Cisco Identity Services Engine Upgrade Guide, Release 2.3

First Published: 2017-07-28

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 **Upgrade Cisco ISE** 1

Cisco ISE Upgrade Overview 1

Upgrade Path 2

Supported Operating System for Virtual Machines 2

CHAPTER 2 **Prepare for Upgrade** 3

Prepare for Upgrade 3

Guidelines to Minimize Upgrade Time and Maximize Efficiency during Upgrade 4

Time Taken for Upgrade 6

Validate Data to Prevent Upgrade Failures 7

Download and Run the Upgrade Readiness Tool 8

Create a Repository and Copy the URT Bundle 8

Run the Upgrade Readiness Tool 9

Change the Name of Authorization Simple Condition if a Predefined Authorization Compound Condition with the Same Name Exists 12

Change VMware Virtual Machine Guest Operating System and Settings 13

Remove Non-ASCII Characters From Sponsor Group Names 13

Firewall Ports that Must be Open for Communication 13

Back Up Cisco ISE Configuration and Operational Data from the Primary Administration Node 13

Back Up System Logs from the Primary Administration Node 14

Check Certificate Validity 15

Delete a Certificate 15

Export Certificates and Private Keys 15

16

Disable PAN Automatic Failover and Disable Scheduled Backups before Upgrading 16

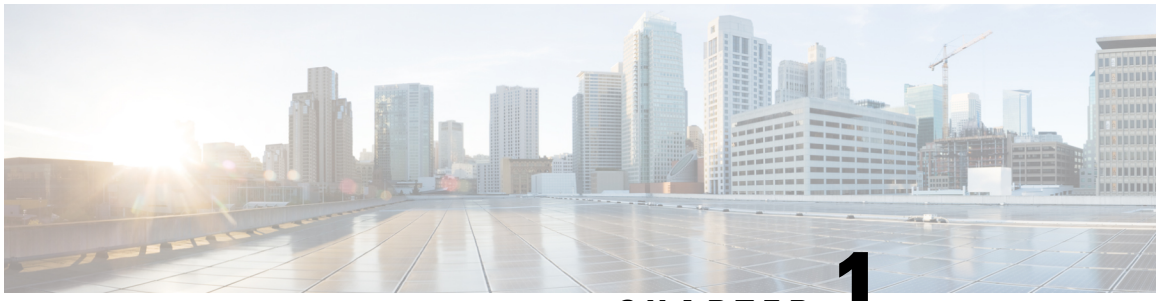
Configure NTP Server and Verify Availability 16

Upgrade Virtual Machine 17
Record Profiler Configuration 17
Obtain Active Directory and Internal Administrator Account Credentials 17
Activate MDM Vendor Before Upgrade 17
Create Repository and Copy the Upgrade Bundle 18
Check the Available Disk Size 19
Check Load Balancer Configuration 19
Log Retention and Resizing MnT Hard Disk 19

CHAPTER 3 **Upgrade a Cisco ISE Deployment from the GUI 21**
Upgrade a Cisco ISE Deployment from the GUI 21
Upgrade From Release 2.0 , 2.0.1, 2.1 or 2.2 to Release 2.3 21
Troubleshoot Upgrade Failures 24

CHAPTER 4 **Upgrade a Cisco ISE Deployment from the CLI 27**

CHAPTER 5 **Perform the Post-Upgrade Tasks 39**
Post-Upgrade Settings and Configurations 39
Verify Virtual Machine Settings 39
Browser Setup 39
Re-Join Active Directory 39
Reverse DNS Lookup 41
Restore Certificates 41
Threat-Centric NAC 41
SMNP Originating Policy Services Node Setting 42
Profiler Feed Service 42
Client Provisioning 42
Online Updates 42
Offline Updates 42
Cipher Suites 43
Monitoring and Troubleshooting 43
Refresh Policies to Trustsec NADs 43
Update Supplicant Provisioning Wizards 43



CHAPTER 1

Upgrade Cisco ISE

- Cisco ISE Upgrade Overview, on page 1
- Upgrade Path, on page 2
- Supported Operating System for Virtual Machines, on page 2

Cisco ISE Upgrade Overview

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

This document describes how to upgrade your Cisco Identity Services Engine (ISE) software on Cisco ISE appliances and virtual machines to Release 2.3.

Note Cisco ISE, Release 2.3 and later offer a new and enhanced **Policy Sets** window that replaces all the existing network access policies and policy sets. When you upgrade from an earlier release to Release 2.3 or later, all the network access policy configurations (including authentication and authorization conditions, rules, policies, profiles, and exceptions) are migrated to the new **Policy Sets** window in the Cisco ISE GUI. For more information on the new policy model, see the "New Policy Model" section in Cisco Identity Services Engine Administrator Guide, Release 2.3

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

Note 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.

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 the following listed references.

Upgrade Path

Two-step Upgrade

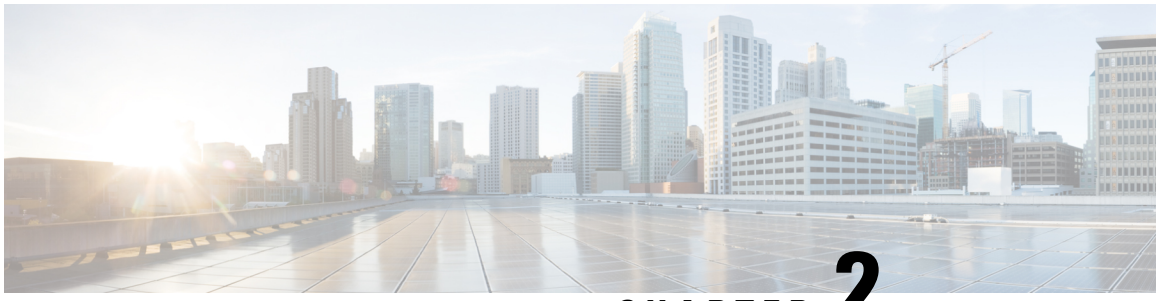
If you are currently using a version earlier than Cisco ISE, Release 2.0, you must first upgrade to one of the releases that are listed above and then upgrade to Release 2.3.

Supported Operating System for Virtual Machines

Cisco ISE runs on the Cisco Application Deployment Engine operating system (ADEOS), which is based on Red Hat Enterprise Linux (RHEL). For Cisco ISE, Release 2.3, ADEOS is based on 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 supported version of Red Hat Enterprise Linux (RHEL). To do this, you must power down the VM, change the Guest Operating System to the supported RHEL version, and power on the VM after the change.

In general, Cisco ISE upgrades with RHEL (Red Hat Enterprise Linux) OS upgrades (later version of Red Hat) take longer time per ISE instance. Additionally, if there are changes in the Oracle Database version in ISE, the new Oracle package is installed during OS upgrade. This may take more time to upgrade. To minimize the time for upgrades, you need to know if the underlying OS is upgraded during ISE upgrades.



CHAPTER 2

Prepare for Upgrade

- Prepare for Upgrade, on page 3
- Guidelines to Minimize Upgrade Time and Maximize Efficiency during Upgrade , on page 4
- Time Taken for Upgrade, on page 6
- Validate Data to Prevent Upgrade Failures, on page 7
- Change the Name of Authorization Simple Condition if a Predefined Authorization Compound Condition with the Same Name Exists, on page 12
- Change VMware Virtual Machine Guest Operating System and Settings, on page 13
- Remove Non-ASCII Characters From Sponsor Group Names, on page 13
- Firewall Ports that Must be Open for Communication, on page 13
- Back Up Cisco ISE Configuration and Operational Data from the Primary Administration Node, on page 13
- Back Up System Logs from the Primary Administration Node, on page 14
- Check Certificate Validity, on page 15
- Delete a Certificate, on page 15
- Export Certificates and Private Keys, on page 15
- Disable PAN Automatic Failover and Disable Scheduled Backups before Upgrading, on page 16
- Configure NTP Server and Verify Availability, on page 16
- Upgrade Virtual Machine, on page 17
- Record Profiler Configuration, on page 17
- Obtain Active Directory and Internal Administrator Account Credentials, on page 17
- Activate MDM Vendor Before Upgrade, on page 17
- Create Repository and Copy the Upgrade Bundle, on page 18
- Check the Available Disk Size , on page 19
- Check Load Balancer Configuration, on page 19
- Log Retention and Resizing MnT Hard Disk, on page 19

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 the 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 2.3, you cannot upgrade to Release 2.3 Patch 1 because of an exception. See CSCvd79546 for details. As a workaround, synchronize the Primary PAN and Secondary PAN before upgrade.

Guidelines to Minimize Upgrade Time and Maximize Efficiency during Upgrade

The following guidelines help you address the issues in your current deployment that you might encounter during the upgrade process. Thus, reducing the overall upgrade downtime with increased efficiency.

- Upgrade to the latest patch in the existing version before starting the upgrade.
- We recommend that you test the upgrade in a staging environment to identify and fix any upgrade issues before upgrading the production networks.
  - All the nodes in the Cisco ISE deployment should be in the same patch level in order to exchange data.

    Note If all the nodes in your deployment are not on the same Cisco ISE version and patch version, you will get a warning message: **Upgrade cannot begin**. This message indicates that the upgrade is in a blocked state. Ensure that all the nodes in the deployment are in the same version (including the patch version, if any) before you begin the upgrade process.

  - Based on the number of PSNs in your deployment and availibilty of personnels, you can install the final version of Cisco ISE you need to upgrade to, apply latest patch, and keep it ready.
  - In case you want to reatain the MnT logs, perform the above tasks for MnT nodes and join the new deployment as MnT nodes. However, if you do not need to retain the operational logs, you can skip the step by re-imaging the MnT nodes.
  - Cisco ISE installation can be done in parallel if you have multi-node deployment without impact to the production deployment. Installing ISE server's in-parallel saves time especially when you are using backup and restore from a previous release.
  - PSN can be added to the new deployment to download the existing polices during the registration process from the PAN. Use ISE latency and bandwidth calculator to understand the latency and bandwidth requirement in Cisco ISE deployment.

- It is a best practice to archieve the old logs and not transit them to the new deployments. This is because operational logs restored in the MnTs are not synchronized to different nodes in case you change the MnT roles later.
- If you have two Data Centers (DC) with full distributed deployment, upgrade the backup DC and test the use cases before upgrading primary DC.

- Download and store the upgrade software in a local repository before upgrade to speed up the process.
- Use the Upgrade Readiness Tool (URT) to detect and fix any configuration data upgrade issues before you start the upgrade process. Most of the upgrade failures occur because of configuration data upgrade issues. The URT validates the data before upgrade to identify, and report or fix the issue, wherever possible. The URT is available as a separate downloadable bundle that can be run on a Secondary Policy Administration node or standalone node. There is no downtime to run this tool. The following video explains how to use the URT:
https://www.cisco.com/c/en/us/td/docs/security/ise/videos/urt/v1-0/cisco-urt.html

Warning Do not run the URT on the Primary Policy Administration Node. The URT tool does not simulate MnT operational data upgrades.

- When upgrading Cisco ISE using the GUI, note that the timeout for the process is four hours. If the process takes more than four hours, the upgrade fails. If upgrading with the Upgrade Readiness Tool (URT) will take you more than four hours, Cisco recommends that you use CLI for this process.
- Take the backup of load balancers before changing the configuration. You can remove the PSNs from the load balancers during the upgrade window and add them back after the upgrade.
- Disable automatic PAN Failover (if configured) and disable Heartbeat between PANs during the upgrade.
- Review the existing policies and rules and remove outdated, redundant, and stale policy and rules.
- Remove unwanted monitoring logs and endpoint data.
- You can take a backup of configuration and operations logs and restore it on a temporary server that is not connected to the network. You can use a remote logging target during the upgrade window.

  You can use the following options after the upgrade to reduce the number of logs that are sent to MnT nodes and improve the performance:

  - Use the MnT collection filters (**Administration > System > Logging > Collection Filters**) to filter incoming logs and avoid duplication of entries in AAA logs.
  - You can create Remote Logging Targets (**Administration > System > Logging > Remote Logging Targets**) and route each individual logging category to specific Logging Target (**System > Logging > Logging categories**).
  - Enable the Ignore Repeated Updates options in the **Administration > System > Settings > Protocols > RADIUS** window to avoid repeated accounting updates.

- Download and use the latest upgrade bundle for upgrade. Use the following query in the Bug Search Tool to find the upgrade related defects that are open and fixed:
https://bst.cloudapps.cisco.com/bugsearch/search?kw=%20ISE%20upgrade&pf=prdNm&sb=anfr&mDt=4&sts=open&bt=custV
- Test all the use cases for the new deployment with fewer users to ensure service continuity.

Time Taken for Upgrade

Upgrade Time Estimation

The following table provides an estimate of the time taken to upgrade Cisco ISE nodes. The exact time taken for upgrade varies depending on several 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.

Note When upgrading ISE using the GUI, note that the timeout for the process is four hours. If the process takes more than four hours, the upgrade fails. If upgrading with the Upgrade Readiness Tool (URT) will take you more than four hours, Cisco recommends that you use CLI for this process.

Type of Deployment	Node Persona	Time Taken for Upgrade
Standalone	Administration, Policy Service, Monitoring	240 minutes + 60 minutes for every 15 GB of data In order to purge old data within the upgrade timeout period, follow the steps in the "Purge Older Operational Data" section in *Cisco Identity Services Engine Administrator Guide, Release 2.4*.
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 2.3 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 will 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
- Number of logs in a Monitoring or Standalone node
- Profiling service, if enabled

Validate Data to Prevent Upgrade Failures

Cisco ISE offers an Upgrade Readiness Tool (URT) that you can run to detect and fix any data upgrade issues before you start the upgrade process.

Most of the upgrade failures occur because of data upgrade issues. The URT is designed to validate the data before upgrade to identify, and report or fix the issue, wherever possible.

The URT is available as a separate downloadable bundle that can be run on a Secondary Administration Node, for high availability and other deployments with multiple nodes, or on the Standalone Node for a single-node deployment. No downtime is necessary when running this tool.

Warning In multiple-node deployments, do not run the URT on the Primary Policy Administration Node.

You can run the URT from the Command-Line Interface (CLI) of the Cisco ISE node. The URT does the following:

1. Checks if the URT is run on a supported version of Cisco ISE. The supported versions are Releases 2.0, 2.0.1, 2.1, and 2.2.
2. Verifies that the URT is run on a standalone Cisco ISE node or a Secondary Policy Administration Node (secondary PAN)
3. Checks if the URT bundle is less than 30 days old—This check is done to ensure that you use the most recent URT bundle
4. Checks if all the prerequisites are met.

   The following prerequisites are checked by the URT:

   - Version compatibility
   - Persona checks
   - Disk space

   Note Verify the available disk size with Disk Requirement Size. If you are required to increase the disk size, reinstall ISE and restore a config backup.

   - NTP server
   - Memory
   - System and trusted certificate validation
5. Clones the configuration database
6. Performs a schema and data upgrade on the cloned database
   - (If the upgrade on the cloned database is successful) Provides an estimate of time it should take for the upgrade to end.

- (If the upgrade is successful) Removes the cloned database.
- (If the upgrade on cloned database fails) Collects the required logs, prompts for an encryption password, generates a log bundle, and stores it in the local disk.

Download and Run the Upgrade Readiness Tool

The Upgrade Readiness Tool (URT) validates the configuration data before you actually run the upgrade to identify any issues that might cause an upgrade failure.

Note The URT bundle (ise-urtbundle-2.3.0.298-1.1.0.SPA.x86_64.tar.gz) is updated with fixes for the following defects:

- CSCvf54091: URT tool fails when importing the config DB to a cloned DB.
- CSCvf58433: ISE URT tool causes backup failure: Could not access the backup script.
- CSCvf53116: Upgrade fails at 25%; ORA-32004: obsolete or deprecated parameter(s).

Before you begin

While running the URT, ensure that you simultaneously do not:

- Back up or restore data
- Perform any persona changes

Step 1 Create a Repository and Copy the URT Bundle, on page 8

Step 2 Run the Upgrade Readiness Tool, on page 9

Create a Repository and Copy the URT Bundle

Create a repository and copy the URT 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.

Before you begin

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

Step 1 Download the URT bundle from Cisco.com (ise-urtbundle-2.3.0.x-1.1.0.SPA.x86_64.tar.gz).

Step 2 Optionally, to save time, copy the URT bundle to the local disk on the Cisco ISE node using the following command:

Run the Upgrade Readiness Tool

The Upgrade Readiness Tool identifies issues with data that might cause an upgrade failure, and reports or fixes the issues, wherever possible. To run the URT:

Before you begin

Having the URT bundle in the local disk saves time.

Enter the **application install** command to install the URT:

```
application install ise-urtbundle-2.3.0.x-1.1.0.SPA.x86_64.tar.gz reponame
```

Example:

```
ise/admin# application install ise-urtbundle-2.3.0.x-1.1.0.SPA.x86_64.tar.gz reponame
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...
Unbundling Application Package...
Verifying Application Signature...
Initiating Application Install...

########################################
# Installing Upgrade Readiness Tool (URT) #
########################################

Checking ISE version compatibility
- Successful

Checking ISE persona
- Successful

Along with Administration, other services (MNT,PROFILER,SESSION) are enabled on this node. Installing
 and running URT might consume additional resources.
Do you want to proceed with installing and running URT now (y/n):y

Checking if URT is recent(<30 days old)
- Successful

Installing URT bundle
- Successful

######################################
# Running Upgrade Readiness Tool (URT) #
######################################
This tool will perform following tasks:
1. Pre-requisite checks
2. Clone config database
3. Copy upgrade files
4. Data upgrade on cloned database
5. Time estimate for upgrade

Pre-requisite checks
====================
Disk Space sanity check
- Successful
NTP sanity
- Successful
Appliance/VM compatibility
```

```
- Successful
Trust Cert Validation
- Successful
System Cert Validation
- Successful
5 out of 5 pre-requisite checks passed

Clone config database
=====================
 [########################################] 100%  Successful


Copy upgrade files
==================
- N/A

Data upgrade on cloned database
===============================
Modifying upgrade scripts to run on cloned database
- Successful

Running schema upgrade on cloned database
- Running db sanity to check and fix if any index corruption
- Auto Upgrading Schema for UPS Model
- Upgrading Schema completed for UPS Model
- Successful

Running sanity after schema upgrade on cloned database
- Successful

Running data upgrade on cloned database
- Data upgrade step 1/97, AuthzUpgradeService(2.0.0.308)... Done in 41 seconds.
- Data upgrade step 2/97, NSFUpgradeService(2.1.0.102)... Done in 1 seconds.
- Data upgrade step 3/97, UPSUpgradeHandler(2.1.0.105)... ..Done in 154 seconds.
- Data upgrade step 4/97, UPSUpgradeHandler(2.1.0.107)... Done in 1 seconds.
- Data upgrade step 5/97, NSFUpgradeService(2.1.0.109)... Done in 0 seconds.
- Data upgrade step 6/97, NSFUpgradeService(2.1.0.126)... Done in 1 seconds.
- Data upgrade step 7/97, NetworkAccessUpgrade(2.1.0.127)... Done in 4 seconds.
- Data upgrade step 8/97, ProfilerUpgradeService(2.1.0.134)... Done in 0 seconds.
- Data upgrade step 9/97, ProfilerUpgradeService(2.1.0.139)... Done in 1 seconds.
- Data upgrade step 10/97, ProfilerUpgradeService(2.1.0.166)... ..Done in 121 seconds.
- Data upgrade step 11/97, NSFUpgradeService(2.1.0.168)... Done in 1 seconds.
- Data upgrade step 12/97, AlarmsUpgradeHandler(2.1.0.169)... Done in 3 seconds.
- Data upgrade step 13/97, RegisterPostureTypes(2.1.0.180)... Done in 2 seconds.
- Data upgrade step 14/97, RegisterPostureTypes(2.1.0.189)... Done in 0 seconds.
- Data upgrade step 15/97, UPSUpgradeHandler(2.1.0.194)... Done in 0 seconds.
- Data upgrade step 16/97, TrustsecWorkflowRegistration(2.1.0.203)... Done in 0 seconds.
- Data upgrade step 17/97, NSFUpgradeService(2.1.0.205)... Done in 0 seconds.
- Data upgrade step 18/97, NetworkAccessUpgrade(2.1.0.207)... Done in 0 seconds.
- Data upgrade step 19/97, NSFUpgradeService(2.1.0.212)... Done in 0 seconds.
- Data upgrade step 20/97, NetworkAccessUpgrade(2.1.0.241)... Done in 2 seconds.
- Data upgrade step 21/97, NetworkAccessUpgrade(2.1.0.242)... Done in 1 seconds.
- Data upgrade step 22/97, UPSUpgradeHandler(2.1.0.244)... Done in 0 seconds.
- Data upgrade step 23/97, ProfilerUpgradeService(2.1.0.248)... Done in 0 seconds.
- Data upgrade step 24/97, NetworkAccessUpgrade(2.1.0.254)... Done in 0 seconds.
- Data upgrade step 25/97, UPSUpgradeHandler(2.1.0.255)... Done in 11 seconds.
- Data upgrade step 26/97, MDMPartnerUpgradeService(2.1.0.257)... Done in 0 seconds.
- Data upgrade step 27/97, NetworkAccessUpgrade(2.1.0.258)... Done in 0 seconds.
- Data upgrade step 28/97, ProfilerUpgradeService(2.1.0.258)... Done in 0 seconds.
- Data upgrade step 29/97, MDMPartnerUpgradeService(2.1.0.258)... Done in 2 seconds.
- Data upgrade step 30/97, UPSUpgradeHandler(2.1.0.279)... Done in 2 seconds.
- Data upgrade step 31/97, NSFUpgradeService(2.1.0.282)... Done in 0 seconds.
- Data upgrade step 32/97, NetworkAccessUpgrade(2.1.0.288)... Done in 0 seconds.
- Data upgrade step 33/97, NetworkAccessUpgrade(2.1.0.295)... Done in 0 seconds.
```

```
- Data upgrade step 34/97, CertMgmtUpgradeService(2.1.0.296)... Done in 0 seconds.
- Data upgrade step 35/97, NetworkAccessUpgrade(2.1.0.299)... Done in 0 seconds.
- Data upgrade step 36/97, NetworkAccessUpgrade(2.1.0.322)... Done in 1 seconds.
- Data upgrade step 37/97, NetworkAccessUpgrade(2.1.0.330)... Done in 1 seconds.
- Data upgrade step 38/97, NSFUpgradeService(2.1.0.353)... Done in 0 seconds.
- Data upgrade step 39/97, ProfilerUpgradeService(2.1.0.354)... Done in 0 seconds.
- Data upgrade step 40/97, NSFUpgradeService(2.1.0.427)... Done in 1 seconds.
- Data upgrade step 41/97, NSFUpgradeService(2.1.101.145)... Done in 0 seconds.
- Data upgrade step 42/97, ProfilerUpgradeService(2.1.101.145)... Done in 0 seconds.
- Data upgrade step 43/97, UPSUpgradeHandler(2.1.101.188)... Done in 1 seconds.
- Data upgrade step 44/97, NetworkAccessUpgrade(2.2.0.007)... Done in 0 seconds.
- Data upgrade step 45/97, UPSUpgradeHandler(2.2.0.118)... Done in 5 seconds.
- Data upgrade step 46/97, GuestAccessUpgradeService(2.2.0.124)... Done in 19 seconds.
- Data upgrade step 47/97, NSFUpgradeService(2.2.0.135)... Done in 0 seconds.
- Data upgrade step 48/97, NSFUpgradeService(2.2.0.136)... Done in 1 seconds.
- Data upgrade step 49/97, NetworkAccessUpgrade(2.2.0.137)... Done in 0 seconds.
- Data upgrade step 50/97, NetworkAccessUpgrade(2.2.0.143)... Done in 17 seconds.
- Data upgrade step 51/97, NSFUpgradeService(2.2.0.145)... Done in 5 seconds.
- Data upgrade step 52/97, NSFUpgradeService(2.2.0.146)... Done in 2 seconds.
- Data upgrade step 53/97, NetworkAccessUpgrade(2.2.0.155)... Done in 0 seconds.
- Data upgrade step 54/97, CdaRegistration(2.2.0.156)... Done in 1 seconds.
- Data upgrade step 55/97, NetworkAccessUpgrade(2.2.0.161)... Done in 0 seconds.
- Data upgrade step 56/97, UPSUpgradeHandler(2.2.0.166)... Done in 0 seconds.
- Data upgrade step 57/97, NetworkAccessUpgrade(2.2.0.169)... Done in 1 seconds.
- Data upgrade step 58/97, UPSUpgradeHandler(2.2.0.169)... Done in 0 seconds.
- Data upgrade step 59/97, NetworkAccessUpgrade(2.2.0.180)... Done in 0 seconds.
- Data upgrade step 60/97, CertMgmtUpgradeService(2.2.0.200)... Done in 0 seconds.
- Data upgrade step 61/97, NetworkAccessUpgrade(2.2.0.208)... Done in 0 seconds.
- Data upgrade step 62/97, RegisterPostureTypes(2.2.0.218)... Done in 2 seconds.
- Data upgrade step 63/97, NetworkAccessUpgrade(2.2.0.218)... Done in 1 seconds.
- Data upgrade step 64/97, NetworkAccessUpgrade(2.2.0.222)... Done in 0 seconds.
- Data upgrade step 65/97, NetworkAccessUpgrade(2.2.0.223)... Done in 0 seconds.
- Data upgrade step 66/97, NetworkAccessUpgrade(2.2.0.224)... Done in 2 seconds.
- Data upgrade step 67/97, SyslogTemplatesRegistration(2.2.0.224)... Done in 0 seconds.
- Data upgrade step 68/97, ReportUpgradeHandler(2.2.0.242)... Done in 0 seconds.
- Data upgrade step 69/97, IRFUpgradeService(2.2.0.242)... Done in 0 seconds.
- Data upgrade step 70/97, LocalHostNADRegistrationService(2.2.0.261)... Done in 0 seconds.
- Data upgrade step 71/97, NetworkAccessUpgrade(2.2.0.300)... Done in 0 seconds.
- Data upgrade step 72/97, CertMgmtUpgradeService(2.2.0.300)... Done in 1 seconds.
- Data upgrade step 73/97, NSFUpgradeService(2.2.0.323)... Done in 0 seconds.
- Data upgrade step 74/97, NetworkAccessUpgrade(2.2.0.330)... Done in 1 seconds.
- Data upgrade step 75/97, NSFUpgradeService(2.2.0.340)... Done in 0 seconds.
- Data upgrade step 76/97, NetworkAccessUpgrade(2.2.0.340)... Done in 0 seconds.
- Data upgrade step 77/97, NetworkAccessUpgrade(2.2.0.342)... Done in 0 seconds.
- Data upgrade step 78/97, AuthzUpgradeService(2.2.0.344)... Done in 0 seconds.
- Data upgrade step 79/97, RegisterPostureTypes(2.2.0.350)... Done in 38 seconds.
- Data upgrade step 80/97, ProfilerUpgradeService(2.2.0.359)... Done in 0 seconds.
- Data upgrade step 81/97, DictionaryUpgradeRegistration(2.2.0.374)... Done in 19 seconds.
- Data upgrade step 82/97, UPSUpgradeHandler(2.2.0.403)... Done in 0 seconds.
- Data upgrade step 83/97, DictionaryUpgradeRegistration(2.2.0.410)... Done in 0 seconds.
- Data upgrade step 84/97, UPSUpgradeHandler(2.3.0.100)... Done in 20 seconds.
- Data upgrade step 85/97, UPSUpgradeHandler(2.3.0.110)... Done in 1 seconds.
- Data upgrade step 86/97, NetworkAccessUpgrade(2.3.0.145)... Done in 0 seconds.
- Data upgrade step 87/97, NodeGroupUpgradeService(2.3.0.155)... Done in 0 seconds.
- Data upgrade step 88/97, IRFUpgradeService(2.3.0.155)... Done in 0 seconds.
- Data upgrade step 89/97, UPSUpgradeHandler(2.3.0.158)... Done in 0 seconds.
- Data upgrade step 90/97, NetworkAccessUpgrade(2.3.0.178)... Done in 1 seconds.
- Data upgrade step 91/97, NetworkAccessUpgrade(2.3.0.182)... Done in 0 seconds.
- Data upgrade step 92/97, CertMgmtUpgradeService(2.3.0.194)... Done in 4 seconds.
- Data upgrade step 93/97, UPSUpgradeHandler(2.3.0.201)... Done in 0 seconds.
- Data upgrade step 94/97, NSFUpgradeService(2.3.0.233)... Done in 0 seconds.
- Data upgrade step 95/97, ProfilerUpgradeService(2.3.0.233)... Done in 1 seconds.
- Data upgrade step 96/97, GuestAccessUpgradeService(2.3.0.233)... Done in 8 seconds.
- Successful
```

```
Running data upgrade for node specific data on cloned database
- Successful

Time estimate for upgrade
=========================
(Estimates are calculated based on size of config and mnt data only. Network latency between PAN and
 other nodes
is not considered in calculating estimates)
Estimated time for each node (in mins):
upsdev-vm11(STANDALONE):102


Application successfully installed
```

In case the application is not installed successfully during the above execution, URT returns the cause of upgrade failure. You need fix the issues and re-run the URT.

Change the Name of Authorization Simple Condition if a Predefined Authorization Compound Condition with the Same Name Exists

Cisco ISE comes with several predefined authorization compound conditions. If you have an authorization simple condition (user defined) in the old deployment that has the same name as that of a predefined authorization compound condition, then the upgrade process fails. Before you upgrade, ensure that you rename the authorization simple conditions that have any of the following predefined authorization compound condition names:

- Compliance_Unknown_Devices
- Non_Compliant_Devices
- Compliant_Devices
- Non_Cisco_Profiled_Phones
- Switch_Local_Web_Authentication
- Catalyst_Switch_Local_Web_Authentication
- Wireless_Access
- BYOD_is_Registered
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MAC_in_SAN
- Network_Access_Authentication_Passed

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 supported Red Hat Enterprise Linux (RHEL) version. To do this, you must power down the VM, update the Guest Operating System, 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-ASCII Characters From Sponsor Group Names

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

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

Firewall Ports that Must be Open for Communication

If you have a firewall that is 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.

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 backup 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 runs 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 the 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 these repository types are all either read-only or their protocol does not support the file listing.

1. Choose **Administration > Maintenance > 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.

   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.

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.

Note Cisco ISE allows you to obtain a backup from an ISE node (A) and restore it on another ISE node (B), both having the same hostnames (but different IP addresses). However, after you restore the backup on node B, do not change the hostname of node B because it might cause issues with certificates and portal group tags.

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 Certificate Validity

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 in the **Expiration Date** field of the **Trusted Certificates** and **System Certificates** windows (**Administration > System > Certificates > Certificate Management**), and renew them, if necessary, before upgrade.

Also check the validity in the **Expiration Date** field of the certificates in the **CA Certificates** window (**Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**), and renew them, if necessary, before upgrade.

Delete a Certificate

In order to delete an expired certificate, perform the following steps:

Step 1 Choose **Administration > System > Certificates > Certificate Management > System Certificates**.
Step 2 Select the expired certificate.
Step 3 Click **Delete**.
Step 4 Choose **Administration > System > Certificates > Certificate Management > Trusted Certificates**.
Step 5 Select the expired certificate.
Step 6 Click **Delete**.
Step 7 Choose **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**.
Step 8 Select the expired certificate.
Step 9 Click **Delete**.

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).

Step 1 Choose **Administration > System > Certificates > Certificate Management > System Certificates**.
Step 2 Select the certificate and click **Export**.
Step 3 Select **Export Certificates and Private Keys** radio button.
Step 4 Enter the **Private Key Password** and **Confirm Password**.
Step 5 Click **Export**.

- All certificates from the Trusted Certificates Store of the Primary Administration Node. Record the certificate configuration (what service the certificate was used for).

Step 1 Choose **Administration > System > Certificates > Certificate Management > Trusted Certificates**.

Step 2 Select the certificate and click **Export**.

Step 3 Click **Save File** to export the certificate.

Step 4 Choose **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**.

Step 5 Select the certificate and click **Export**.

Step 6 Select **Export Certificates and Private Keys** radio button.

Step 7 Enter the **Private Key Password** and **Confirm Password**.

Step 8 Click **Export**.

Step 9 Click **Save File** to export the certificate.

Disable PAN Automatic Failover and Disable Scheduled Backups before Upgrading

You cannot perform deployment changes when running a backup in Cisco ISE. Therefore, you must disable automatic configurations in order to ensure that they do not interfere with the upgrade. Ensure that you disable the following configurations before you upgrade Cisco ISE:

- Primary Administration Node Automatic Failover—If you have configured the Primary Administration Node for an automatic failover, be sure to disable the automatic failover option before you upgrade Cisco ISE.
- Scheduled Backups—When planning your deployment upgrade, reschedule the backups after the upgrade. You can choose to disable the backup schedules and recreate them after the 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 only a single time, be sure to disable it before upgrade.

Configure NTP Server and Verify Availability

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.

Upgrade Virtual Machine

Cisco ISE software has to be in synchronization with the chip and appliance capacity to support latest CPU/Memory capacity available in the UCS Hardware. As ISE version progresses, support for older hardware will be phased out and newer hardware is introduced. It is a good practice to upgrade Virtual Machine (VM) capacity for better performance. When planning VM upgrades, we highly recommend to use OVA files to install ISE software. Each OVA file is a package that contains files used to describe the VM and reserves the required hardware resources on the appliance for Cisco ISE Software Installation.

For more information about the VM and hardware requirements, see the "Hardware and Virtual Appliance Requirements" in Cisco Identity Services Engine Installation Guide

Cisco ISE VMs need dedicated resources in the VM infrastructure. ISE needs adequate amount of CPU cores akin to hardware appliance for performance and scale. Resource sharing is found to impact performance with high CPU, delays in user authentications, registrations, delay and drops in logs, reporting, dashboard responsiveness, etc. This directly impacts the end-user and admin user experience in your enterprise.

Note It is important that you use reserved resources for CPU, memory and hard disk space during the upgrade instead of shared resources.

If you are upgrading from VM based out of 33x5 appliance, then the upgraded VM need to use more CPU core(OVA for 3515 allocated approximately 6 Core and OVA for 3595 uses 8 Core/64GB RAM with HT enabled). Check out the OVA requirements for ISE 2.4 for more details.

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>** >). Select the node and click **Edit Node**. In the **Edit Node** page, go to the **Profiling Configuration** tab. You can make a note of the configuration information 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 the 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.

Ensure that your Internet connection to the repository is good.

Note When you download an upgrade bundle from a repository to a node, the download times out if it takes more than 35 minutes to complete. This issue occurs because of poor Internet bandwidth.

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 (file size is around 9GB) from the repository to the node, the download times out if it takes more than 35 minutes to complete.
- If you are using a local disk to store your configuration files, the files will be deleted when you perform the upgrade. Hence, we recommend that you create a Cisco ISE repository and copy the files to this repository.

Download the upgrade bundle from Cisco.com.

To upgrade to Release 2.3, there are two upgrade bundles available:

- ise-upgradebundle-2.0.x-to-2.3.0.x.SPA.x86_64.tar.gz—Use this bundle to upgrade from Release 2.0 or 2.0.1 to 2.3
- ise-upgradebundle-2.3.0.x.SPA.x86_64.tar.gz—Use this bundle to upgrade from Release 2.1 or 2.2 to 2.3

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-2.0.x-to-2.3.0.x.SPA.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-2.0.x-to-2.3.0.x.SPA.x86_64.tar.gz* **disk:/**

   aaa.bbb.ccc.ddd is the IP address or hostname of the SFTP server and *ise-upgradebundle-2.0.x-to-2.3.0.x.SPA.x86_64.tar.gz* is the name of the upgrade bundle.

Check the Available Disk Size

Ensure that you have allocated the required disk space for virtual machines. See Cisco ISE Installation Guide for more details. If you need to increase the disk size, you will need to reinstall ISE and restore a config backup.

Check Load Balancer Configuration

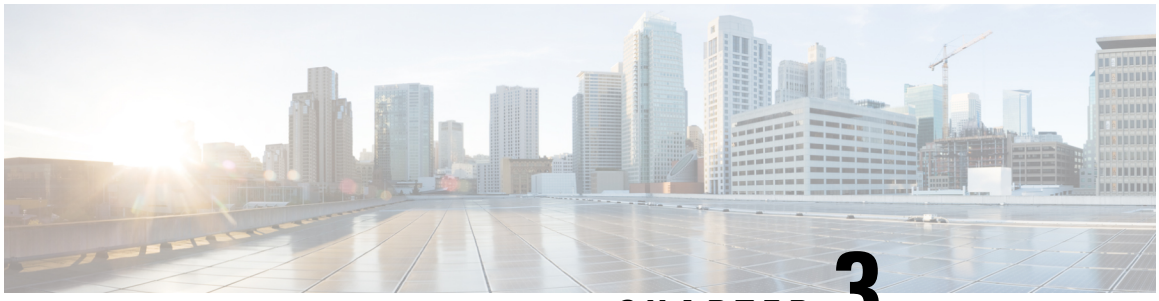
If you are using any load balancer between the Primary Administration Node (PAN) and the Policy Service node (PSN), ensure that the session timeout that is configured on the load balancer does not affect the upgrade process. If the session timeout is set to a lower value, it might affect the upgrade 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.

Log Retention and Resizing MnT Hard Disk

Upgrade does not need changes to the MnT disk capacity. However, if you are consistently filling up the logs and need greater hardware capacity you can plan out the hard disk size for MnT depending on your log retention needs. It is important to understand that log retention capacity has increased many folds from Cisco ISE, Release 2.2.

You can also active collection filters (go to **Administration** > **System** > **Logging** > **Collection filters**) for unnecessary logs from different devices that can overwhelm your Cisco ISE MnT.

See the ISE storage requirements under Cisco ISE performance and scalability community page. The table lists log retention based on number of endpoints for RADIUS and number of Network devices for TACACS+. Log retention should be calculated for both TACACS+ and/or RADIUS separately.



CHAPTER 3

Upgrade a Cisco ISE Deployment from the GUI

- Upgrade a Cisco ISE Deployment from the GUI, on page 21
- Upgrade From Release 2.0 , 2.0.1, 2.1 or 2.2 to Release 2.3, on page 21
- Troubleshoot Upgrade Failures, on page 24

Upgrade a Cisco ISE Deployment from the GUI

Cisco ISE offers a GUI-based centralized upgrade from the Admin portal. The upgrade process is much simplified, and the progress of the upgrade and the status of the nodes are displayed on the screen.

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

The GUI-based upgrade from the Admin portal is supported only if you are currently on Release 2.0 or later and want to upgrade to Release 2.0.1 or later.

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

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

Before you begin

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

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

Step 2

Step 3 Click **Proceed**.

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

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

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

Step 5 Download the upgrade bundle from the repository to the nodes:

a) Check the check box next to the nodes to which you want to download the upgrade bundle.

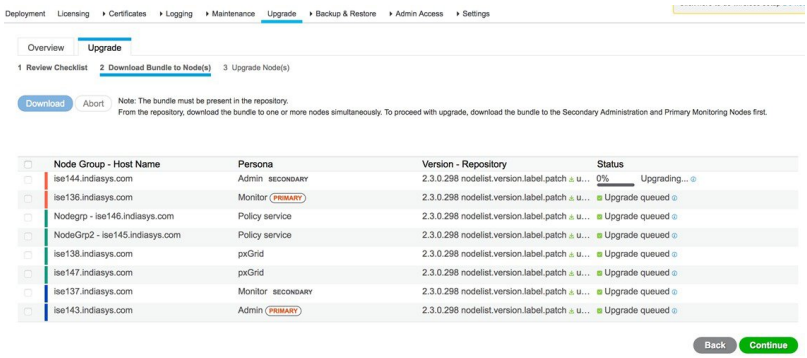
b) Click **Download**.

The **Select Repository and Bundle** window appears.

c) Select the repository.

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

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.

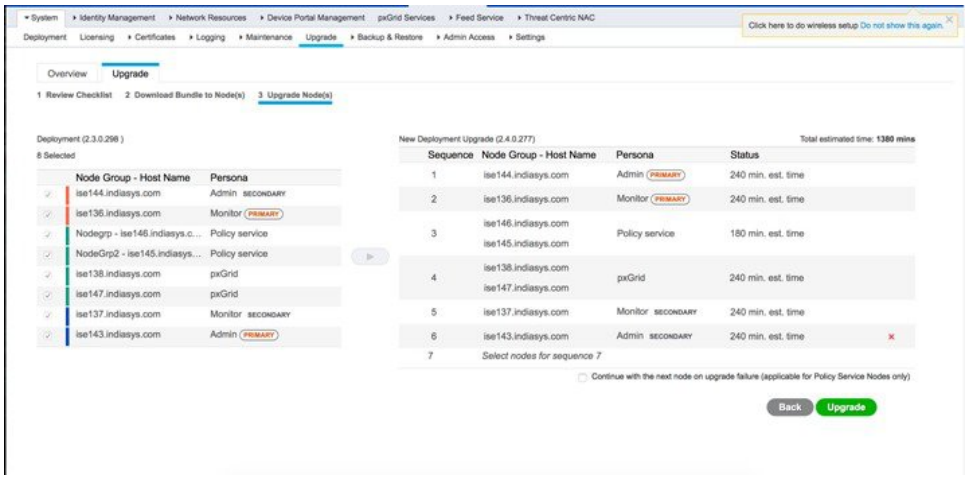
e) Click **Confirm**.

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

Step 6 Click **Continue**.

The **Upgrade Nodes** window appears.

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



Step 7 Choose the upgrade sequence.

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

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

   You can upgrade the Policy Service Nodes in sequence or in parallel. You can select a set of Policy Service Nodes and upgrade them in parallel.

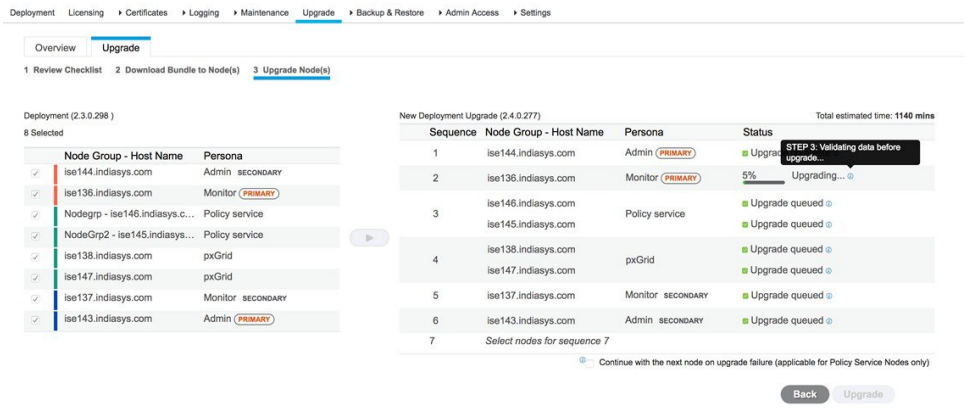
d) Select the Secondary Monitoring Node and move it to the new deployment.
e) Finally, select the Primary Administration Node and move it to the new deployment.

Step 8 Check the **Continue with upgrade on failure** check box if you want to continue with the upgrade even if the upgrade fails on any of the Policy Service Nodes in the upgrade sequence.

This option is not applicable for the Secondary Administration Node and the Primary Monitoring Node. If any one of these nodes fail, the upgrade process is rolled back. If any of the Policy Service Nodes fail, the Secondary Monitoring Node and the Primary Administration Node are not upgraded and remain in the old deployment.

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

Figure 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*.

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

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

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

Note If the posture data update process is running on the Primary Administration Node in the new deployment, you cannot register a node to the Primary Administration Node. You can either wait till the posture update process is over (which might take approximately 20 minutes) or disable the posture auto-update feature from the **Updates** window while upgrading or registering a node to the new deployment. The navigation path for this window is **Administration** > **System** > **Settings** > **Posture** > **Updates**.

Troubleshoot Upgrade Failures

Upgrade Bundle Download Via the GUI Times Out

Before the 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 Cisco ISE version and patch version.

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

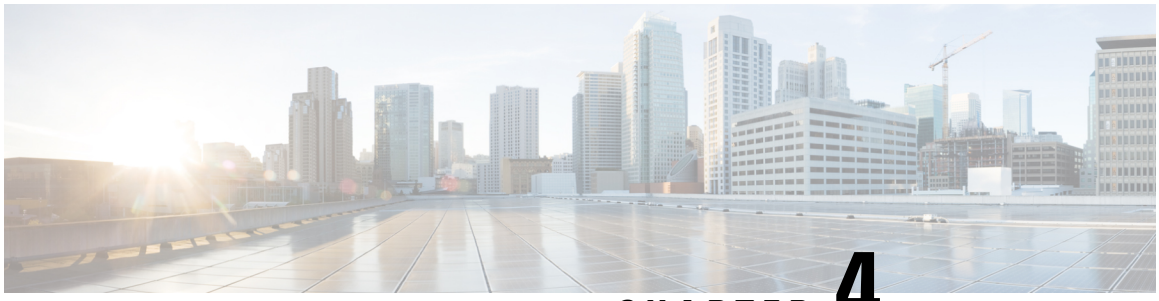
    Note If you remove the Secondary Administration Node from the Upgrade page in the Admin portal, you cannot continue with the upgrade from the GUI. Hence, we recommend that you continue the upgrade from the CLI for the rest of the nodes.

  - 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 the screen to proceed with your 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 2.3. Register the node to the new deployment as a Secondary Administration Node.



CHAPTER 4

Upgrade a Cisco ISE Deployment from the CLI

- Upgrade Process, on page 27
- Verify the Upgrade Process, on page 35
- Recover from Upgrade Failures, on page 35
- Roll Back to the Previous Version of ISO Image, on page 38

Upgrade Process

The upgrade process using CLI depends on the deployment type.

Upgrade a Standalone Node

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

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

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

We recommend that you run the **application upgrade prepare** and **proceed** commands as described below.

Before you begin

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

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-2.3.0.x.x86_64.tar.gz upgrade

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

Application upgrade preparation successful
```

Step 3 **Note** After beginning the upgrade, you can view the progress of the upgrade by logging in via SSH and using the **show application status ise** command. The following message appears: % NOTICE: Identity Services Engine upgrade is in progress...

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

Example:

```
ise/admin# application upgrade proceed
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
-Checking VM for minimum hardware requirements
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
-Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: Taking backup of the configuration data...
STEP 5: Running ISE configuration database schema upgrade...
- Running db sanity to check and fix if any index corruption
- Auto Upgrading Schema for UPS Model
- Upgrading Schema completed for UPS Model
ISE database schema upgrade completed.
% Warning: Sanity test found some indexes missing in CEPM schema. Please recreate missing indexes
after upgrade using app configure ise cli
STEP 6: Running ISE configuration data upgrade...
- Data upgrade step 1/14, UPSUpgradeHandler(2.3.0.100)... Done in 53 seconds.
- Data upgrade step 2/14, UPSUpgradeHandler(2.3.0.110)... Done in 1 seconds.
- Data upgrade step 3/14, NetworkAccessUpgrade(2.3.0.145)... Done in 0 seconds.
- Data upgrade step 4/14, NodeGroupUpgradeService(2.3.0.155)... Done in 0 seconds.
- Data upgrade step 5/14, IRFUpgradeService(2.3.0.155)... Done in 0 seconds.
- Data upgrade step 6/14, UPSUpgradeHandler(2.3.0.158)... Done in 0 seconds.
- Data upgrade step 7/14, NetworkAccessUpgrade(2.3.0.178)... Done in 0 seconds.
- Data upgrade step 8/14, NetworkAccessUpgrade(2.3.0.182)... Done in 0 seconds.
- Data upgrade step 9/14, CertMgmtUpgradeService(2.3.0.194)... Done in 3 seconds.
- Data upgrade step 10/14, UPSUpgradeHandler(2.3.0.201)... Done in 0 seconds.
- Data upgrade step 11/14, NSFUpgradeService(2.3.0.233)... Done in 0 seconds.
- Data upgrade step 12/14, ProfilerUpgradeService(2.3.0.233)... Done in 0 seconds.
- Data upgrade step 13/14, GuestAccessUpgradeService(2.3.0.233)... Done in 7 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.

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/gc/pxgrid-controller-1.0.4.18-dist.tar.gz: remove failed: No such file or
directory

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

Broadcast message from root@IS137 (pts/3) (Fri Jun  2 12:22:49 2017):

Trying to stop processes gracefully. Reload might take approximately 3 mins

Broadcast message from root@IS137 (pts/3) (Fri Jun  2 12:22:49 2017):

Trying to stop processes gracefully. Reload might take approximately 3 mins

Broadcast message from root@IS137 (pts/3) (Fri Jun  2 12:23:10 2017):

The system is going down for reboot NOW

Broadcast message from root@IS137 (pts/3) (Fri Jun  2 12:23:10 2017):

The system is going down for reboot NOW
```

The upgrade is now complete.

What to do next

Verify the Upgrade Process, on page 35

Upgrade a Two-Node Deployment

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

Figure 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 upgraded primary node when it restarts.

Step 2 Upgrade node A.

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

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

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

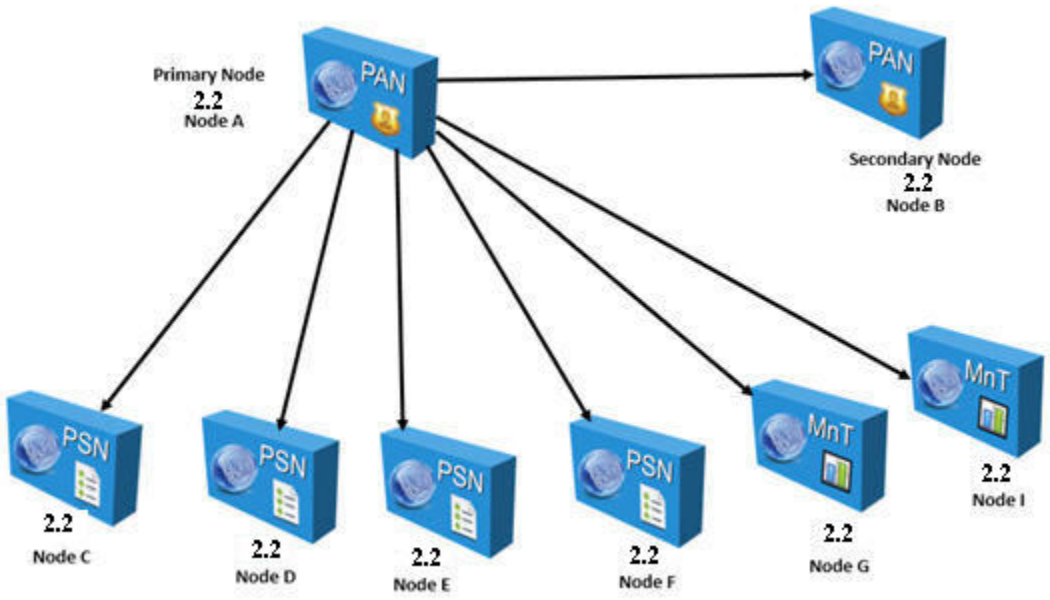
What to do next

Verify the Upgrade Process, on page 35

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



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

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 *Prepare for Upgrade* section.
- When you upgrade a complete Cisco ISE deployment, Domain Name System (DNS) server resolution (both forward and reverse lookups) is mandatory; otherwise, the upgrade fails.

Step 1 Upgrade the Secondary Administration Node (node B) from the CLI.

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

Step 2 Upgrade one of your Monitoring nodes (node G) to the new deployment.

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

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

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

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

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

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

Step 4 (If you have an IPN node in your deployment) Deregister the IPN node from the Primary Administration Node.

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

Step 5 If you have a second Monitoring node (node I) in your old deployment, you must do the following:

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

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

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

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

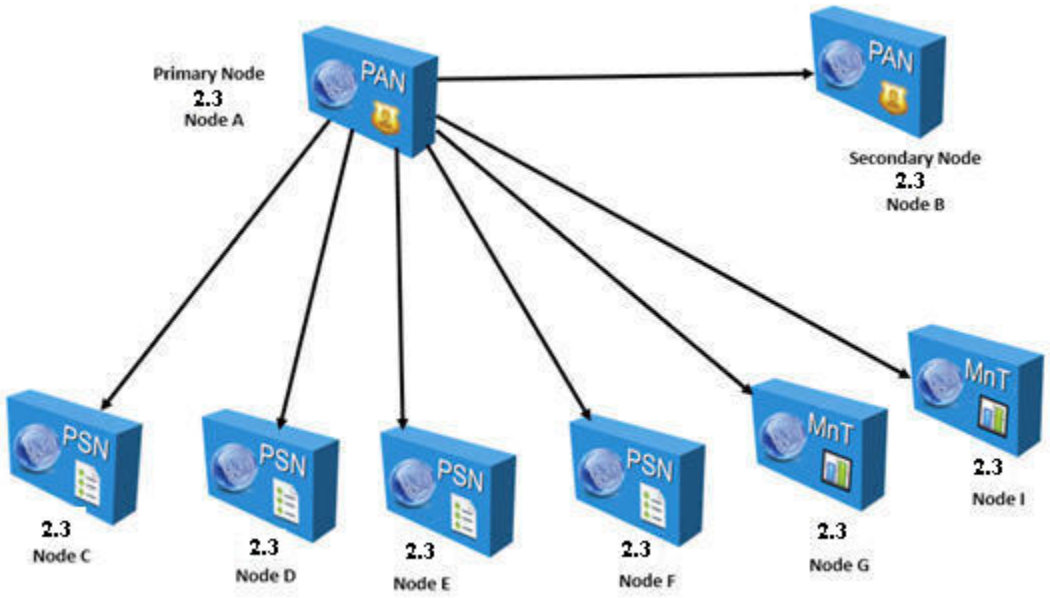
Step 6 Finally, upgrade the Primary Administration Node (node A).

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

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

Example

Figure 6: Cisco ISE Deployment After Upgrade



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

```
ise74/admin# application upgrade proceed
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
-Checking VM for minimum hardware requirements
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
-Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: De-registering node from current deployment...
STEP 5: Taking backup of the configuration data...
STEP 6: Running ISE configuration database schema upgrade...
- Running db sanity to check and fix if any index corruption
- Auto Upgrading Schema for UPS Model
- Upgrading Schema completed for UPS Model
ISE database schema upgrade completed.
% Warning: Sanity test found some indexes missing in CEPM schema. Please recreate missing
indexes after upgrade using app configure ise cli
STEP 7: Running ISE configuration data upgrade...
- Data upgrade step 1/14, UPSUpgradeHandler(2.3.0.100)... Done in 48 seconds.
- Data upgrade step 2/14, UPSUpgradeHandler(2.3.0.110)... Done in 2 seconds.
- Data upgrade step 3/14, NetworkAccessUpgrade(2.3.0.145)... Done in 0 seconds.
- Data upgrade step 4/14, NodeGroupUpgradeService(2.3.0.155)... Done in 0 seconds.
- Data upgrade step 5/14, IRFUpgradeService(2.3.0.155)... Done in 0 seconds.
- Data upgrade step 6/14, UPSUpgradeHandler(2.3.0.158)... Done in 0 seconds.
- Data upgrade step 7/14, NetworkAccessUpgrade(2.3.0.178)... Done in 0 seconds.
- Data upgrade step 8/14, NetworkAccessUpgrade(2.3.0.182)... Done in 0 seconds.
- Data upgrade step 9/14, CertMgmtUpgradeService(2.3.0.194)... Done in 3 seconds.
- Data upgrade step 10/14, UPSUpgradeHandler(2.3.0.201)... Done in 0 seconds.
- Data upgrade step 11/14, NSFUpgradeService(2.3.0.233)... Done in 0 seconds.
- Data upgrade step 12/14, ProfilerUpgradeService(2.3.0.233)... Done in 1 seconds.
- Data upgrade step 13/14, GuestAccessUpgradeService(2.3.0.233)... Done in 9 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 database upgrade...
ISE M&T Log Processor is not running
ISE database M&T schema upgrade completed.

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/gc/pxgrid-controller-1.0.4.18-dist.tar.gz: remove failed: No such
 file or directory

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

Broadcast message from root@IS133 (pts/1) (Fri Jun  2 12:36:51 2017):

Trying to stop processes gracefully. Reload might take approximately 3 mins

Broadcast message from root@IS133 (pts/1) (Fri Jun  2 12:36:51 2017):

Trying to stop processes gracefully. Reload might take approximately 3 mins

Broadcast message from root@IS133 (pts/1) (Fri Jun  2 12:37:12 2017):

The system is going down for reboot NOW

Broadcast message from root@IS133 (pts/1) (Fri Jun  2 12:37:12 2017):

The system is going down for reboot 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...
% Warning: Sanity test found some indexes missing in CEPM schema. Please recreate missing
indexes after upgrade using app configure ise cli
STEP 9: Running ISE configuration data upgrade for node specific data...
STEP 10: Running ISE M&T database upgrade...
ISE M&T Log Processor is disabled
ISE database M&T schema upgrade completed.

Gathering Config schema(CEPM) stats ....
% NOTICE: Upgrading ADEOS. Appliance will be rebooted after upgrade completes successfully.
warning: file /opt/xgrid/gc/pxgrid-controller-1.0.4.18-dist.tar.gz: remove failed: No such
 file or directory

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

Broadcast message from root@IS136 (pts/1) (Fri Jun  2 15:16:14 2017):

Trying to stop processes gracefully. Reload might take approximately 3 mins

Broadcast message from root@IS136 (pts/1) (Fri Jun  2 15:16:14 2017):
```

```
Trying to stop processes gracefully. Reload might take approximately 3 mins

Broadcast message from root@IS136 (pts/1) (Fri Jun  2 15:16:35 2017):

The system is going down for reboot NOW

Broadcast message from root@IS136 (pts/1) (Fri Jun  2 15:16:35 2017):

The system is going down for reboot NOW
```

What to do next

Verify the Upgrade Process, on page 35

Verify the Upgrade Process

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

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

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

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

Recover from Upgrade Failures

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

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

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

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

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

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

Upgrade Failures

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

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

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

Configuration and Data Upgrade Errors

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

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

Remediation Errors

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

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

Validation Errors

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

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

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

Application Binary Upgrade Errors

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

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

Other Types of Errors

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

Reimage

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

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

Upgrade after Failure

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

- Analyze the logs. Check the support bundle for errors.

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

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

Upgrade Progress

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

Upgrade Failures during Binary Install

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

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

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

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

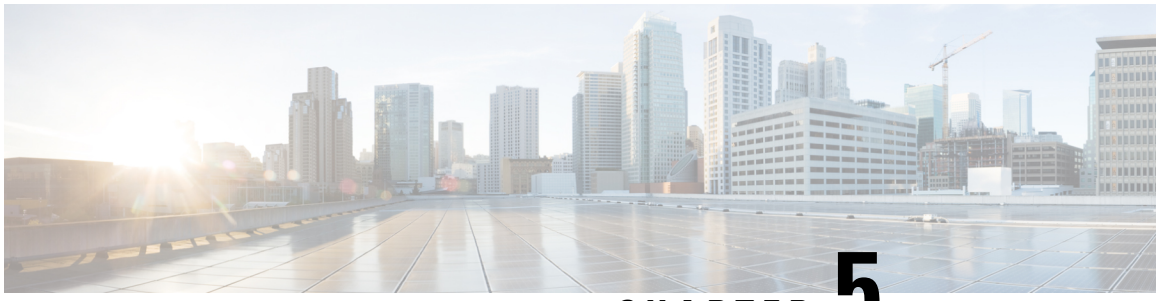
- Analyze the logs. Check the support bundle for errors.
- Identify and resolve the problem by submitting the support bundle that you generated to the Cisco Technical Assistance Center (TAC).

Roll Back to the Previous Version of ISO Image

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

Sometimes, upgrade failures that occur because of issues in the configuration and monitoring database are not rolled back automatically. When this occurs, you get a notification stating that the database is not rolled back, along with an upgrade failure message. In such scenarios, you should manually reimage your system, install Cisco ISE, and restore the configuration data and monitoring data (if the Monitoring persona is enabled).

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



CHAPTER 5

Perform the Post-Upgrade Tasks

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

- Post-Upgrade Settings and Configurations, on page 39

Post-Upgrade Settings and Configurations

Perform the following tasks after upgrading Cisco ISE.

Verify Virtual Machine 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 (64-bit) or Red Hat Enterprise Linux (RHEL) 6 (64-bit). To do this, you must power down the VM, change the Guest Operating System to the supported RHEL version, 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.

If you are running ISE 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.

Browser Setup

After upgrade, clear the browser cache, close the browser, and open a new browser session, before you access the Cisco ISE Admin portal. Also verify that you are using a supported browser, which are listed in the release notes: https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html

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

Re-Join Active Directory

If you use Active Directory as your external identity source, and the connection to Active Directory is lost, then you must join all Cisco ISE nodes with Active Directory again. After the joins are complete, 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 enabled certificate-based authentication for administrative access to Cisco ISE, and used Active Directory as your identity source, then you will not be able to launch the ISE login page after upgrade. This because the join to Active Directory is lost during upgrade. To restore joins to Active Directory, connect to the Cisco ISE CLI, and start the ISE application in safe mode by using the following command:

  application start ise safe

  After Cisco ISE starts in safe mode, perform the following tasks:

  - 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 Administrator Access to Cisco ISE in the Administrators Guide for information on how to reset an administrator password.

  - Join Cisco ISE with Active Directory.

  For more information about joining Active Directory, see:

  Configure Active Directory as an External Identity Source

Certificate Attributes Used with Active Directory

Cisco ISE identifies users using the attributes SAM, CN, or both. Cisco ISE, Release 2.2 Patch 5 and above, and 2.3 Patch 2 and above, use the `sAMAccountName` attribute as the default attribute. In earlier releases, both SAM and CN attributes were searched by default. This behavior has changed in Release 2.2 Patch 5 and above, and 2.3 Patch 2 and above, as part of CSCvf21978 bug fix. In these releases, only the sAMAccountName attribute is used as the default attribute.

You can configure Cisco ISE to use SAM, CN, or both, if your environment requires it. When SAM and CN are used, and the value of the SAMAccountName attribute is not unique, Cisco ISE also compares the CN attribute value.

To configure attributes for Active Directory identity search:

- 1. Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory** . In the **Active Directory** window, click **Advanced Tools**, and choose **Advanced Tuning**. Enter the following details:
  - **ISE Node**—Choose the ISE node that is connecting to Active Directory.
  - **Name**—Enter the registry key that you are changing. To change the Active Directory search attributes, enter: `REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField`
  - **Value**—Enter the attributes that ISE uses to identify a user:
    - *SAM*—To use only SAM in the query (this option is the default).
    - *CN*—To use only CN in the query.
    - *SAMCN*—To use CN and SAM in the query.
  - **Comment**—Describe what you are changing, for example: Changing the default behavior to SAM and CN.

- 2. Click **Update Value** to update the registry.

  A pop-up window appears. Read the message and accept the change. The AD connector service in ISE restarts.

Reverse DNS Lookup

Ensure that you have Reverse DNS lookup configured for all Cisco ISE nodes in your distributed deployment for all DNS server(s). Otherwise, you may run into deployment-related issues after upgrade.

Restore Certificates

Restore Certificates on the PAN

When you upgrade a distributed deployment, the Primary Administration Node's root CA certificates are not added to the Trusted Certificates store if both of the following conditions are met:

- Secondary Administration Node is promoted to be the Primary Administration Node in the new deployment.
- Session services are disabled on the Secondary Administration Node.

If the certificates are not in the store, you may see authentication failures with the following errors:

- `Unknown CA in the 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.

To restore the Primary Administration Node's root CA certificates, generate a new Cisco ISE Root CA certificate chain. Choose **Administration** > **Certificates** > **Certificate Signing Requests** > **Replace ISE Root CA certificate chain**.

Restore Certificates and Keys to Secondary Administration Node

If you are using a secondary Administration node, 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 allows the Secondary Administration Node to function as the root CA or subordinate CA of an external PKI if the primary PAN fails, and you promote the Secondary Administration Node to be the Primary Administration Node.

For more information about backing up and restoring certificates and keys, see:

Backup and Restore of Cisco ISE CA Certificates and Keys

Threat-Centric NAC

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.

SMNP Originating Policy Services Node Setting

If you had manually configured the Originating Policy Services Node value under SNMP settings, this configuration is lost during upgrade. You must reconfigure the SNMP settings.

For more information, see:

See SNMP Settings under Network Device Definition Settings.

Profiler Feed Service

Update the profiler feed service after upgrade to ensure that the most up-to-date OUIs are installed.

From the Cisco ISE Admin portal:

Step 1 Choose **Administration** > **FeedService** > **Profiler**. Ensure that the profiler feed service is enabled.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **FeedService** > **Profiler**. Ensure that the profiler feed service is enabled.

Step 3 Click **Update Now**.

Client Provisioning

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.

Update client provisioning resources on ISE:

Online Updates

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources** to configure the client provisioning resources.

Step 2 Click **Add**.

Step 3 Choose **Agent Resources From Cisco Site**.

Step 4 In the **Download Remote Resources** window, select the Cisco Temporal Agent resource.

Step 5 Click **Save** and verify that the downloaded resource appears in the Resources page.

Offline Updates

Step 1 Click **Add**.

Step 2 Choose **Agent Resources from Local Disk**.

Step 3 From the **Category** drop-down, choose **Cisco Provided Packages**.

Cipher Suites

If you have legacy devices, such as old IP phones, that use these deprecated ciphers authenticating against Cisco ISE,authentication fails because these devices use legacy ciphers. To allow Cisco ISE to authenticate legacy devices after upgrading, ensure that you update the **Allowed Protocols** configuration as follows:

Step 1 From the Admin portal, choose **Policy** > **Policy Elements** > **Results** > **Authentication** > **Allowed Protocols**.

Step 2 Edit the Allowed Protocols service and check the **Allow weak ciphers for EAP** check box.

Step 3 Click **Submit**.

Related Topics

Release Notes for Cisco Identity Services Engine

Cisco Identity Services Engine Network Component Compatibility

Monitoring and Troubleshooting

- Reconfigure email settings, favorite reports, and data purge settings.
- Check the threshold and 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.

Restore MnT Backup

With the operational data backup of MnT data that you created before update, restore the backup.

For more information, see:

Backup and Restore Operations in the Cisco ISE Administrator Guide for more information.

Refresh Policies to Trustsec NADs

Run the following commands, in the following order, to download the policies on Cisco TrustSec-enabled Layer 3 interfaces in the system:

- `no cts role-based enforcement`
- `cts role-based enforcement`

Update Supplicant Provisioning Wizards

When you upgrade to a new release, or apply a patch, the Supplicant Provisioning Wizards (SPW) are not updated. You must manually update the SPWs, then create new native supplicant profiles and new client provisioning policies that reference the new SPWs. New SPWs are available on the ISE download page.