



Cisco Identity Services Engine Upgrade Guide, Release 2.4

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Upgrade Cisco ISE 1

- Cisco ISE Upgrade Overview 1
- Upgrade Path 2
- Supported Operating System for Virtual Machines 2
- Licensing Changes 3

CHAPTER 2

Prepare for Upgrade 5

- Prepare for Upgrade 5
- Guidelines to Minimize Upgrade Time and Maximize Efficiency during Upgrade 6
- Time Taken for Upgrade 8
- Validate Data to Prevent Upgrade Failures 9
 - Download and Run the Upgrade Readiness Tool 10
 - Create a Repository and Copy the URT Bundle 10
 - Run the Upgrade Readiness Tool 11
- Change the Name of Authorization Simple Condition if a Predefined Authorization Compound Condition with the Same Name Exists 14
- Change VMware Virtual Machine Guest Operating System and Settings 15
- Remove Non-ASCII Characters From Sponsor Group Names 15
- Firewall Ports that Must be Open for Communication 15
- Back Up Cisco ISE Configuration and Operational Data from the Primary Administration Node 16
- Back Up System Logs from the Primary Administration Node 17
- Check Certificate Validity 17
- Delete a Certificate 17
- Export Certificates and Private Keys 17
- 18
- Disable PAN Automatic Failover and Disable Scheduled Backups before Upgrading 18

Configure NTP Server and Verify Availability	18
Upgrade Virtual Machine	19
Record Profiler Configuration	19
Obtain Active Directory and Internal Administrator Account Credentials	19
Activate MDM Vendor Before Upgrade	20
Create Repository and Copy the Upgrade Bundle	20
Check the Available Disk Size	21
Check Load Balancer Configuration	21
Log Retention and Resizing MnT Hard Disk	21

CHAPTER 3**Choose a Upgrade Method 23**

Upgrade Sequence of the Nodes	23
Choose your Upgrade Method	25
Upgrade Cisco ISE Deployment Using Backup and Restore Method (Recommended)	28
Overview of the Backup and Restore Upgrade Method	28
Backup and Restore Upgrade Process	29
Upgrade Secondary PAN and Secondary MnT Nodes to Cisco ISE, Release 2.0, 2.1, 2.2 or 2.3.	29
Upgrade Secondary PAN and MnT Nodes to Cisco ISE, Release 2.4	30
Join Policy Service Nodes to Cisco ISE, Release 2.4	30
Upgrade Primary PAN and MnT to Cisco ISE, Release 2.4	30
Upgrade a Cisco ISE Deployment from the GUI	31
Upgrade a Cisco ISE Deployment from the GUI	31
Upgrade From Release 2.0 , 2.0.1, 2.1, 2.2 or 2.3 to Release 2.4	31
Upgrade a Cisco ISE Deployment from the CLI	34
Upgrade Process	34
Upgrade a Standalone Node	34
Upgrade a Two-Node Deployment	36
Upgrade a Distributed Deployment	38
Verify the Upgrade Process	42
Roll Back to the Previous Version of ISO Image	43

CHAPTER 4**Install Cisco ISE Software Patch 45**

Cisco ISE Software Patches	45
----------------------------	----

Software Patch Installation Guidelines	46
Install a Software Patch	46
Roll Back Software Patches	47
Software Patch Rollback Guidelines	47
View Patch Install and Rollback Changes	48

CHAPTER 5

Perform the Post-Upgrade Tasks	49
Post-Upgrade Settings and Configurations	49
Verify Virtual Machine Settings	49
Browser Setup	49
Re-Join Active Directory	49
Reverse DNS Lookup	51
Restore Certificates	51
Threat-Centric NAC	51
SMNP Originating Policy Services Node Setting	51
Profiler Feed Service	52
Client Provisioning	52
Online Updates	52
Offline Updates	52
Cipher Suites	53
Monitoring and Troubleshooting	53
Refresh Policies to Trustsec NADs	53
Update Supplicant Provisioning Wizards	53



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](#)
- [Licensing Changes, on page 3](#)

Cisco ISE Upgrade Overview

This document describes how to upgrade your Cisco Identity Services Engine (ISE) software on Cisco ISE appliances and virtual machines to Release 2.4. (See the section "[What is New in Cisco ISE, Release 2.4](#)" in *Release Notes for Cisco Identity Services Engine, Release 2.4*.)



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

Single-step Upgrade

You can directly upgrade to Release 2.4, from any of the following releases:

- Cisco ISE, Release 2.0
- Cisco ISE, Release 2.0.1
- Cisco ISE, Release 2.1
- Cisco ISE, Release 2.2
- Cisco ISE, Release 2.3

You can download the upgrade bundle from Cisco.com. The following upgrade bundle is available for Release 2.4:

ise-upgradebundle-2.x-to-2.4.0.xxx.SPA.x86_64.tar.gz: Use this bundle to upgrade from Release 2.0, 2.0.1, 2.1, 2.2, or 2.3 to 2.4

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 2.4.

Supported Operating System for Virtual Machines

Cisco ISE, Release 2.4 supports Red Hat Enterprise Linux (RHEL) 7.0 and 7.3.

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.

The following table shows if OS upgrade happens when upgrading Cisco ISE. In the following table **Yes** indicates that underlying OS will upgrade during ISE upgrade and **-** indicates the absence of OS upgrade during ISE upgrade. ISE upgrades that includes OS upgrades can easily be perceived from the size of the upgrade bundle in [Cisco's software download center for ISE](#).

Table 1:

Upgrading From	Upgrading to ISE 1.3	Upgrading to ISE 1.4	Upgrading to ISE 2.0	Upgrading to ISE 2.0.1	Upgrading to ISE 2.1	Upgrading to ISE 2.2	Upgrading to ISE 2.3	Upgrading to ISE 2.4	Upgrading to ISE 2.6	Upgrading to ISE 2.7
ISE 1.3	-	No	No	Yes	Yes	-	-	-	-	-
ISE 1.4	-	-	No	Yes	Yes	Yes	Yes	-	-	-
ISE 2.0	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes
ISE 2.0.1	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes
ISE 2.0	-	-	-	-	-	No	Yes	Yes	Yes	Yes
ISE 2.1	-	-	-	-	-	-	-	Yes	Yes	Yes
ISE 2.2	-	-	-	-	-	-	-	Yes	Yes	Yes
ISE 2.3	-	-	-	-	-	-	-	Yes	Yes	Yes
ISE 2.4	-	-	-	-	-	-	-	Yes	Yes	Yes

Licensing Changes

Device Administration Licenses

For Cisco ISE 2.3 and earlier versions, a perpetual Device Administration license is required per deployment, regardless of the number of device administration nodes in the deployment. From Cisco ISE, Release 2.4, the number of Device Administration licenses must be equal to the number of device administration nodes (PSNs configured for the device administration service) in a deployment.

If you are currently using a Device Administration license and plan to upgrade to Release 2.4 or above, TACACS+ features will be supported for 50 Device Administration nodes in Release 2.4 and above.

If you install a PAK generated from a new PID, Device Administration license count is displayed as per the quantity available in the PAK file. You can add multiple Device Administration licenses to your deployment based on the number of Device Administration nodes that you require. Evaluation license supports one Device Administration node.

Licenses for VM nodes

Cisco ISE is also sold as a virtual appliance. For Release 2.4 and above, it is recommended that you install appropriate VM licenses for the VM nodes in your deployment. You must install the VM licenses based on the number of VM nodes and each VM node's resources such as CPU and memory. Otherwise, you will receive warnings and notifications to procure and install the VM license keys in Release 2.4 and above, however, the services are not interrupted.

VM licenses are offered under three categories—Small, Medium, and Large. For instance, if you are using 3595 equivalent VM node with 8 cores and 64-GB RAM, you might need a Medium category VM license, if you want to replicate the same capabilities on the VM. You need to install multiple VM licenses based on the number of VMs and their resources as per your deployment requirements.

VM licenses are Infrastructure licenses, therefore, you can install VM licenses irrespective of the endpoint licenses available in your deployment. You can install a VM license even if you have not installed any Evaluation, Base, Plus, or Apex license in your deployment. However, in order to use the features enabled by the Base, Plus, or Apex licenses, you must install the appropriate licenses.

After installing or upgrading to Release 2.4 or above, if there is any mismatch between the number of deployed VM nodes and installed VM licenses, alarms are displayed in the Alarms dashlet for every 14 days. Alarms are also displayed if there are any changes in the VM node's resources or whenever a VM node is registered or deregistered.

VM licenses are perpetual licenses. VM licensing changes are displayed every time you log in to the Cisco ISE GUI, until you check the **Do not show this message again** check box in the notification dialog box.

If you have not purchased any ISE VM license before, refer to the [ISE Ordering Guide](#) to choose the appropriate VM license to be purchased. If you have purchased ISE VM licenses with no Product Authorization Key (PAK) associated, you can request VM PAKs by reaching out to licensing@cisco.com with Sales Order numbers that reflect the ISE VM purchase. This request will be processed to provide one medium VM license key for each ISE VM purchase you made in the past.

The following table shows the minimum VM resources by category:

VM Category	Hardware Appliances	RAM Range	Number of CPUs
Small	SNS-3515	16 GB	12 CPUs
Medium	SNS-3595 SNS- 3655	64 GB	16 CPUs
Large	SNS-3695	256 GB	16 CPUs

For more information about the licenses, see the "Cisco ISE Licenses" chapter in the [Cisco Identity Services Engine Administrator Guide](#).



CHAPTER 2

Prepare for Upgrade

- [Prepare for Upgrade, on page 5](#)
- [Guidelines to Minimize Upgrade Time and Maximize Efficiency during Upgrade , on page 6](#)
- [Time Taken for Upgrade, on page 8](#)
- [Validate Data to Prevent Upgrade Failures, on page 9](#)
- [Change the Name of Authorization Simple Condition if a Predefined Authorization Compound Condition with the Same Name Exists, on page 14](#)
- [Change VMware Virtual Machine Guest Operating System and Settings, on page 15](#)
- [Remove Non-ASCII Characters From Sponsor Group Names, on page 15](#)
- [Firewall Ports that Must be Open for Communication, on page 15](#)
- [Back Up Cisco ISE Configuration and Operational Data from the Primary Administration Node, on page 16](#)
- [Back Up System Logs from the Primary Administration Node, on page 17](#)
- [Check Certificate Validity, on page 17](#)
- [Delete a Certificate, on page 17](#)
- [Export Certificates and Private Keys, on page 17](#)
- [Disable PAN Automatic Failover and Disable Scheduled Backups before Upgrading, on page 18](#)
- [Configure NTP Server and Verify Availability, on page 18](#)
- [Upgrade Virtual Machine, on page 19](#)
- [Record Profiler Configuration, on page 19](#)
- [Obtain Active Directory and Internal Administrator Account Credentials, on page 19](#)
- [Activate MDM Vendor Before Upgrade, on page 20](#)
- [Create Repository and Copy the Upgrade Bundle, on page 20](#)
- [Check the Available Disk Size , on page 21](#)
- [Check Load Balancer Configuration, on page 21](#)
- [Log Retention and Resizing MnT Hard Disk, on page 21](#)

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 availability 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 retain 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 policies 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 archive 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 (**System > Logging > Collection Filters**) to filter incoming logs and avoid duplication of entries in AAA logs.
- You can create Remote Logging Targets (**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 2.4 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, 2.2, and 2.3.
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 45 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. Copies latest upgrade files to the upgrade bundle



Note If there are no patches in URT bundle then the output will return: N/A. This is an expected behaviour while installing a hot patch.

7. 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.

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 10](#)

Step 2 [Run the Upgrade Readiness Tool, on page 11](#)

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-2.4.0.xxx-1.0.0.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:

```
copy repository_url/path/ise-urtbundle-2.4.0.xxx-1.0.0.SPA.x86_64.tar.gz disk:/
```

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

```
(Add the host key if it does not exist) crypto host_key add host mySftpserver
copy sftp://aaa.bbb.ccc.ddd/ ise-urtbundle-2.4.0.xxx-1.0.0.SPA.x86_64.tar.gz disk:/
```


aaa.bbb.ccc.ddd is the IP address or hostname of the SFTP server and ise-urtbundle-2.4.0.xxx-1.0.0.SPA.x86_64.tar.gz is the name of the URT bundle.

Having the URT bundle in the local disk saves time.

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-2.4.0.x.SPA.x86_64.tar.gz reponame
```

Example:

```
ise/admin# application install ise-urtbundle-2.4.0.x.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
Invalid MDMServerNames in Authorization Policies check
-Successful
6 out of 6 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 Red Hat Enterprise Linux (RHEL) 7. To do this, you must power down the VM, change the Guest Operating System to RHEL 7, and power on the VM after the change. RHEL 7 supports only E1000 and VMXNET3 network adapters. Be sure to change the network adapter type before you upgrade.

Remove Non-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.

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

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



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.

34xx series appliances are not supported in Cisco ISE, Release 2.4 and later.

Cisco ISE, Release 2.4 and later requires a minimum disk size of 300GB for virtual machines as the local disk allocation is increased to 29GB.

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.

If an MDM server name is used in an authorization policy and the corresponding MDM server is disabled, the upgrade process fails. As a workaround, you can do one of the following:

1. Enable the MDM server before upgrade.
2. Delete the condition that uses the MDM server name attribute from the authorization policy.

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.

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](https://www.cisco.com).

To upgrade to Release 2.4, use the following upgrade bundle:
ise-upgradebundle-2.x-to-2.4.0.xxx.SPA.x86_64.tar.gz

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.x-to-2.4.0.xxx.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.x-to-2.4.0.xxx.SPA.x86_64.tar.gz disk:/**
aaa.bbb.ccc.ddd is the IP address or hostname of the SFTP server and
ise-upgradebundle-2.x-to-2.4.0.xxx.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.

For more information on collection filter, see "[Configure Collection Filters section](#)" in "Maintain & Monitor" Chapter in *Cisco Identity Services Engine Administrator Guide*

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

Choose a Upgrade Method

- [Upgrade Sequence of the Nodes, on page 23](#)
- [Choose your Upgrade Method, on page 25](#)
- [Upgrade Cisco ISE Deployment Using Backup and Restore Method \(Recommended\), on page 28](#)
- [Upgrade a Cisco ISE Deployment from the GUI, on page 31](#)
- [Upgrade a Cisco ISE Deployment from the CLI, on page 34](#)

Upgrade Sequence of the Nodes

You can upgrade Cisco ISE using GUI, Backup and Restore, or CLI. In case you are using GUI to upgrade you can choose the order of nodes to be upgraded. However, we recommend that you follow the below provided order of the nodes for upgrading your deployment. This will help you to reduce downtime while providing maximum resiliency and ability to roll back.

1. Backup all configuration and monitoring data. This task should be done before initiating upgrade in order to ensure that you can easily roll back manually, if necessary.
2. Secondary Administration Node
At this point, the Primary Administration Node remains at the previous version and can be used for rollback if the upgrade fails.
3. Primary Monitoring Node or Secondary Monitoring Node
If you have a distributed deployment, upgrade all the nodes that are available in the site that has Secondary Administration Node of your existing Cisco ISE deployment.
4. Secondary Monitoring Node or Primary Monitoring Node
5. Policy Service Nodes
After you upgrade a set of Policy Service nodes, verify whether the upgrade is successful (see Verify the Upgrade Process) and run the necessary network tests to ensure that the new deployment is functioning as expected. If the upgrade is successful, you can upgrade the next set of Policy Service nodes.
6. Primary Administration Node
Rerun the upgrade verification and network tests after you upgrade the Primary Administration Node.



Note If upgrade fails during the registration of the Primary Administration node (the last node from the old deployment that has to be upgraded), the upgrade is rolled back and the node becomes a standalone node. From the CLI, upgrade the node as a standalone node. Register the node to the new deployment as a Secondary Administration node.

After the upgrade, the Secondary Administration Node becomes the Primary Administration Node, and the original Primary Administration Node becomes the Secondary Administration Node. In the Edit Node window, click Promote to Primary to promote the Secondary Administration Node as the Primary Administration Node (as in your old deployment), if necessary.

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

Node Personas In The Current Deployment	Upgrade Sequence
Secondary Administration/Primary Monitoring Node, Policy Service Nodes, Primary Administration/Secondary Monitoring Node	<ol style="list-style-type: none"> 1. Secondary Administration/Secondary Monitoring Node 2. Policy Service Nodes 3. Primary Administration/Primary Monitoring Node
Secondary Administration/Secondary Monitoring Node, Policy Service Nodes, Primary Administration/Primary Monitoring Node	<ol style="list-style-type: none"> 1. Secondary Administration/Primary Monitoring Node 2. Policy Service Nodes 3. Primary Administration/Secondary Monitoring Node
Secondary Administration Node, Primary Monitoring Node, Policy Service Nodes, Primary Administration/Secondary Monitoring Node	<ol style="list-style-type: none"> 1. Secondary Administration Node 2. Primary Monitoring Node 3. Policy Service Nodes 4. Primary Administration/Secondary Monitoring Node
Secondary Administration Node, Secondary Monitoring Node, Policy Service Nodes, Primary Administration/Primary Monitoring Node	<ol style="list-style-type: none"> 1. Secondary Administration Node 2. Secondary Monitoring Node 3. Policy Service Nodes 4. Primary Administration/Primary Monitoring Node

Node Personas In The Current Deployment	Upgrade Sequence
Secondary Administration/Primary Monitoring Node, Policy Service Nodes, Secondary Monitoring Node, Primary Administration Node	<ol style="list-style-type: none"> 1. Secondary Administration/Primary Monitoring Node 2. Policy Service Nodes 3. Secondary Monitoring Node 4. Primary Administration Node
Secondary Administration/Secondary Monitoring Node, Policy Service Nodes, Primary Monitoring Node, Primary Administration Node	<ol style="list-style-type: none"> 1. Secondary Administration/Secondary Monitoring Node 2. Policy Service Nodes 3. Primary Monitoring Node 4. Primary Administration Node

You will get a error message **No Secondary Administration Node in the Deployment** under the following circumstances:

- 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. Typically, this occurs when you use the **Refresh Deployment Details** option after the Secondary Administration node is upgraded.

To resolve this issue, perform one of the tasks, as applicable:

- If the deployment does not have a Secondary Administration node, configure a Secondary Administration node 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, use the CLI to manually upgrade the other nodes in the deployment.

Choose your Upgrade Method

This release of Cisco ISE supports the following upgrade processes. You can choose from the below upgrade processes depending on your technical expertise and time availability for the upgrade.

- Upgrade Cisco ISE using Backup and Restore Procedure (Recommended)
- Upgrade a Cisco ISE deployment from GUI

A detailed comparison of the upgrade methods is as follows:

Upgrade Cisco ISE using Backup and Restore Method

Re-imaging of the Cisco ISE node is done as a part the initial deployment and during troubleshooting, however you can also re-image Cisco ISE node to upgrade a deployment while providing for restoration of the policy onto the new deployment once the new version is deployed.

In case the resources are limited, and new deployment is unable to spin up a parallel ISE node, Secondary PAN & MnT is removed from production deployment to be upgraded before upgrading the other nodes. Nodes are moved into the new deployment; a configuration & operational backup is restored from the previous deployment on respective nodes creating a parallel deployment. This allows to restore the policy sets, custom profiles, network access devices, and endpoints into the new deployment without need for manual intervention.

The advantages of upgrading Cisco ISE using Backup and Restore process are as follows:

- You can restore the configuration setting and the operational logs from the previous ISE deployment. Thus, preventing from data loss.
- You can manually choose the nodes that should be reused for the new deployment.
- You can upgrade multiple PSNs parallely thus reducing the upgrade downtime.
- You can stage the nodes outside of maintenance windows, reducing the time of the upgrade during the production.

Things to consider before upgrading Cisco ISE using Backup and Restore

Resources Required: The backup and restore upgrade process requires additional resources which can be reserved for the ISE deployment before being released. In the case of reusing existing hardware, additional load will need to be balanced to nodes which remain online. Hence, you need to evaluate the current load and latency limits before the deployment begins in order to ensure that the deployment can handle an increase in number of users per node.

Personnel Required: You will require involvement from multiple business units including network administration, security administration, data centre, and virtualization resources to perform upgrade. In addition, you will need to re-join the node to the new deployment, restore certificates, re-join to active directory, and wait for policy synchronization. This can lead to multiple reloads and requires timeframe that of a net-new deployment.

Rollback Mechanism: Due to the re-imaging of the nodes, all information and configuration setting are erased from the previous deployment. Thus, the rollback mechanism for a backup and restore upgrade is the same procedure as re-imaging of the nodes for the second time.

Best Practice for the Backup and Restore Upgrade Process:

- Create an standalone environment or dedicate load balancers to switch Virtual IP address for RADIUS requests.
- You can start the deployment process well before the maintenance window and point the user load balancer to the new deployment.

For more information on the backup and restore upgrade method, see the [Upgrade Cisco ISE Deployment Using Backup and Restore Method \(Recommended\)](#)

Upgrade a Cisco ISE deployment from GUI

You can also upgrade Cisco ISE from the GUI in a single click with some customizable options. A GUI upgrade is executed from th **ISE Administration > Upgrade** menu and requires a new repository to download the ISO image.

During the upgrade the Secondary PAN is moved into an upgraded deployment automatically and is upgraded first, followed by Primary MnT. As a result, if either of these upgrades fail, it is mandatory that the node will be rolled back to the previous version and re-join to the previous ISE deployment. Later PSN's are moved one by one to the new deployment and upgraded. In case of an upgrade failure, you can also choose to continue or cease the upgrade. This will result in a dual-version of same Cisco ISE deployment, allowing for troubleshooting to occur before the upgrade continues. Once all PSN's are upgraded, the Secondary MnT and Primary PAN is upgraded and joined to the new Cisco ISE deployment.

Given that this upgrade process requires limited technical expertise, a single administrator start the upgrade and assign NOC or SOC engineers to monitor and report the upgrade status or open a TAC case.

The advantages of upgrading Cisco ISE from the GUI are as follows:

- The upgrade is automated with minimal intervention.
- You can choose the upgrade order of the PSNs to ensure continuity whenever possible, especially when redundancy available between data centres.
- A single administrator can execute the upgrade without any additional personnel, third party hypervisors or network access devices.

Things to consider before upgrading Cisco ISE from GUI

Continuation in Failure Scenarios: In case of an upgrade failure, you can also choose to continue or cease the upgrade. This will result in a dual-version of same Cisco ISE deployment, allowing for troubleshooting to occur before the upgrade continues. While the Cisco Upgrade Readiness Tool should indicate any incompatibilities or misconfigurations, if the Proceed field is checked, additional errors may be encountered if due diligence was not acted upon before the upgrade.

Rollback Mechanism: If an upgrade fails on a PAN or MnT node, the nodes are automatically rolled back. However, if a PSN fails to upgrade, the nodes remain on the same Cisco ISE version and can be fixed while impairing redundancy. Cisco ISE is still operational during this time, and therefore rollback abilities are limited without re-imaging.

Time Required: Each PSN takes around 90-120 minutes to upgrade, hence if you have a large number PSNs it takes time to upgrade all of them.

Best Practice for the Upgrade from GUI: If you have a larger number of PSNs, group the PSNs in batches and perform the upgrade.

For more information on the upgrade from GUI, see [Upgrade a Cisco ISE Deployment from the GUI](#)

Upgrade a Cisco ISE deployment from CLI

Upgrading Cisco ISE from the CLI is an elaborate process and requires the administrator to download the upgrade image to the local node, execute the upgrade, and monitor each node individually throughout the upgrade process. While the upgrade sequence is similar in nature to that of the GUI upgrade, this approach operationally intensive from a monitoring and actions point of view.

Upgrading from CLI is recommended for troubleshooting purposes only due to the level of effort required.

The advantages of upgrading Cisco ISE from the CLI are as follows:

- CLI presents additional logging messages to the administrator while the upgrade is performed.
- The nodes which are upgraded can be chosen with more control and upgraded in parallel. Nodes that are not being upgraded can handle additional load as endpoints are rebalanced across the deployment.
- Rolling back at the CLI is much easier due to the ability to instruct scripts to undo previous changes.

- As the image resides on the node locally, copy errors between PAN and PSNs, if any, can be eliminated.

Things to consider before upgrading Cisco ISE from CLI

You need technical expertise and longer time to upgrade your Cisco ISE using CLI.

For more information on the upgrade from CLI, see [Upgrade a Cisco ISE Deployment from the CLI](#)

Upgrade Cisco ISE Deployment Using Backup and Restore Method (Recommended)

Overview of the Backup and Restore Upgrade Method

We recommend backup and restore upgrade process over the other upgrade processes as it helps to reinstate your current Cisco ISE deployment node settings and prevent data loss, in case of any breakage during the upgrade process. This procedure starts by creating configuration and operational backups of the existing Cisco ISE deployment and then apply them to the new deployment.

Best Practice for the Backup and Restore Upgrade Process:

- Create a standalone environment or dedicate load balancers to switch Virtual IP address for RADIUS requests.
- You can start the deployment process well before the maintenance window and point the user load balancer to the new deployment.

The following is a broad overview of the steps involved in the Backup and Restore Upgrade method:

1. Deregister a Node

In order to remove a node from the deployment, you need to deregister the node. For more information about node deregistration or removal, see the "Remove a Node from Deployment" section in [Cisco Identity Services Engine Administrator Guide, Release](#).

2. Reimage a Node

In order to reimage a node, you need to freshly install the node in the Cisco ISE deployment. For more information about Cisco ISE installation, see the "Install Cisco ISE " chapter in the [Cisco Identity Services Engine Installation Guide, Release](#).

We recommend that you apply the latest patch of newly installed Cisco ISE Release.

3. Backup and Restore the Configuration or Operational Database

For more information about the backup and restore operations, see the "Backup and Restore Operations" section in [Cisco Identity Services Engine Administrator Guide, Release](#) .

4. Assign Primary or Secondary Roles to a Node.

You can assign primary or secondary role to a node as per your requirement.

For more information about how to assign a role to a Policy Administration Node (PAN), see the "Manually Promote Secondary PAN To Primary" section in the [Cisco Identity Services Engine Administrator Guide, Release](#).

For more information about how to assign a role to a Monitoring and Troubleshooting (MnT) node, see the "Manually Modify MnT Role" section in [Cisco Identity Services Engine Administrator Guide, Release](#).

5. Join the Policy Service Nodes

In order to join a Policy Service Node (PSN) to the new deployment, you need to register the node as PSN. For more information about registering or joining a PSN, see the "Register a Secondary Cisco ISE Node" in [Cisco Identity Services Engine Administrator Guide, Release](#).

6. Import Certificates

You need to import the system certificates to the newly deployed nodes in the Cisco ISE. For more information about how to import system certificates to a Cisco ISE node, see the "Import a System Certificate" section in [Cisco Identity Services Engine Administrator Guide, Release](#).

Backup and Restore Upgrade Process

This section describes the upgrade process using the recommended Backup and Restore Upgrade method.

If you are currently using Cisco ISE, Release 2.0 or later, you can directly upgrade to Cisco ISE, Release 2.4.

- [Upgrade Secondary PAN and MnT Nodes to Cisco ISE, Release 2.4](#)
- [Join Policy Service Nodes to Cisco ISE, Release 2.4](#)
- [Upgrade Primary PAN and MnT to Cisco ISE, Release 2.4](#)

In case you are using a Cisco ISE version that is not compatible to Cisco ISE Release 2.4, you need to first upgrade to an intermediate version, compatible to Cisco ISE, Release 2.4. And then you can upgrade from the intermediate version to Cisco ISE, Release 2.4. Follow the below steps to upgrade to an intermediate Cisco ISE version.

Upgrade Secondary PAN and Secondary MnT Nodes to Cisco ISE, Release 2.0, 2.1, 2.2 or 2.3.

Before you begin

Restore backup from your existing Cisco ISE to intermediate Cisco ISE Release.

-
- Step 1** De-register Secondary PAN node.
 - Step 2** Re-image the deregistered Secondary PAN node to the intermediate Cisco ISE Release, as a standalone node. After the upgrade, make this node the Primary Administration Node in the new deployment.
 - Step 3** Restore Cisco ISE configuration from the backup data.
 - Step 4** De-register Secondary MnT node.
 - Step 5** Re-image the deregistered Secondary MnT node to the intermediate Cisco ISE Release, as a standalone node.
 - Step 6** Assign Primary role to this MnT node and restore the operational backup from the backup repository. This is an optional step and needs to be performed only if you need to report of the older logs

Step 7 Import ise-https-admin CA certificates from your original Cisco ISE backup repository.

Upgrade Secondary PAN and MnT Nodes to Cisco ISE, Release 2.4

- Step 1** Take a backup of Cisco ISE configuration settings and operational logs.
- Step 2** De-register Secondary PAN node.
- Step 3** Re-image the deregistered secondary PAN node to Cisco ISE, Release 2.4.
- Step 4** Restore ISE configuration from the backup data and make this node as the Primary Node for your new deployment.
- Step 5** Import ise-https-admin CA certificates from Secondary PAN unless you are using wild card certificates.
- Step 6** De-register Secondary MnT node.
- Step 7** Re-Image the deregistered Secondary MnT node to Cisco ISE, Release 2.4.
- Step 8** Restore your current ISE operational backup and join node as Primary MnT for new deployment. This is an optional step and needs to be performed only if you need to report of the older logs.
-

Join Policy Service Nodes to Cisco ISE, Release 2.4

In case you have Cisco ISE nodes deployed in multiple sites, join the PSNs available in the site (that has Secondary PAN and MnT nodes) first and then join the PSNs available in the other sites followed by the PSNs available at the site (that has Primary PAN and MnT nodes of your existing Cisco ISE).

- Step 1** De-register PSNs.
- Step 2** Reimage PSN to Cisco ISE, Release 2.4 latest patch and join PSN to new Cisco ISE, Release 2.4 deployment.
-

What to do next

We recommend that you test your partially upgraded deployment at this point. You can do so by checking if logs are present and the upgraded nodes function as expected.

Upgrade Primary PAN and MnT to Cisco ISE, Release 2.4

- Step 1** Reimage Primary MnT node and join as Secondary MnT to new deployment.
In case you want to preserve the data for reporting, restore a copy of the operational backup to the Secondary MnT node.
- Step 2** Reimage Primary PAN node and join as Secondary PAN to new deployment.
-

Upgrade a Cisco ISE Deployment from the GUI

Upgrade a Cisco ISE Deployment from the GUI

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

The **Overview** page under **Administration > Upgrade** 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, 2.2 or 2.3 to Release 2.4

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



Note

If you are upgrading a Cisco ISE STANDALONE node or have de-registered a node from an existing deployment and wish to run a STANDALONE upgrade, then prior to starting the upgrade, there is a need to remove all the `upgradedb_*.properties` files located in the path : `"/opt/oracle/base/admin/cpm10/dpdump"`.

Please contact Cisco TAC for deleting the above mentioned files, as root privilege is required to remove them. See [CSCvi87302](#) for details.

The above workaround is required only if the upgrade file (`ise-upgradebundle-2.0.x-2.3.x-to-2.4.0.357.SPA.x86_64.tar.gz`) is downloaded before April 13, 2018.

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

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

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

Step 2 Click **Proceed**.

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

Step 3 Check the **I have reviewed the checklist** check box, and click **Continue**.

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

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

- Check the check box next to the nodes to which you want to download the upgrade bundle.
- Click **Download**.

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

- 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.

- Check the check box next to the bundle that you want to use for the upgrade.
- Click **Confirm**.

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

Step 5 Click **Continue**.

The **Upgrade Nodes** window appears.

Figure 1: Upgrade Window Showing the Current Deployment and the New Deployment

Node Group - Host Name	Persona	Status
ise144.indiasys.com	Admin secondary	
ise136.indiasys.com	Monitor PRIMARY	
Nodegrp - ise146.indiasys.c...	Policy service	
NodeGrp2 - ise145.indiasys...	Policy service	
ise138.indiasys.com	pxGrid	
ise147.indiasys.com	pxGrid	
ise137.indiasys.com	Monitor secondary	
ise143.indiasys.com	Admin PRIMARY	

Sequence	Node Group - Host Name	Persona	Status
1	ise144.indiasys.com	Admin PRIMARY	240 min. est. time
2	ise136.indiasys.com	Monitor PRIMARY	240 min. est. time
3	ise146.indiasys.com ise145.indiasys.com	Policy service	180 min. est. time
4	ise138.indiasys.com ise147.indiasys.com	pxGrid	240 min. est. time
5	ise137.indiasys.com	Monitor secondary	240 min. est. time
6	ise143.indiasys.com	Admin secondary	240 min. est. time
7	Select nodes for sequence 7		

Step 6 Choose the upgrade sequence.

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

- 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.
- The Primary Monitoring Node is the next one in the sequence to be upgraded to the new deployment.
- 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.

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

Step 7 Check the **Continue with upgrade on failure** check box if you want to continue with the upgrade even if the upgrade fails on any of the Policy Service Nodes in the upgrade sequence.

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

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

Figure 2: Upgrade Window Showing the Upgrade Progress

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Overview Upgrade

1 Review Checklist 2 Download Bundle to Node(s) 3 Upgrade Node(s)

Deployment (2.3.0.298)

8 Selected

Node Group - Host Name	Persona
ise144.indiasys.com	Admin secondary
ise136.indiasys.com	Monitor PRIMARY
Nodegrp - ise146.indiasys.c...	Policy service
NodeGrp2 - ise145.indiasys...	Policy service
ise138.indiasys.com	pxGrid
ise147.indiasys.com	pxGrid
ise137.indiasys.com	Monitor secondary
ise143.indiasys.com	Admin PRIMARY

New Deployment Upgrade (2.4.0.277) Total estimated time: 1140 mins

Sequence	Node Group - Host Name	Persona	Status
1	ise144.indiasys.com	Admin PRIMARY	Upgrade 5% STEP 3: Validating data before upgrade...
2	ise136.indiasys.com	Monitor PRIMARY	Upgrade 5%
3	ise146.indiasys.com	Policy service	Upgrade queued
	ise145.indiasys.com	Policy service	Upgrade queued
4	ise138.indiasys.com	pxGrid	Upgrade queued
	ise147.indiasys.com	pxGrid	Upgrade queued
5	ise137.indiasys.com	Monitor secondary	Upgrade queued
6	ise143.indiasys.com	Admin secondary	Upgrade queued
7	Select nodes for sequence 7		

Continue with the next node on upgrade failure (applicable for Policy Service Nodes only)

Back Upgrade

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 **Administration > System > Settings > Posture > Updates** page while upgrading or registering a node to the new deployment.

Upgrade a Cisco ISE Deployment from the CLI

Upgrade Process



Note If you are upgrading a Cisco ISE standalone node or have de-registered a node from an existing deployment and wish to run a standalone upgrade, then before starting the upgrade, you must first remove all the `upgradedb_*.properties` files located in the path: `"/opt/oracle/base/admin/cpm10/dpdump"`.

Because root privileges are required to remove these files, you should contact Cisco TAC in order to delete them. See [CSCvi87302](#) for details.

This workaround is required only if the upgrade file (`ise-upgradebundle-2.0.x-2.3.x-to-2.4.0.357.SPA.x86_64.tar.gz`) is downloaded before April 13, 2018.

Upgrade a Standalone Node

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

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

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

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

Before you begin

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

Step 1 Create a repository on the local disk. For example, you can create a repository called "upgrade."

Example:

```
ise/admin# conf t
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# repository upgrade
ise/admin(config-Repository)# url disk:
% Warning: Repositories configured from CLI cannot be used from the ISE web UI and are not replicated
to other ISE nodes.
If this repository is not created in the ISE web UI, it will be deleted when ISE services restart.
ise/admin(config-Repository)# exit
ise/admin(config)# exit
```

Step 2 From the Cisco ISE command line interface (CLI), enter **application upgrade prepare** command.

This command copies the upgrade bundle to the local repository "upgrade" that you created in the previous step and lists the MD5 and SHA256 checksum.

Example:

```
ise/admin# application upgrade prepare application upgrade prepare
ise-upgradebundle-2.0.x-2.1.x-2.2.x-2.3.x-to-2.4.0.x.SPA.x86_64.tar.gz upgrade

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

Application upgrade preparation successful
```

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

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

Example:

```
ise/admin# application upgrade proceed
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
-Checking VM for minimum hardware requirements
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
-Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: Taking backup of the configuration data...
STEP 5: Running ISE configuration database schema upgrade...
```

```

- Running db sanity 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 1/30, UPSUpgradeHandler(2.4.0.101)... Done in 50 seconds.
- Data upgrade step 2/30, UPSUpgradeHandler(2.4.0.116)... Done in 0 seconds.
- Data upgrade step 3/30, MachineAuthenticationSettingsRegistration(2.4.0.120)... Done in 0 seconds.
- Data upgrade step 4/30, GuestAccessUpgradeService(2.4.0.126)... Done in 15 seconds.
- Data upgrade step 5/30, RegisterPostureTypes(2.4.0.127)... Done in 1 seconds.
- Data upgrade step 6/30, UPSUpgradeHandler(2.4.0.127)... Done in 0 seconds.
- Data upgrade step 7/30, UPSUpgradeHandler(2.4.0.134)... Done in 0 seconds.
- Data upgrade step 8/30, NSFUpgradeService(2.4.0.140)... Done in 0 seconds.
- Data upgrade step 9/30, NSFUpgradeService(2.4.0.155)... Done in 1 seconds.
- Data upgrade step 10/30, UPSUpgradeHandler(2.4.0.158)... Done in 1 seconds.
- Data upgrade step 11/30, NSFUpgradeService(2.4.0.160)... Done in 0 seconds.
- Data upgrade step 12/30, NSFUpgradeService(2.4.0.161)... Done in 0 seconds.
- Data upgrade step 13/30, NSFUpgradeService(2.4.0.179)... Done in 0 seconds.
- Data upgrade step 14/30, NetworkAccessUpgrade(2.4.0.182)... Done in 1 seconds.
- Data upgrade step 15/30, StorageUpgradeService(2.4.0.183)... Done in 0 seconds.
- Data upgrade step 16/30, DnsHostnameResolutionRegistration(2.4.0.190)... Done in 0 seconds.
- Data upgrade step 17/30, ProfilerUpgradeService(2.4.0.194)... ..Done in 131 seconds.
- Data upgrade step 18/30, CertMgmtUpgradeService(2.4.0.200)... ..Done in 167 seconds.
- Data upgrade step 19/30, NSFUpgradeService(2.4.0.214)... Done in 0 seconds.
- Data upgrade step 20/30, ERSDictionaryRegistration(2.4.0.215)... Done in 0 seconds.
- Data upgrade step 21/30, NetworkAccessUpgrade(2.4.0.216)... Done in 0 seconds.
- Data upgrade step 22/30, ProfilerUpgradeService(2.4.0.227)... Done in 0 seconds.
- Data upgrade step 23/30, ProfilerUpgradeService(2.4.0.228)... Done in 6 seconds.
- Data upgrade step 24/30, ProfilerUpgradeService(2.4.0.229)... Done in 0 seconds.
- Data upgrade step 25/30, NetworkAccessUpgrade(2.4.0.240)... Done in 0 seconds.
- Data upgrade step 26/30, CertMgmtUpgradeService(2.4.0.293)... Done in 7 seconds.
- Data upgrade step 27/30, ProvisioningUpgradeService(2.4.0.299)... Done in 0 seconds.
- Data upgrade step 28/30, NSFUpgradeService(2.4.0.336)... Done in 2 seconds.
- Data upgrade step 29/30, ProfilerUpgradeService(2.4.0.336)... Done in 0 seconds.
- Data upgrade step 30/30, GuestAccessUpgradeService(2.4.0.336)... Done in 26 seconds.
STEP 7: Running ISE configuration data upgrade for node specific data...
STEP 8: Running ISE M&T database upgrade...
M&T Log Processor is not running
ISE database M&T schema upgrade completed.
cat: /opt/oracle/base/admin/cpl10/dpdump/upgradedb*.properties: No such file or directory

Gathering Config schema(CEPM) stats ....
Gathering Operational schema(MNT) stats ....
% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS. During this time progress
of the upgrade is visible on console. It could take up to 30 minutes for this to complete.
Rebooting to do Identity Service Engine upgrade...

```

The upgrade is now complete.

What to do next

[Verify the Upgrade Process, on page 42](#)

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 3: 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.

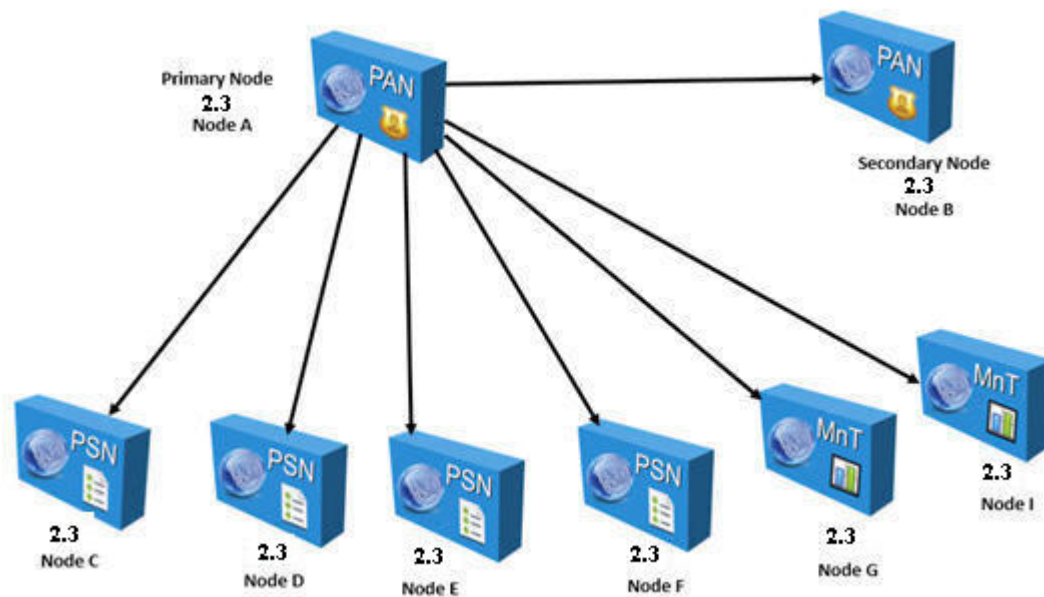
What to do next

[Verify the Upgrade Process, on page 42](#)

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 4: 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

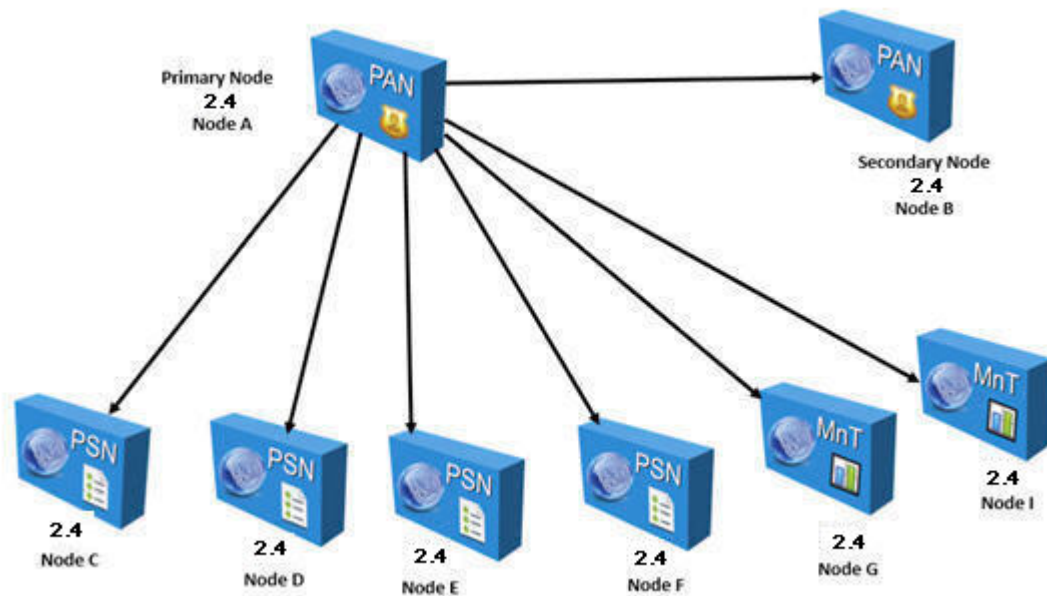
- If you do not have a Secondary Administration Node in the deployment, configure a Policy Service Node to be the Secondary Administration Node before beginning the upgrade process.
- Ensure that you have read and complied with the instructions given in the [Prepare for Upgrade](#) chapter.
- When you upgrade a complete Cisco ISE deployment, Domain Name System (DNS) server resolution (both forward and reverse lookups) is mandatory; otherwise, the upgrade fails.

-
- Step 1** Upgrade the Secondary Administration Node (node B) from the CLI.
- The upgrade process automatically deregisters node B from the deployment and upgrades it. Node B becomes the primary node of the new deployment when it restarts. Because each deployment requires at least one Monitoring node, the upgrade process enables the Monitoring persona on node B even if it was not enabled on this node in the old deployment. If the Policy Service persona was enabled on node B in the old deployment, this configuration is retained after upgrading to the new deployment.
- Step 2** Upgrade one of your Monitoring nodes (node G) to the new deployment.
- We recommend that you upgrade your Primary Monitoring Node before the Secondary Monitoring Node (this is not possible if your Primary Administration Node in the old deployment functions as your Primary Monitoring Node as well). Your primary Monitoring node starts to collect the logs from the new deployment and you can view the details from the Primary Administration Node dashboard.
- If you have only one Monitoring node in your old deployment, before you upgrade it, ensure that you enable the Monitoring persona on node A, which is the Primary Administration Node in the old deployment. Node persona changes result in a Cisco ISE application restart. Wait for node A to come up before you proceed. Upgrading the Monitoring node to the new deployment takes longer than the other nodes because operational data has to be moved to the new deployment.
- If node B, the Primary Administration Node in the new deployment, did not have the Monitoring persona enabled in the old deployment, disable the Monitoring persona on it. Node persona changes result in a Cisco ISE application restart. Wait for the Primary Administration Node to come up before you proceed.
- Step 3** Upgrade the Policy Service Nodes (nodes C, D, E, and F) next. You can upgrade several PSNs in parallel, but if you upgrade all the PSNs concurrently, your network will experience a downtime.
- If your PSN is part of a node group cluster, you must deregister the PSN from the PAN, upgrade it as a standalone node, and register it with the PAN in the new deployment.
- After the upgrade, the PSNs are registered with the primary node of the new deployment (node B), and the data from the primary node (node B) is replicated to all the PSNs. The PSNs retain their personas, node group information, and profiling probe configurations.
- Step 4** (If you have an IPN node in your deployment) Deregister the IPN node from the Primary Administration Node.
- Cisco ISE, Release 2.0 and later, does not support IPN nodes.
- Step 5** If you have a second Monitoring node (node I) in your old deployment, you must do the following:
- 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.
 - 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 5: 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 1/30, UPSUpgradeHandler(2.4.0.101)... Done in 42 seconds.
- Data upgrade step 2/30, UPSUpgradeHandler(2.4.0.116)... Done in 0 seconds.
- Data upgrade step 3/30, MachineAuthenticationSettingsRegistration(2.4.0.120)... Done in
0 seconds.
- Data upgrade step 4/30, GuestAccessUpgradeService(2.4.0.126)... Done in 14 seconds.
- Data upgrade step 5/30, RegisterPostureTypes(2.4.0.127)... Done in 1 seconds.
- Data upgrade step 6/30, UPSUpgradeHandler(2.4.0.127)... Done in 0 seconds.
- Data upgrade step 7/30, UPSUpgradeHandler(2.4.0.134)... Done in 0 seconds.
```

```

- Data upgrade step 8/30, NSFUpgradeService(2.4.0.140)... Done in 0 seconds.
- Data upgrade step 9/30, NSFUpgradeService(2.4.0.155)... Done in 1 seconds.
- Data upgrade step 10/30, UPSUpgradeHandler(2.4.0.158)... Done in 1 seconds.
- Data upgrade step 11/30, NSFUpgradeService(2.4.0.160)... Done in 0 seconds.
- Data upgrade step 12/30, NSFUpgradeService(2.4.0.161)... Done in 0 seconds.
- Data upgrade step 13/30, NSFUpgradeService(2.4.0.179)... Done in 0 seconds.
- Data upgrade step 14/30, NetworkAccessUpgrade(2.4.0.182)... Done in 1 seconds.
- Data upgrade step 15/30, StorageUpgradeService(2.4.0.183)... Done in 0 seconds.
- Data upgrade step 16/30, DnsHostnameResolutionRegistration(2.4.0.190)... Done in 0 seconds.
- Data upgrade step 17/30, ProfilerUpgradeService(2.4.0.194)... ..Done in 122 seconds.
- Data upgrade step 18/30, CertMgmtUpgradeService(2.4.0.200)... ....Done in 248 seconds.
- Data upgrade step 19/30, NSFUpgradeService(2.4.0.214)... Done in 0 seconds.
- Data upgrade step 20/30, ERSDictionaryRegistration(2.4.0.215)... Done in 0 seconds.
- Data upgrade step 21/30, NetworkAccessUpgrade(2.4.0.216)... Done in 0 seconds.
- Data upgrade step 22/30, ProfilerUpgradeService(2.4.0.227)... Done in 0 seconds.
- Data upgrade step 23/30, ProfilerUpgradeService(2.4.0.228)... Done in 4 seconds.
- Data upgrade step 24/30, ProfilerUpgradeService(2.4.0.229)... Done in 0 seconds.
- Data upgrade step 25/30, NetworkAccessUpgrade(2.4.0.240)... Done in 0 seconds.
- Data upgrade step 26/30, CertMgmtUpgradeService(2.4.0.293)... Done in 7 seconds.
- Data upgrade step 27/30, ProvisioningUpgradeService(2.4.0.299)... Done in 0 seconds.
- Data upgrade step 28/30, NSFUpgradeService(2.4.0.336)... Done in 3 seconds.
- Data upgrade step 29/30, ProfilerUpgradeService(2.4.0.336)... Done in 0 seconds.
- Data upgrade step 30/30, GuestAccessUpgradeService(2.4.0.336)... Done in 23 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...
M&T Log Processor is not running
ISE database M&T schema upgrade completed.
cat: /opt/oracle/base/admin/cpml0/dpdump/upgradedb*.properties: No such file or directory

Gathering Config schema(CEPM) stats .....
Gathering Operational schema(MNT) stats ....
% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS. During this time
progress of the upgrade is visible on console. It could take up to 30 minutes for this to
complete.
Rebooting to do Identity Service Engine upgrade...

```

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

```

ise/admin# application upgrade 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 1/30, UPSUpgradeHandler(2.4.0.101)... Done in 42 seconds.
- Data upgrade step 2/30, UPSUpgradeHandler(2.4.0.116)... Done in 0 seconds.
- Data upgrade step 3/30, MachineAuthenticationSettingsRegistration(2.4.0.120)... Done in
0 seconds.
- Data upgrade step 4/30, GuestAccessUpgradeService(2.4.0.126)... Done in 14 seconds.
- Data upgrade step 5/30, RegisterPostureTypes(2.4.0.127)... Done in 1 seconds.
- Data upgrade step 6/30, UPSUpgradeHandler(2.4.0.127)... Done in 0 seconds.

```

```

- Data upgrade step 7/30, UPSUpgradeHandler(2.4.0.134)... Done in 0 seconds.
- Data upgrade step 8/30, NSFUpgradeService(2.4.0.140)... Done in 0 seconds.
- Data upgrade step 9/30, NSFUpgradeService(2.4.0.155)... Done in 1 seconds.
- Data upgrade step 10/30, UPSUpgradeHandler(2.4.0.158)... Done in 1 seconds.
- Data upgrade step 11/30, NSFUpgradeService(2.4.0.160)... Done in 0 seconds.
- Data upgrade step 12/30, NSFUpgradeService(2.4.0.161)... Done in 0 seconds.
- Data upgrade step 13/30, NSFUpgradeService(2.4.0.179)... Done in 0 seconds.
- Data upgrade step 14/30, NetworkAccessUpgrade(2.4.0.182)... Done in 1 seconds.
- Data upgrade step 15/30, StorageUpgradeService(2.4.0.183)... Done in 0 seconds.
- Data upgrade step 16/30, DnsHostnameResolutionRegistration(2.4.0.190)... Done in 0 seconds.
- Data upgrade step 17/30, ProfilerUpgradeService(2.4.0.194)... ..Done in 122 seconds.
- Data upgrade step 18/30, CertMgmtUpgradeService(2.4.0.200)... ....Done in 248 seconds.
- Data upgrade step 19/30, NSFUpgradeService(2.4.0.214)... Done in 0 seconds.
- Data upgrade step 20/30, ERSDictionaryRegistration(2.4.0.215)... Done in 0 seconds.
- Data upgrade step 21/30, NetworkAccessUpgrade(2.4.0.216)... Done in 0 seconds.
- Data upgrade step 22/30, ProfilerUpgradeService(2.4.0.227)... Done in 0 seconds.
- Data upgrade step 23/30, ProfilerUpgradeService(2.4.0.228)... Done in 4 seconds.
- Data upgrade step 24/30, ProfilerUpgradeService(2.4.0.229)... Done in 0 seconds.
- Data upgrade step 25/30, NetworkAccessUpgrade(2.4.0.240)... Done in 0 seconds.
- Data upgrade step 26/30, CertMgmtUpgradeService(2.4.0.293)... Done in 7 seconds.
- Data upgrade step 27/30, ProvisioningUpgradeService(2.4.0.299)... Done in 0 seconds.
- Data upgrade step 28/30, NSFUpgradeService(2.4.0.336)... Done in 3 seconds.
- Data upgrade step 29/30, ProfilerUpgradeService(2.4.0.336)... Done in 0 seconds.
- Data upgrade step 30/30, GuestAccessUpgradeService(2.4.0.336)... Done in 23 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...
M&T Log Processor is not running
ISE database M&T schema upgrade completed.
cat: /opt/oracle/base/admin/cpm10/dpdump/upgradedb*.properties: No such file or directory

Gathering Config schema(CEPM) stats .....
Gathering Operational schema(MNT) stats ....
% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS. During this time
progress of the upgrade is visible on console. It could take up to 30 minutes for this to
complete.
Rebooting to do Identity Service Engine upgrade...

```

What to do next

[Verify the Upgrade Process, on page 42](#)

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.
-

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 4

Install Cisco ISE Software Patch

- [Cisco ISE Software Patches](#), on page 45
- [Roll Back Software Patches](#), on page 47
- [View Patch Install and Rollback Changes](#), on page 48

Cisco ISE Software Patches

Cisco ISE software patches are usually cumulative. Cisco ISE allows you to perform patch installation and rollback from CLI or GUI.

You can install patches on Cisco ISE servers in your deployment from the Primary PAN. To install a patch from the Primary PAN, you must download the patch from Cisco.com to the system that runs your client browser.

If you are installing the patch from the GUI, the patch is automatically installed on the Primary PAN first. The system then installs the patch on the other nodes in the deployment in the order listed in the GUI. You cannot control the order in which the nodes are updated. You can also manually install, roll back, and view patch version from the **Administrator > System > Maintenance > Patch management** window in the GUI.

If you are installing the patch from the CLI, you can control the order in which the nodes are updated. However, we recommend that you install the patch on the Primary PAN first.

If you want to validate the patch on some of the nodes before upgrading the entire deployment, you can use the CLI to install the patch on selected nodes. Use the following CLI command to install the patch:

```
patch install <patch_bundle> <repository_that_stores_patch_file>
```

For more information, see the "install Patch" section in the "Cisco ISE CLI Commands in EXEC Mode" chapter in [Cisco Identity Services Engine CLI Reference Guide](#).

You can install the required patch version directly. For example, if you are currently using Cisco ISE 2.x and would like to install Cisco ISE 2.x patch 5, you can directly install Cisco ISE 2.x patch 5, without installing the previous patches (in this example, Cisco ISE 2.x patches 1 – 4). To view the patch version in the CLI, use the following CLI command:

```
show version
```

Related Topics

- [Software Patch Installation Guidelines](#), on page 46
- [Software Patch Rollback Guidelines](#), on page 47
- [Install a Software Patch](#), on page 46

[Roll Back Software Patches](#), on page 47

Software Patch Installation Guidelines

When you install a patch on an ISE node, the node is rebooted after the installation is complete. You might have to wait for a few minutes before you can log in again. You can schedule patch installations during a maintenance window to avoid temporary outage.

Ensure that you install patches that are applicable for the Cisco ISE version that is deployed in your network. Cisco ISE reports any mismatch in versions as well as any errors in the patch file.

You cannot install a patch with a version that is lower than the patch that is currently installed on Cisco ISE. Similarly, you cannot roll back changes of a lower-version patch if a higher version is currently installed on Cisco ISE. For example, if patch 3 is installed on your Cisco ISE servers, you cannot install or roll back patch 1 or 2.

When you install a patch from the Primary PAN that is part of a distributed deployment, Cisco ISE installs the patch on the primary node and then all the secondary nodes in the deployment. If the patch installation is successful on the Primary PAN, Cisco ISE then continues patch installation on the secondary nodes. If it fails on the Primary PAN, the installation does not proceed to the secondary nodes. However, if the installation fails on any of the secondary nodes for any reason, it still continues with the next secondary node in your deployment.

When you install a patch from the Primary PAN that is part of a two-node deployment, Cisco installs the patch on the primary node and then on the secondary node. If the patch installation is successful on the Primary PAN, Cisco then continues patch installation on the secondary node. If it fails on the Primary PAN, the installation does not proceed to the secondary node.

Install a Software Patch

Before you begin

- You must have the Super Admin or System Admin administrator role assigned.
- Go to **Administration > System > Deployment > PAN Failover**, and ensure that the **Enable PAN Auto Failover** check box is unchecked. The PAN auto-failover configuration must be disabled for the duration of this task.

Step 1 Choose **Administration > System > Maintenance > Patch Management > Install**.

Step 2 Click **Browse** and choose the patch that you downloaded from Cisco.com.

Step 3 Click **Install** to install the patch.

After the patch is installed on the PAN, Cisco ISE logs you out and you have to wait for a few minutes before you can log in again.

Note When patch installation is in progress, **Show Node Status** is the only function that is accessible on the Patch Management page.

Step 4 Choose **Administration > System > Maintenance > Patch Management** to return to the Patch Installation page.

- Step 5** Click the radio button next to the patch that you have installed on any secondary node and click **Show Node Status** to verify whether installation is complete.
-

What to do next

If you need to install the patch on one or more secondary nodes, ensure that the nodes are up and repeat the process to install the patch on the remaining nodes.

Roll Back Software Patches

When you roll back a patch from the PAN that is part of a deployment with multiple nodes, Cisco ISE rolls back the patch on the primary node and then all the secondary nodes in the deployment.

Before you begin

- You must have either the Super Admin or System Admin administrator role assigned.
-

- Step 1** Choose **Administration > System > Maintenance > Patch Management**.

- Step 2** Click the radio button for the patch version whose changes you want to roll back and click **Rollback**.

Note When a patch rollback is in progress, **Show Node Status** is the only function that is accessible on the Patch Management page.

After the patch is rolled back from the PAN, Cisco ISE logs you out and you have to wait a few minutes before you can log in again.

- Step 3** After you log in, click the **Alarms** link at the bottom of the page to view the status of the rollback operation.

- Step 4** Choose **Administration > System > Maintenance > Patch Management**.

- Step 5** To view the progress of the patch rollback, choose the patch in the Patch Management page and click **Show Node Status**.

- Step 6** Click the radio button for the patch and click **Show Node Status** on a secondary node to ensure that the patch is rolled back from all the nodes in your deployment.

If the patch is not rolled back from any of the secondary nodes, ensure that the node is up and repeat the process to roll back the changes from the remaining nodes. Cisco ISE only rolls back the patch from the nodes that still have this version of the patch installed.

Software Patch Rollback Guidelines

To roll back a patch from Cisco ISE nodes in a deployment, you must first roll back the change from the PAN. If this is successful, the patch is then rolled back from the secondary nodes. If the rollback process fails on the PAN, the patches are not rolled back from the secondary nodes. However, if the patch rollback fails on any secondary node, it still continues to roll back the patch from the next secondary node in your deployment.

While Cisco ISE rolls back the patch from the secondary nodes, you can continue to perform other tasks from the PAN GUI. The secondary nodes will be restarted after the rollback.

View Patch Install and Rollback Changes

To view reports related to installed patches, perform the following steps.

Before you begin

You must have either the Super Admin or System Admin administrator role assigned. You can install or rollback patches in the **Administration > System > Maintenance > Patch Management** page. You can also view the status (installed/in-progress/not installed) of a particular patch on each node in the deployment, by selecting a specific patch and clicking the **Show Node Status** button.

-
- Step 1** Choose **Operations > Reports > Audit > Operations Audit**. By default, records for the last seven days are displayed.
- Step 2** Click the **Filter** drop-down, and choose **Quick Filter** or **Advanced Filter** and use the required keyword, for example, patch install initiated, to generate a report containing the installed patches.
-



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 49](#)

Post-Upgrade Settings and Configurations

Perform the following tasks after upgrading Cisco ISE.

Verify Virtual Machine Settings

Ensure that the Guest Operating System on the VMware virtual machine is set to Red Hat Enterprise Linux (RHEL) 7, and that the network adapter is set to E1000 or VMXNET3.

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>

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.

SNMP 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** 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** Choose **Policy > Policy Elements > Results > Client Provisioning > Resources** to configure the client provisioning resources.
 - Step 2** Click **Add**.
 - Step 3** Choose **Agent Resources from Local Disk**.
 - Step 4** 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.

