Cisco ISE 2.7 Upgrade Guide: Post-Upgrade Tasks

First Published: 2022-09-29

Post-Upgrade Settings and Configurations

Perform the following tasks after upgrading Cisco ISE.

Verify Virtual Machine Settings

If you are upgrading Cisco ISE nodes on virtual machines, ensure that you change the Guest Operating System to Red Hat Enterprise Linux (RHEL) 7 (64-bit) or Red Hat Enterprise Linux (RHEL) 6 (64-bit). To do this, you must power down the VM, change the Guest Operating System to the supported RHEL version, and power on the VM after the change.

RHEL 7 supports only E1000 and VMXNET3 network adapters. Be sure to change the network adapter type before you upgrade.

If you are running ISE on an ESXi 5.x server (5.1 U2 minimum), you must upgrade the VMware hardware version to 9 before you can select RHEL 7 as the Guest OS.

Browser Setup

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

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

Regenerate the Root CA Chain

In specific upgrade scenarios, you must regenerate the root CA chain after the upgrade process is complete. Regenerate the root CA chain by following these steps:

1. From the Cisco ISE main menu, choose **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**.

Table 1: Root CA Chain Regeneration Scenarios

Upgrade scenario	Mode	Root CA Chain Regeneration
Full upgrade process	Deployment	Regeneration of root CA is not required as the deployment does not change during the upgrade process.
Split upgrade process	Deployment	Regenerate the root CA chain.
Configuration database restoration process	Standalone	Regenerate the root CA chain.
Node Promotion: Promoting a secondary PAN to primary PAN after the split upgrade process	Deployment	Regenerate the root CA chain.
Change in the domain name or hostname of any Cisco ISE node	Standalone and Deployment	Regenerate the root CA chain.

After the upgrade process, you might encounter the following events:

1. No data in live logs.
2. Queue link errors.
3. Health status is unavailable.
4. No date available in the system summary for some nodes.

You must reset the MnT Database and replace the ISE Root CA certificate chain to resolve the queue link error and reinstate the information.

Threat-Centric NAC

If you have enabled the Threat-Centric NAC (TC-NAC) service, after you upgrade, the TC-NAC adapters might not be functional. You must restart the adapters from the Threat-Centric NAC pages of the ISE GUI. Select the adapter and click Restart to start the adapter again.

SMNP Originating Policy Services Node Setting

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

For more information, see:

See SNMP Settings under Network Device Definition Settings.

Profiler Feed Service

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

From the Cisco ISE Admin portal:

Procedure

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

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

Step 3 Click **Update Now**.

Client Provisioning

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

Update client provisioning resources on ISE:

Online Updates

Procedure

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

Procedure

Step 1 Click **Add**.

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

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

Cipher Suites

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

Procedure

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.

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.

Profiler Endpoint Ownership Synchronization/ Replication

When you upgrade to Cisco ISE 2.7 and later version, as part of JEDIS framework the port 6379 is required to be opened between all nodes in the deployment for to-and-fro communication.

© Cisco Systems, Inc. All rights reserved.