

Revised: June 2, 2026

Postupgrade Tasks

Postupgrade settings and configurations

Perform these tasks after upgrading Cisco ISE.

Convert to new license types

To convert to new license types, perform these steps:

1. Convert your old licenses to the new license types through the Cisco Smart Software Manager (CSSM).
2. Enable the new licenses in your Cisco ISE administrator portal.

For more information, refer to "Cisco ISE Licenses" in the "[Licensing](#)" chapter in the *Cisco ISE Administrator Guide, Release 3.5*.

Verify VM settings

If you are upgrading Cisco ISE nodes on VMs, change the Guest OS to RHEL 8.4 (64-bit). To do this

1. power down the VM
2. change the Guest OS to the supported RHEL version, and then
3. power on the VM.

RHEL 7 and later support only E1000 and VMXNET3 network adapters. Change your network adapter type before you upgrade.

Browser setup

After you upgrade your Cisco ISE deployment, you must

1. clear your browser cache
2. close your browser, and
3. open a new browser session (on a supported browser) to access the Cisco ISE Admin portal.



Note

Refer to the release notes for a list of supported browsers: <https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html>.

Rejoin Active Directory

If you log in to the Cisco ISE user interface with an Active Directory administrator account after the upgrade, the login fails because the Active Directory join is lost during the upgrade.

If you use certificate-based authentication for administrative access and Active Directory is your identity source, you cannot access the login page after an upgrade. This is because the Active Directory join is lost during the upgrade.

If you use Active Directory as your external identity source and lose connection, complete these steps:

1. Enter this command to start Cisco ISE in safe mode:

application start ise safe

2. Log in to the Cisco ISE user interface using the internal administrator account.



Note

If you forgot your Cisco ISE password or your administrator account is locked, refer to the "[Administrator Access to Cisco ISE](#)" chapter in the *Cisco ISE Administrator Guide, Release 3.5*.

3. Rejoin Cisco ISE with Active Directory.
4. Run the external identity source workflows to verify that the connection is restored.

Certificate attributes with AD

Cisco ISE identifies users by their attributes *SAM*, *CN*, or both, with *sAMAccountName* attribute used as default.

You can configure Cisco ISE to use *SAM*, *CN*, or both, depending on your environment. If both *SAM* and *CN* are used and the *sAMAccountName* attribute is not unique, Cisco ISE also compares the *CN* attribute value.

To configure attributes for AD identity search, complete these steps:

1. In the Cisco ISE GUI, navigate to **Administration > Identity Management > External Identity Sources > Active Directory**.
2. Click **Advanced Tools**.
3. Choose **Advanced Tuning** and enter these details:
 - **ISE Node:** Choose the Cisco 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 Cisco 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*.
4. Click **Update Value** to update the registry.

When the pop-up window appears, read the message and accept the change. The AD connector service in Cisco ISE restarts automatically.

Reverse DNS lookup

Configure Reverse DNS lookup for all Cisco ISE nodes in your distributed deployment on every DNS server. If you do not configure reverse DNS lookup, deployment-related issues may occur after the upgrade.

Restore certificates

This section details how to restore certificates and keys on Cisco ISE Administration Nodes to prevent authentication failures that may occur during upgrades.

Restore certificates on the PAN

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

- SAN is promoted to be the PAN in the new deployment.
- Session services are disabled on the SAN.

If the certificates are not in the store, you may get authentication failures with these errors:

- Unknown CA in the chain during a BYOD flow
- OCSP unknown error during a BYOD flow

You can get these messages when you click the **More Details** link from the **Live Logs** page for failed authentications.

To restore the root CA certificates of PAN, generate a new Cisco ISE Root CA certificate chain. In the Cisco ISE GUI, navigate to **Administration > Certificates > Certificate Signing Requests > Replace ISE Root CA certificate chain**.

Restore certificates and keys to SAN

If you are using a SAN, obtain a backup of the Cisco ISE CA certificates and keys from the PAN, and restore it on the SAN. This allows the SAN to function as the root CA or subordinate CA of an external PKI if the primary PAN fails, and you promote the SAN to be the PAN.

For more information, refer to "Backup and restoration of Cisco ISE CA certificates and keys" in the "[Basic Setup](#)" chapter in the *Cisco ISE Administrator Guide, Release 3.5*.

Regenerate the root CA chain

If your deployment matches specific upgrade scenarios, you must regenerate the root CA chain after the upgrade is complete.

To regenerate the root CA chain, complete these steps:

1. In the Cisco ISE GUI, navigate to **Administration > System > Certificates > Certificate Management > Certificate Signing Request**.
2. Click **Generate Certificate Signing Request (CSR)**.
3. Choose **ISE Root CA** in the **Certificate(s) will be used for** drop-down list.
4. Click **Replace ISE root CA Certificate Chain**.

This table defines various root CA chain regeneration scenarios.

Table 1: Root CA chain regeneration scenarios

Upgrade scenario	Mode
Full upgrade process	Deployment and Standalone
Split upgrade process	Deployment and Standalone

Upgrade scenario	Mode	
Configuration database restoration process	Standalone	T
Node Promotion: Promoting a secondary PAN to primary PAN after the split upgrade process	Deployment	F
Change in the domain name or hostname of any Cisco ISE node	Standalone and Deployment	F

After the upgrade process, you might encounter these events:

- Data might not be available in live logs.
- You might get queue link errors.
- The system might show the health status as unavailable.
- System summary might not display data for some nodes.

To resolve queue link errors and restore system information,

- reset the MnT Database , and
- replace the ISE Root CA certificate chain.

Threat-centric NAC

If you enable the Threat-centric NAC (TC-NAC) service, the TC-NAC adapters might not function after an upgrade. Restart the adapters from the TC-NAC pages of the Cisco ISE GUI. Select an adapter and click **Restart**.

Set the SNMP originating policy services node

If you manually configure the SNMP originating policy services node setting value under SNMP settings, you lose the configuration during an upgrade. Reconfigure the SNMP settings to restore the SNMP functionality.

Profiler feed service

After you upgrade, update the profiler feed service to ensure that the most up-to-date Organizationally Unique Identifiers (OUIs) are installed.

Follow these steps to update the profiler feed service:

- Step 1** In the Cisco ISE GUI, navigate to **Administration** > **FeedService** > **Profiler**.
- Step 2** Ensure the profiler feed service is enabled.
- Step 3** Click **Update Now**.

Client provisioning

Review these considerations before updating client provisioning resources:

- Check the native supplicant profile used in the client provisioning policy.
- Ensure that the wireless SSID is correct.
- For iOS devices, if the network you are trying to connect to is hidden, check the **Enable if target network is hidden** check box in the **iOS Settings** area.

Follow these steps to update client provisioning resources:

Online updates

- Step 1** In the Cisco ISE GUI, navigate to **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** In the Cisco ISE GUI, navigate to **Policy > Policy Elements > Results > Client Provisioning > Resources** to configure the client provisioning resources.
- Step 2** Click **Add** to add a new resource.
- Step 3** Choose **Agent Resources from Local Disk**.
- Step 4** From the **Category** drop-down list, choose **Cisco Provided Packages**.

Cipher suites

Authentication may fail for legacy devices that use deprecated ciphers when connecting to Cisco ISE.

To enable Cisco ISE to authenticate these legacy devices after an upgrade, update the **Allowed Protocols** configuration by performing these steps:

- Step 1** In the Cisco ISE GUI, navigate to **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**.

Monitor and troubleshoot

Consider these steps to monitor and troubleshoot:

- Reconfigure your email settings.
- Update your favorite reports.
- Change your data purge settings.
- Check thresholds and filters for specific alarms you need.



Note

By default, all alarms are enabled after an upgrade.

- Customize reports based on your needs.



Note

If you customized reports during the previous deployment, your changes will be replaced during the upgrade.

Restore the MnT backup that you created before the update.

Refresh policies to Trustsec NADs

Run these commands to download the policies to Cisco TrustSec-enabled Layer 3 interfaces in your system:

1. `no cts role-based enforcement`
2. `cts role-based enforcement`

Update Supplicant Provisioning Wizards

The Supplicant Provisioning Wizards (SPWs) are not updated when you upgrade to a new release or apply a patch. You must manually update the SPWs. Then, create new native supplicant profiles and new client provisioning policies that reference the new SPWs. You can find new SPWs on the Cisco ISE Download page. Visit the Cisco software download site for more information.

Profiler endpoint ownership synchronization or replication

During an upgrade, the JEDIS framework requires port 6379 to be open between all nodes in the deployment to allow two-way communication.