Cisco ISE 3.0 Upgrade Guide: Overview

Cisco ISE Upgrade Overview

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

This document describes how to upgrade your Cisco Identity Services Engine (ISE) software on Cisco ISE appliances and virtual machines to Release 3.0. (See the section "What is New in Cisco ISE, Release 3.0" in *Release Notes for Cisco Identity Services Engine, Release 3.0.*)

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.

Regenerate the Root CA Chain

In case of the following events, you must regenarate the root CA chain:

- Changing the domain name or hostname of your PAN or PSN.

- Restoring a backup on a new deployment.

- Promoting the old Primary PAN to new Primary PAN post upgrade.

In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration > System > Certificates > Certificate Management > Certificate Signing Request**. Click on **Generate Certificate Signing Request (CSR)**. Select the **ISE Root CA** in the **Certificate(s) will be used for** drop-down list. Click on **Replace ISE root CA Certificate Chain**.

Upgrade Path

Single-step Upgrade

You can directly upgrade to 3.0, from any of the following releases:

- Cisco ISE, Release 2.4

- Cisco ISE, Release 2.6

- Cisco ISE, Release 2.7

You can download the upgrade bundle from Cisco.com. The following upgrade bundle is available for Release 3.0:

ise-upgradebundle-2.4.x-2.7.x-to-3.0.0.458.SPA.x86_64.tar.gz—Use this bundle to upgrade from Release 2.4, 2.6 or 2.7 to 3.0

Two-step Upgrade

If you are currently using a version earlier than Cisco ISE, Release 2.4, you must first upgrade to one of the releases that are listed above and then upgrade to Release 3.0.

Supported Operating System for Virtual Machines

Cisco ISE runs on the Cisco Application Deployment Engine operating system (ADEOS), which is based on Red Hat Enterprise Linux (RHEL). For Cisco ISE 3.0, ADEOS is based on RHEL 7.6.

The following table shows the RHEL versions used in different versions of Cisco ISE:

Table 1: RHEL Releases

Cisco ISE Release	RHEL Release
Cisco ISE 1.3	RHEL 6.4
Cisco ISE 1.4	RHEL 6.4
Cisco ISE 2.0	RHEL 7.0
Cisco ISE 2.1	RHEL 7.0

Cisco ISE Release	RHEL Release
Cisco ISE 2.2	RHEL 7.0
Cisco ISE 2.3	RHEL 7.0
Cisco ISE 2.4	RHEL 7.3
Cisco ISE 2.6	RHEL 7.5
Cisco ISE 2.7	RHEL 7.6
Cisco ISE 3.0	RHEL 7.6

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.

Smart Licensing for Air-Gapped Networks

Cisco ISE Smart Licensing requires Cisco ISE to be connected to the CSSM. If your network is air-gapped, Cisco ISE is unable to report license usage to CSSM. This lack of reporting results in loss of administrative access to Cisco ISE and restrictions in Cisco ISE features.

To avoid licensing issues in air-gapped networks and enable full Cisco ISE functionality, configure Smart Software Manager (SSM) On-Prem. This licensing method is available in Cisco ISE Release 3.0 Patch 2 and later. You can configure the SSM On-Prem server on a node in your deployment and ensure that Cisco ISE can reach this server. This server takes over the role of CSSM in your air-gapped network, releasing license entitlements as needed and tracking usage metrics. The SSM On-Prem server also sends notifications, alarms, and warning messages that are related to licensing consumption and validity.

If you buy or modify your license purchases, you must connect the SSM On-Prem to CSSM for the changes to be available in your local server.

Note

- If you enable the SSM On-Prem licensing solution, you will not be able to use proxy services in Cisco ISE. You will also not be able to use any Cisco ISE services that are enabled by external CA certificates.

- ISE-PIC 3.0 does not support Smart Licensing.

Configure Smart Software Manager On-Prem for Smart Licensing

Before you begin

Configure SSM On-Prem server on a node in your deployment and ensure that Cisco ISE can reach this server. This node must be a dedicated server. Do not enable any Cisco ISE personas on this node.

See Smart Software Manager On-Prem Resources.

Procedure

Step 1	In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration > System > Licensing**.
Step 2	Click **Registration Details**.
Step 3	In the **Registration Details** area displayed, enter the registration token that you received from CSSM in the **Registration Token** field.
Step 4	Choose **SSM On-Prem Server** from the **Connection Method** drop-down list.
	The **Certificate** window in the SSM On-Prem portal displays either the IP address or the hostname (or FQDN) of the connected SSM On-Prem server.
Step 5	Enter the configured IP address or the hostname (or FQDN) in the **SSM On-Prem server Host** field.
Step 6	From the **Tier** and **Virtual Appliance** areas, check the check boxes for all the licenses you need to enable. The chosen licenses will be activated and their consumption is tracked by CSSM.
Step 7	Click **Register**.

Permanent License Reservation

Cisco ISE Release 3.0 Patch 2 and later support the Permanent License Reservation licensing method.

Without a persistent connection to the Internet, Cisco ISE Smart Licensing is unable to update the CSSM regarding license usage. This lack of communication between Cisco ISE and the CSSM could result in loss of administrative access and sub-optimal Cisco ISE functionality. Permanent License Reservation is a licensing method that is suited for Cisco ISE deployments that do not have a persistent connection to the Internet.

☞

Important   Permanent License Reservation is a licensing method that is available by approval only. Contact your Cisco account manager to determine if Permanent License Reservation can be used in your environment.

With Permanent License Reservation, you install a universal reservation in your Cisco ISE. This licensing method allows you to use any Cisco ISE license entitlement on your network.

When this licensing method is enabled, Cisco ISE licensing does not require to connect to the CSSM to facilitate or report licenses consumption when the corresponding Cisco ISE features are used. You will not receive notifications, warnings, or alerts regarding license consumption and usage.

You must install Permanent License Reservation in every primary Policy Administration node (PAN) in your deployment. Though optional, we recommend that you enable this licensing method in all the secondary PANs as well.

When you enable Permanent License Reservation in your secondary PANs, you avoid service disruption in the following scenarios:

- Primary PAN failover

- High availability primary PAN configuration

- Upgrade workflows, where the primary PAN is temporarily demoted as the secondary PAN

Licensing Changes

Device Administration Licenses

The licenses that are used for Cisco ISE Releases 2.x, such as Base, Plus, and Apex, have been replaced with new license types. Cisco ISE Release 3.0 uses Essentials, Advantage, and Premier licenses. See the Chapter "Licensing" in the *Cisco Identity Services Engine Administrator Guide*. For more information on license migration, see the ISE 3.0 License Migration Guide.

You must convert your existing smart or traditional licenses to the new license type through the Cisco Smart Software Manager (CSSM), to enable license consumption in Cisco ISE Release 3.0.

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 shipped 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 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.

VM License Categories

VM licenses are offered under three categories: Small, Medium, and Large. These categories depend on the resources such as hardware appliances, RAM capacity and number of CPUs. 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.

The following table shows the minimum VM resources required for the VM categories:

VM Category	VM License Specifications
Small	• Minimum 16GB RAM and 12 CPU cores for SNS-3515 equivalent. • Minimum 32GB RAM and 16 CPU cores for SNS-3615 equivalent.
Medium	• Minimum 64GB RAM and 16 CPU cores for SNS-3595 equivalent. • Minimum 96GB RAM and 24 CPU cores for SNS-3655 equivalent.
Large	• Minimum 256GB RAM and 16 CPU cores for MnT in clusters supporting more than 500,000 concurrent sessions. • Minimum 256GB RAM and 24 CPU cores for SNS-3695 equivalent.

For more information about the licenses, see the "Cisco ISE Licenses" chapter in the *Cisco Identity Services Engine Administrator Guide*.