The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.
CONTENTS

CHAPTER 1

Before You Begin 1

Supported Upgrade Paths 1
Cisco Secure ACS to Cisco ISE Migration 2
Time Taken for Upgrade 2
Firewall Ports That Must be Open for Communication 3
Export Certificates and Private Keys 3
Create Repository and Copy the Upgrade Bundle 3
Back Up Cisco ISE Configuration and Operational Data from the Primary Administration Node 4
Back Up System Logs from the Primary Administration Node 5
Obtain Active Directory and Internal Administrator Account Credentials 5
Activate MDM Vendor Before Upgrade 5
Record Profiler Configuration 5
Check Load Balancer Configuration 5

CHAPTER 2

Upgrade Methods for Different Types of Deployments 7

Upgrade a Standalone Node 7
Upgrade a Two-Node Deployment 9
Upgrade a Distributed Deployment 11
Verify the Upgrade Process 14

CHAPTER 3

Post-Upgrade Tasks 15

Post-Upgrade Tasks 15

CHAPTER 4

Recover from Upgrade Failures 23

Upgrade Failures 23
Upgrade Fails During Binary Install 25
Before You Begin

Read the following information carefully, and record these configurations (back up, export, obtain screen shots) wherever possible before you begin an upgrade:

- Supported Upgrade Paths, page 1
- Cisco Secure ACS to Cisco ISE Migration, page 2
- Time Taken for Upgrade, page 2
- Firewall Ports That Must be Open for Communication, page 3
- Export Certificates and Private Keys, page 3
- Create Repository and Copy the Upgrade Bundle, page 3
- Back Up Cisco ISE Configuration and Operational Data from the Primary Administration Node, page 4
- Back Up System Logs from the Primary Administration Node, page 5
- Obtain Active Directory and Internal Administrator Account Credentials, page 5
- Activate MDM Vendor Before Upgrade, page 5
- Record Profiler Configuration, page 5
- Check Load Balancer Configuration, page 5

**Supported Upgrade Paths**

You can directly upgrade to Cisco ISE, Release 2.0, from any of the following releases:

- Cisco ISE, Release 1.3
- Cisco ISE, Release 1.3 patch 1 or later
- Cisco ISE, Release 1.4
- Cisco ISE, Release 1.4 patch 3
If you are on a version earlier than Cisco ISE, Release 1.3, you must first upgrade to one of the releases listed above and then upgrade to Release 2.0.

Cisco Secure ACS to Cisco ISE Migration

You can directly migrate to Cisco ISE, Release 2.0 only from Cisco Secure ACS, Releases 5.5 and 5.6. For information about migrating from Cisco Secure ACS, Releases 5.5 and 5.6 to Cisco ISE, Release 2.0, see the Cisco Identity Services Engine Migration Tool Guide.

You cannot migrate to Release 2.0 from Cisco Secure ACS 4.x or earlier versions, Cisco Secure ACS 5.1, 5.2, 5.3, or 5.4, or from Cisco Network Admission Control (NAC) Appliance. From Cisco Secure ACS, Releases 4.x, 5.1, 5.2, 5.3, and 5.4, you must upgrade to ACS, Release 5.5 or 5.6 and then migrate to Cisco ISE, Release 2.0.

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. The data presented here is from a deployment with 25000 users and 250,000 endpoints.

<table>
<thead>
<tr>
<th>Type of Deployment</th>
<th>Node Persona</th>
<th>Time Taken for Upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standalone (2000 endpoints)</td>
<td>Administration, Policy Service, Monitoring</td>
<td>1 hour 20 minutes</td>
</tr>
<tr>
<td>Distributed (25,000 users and 250,000 endpoints)</td>
<td>Secondary Administration</td>
<td>2 hours</td>
</tr>
<tr>
<td></td>
<td>Monitoring</td>
<td>2 hours</td>
</tr>
<tr>
<td></td>
<td>Policy Service</td>
<td>2 hours</td>
</tr>
<tr>
<td></td>
<td>pxGrid</td>
<td>2 hours</td>
</tr>
</tbody>
</table>

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.
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 Identity Services Engine Hardware Installation Guide.

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).

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.

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-1.3.x-and-1.4.x-to-2.0.0.291.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-1.3.x-and-1.4.x-to-2.0.0.291.x86_64.tar.gz disk:`

where `aaa.bbb.ccc.ddd` is the IP address or hostname of the SFTP server and `ise-upgradebundle-1.3.x-and-1.4.x-to-2.0.0.291.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.
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.

---

**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
```

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.

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.

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.
Upgrade Methods for Different Types of Deployments

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

- Upgrade a Standalone Node, page 7
- Upgrade a Two-Node Deployment, page 9
- Upgrade a Distributed Deployment, page 11
- Verify the Upgrade Process, page 14

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."
Upgrade a Standalone Node

Example:
ise/admin# conf
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# repository upgrade
ise/admin(config-Repository)# url disk:
% Warning: Repositories configured from CLI cannot be used from the ISE web UI and are not replicated to other ISE nodes.
ise/admin(config-Repository)# exit
ise/admin(config)# exit

Step 2
From the Cisco ISE command line interface (CLI), enter application upgrade prepare command.
This command copies the upgrade bundle to the local repository “upgrade” that you created in the previous step and lists the MD5 and SHA256 checksum.

Example:
ise/admin# application upgrade prepare ise-upgradebundle-1.3.x-and-1.4.x-to-2.0.0.291.x86_64.tar.gz upgrade
Getting bundle to local machine...
md5: 35a159416afd0900c9da7b3dc6c72043
sha256: e3358ca424d97af67f8bb2bb3574b3e559ce9578d2f36c44cd8ba9e6dddfefd
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y]?

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

Example:
Getting bundle to local machine...
md5: 35a159416ad0f00c9da7dcd6c72043
sha256: e3358ca424d97af67f8bb2bb3574b3e559ce9578d2f36c44cd8ba9e6dddfefd
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y]?

Step 4
From the Cisco ISE CLI, enter the application upgrade proceed command.

Example:
ise45/admin# application upgrade proceed
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
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...
- 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 1/50, RBACUpgradeService(1.5.0.111)... Done in 13 seconds.
- Data upgrade step 2/50, UPSUpgradeHandler(1.5.0.136)... Done in 6 seconds.
- Data upgrade step 3/50, UPSUpgradeHandler(1.5.0.139)... Done in 0 seconds.
- Data upgrade step 4/50, ANCRRegistration(1.5.0.140)... Done in 0 seconds.
- Data upgrade step 5/50, NSFUpgradeService(1.5.0.149)... Done in 11 seconds.
- Data upgrade step 6/50, UPSUpgradeHandler(1.5.0.150)... Done in 3 seconds.
- Data upgrade step 7/50, NetworkAccessUpgrade(1.5.0.151)... Done in 0 seconds.
- Data upgrade step 8/50, UPSUpgradeHandler(1.5.0.156)... Done in 0 seconds.
- Data upgrade step 9/50, NetworkAccessUpgrade(1.5.0.159)... Done in 0 seconds.
- Data upgrade step 10/50, NetworkAccessUpgrade(1.5.0.162)... Done in 1 seconds.
- Data upgrade step 11/50, NSFUpgradeService(1.5.0.180)... Done in 0 seconds.
- Data upgrade step 12/50, NetworkAccessUpgrade(1.5.0.180)... Done in 0 seconds.
Upgrade Methods for Different Types of Deployments

Upgrade a Two-Node Deployment

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

**Figure 1: Cisco ISE Two-Node Administrative Deployment**

![Diagram of 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` command and choose 5 (Refresh Database Statistics) on those nodes.
Upgrade Methods for Different Types of Deployments

Upgrade a Distributed Deployment

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

Figure 2: Cisco ISE Deployment Before Upgrade

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.

Note

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

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

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

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

If your PSN is part of a node group cluster, you must deregister the PSN from the PAN, upgrade it as a standalone node, and register it with the PAN in the new deployment.

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

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

---

**CLI Transcripts of Successful Upgrades**

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

```plaintext
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, CertRegMgmtBootstrapService(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 ....

% 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.

```plaintext
ise/admin# application upgrade ise-upgradebundle-1.3.x-and-1.4.x-to-2.0.0.291.x86_64.tar.gz
sftp
Save the current ADE-OS running configuration? (yes/no) [yes] ?
Please enter yes or no
```
Save the current ADE-OS running configuration? (yes/no) [yes] ?
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Getting bundle to local machine...
  md5: 35a159416afbd090c9da7b3dc6c72043
  sha256: 8b3b43057067b0995ecaf5673c69565c0d0dfa790d8e58d1e998a9f8c7427a
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y] ?
Unbundling Application Package...
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
-Checking VM for minimum hardware requirements
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
STEP 3: Validating data before upgrade...
STEP 4: De-registering node from current deployment.
STEP 5: Taking backup of the configuration data...
STEP 6: Registering this node to primary of new deployment...
STEP 7: Downloading configuration data from primary of new deployment...
STEP 8: Importing configuration data...
STEP 9: Running ISE configuration data upgrade for node specific data...
STEP 10: Running ISE M&T DB upgrade...
ISE Database Mnt schema upgrade completed.
No gather stats needed as this is not PAP or MNT node
% NOTICE: Upgrading ADEOS. Appliance will be rebooted after upgrade completes successfully.
% This application Install or Upgrade requires reboot, rebooting now...

What to Do Next

Verify the Upgrade Process, on page 14

Verify the Upgrade Process

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

• Check the ade.log file for the upgrade process. To display the ade.log file, enter the following command from the Cisco ISE CLI: show logging system ade/ADE.log

• Enter the show version command to verify the build version.

• Enter the show application status ise command to verify that all the services are running.

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

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

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

- Post-Upgrade Tasks, page 15

### 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

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 version 39 and later
- Google Chrome version 43 and later
- Microsoft Internet Explorer 9.x, 10.x and 11.x

**Note**  
If you are using Internet Explorer 10.x, enable TLS 1.1 and TLS 1.2, and disable SSL 3.0 and TLS 1.0 (Internet Options > Advanced).

Adobe Flash Player 11.1.0.0 or above must be installed on the system running your client browser.

The minimum required screen resolution to view the Cisco ISE Admin portal and for a better user experience is 1280 x 800 pixels.

### Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide

---
### Task Description

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 into 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, Release 2.0 for information on how to reset an administrator password.


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.

### Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide

- Configure Active Directory as an External Identity Source

---
<table>
<thead>
<tr>
<th>Task Description</th>
<th>Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Backup and Restore of Cisco ISE CA Certificates and Keys</td>
</tr>
</tbody>
</table>
| 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 | Generate Root CA and Subordinate CAs on the PAN and PSN |
| 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). | |
<table>
<thead>
<tr>
<th>Task Description</th>
<th>Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ISE, Release 2.0 introduces support for some non-Cisco Network Access Devices (NADs).</td>
<td>Network Device Profiles</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Release 2.0 offers 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.</td>
<td></td>
</tr>
<tr>
<td>To view the network device profiles, from the Admin portal, choose Administration &gt; Network Resources &gt; Network Device Profiles.</td>
<td></td>
</tr>
<tr>
<td>To apply a network device profile to a NAD:</td>
<td></td>
</tr>
<tr>
<td>1. Choose Administration &gt; Network Resources &gt; Network Devices.</td>
<td></td>
</tr>
<tr>
<td>2. Edit the NAD and select the appropriate profile.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Reset the RSA node secret if you use RSA SecurID server as your external identity source.</td>
<td>RSA Node Secret Reset</td>
</tr>
<tr>
<td>Perform a posture update from the Primary Administration Node after upgrade if you have enabled the Posture service.</td>
<td>Download Posture Updates to Cisco ISE</td>
</tr>
<tr>
<td>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.</td>
<td>See SNMP Settings under Network Device Definition Settings.</td>
</tr>
<tr>
<td>Update the profiler feed service after upgrade to ensure that the most up-to-date OUIs are installed.</td>
<td>From the Cisco ISE Admin portal:</td>
</tr>
<tr>
<td>1. Choose Administration &gt; FeedService &gt; Profiler. Ensure that the profiler feed service is enabled.</td>
<td>1. Choose Administration &gt; FeedService &gt; Profiler. Ensure that the profiler feed service is enabled.</td>
</tr>
<tr>
<td>2. Click Update Now.</td>
<td>2. Click Update Now.</td>
</tr>
<tr>
<td>Task Description</td>
<td>Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>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 <strong>Enable if target network is hidden</strong> check box in the <strong>iOS Settings</strong> area.</td>
<td>—</td>
</tr>
</tbody>
</table>

Cisco ISE, Release 2.0 supports the following FIPS-compliant ciphers. TLS versions 1.0, 1.1, and 1.2 are supported.

For EAP-TLS, PEAP, EAP-FAST, EAP-TTLS:
- DHE_RSA_WITH_AES_256_SHA256
- DHE_RSA_WITH_AES_128_SHA256
- RSA_WITH_AES_256_SHA256
- RSA_WITH_AES_128_SHA256
- DHE_RSA_WITH_AES_256_SHA
- DHE_RSA_WITH_AES_128_SHA
- RSA_WITH_AES_256_SHA
- RSA_WITH_AES_128_SHA

For EAP-FAST Anonymous Provisioning:
ADH_WITH_AES_128_SHA

Cisco ISE, Release 2.0 does not support non-FIPS compliant ciphers. The following ciphers are not supported:
- RSA_DES_192_CBC3_SHA
- EDH_RSA_DES_192_CBC3_SHA
- EDH_DSS_DES_192_CBC3_SHA
- RSA_RC4_128_SHA
- RSA_RC4_128_MD5
- EDH_RSA_DES_64_CBC_SHA
- EDH_DSS_DES_64_CBC_SHA
- RSA_RC4_128_SHA

**Note** If you have legacy devices that use these deprecated ciphers, contact the Cisco Technical Assistance Center for support.
<table>
<thead>
<tr>
<th>Task Description</th>
<th>Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconfigure e-mail settings, favorite reports, and data purge settings.</td>
<td>See the Monitoring and Troubleshooting section of the Cisco ISE Administrator Guide.</td>
</tr>
<tr>
<td>Check the threshold and/or filters for specific alarms that you need. All the</td>
<td></td>
</tr>
<tr>
<td>alarms are enabled by default after an upgrade.</td>
<td></td>
</tr>
<tr>
<td>Customize reports based on your needs. If you had customized the reports in the</td>
<td></td>
</tr>
<tr>
<td>old deployment, the upgrade process overwrites the changes that you made.</td>
<td></td>
</tr>
</tbody>
</table>
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 2.0.

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 2.0, and restore the configuration and monitoring data on it.

---

• Upgrade Failures, page 23
• Upgrade Fails During Binary Install, page 25

Upgrade Failures

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

```text
% 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.

```text
% 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.

```text
% 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).