrade bundle to the local disk and extract it.

Note Ensure that you have a good bandwidth connection with the repository. When you download the upgrade bundle from the repository to the node, the download times out if it takes more than 35 minutes to complete.

Check Load Balancer Configuration

If you are using any load balancer between the Primary Administration Node (PAN) and the Policy Service node (PSN), ensure that the session timeout configured on the load balancer does not affect the upgrade process. If the session timeout is set to a lower value, it might affect the upgrade process on the PSNs located behind the load balancer. For example, if a session times out during the database dump from PAN to a PSN, the upgrade process may fail on the PSN.



CHAPTER 3

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 screen.

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

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

Different Types of Deployment

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

ISE Community Resource

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

Upgrade From Release 2.0 , 2.0.1 or 2.1 to Release 2.2

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

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

Before You Begin

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

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

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

Step 2 Click **Proceed**.
The **Review Checklist** window appears. Read the given instructions carefully.

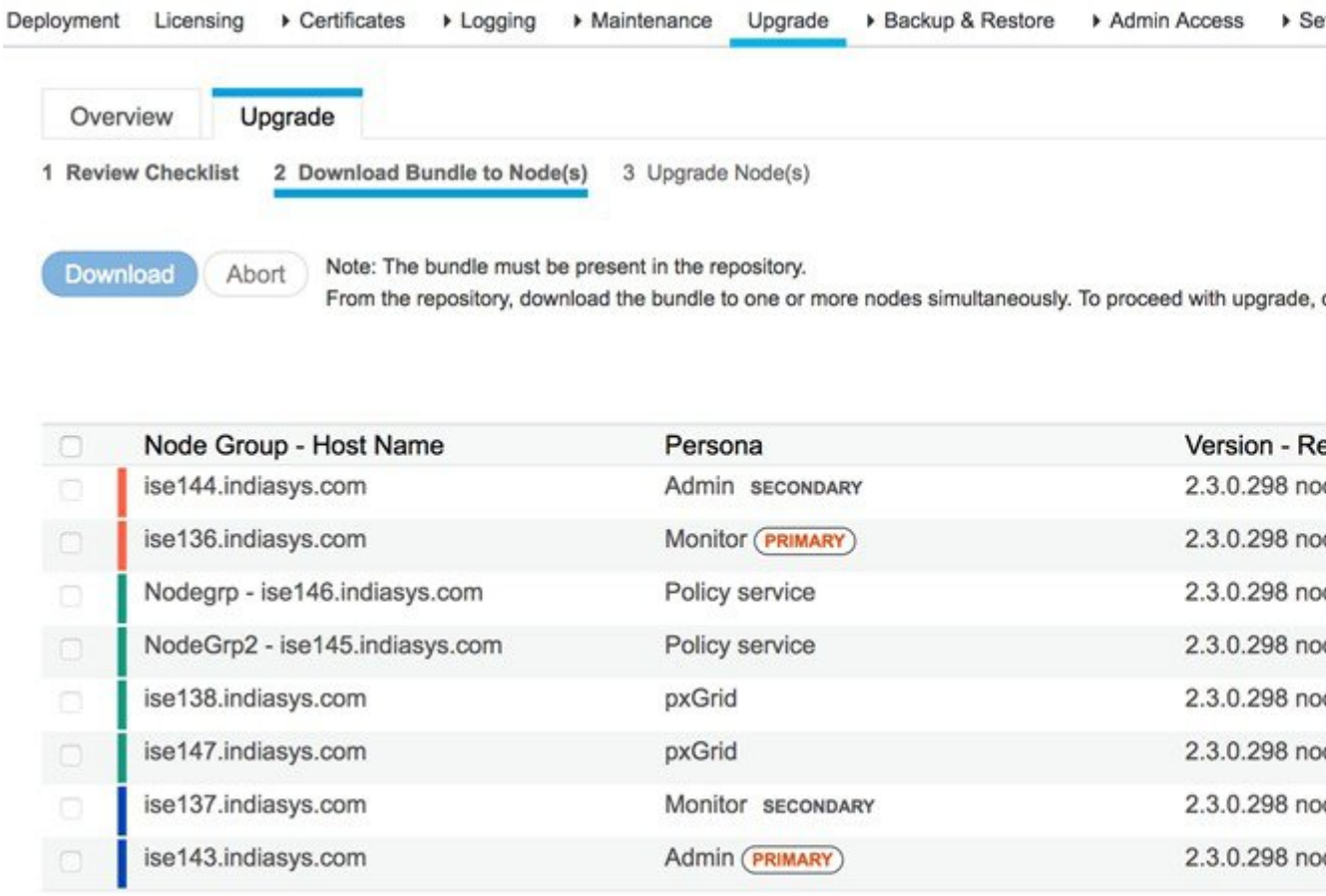
Step 3 Check the **I have reviewed the checklist** check box, and click **Continue**.
The **Download Bundle to Nodes** window appears.

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

a) Check the check box next to the nodes to which you want to download the upgrade bundle.
b) Click **Download**.
The **Select Repository and Bundle** window appears.
c) Select the repository.

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

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

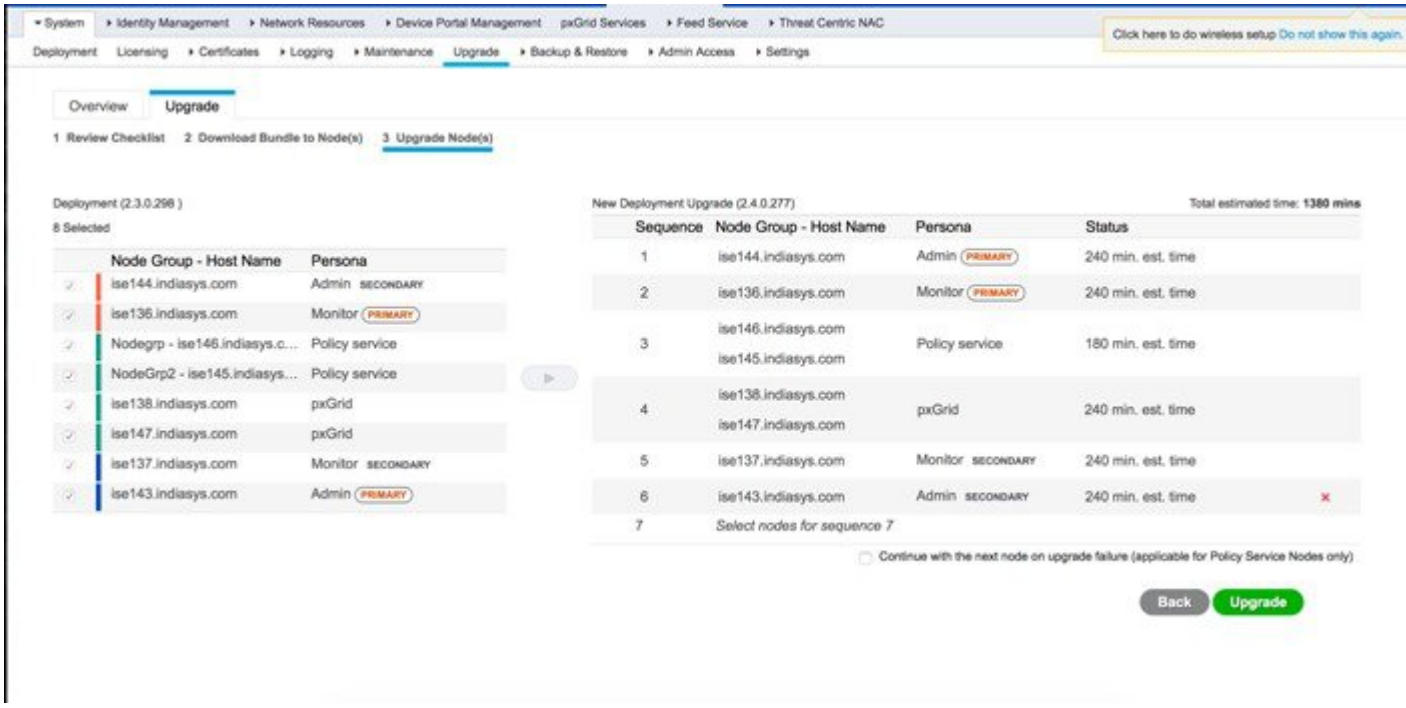


d) Check the check box next to the bundle that you want to use for the upgrade.
e) Click **Confirm**.
Once the bundle is downloaded to the node, the node status changes to **Ready for Upgrade**.

Step 5 Click **Continue**.

The **Upgrade Nodes** window appears.

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



Step 6 Choose the upgrade sequence.
When you move a node to the new deployment, a time estimate for the upgrade is displayed on the **Upgrade Nodes** window. You can use this information to plan for upgrade and minimize downtime. Use the sequence given below if you have a pair of Administration and Monitoring Nodes, and several Policy Service Nodes.

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

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

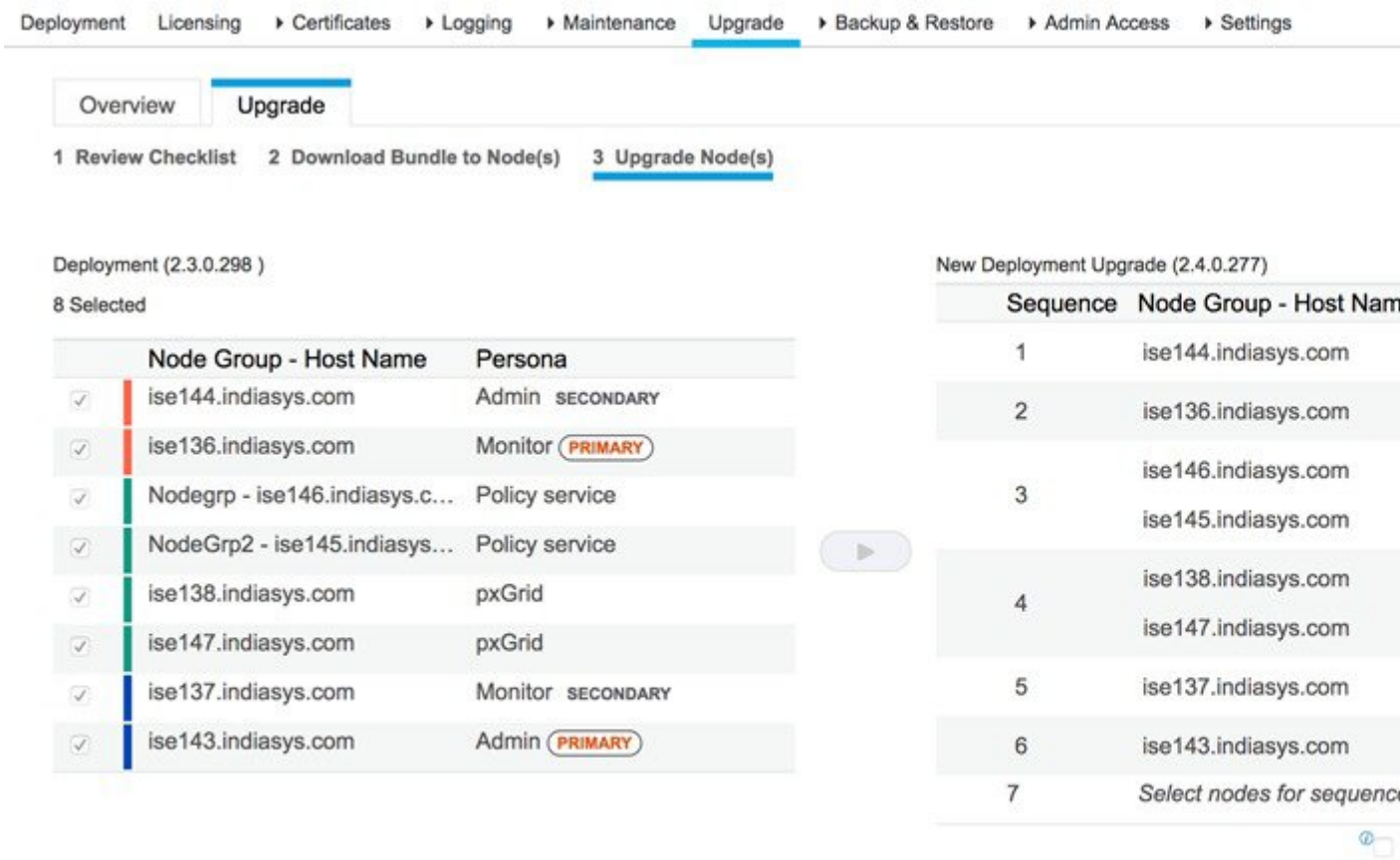
Node Personas In The Current Deployment	Upgrade Sequence
Secondary Administration/Primary Monitoring Node, Policy Service Nodes, Primary Administration/Secondary Monitoring Node	**1** Secondary Administration/Primary Monitoring Node **2** Policy Service Nodes **3** Primary Administration/Secondary Monitoring Node

Node Personas In The Current Deployment	Upgrade Sequence
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

Step 7 Check the **Continue with upgrade on failure** check box if you want to continue with the upgrade even if the upgrade fails on any of the Policy Service Nodes in the upgrade sequence.
This option is not applicable for the Secondary Administration Node and the Primary Monitoring Node. If any one of these nodes fail, the upgrade process is rolled back. If any of the Policy Service Nodes fail, the Secondary Monitoring Node and the Primary Administration Node are not upgraded and remain in the old deployment.

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

Figure 3: Upgrade Window Showing the Upgrade Progress



The 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*.

Troubleshoot Upgrade Failures

Upgrade Bundle Download Via the GUI Times Out

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

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

Generic Upgrade Error

The following generic upgrade error appears:

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

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

Upgrade is in Blocked State

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

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

No Secondary Administration Node in the Deployment

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

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

Workaround:

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

Upgrade Times Out

The ISE node upgrade times out with the following message:

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

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

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

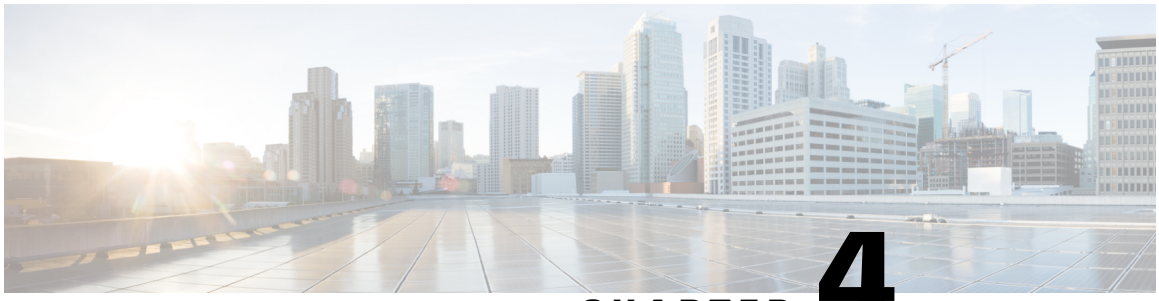
    Note If you remove the Secondary Administration Node from the Upgrade page in the Admin portal, you cannot continue with upgrade from the GUI. Hence, we recommend that you continue the upgrade from the CLI for the rest of the nodes.

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

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

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

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



CHAPTER 4

Upgrade a Cisco ISE Deployment from the CLI

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.

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 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 28

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 4: 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 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 28

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 5: Cisco ISE Deployment Before Upgrade

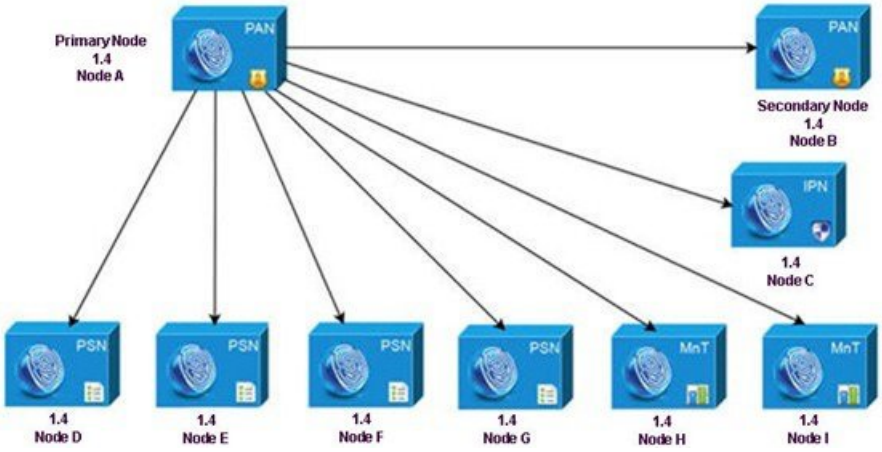
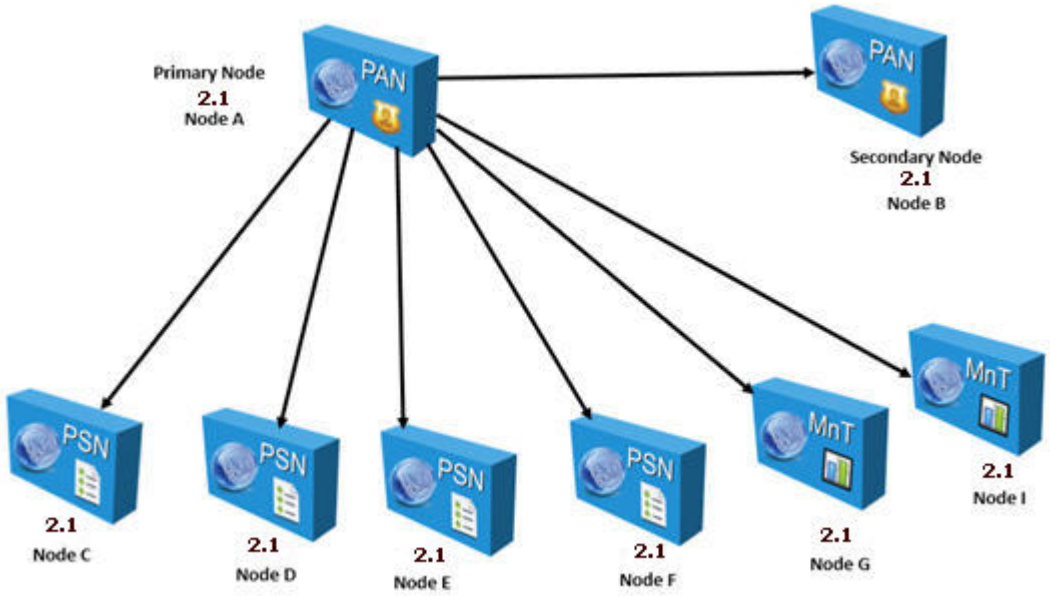


Figure 6: Cisco ISE Deployment Before Upgrade



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 (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 28 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.

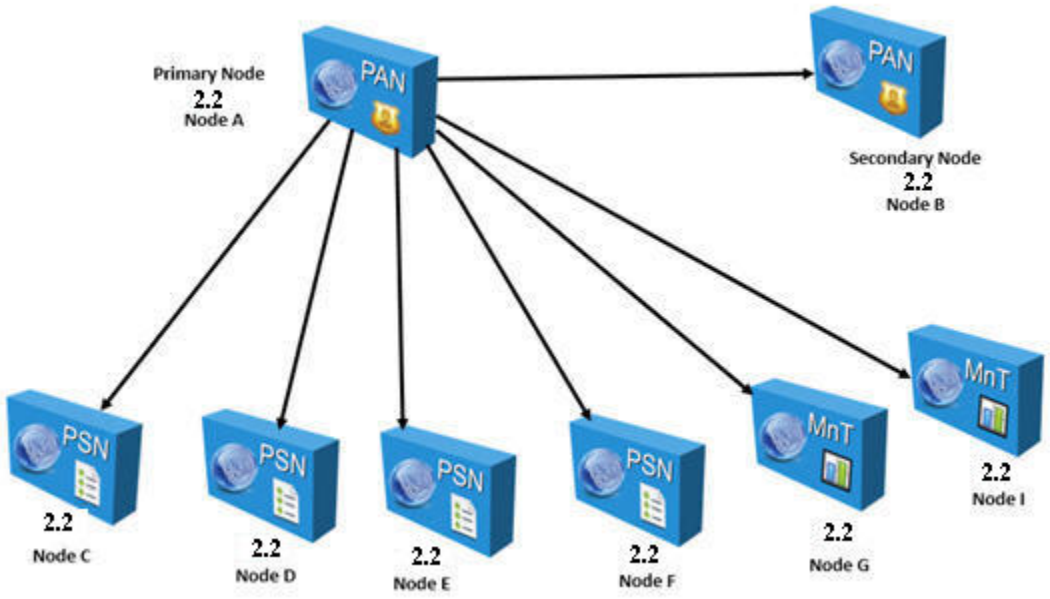
b) Upgrade the Secondary Monitoring Node (node I) from the old deployment to the new deployment.

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.

Figure 7: Cisco ISE Deployment After Upgrade



CLI Transcripts of Successful Upgrades

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

```
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 28

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.

Recover from Upgrade Failures

This section describes what you need to do while recovering from upgrade failures.

The upgrade software performs some validations. If upgrade fails, follow the instructions provided on screen to recover and successfully upgrade to Release 2.2.

At times, 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 even though 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 2.2, 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 progress of upgrade. 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

If there are any validation errors, which is not an actual upgrade failure, the following message appears. 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:

- 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 Nodes—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, 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).

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.

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 Fails During Binary Install

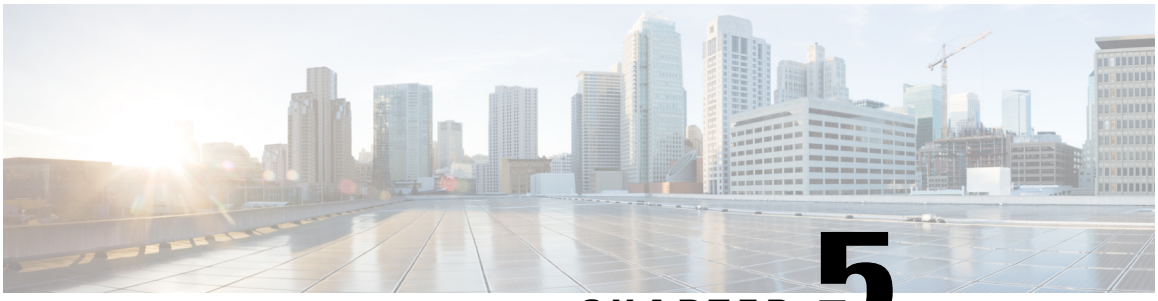
Problem An application binary upgrade occurs after the database upgrade. If a binary upgrade failure happens, the following message appears on the console and ADE.log:

```
% 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).



CHAPTER 5

Post-Upgrade Tasks

After you upgrade your deployment, perform the tasks listed in this chapter.

Post-Upgrade Tasks

See the *Cisco Identity Services Engine Administrator Guide* for details about each of these tasks.

Note If you are upgrading to Release 2.1 or Release 2.2, see the following links:

- For release 2.1, Post-Upgrade Tasks
- For release 2.2, Post-Upgrade Tasks

Task Description	Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide
Ensure that the Guest Operating System on the VMware virtual machine is set to Red Hat Enterprise Linux (RHEL) 7 and the network adapter is set to E1000 or VMXNET3. **Note** If you are upgrading to Release 2.2 on an ESXi 5.x server (5.1 U2 minimum), you must upgrade the VMware hardware version to 9 before you can select RHEL 7 as the Guest OS.	—

Task Description	Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide
After upgrade, ensure that you clear the browser cache, close the browser, and open a new browser session before you access the Cisco ISE Admin portal. Supported browsers are: • Mozilla Firefox 45.*x* ESR, and 48.0 and above • Google Chrome 53.0 and above • Microsoft Internet Explorer 10.*x* and 11.*x*	—
After upgrade to Release 2.2, the Guest Portals and Guest Types pages appear to be empty initially. This issue occurs when you have From First Login guest type accounts created in Release 1.2 that were never used or is still active. After upgrade, when the system initializes, these accounts take time to migrate. After some time (depending on the number of “From First Login" guest accounts that you created in 1.2), once the data is successfully migrated, you can refresh the Guest Portals and Guest Types pages to view the information. If you no longer need these accounts, you can delete them manually from the Sponsor portal.	—

Task Description	Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide
Join all Cisco ISE nodes with Active Directory again, if you use Active Directory as your external identity source and the connection to Active Directory is lost. After rejoining, perform the external identity source call flows to ensure the connection. • After upgrade, if you log in to the Cisco ISE user interface using an Active Directory administrator account, your login fails because Active Directory join is lost during upgrade. You must use the internal administrator account to log in to Cisco ISE and join Active Directory with it. • If you had enabled certificate-based authentication for administrative access to Cisco ISE (Administration > Admin Access) before upgrade and used Active Directory as your identity source, after upgrade, you will not be able to launch the ISE login page because Active Directory join is lost during upgrade. If you run in to this issue, from the Cisco ISE CLI, start the ISE application in safe mode using the following command: **application start ise safe** This command brings up the Cisco ISE node in safe mode. Perform the following tasks: **1** Log in to the Cisco ISE user interface using the internal administrator account. If you do not remember your password or if your administrator account is locked, see the Cisco Identity Services Engine Hardware Installation Guide Cisco Identity Services Engine Hardware Installation Guide for information on how to reset an administrator password. **2** Join Cisco ISE with Active Directory.	Configure Active Directory as an External Identity Source
Ensure that you have Reverse DNS lookup configured for all Cisco ISE nodes in your distributed deployment in the DNS server(s). Otherwise, you may run into deployment-related issues after upgrade.	—

Task Description	Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide
If you have enabled the Threat-Centric NAC (TC-NAC) service, after you upgrade, the TC-NAC adapters might not be functional. You must restart the adapters from the Threat-Centric NAC pages of the ISE GUI. Select the adapter and click Restart to start the adapter again.	—
Obtain a backup of the Cisco ISE CA certificates and keys from the Primary Administration Node and restore it on the Secondary Administration Node. This ensures that the Secondary Administration Node can function as the root CA or subordinate CA of an external PKI in case of a PAN failure and you promote the Secondary Administration Node to be the Primary Administration Node.	Backup and Restore of Cisco ISE CA Certificates and Keys
After you upgrade a distributed deployment, the Primary Administration Node's root CA certificates are not added to the Trusted Certificates store when both of the following conditions are met: • Secondary Administration Node (Primary Administration Node in the old deployment) is promoted to be the Primary Administration Node in the new deployment • Session services are disabled on the Secondary Administration Node This might result in authentication failures with the following errors: • Unknown CA in chain during a BYOD flow • OCSP unknown error during a BYOD flow You can see these messages when you click the More Details link from the Live Logs page for failed authentications. As a workaround, after you upgrade your deployment and you promote the Secondary Administration Node to become the Primary Administration Node in the new deployment, generate a new ISE Root CA certificate chain from the Admin portal (choose **Administration** > **Certificates** > **Certificate Signing Requests** > **Replace ISE Root CA certificate chain**).	Generate Root CA and Subordinate CAs on the PAN and PSN

Task Description	Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide
Cisco ISE supports some non-Cisco Network Access Devices (NADs). If you deployed non-Cisco NADs prior to Release 2.0 and created policy rules or RADIUS dictionaries to use them, these will continue to work as usual. Release 2.0 and later releases offer several predefined network device profiles that can be applied to non-Cisco devices to support a variety of features such as MAB, dot1x, Change Of Authorization (CoA), and URL redirection to enable flows such as Guest, Posture, and so on. To view the network device profiles, from the Admin portal, choose **Administration** > **Network Resources** > **Network Device Profiles**. To apply a network device profile to a NAD: **1** Choose **Administration** > **Network Resources** > **Network Devices**. **2** Edit the NAD and select the appropriate profile. You can easily apply network device profiles to many NADs at a time by exporting the list of NADs, adding the profiles, and then reimporting the NADs.	Third-Party Network Access Device Support in Cisco ISE
Reset the RSA node secret if you use RSA SecurID server as your external identity source.	RSA Node Secret Reset
Perform a posture update from the Primary Administration Node after upgrade if you have enabled the Posture service.	Download Posture Updates to Cisco ISE
If you had manually configured the Originating Policy Services Node value under SNMP settings, this configuration is lost during upgrade. You must reconfigure this value.	See SNMP Settings under Network Device Definition Settings.
Update the profiler feed service after upgrade to ensure that the most up-to-date OUIs are installed.	From the Cisco ISE Admin portal: **1** Choose **Administration** > **FeedService** > **Profiler**. Ensure that the profiler feed service is enabled. **2** Click **Update Now**.
	—

Task Description	Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide
Check the native supplicant profile that is used in the client provisioning policy and ensure that the wireless SSID is correct. For iOS devices, if the network that you are trying to connect is hidden, check the **Enable if target network is hidden** check box in the **iOS Settings** area.	—

Task Description	Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide
	—

Task Description	Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide
Cisco ISE, Release 2.2 supports the following ciphers. TLS versions 1.0, 1.1, and 1.2 are supported. For EAP-TLS, PEAP, EAP-FAST, EAP-TTLS: • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DES-CBC3-SHA The following ciphers are supported when you check the **Allow weak ciphers for EAP** check box: • RC4-SHA • RC4-MD5 For EAP-FAST Anonymous Provisioning: ADH_WITH_AES_128_SHA **Note** If you have legacy devices such as old IP phones that use these deprecated ciphers authenticating against Cisco ISE, the authentication fails because these devices use legacy ciphers. To allow Cisco ISE to authenticate such legacy devices, after upgrade to Release 2.2, ensure that you update the Allowed Protocols configuration as follows: **1** From the Admin portal, choose **Policy** > **Policy Elements** > **Authentication** > **Allowed Protocols**. **2** Edit the Allowed Protocols service and check the **Allow weak ciphers for EAP** check box. **3** Click **Submit**.	

Task Description	Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide
See the Cisco Identity Services Engine Network Component Compatibility, Release 2.2 for the complete list of Supported Cipher Suites.	
Reconfigure e-mail settings, favorite reports, and data purge settings.	See the Monitoring and Troubleshooting section of the Cisco ISE Administrator Guide.
Check the threshold and/or filters for specific alarms that you need. All the alarms are enabled by default after an upgrade.	
Customize reports based on your needs. If you had customized the reports in the old deployment, the upgrade process overwrites the changes that you made.	
(Applicable only when you upgrade from a Cisco ISE, Release 2.2 LA build to a later release) If you have created SFTP repositories using RSA keys, then when you upgrade the Secondary Administration node to a later release, the SFTP repository becomes inaccessible because the RSA keys were generated from the Primary Administration node. After you upgrade, if you want to access the SFTP repository, you can do one of the following: • Regenerate the RSA keys from the new Primary Administration node. • After upgrade, promote the new Secondary Administration node to be the Primary Administration node.	See the Create Repositories section in the Cisco ISE Administrator Guide for more information.

Post-Upgrade Tasks