Troubleshoot and Settings Post ISE Upgrade

Contents

Introduction

This document describes the Settings and Tasks you must perform after ISE Deplyment Upgrade.

Components Used

The information in this document is based on these software and hardware versions:

- ISE, Release 3.0.
- ISE, Release 3.1.
- ISE, Release 3.2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Post-Upgrade Settings and Configurations

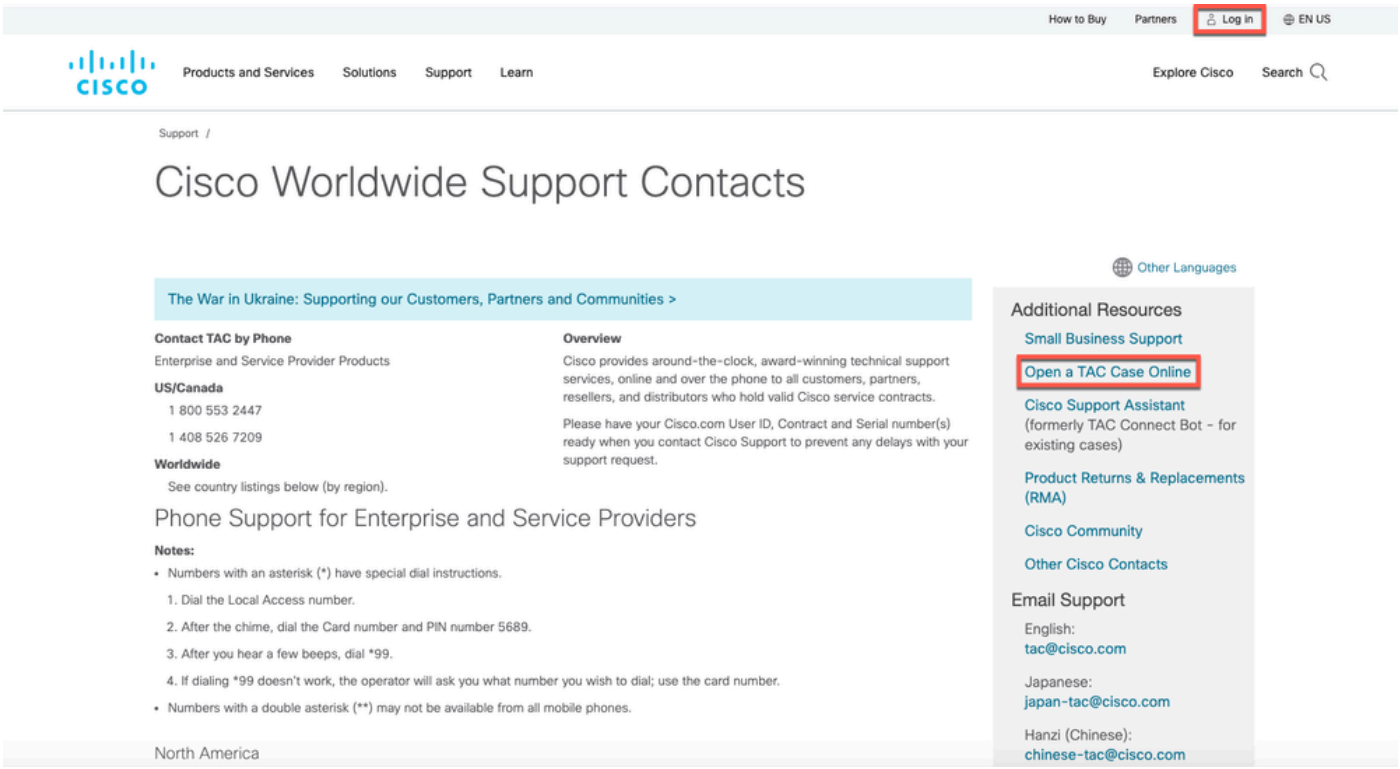
Perform the settings and tasks after upgrading Cisco ISE.

Convert To New License Types

Convert your old licenses to the new license types through the Cisco Smart Software Manager (CSSM).

If you are upgrading to Cisco ISE Release 3.0 and later releases with Base, Apex, and Plus licenses smart licenses, your smart licenses are upgraded to the new license types in Cisco ISE. However, you must register the new license types in CSSM to activate the licenses in the Cisco ISE release that you upgrade to.

If you own traditional Cisco ISE licenses, you must convert them to smart licenses to enable license consumption in Cisco ISE Release 3.0 and later releases. To convert Cisco ISE 2.x licenses to the new license types, open a case online through the Support Case Manager, or use the contact information that is provided at TAC-WorldWide Suppot.



Cisco WorldWide Support Contacts

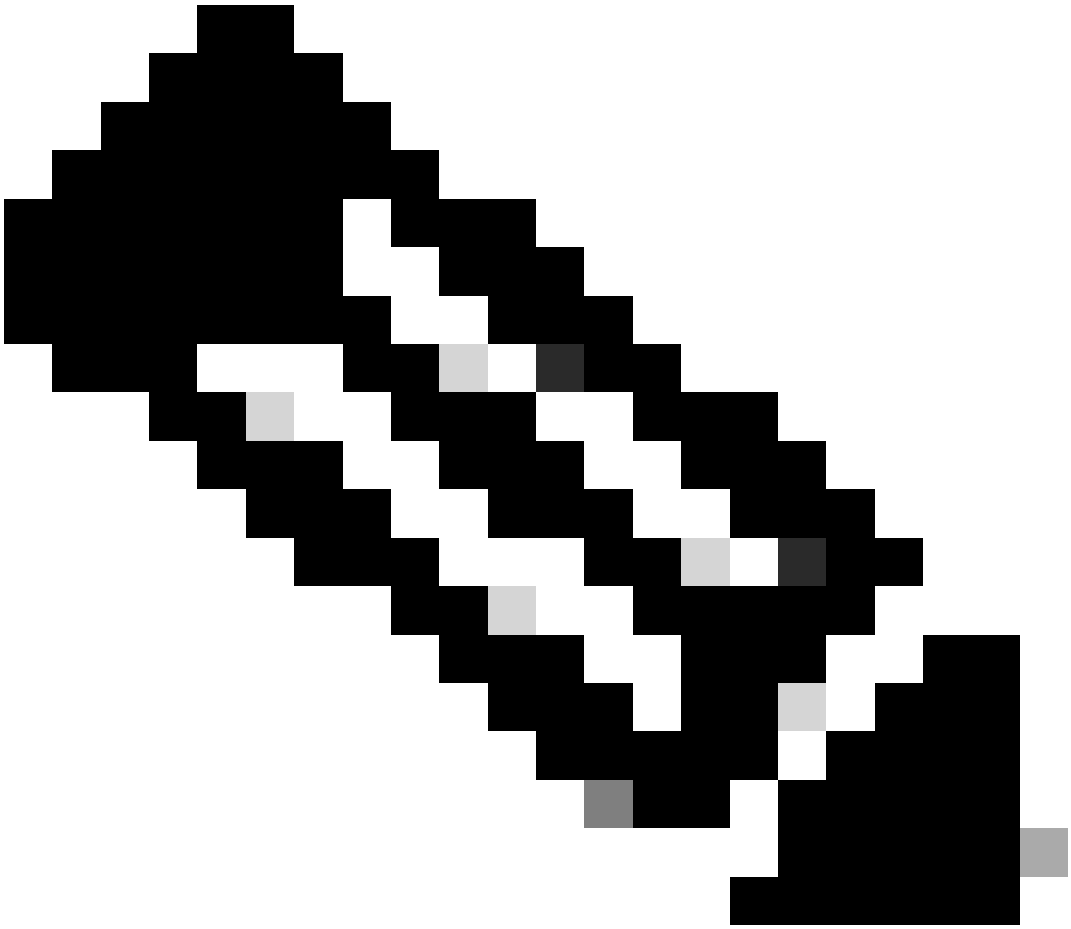
Notifications about noncompliant license consumption are also displayed in Cisco ISE.If your license consumption is out of compliance for45 days in a 60-day period, you can lose all administrative control of Cisco ISE until you purchase and activate the required licenses.

When upgrading from one licensing package to another, Cisco ISE continues to offer all the features that were available in the earlier package before the upgrade. However, you do have to reconfigure any settings that you had already configured. For example, if you currently use an Essentials license and later add an Advantage license, the features that are already configured using the Essentials license would not change.

Verify Virtual Machine Settings

If you are upgrading Cisco ISE nodes on virtual machines, ensure that you change the Guest Operating System toRed Hat Enterprise Linux (RHEL) 8.4 (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 7and latersupportonly E1000 and VMXNET3 network adapters. Be sure to change the network adapter type before you upgrade.



Note: 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 ISE Release Notes.

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 would 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 next command:

application stop ise

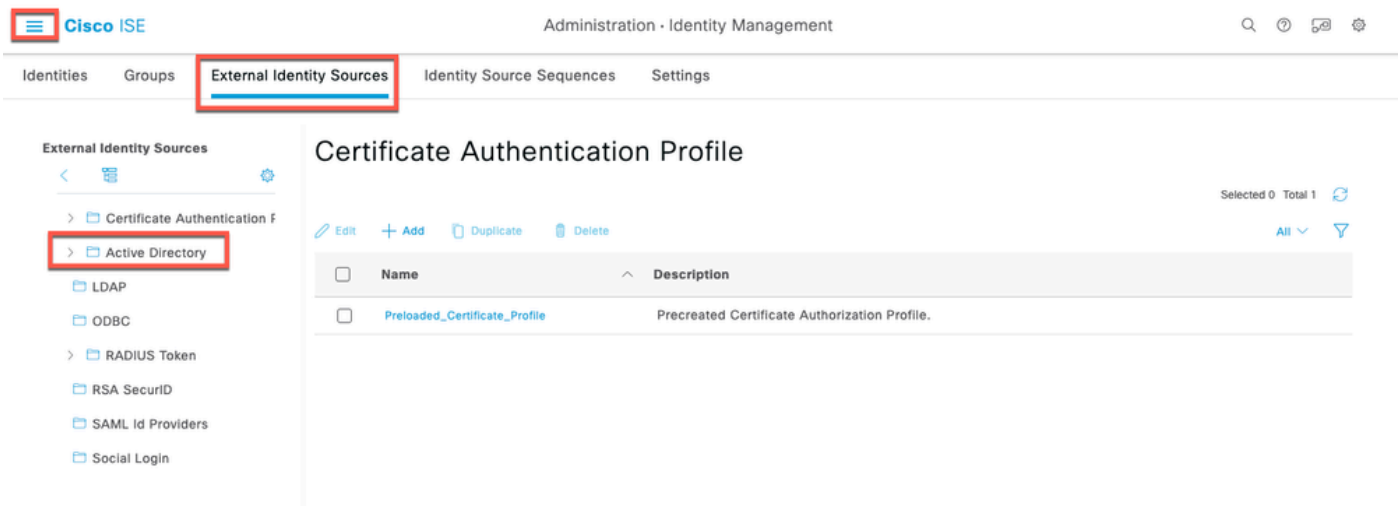
application start ise safe

After Cisco ISE starts in **Safe Mode**, perform the tasks:

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

2. Join Cisco ISE with Active Directory.

In the Cisco ISE GUI, click the **Menu** icon ( ) and choose **Administration > Identity Management > External Identity Sources > Active Directory.**
For more information about joining Active Directory, see: [Configure Active Directory as an External Identity Source.]



Active Directory Configuration

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 can run into deployment-related issues after upgrade.

Restore Certificates

Restore Certificates on the PAN**.** When you upgrade a distributed deployment, the Primary Administration Node root CA certificates are not added to the Trusted Certificates store if both of the conditions are met:

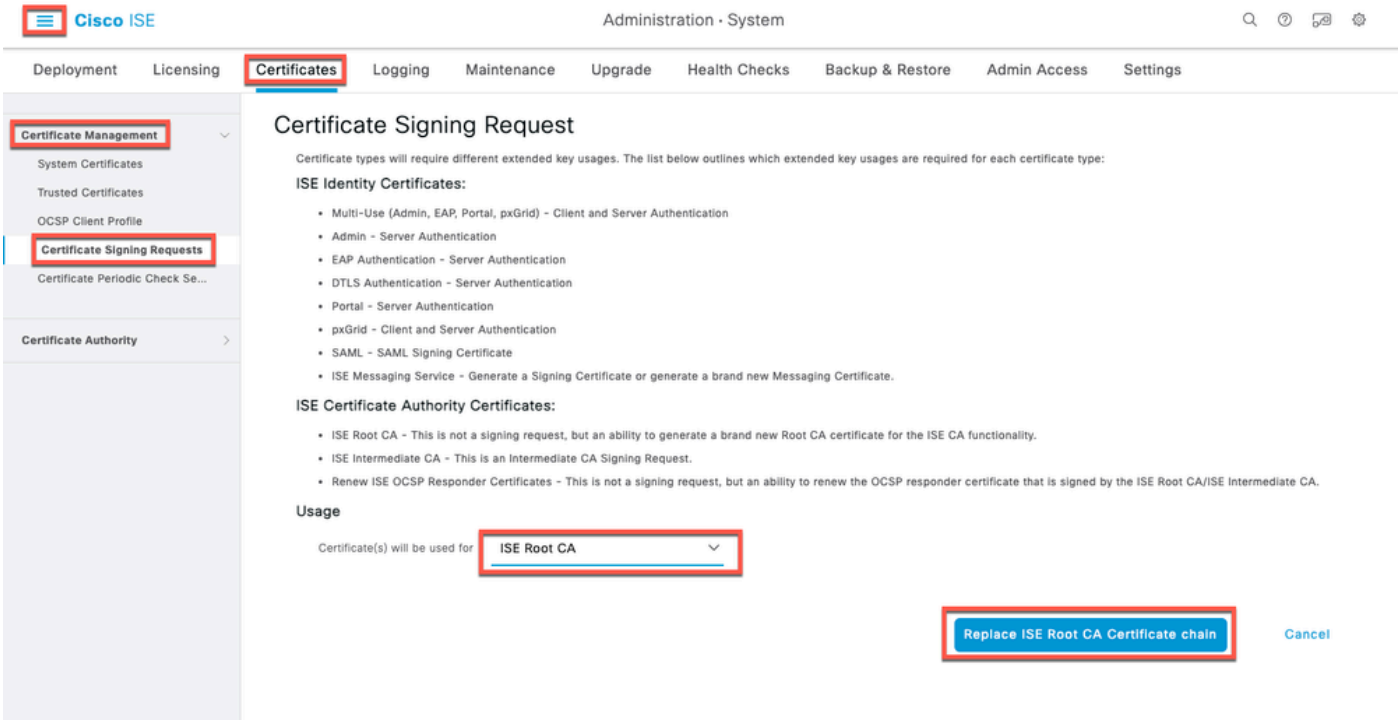
- Secondary Administration Node is promoted to be the Primary Administration Node in the new deployment.
- Session services are disabled on the Secondary Administration Node.

If the certificates are not in the store, you can see authentication failures with the 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 root CA certificates, generate a new Cisco ISE Root CA certificate chain. In the Cisco ISE GUI, click the **Menu** icon () and choose **Administration > Certificates > Certificate Signing Requests > Replace ISE Root CA certificate chain**.



Regenerate ISE Root CA

Restore Certificates and Keys to Secondary Administration Node

If you are using a secondary Administration node, you can 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 completing these steps:

Step (1): From the Cisco ISE main menu, choose**Administration > System > Certificates > Certificate Management > Certificate Signing Request**.

Step (2): Click**Generate Certificate Signing Request (CSR)**.

Step (3): Choose**ISE Root CA**in the**Certificate(s) would be used for**drop-down list.

Step (4): Click**Replace ISE root CA Certificate Chain**.

Table ShowsRoot CA Chain Regeneration Scenarios:

Upgrade scenario	Mode	Root CA Chain Regeneration
Full upgrade process	Deployment and Standalone	Regeneration of root CA is not required as the deployment does not change during the upgrade process.
Split upgrade process	Deployment and Standalone	The root CA chain is automatically regenerated during the upgrade process.
Configuration database restoration process	Standalone	The root CA chain is automatically regenerated during the restore process.
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.

Threat-Centric NAC

If you have enabled the Threat-Centric NAC (TC-NAC) service, after you upgrade, the TC-NAC adapters could 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

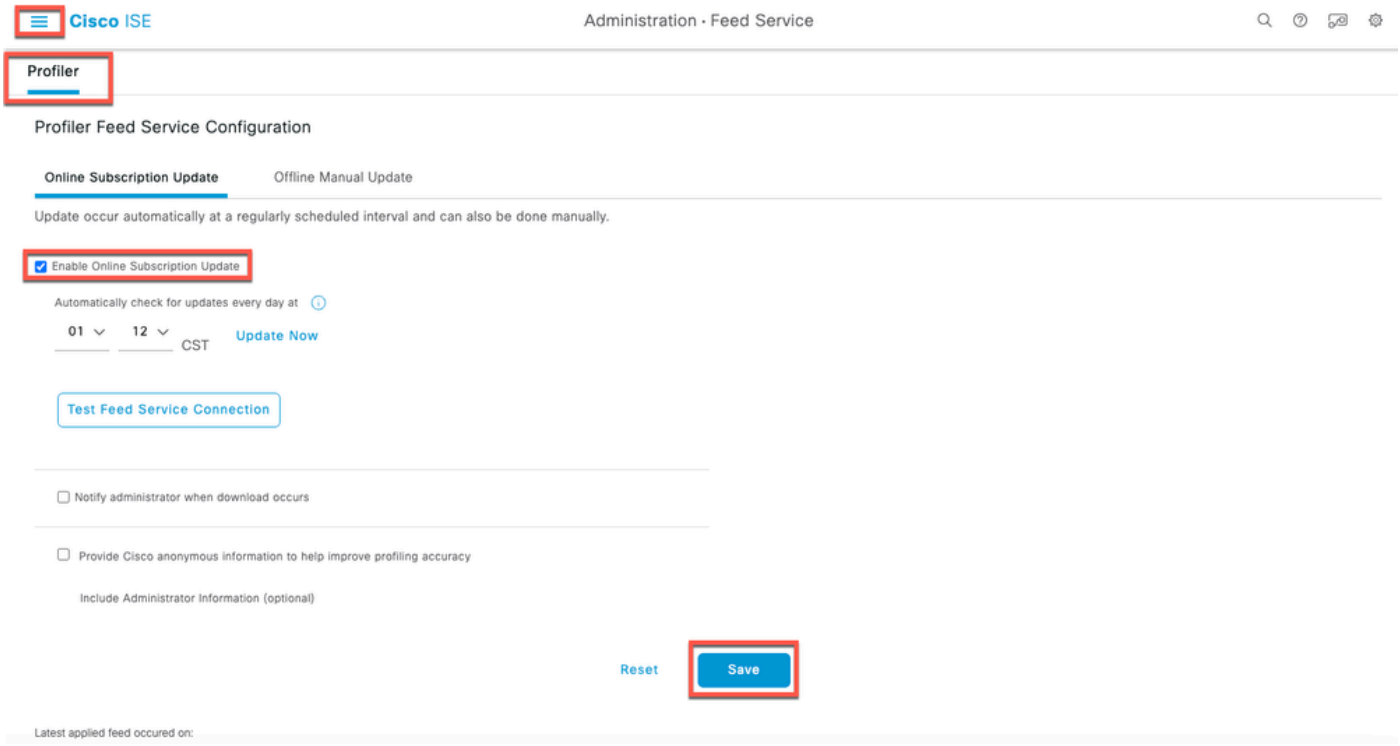
If you had manually configured the Originating Policy Services Node value under SNMP settings, this configuration is lost during upgrade. You must reconfigure the SNMP settings.

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:

- In the Cisco ISE GUI, click theMenuicon ( ) and choose**Administration > FeedService > Profiler**. Ensure that the profiler feed service is enabled.

Click **Update Now**.



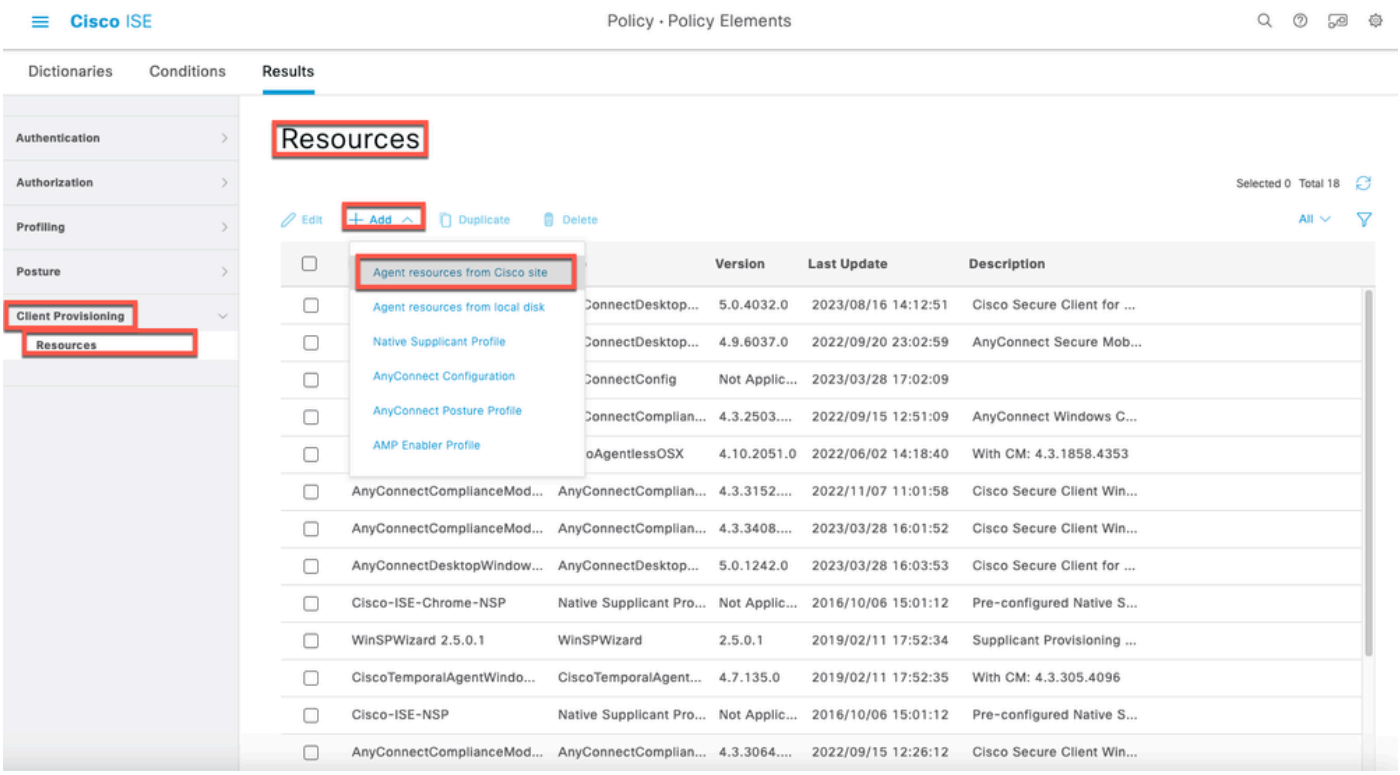
Profiler Update

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.

Online Updates

- In the Cisco ISE GUI, click the**Menu**icon ( ) and choose**Policy > Policy Elements > Results > Client Provisioning >** Resources to configure the client provisioning resources.
- Click **Add**.
- Choose **Agent Resources From Cisco Site**.
- In the **Download Remote Resources**window, select the Cisco Temporal Agent resource.
- Click **Save** and verify that the downloaded resource appears in the Resources page.



Online Update - Client Provisioning

Offline Updates

- In the Cisco ISE GUI, click the **Menu** icon ( ) and choose**Policy > Policy Elements > Results > Client Provisioning > Resources**to configure the client provisioning resources.
- Click **Add**.
- Choose **Agent Resources from Local Disk**.
- From the **Category** drop-down, choose **Cisco Provided Packages**.

Post Upgrade 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

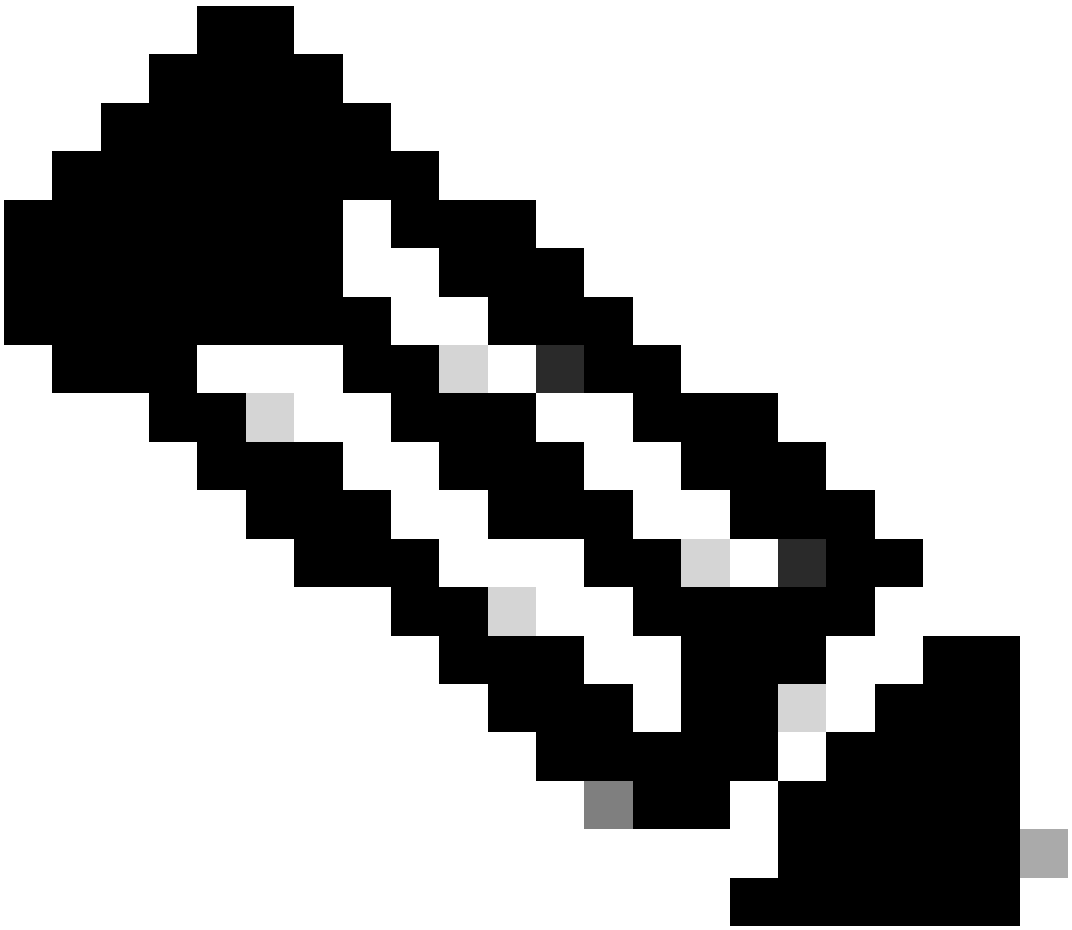
upgrade process overwrites the changes that you made.

Refresh Policies to Trustsec NADs

Run the commands, in the showing order, to download the policies on Cisco TrustSec-enabled Layer 3 interfaces in the system. If you faced any enforcement issues after a successful upgrade.

- **no cts role-based enforcement**
- **cts role-based enforcement**

Profiler Endpoint Ownership Synchronization/ Replication



Note: 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.

After the upgrade process, you could encounter the events

1. No data in live logs.

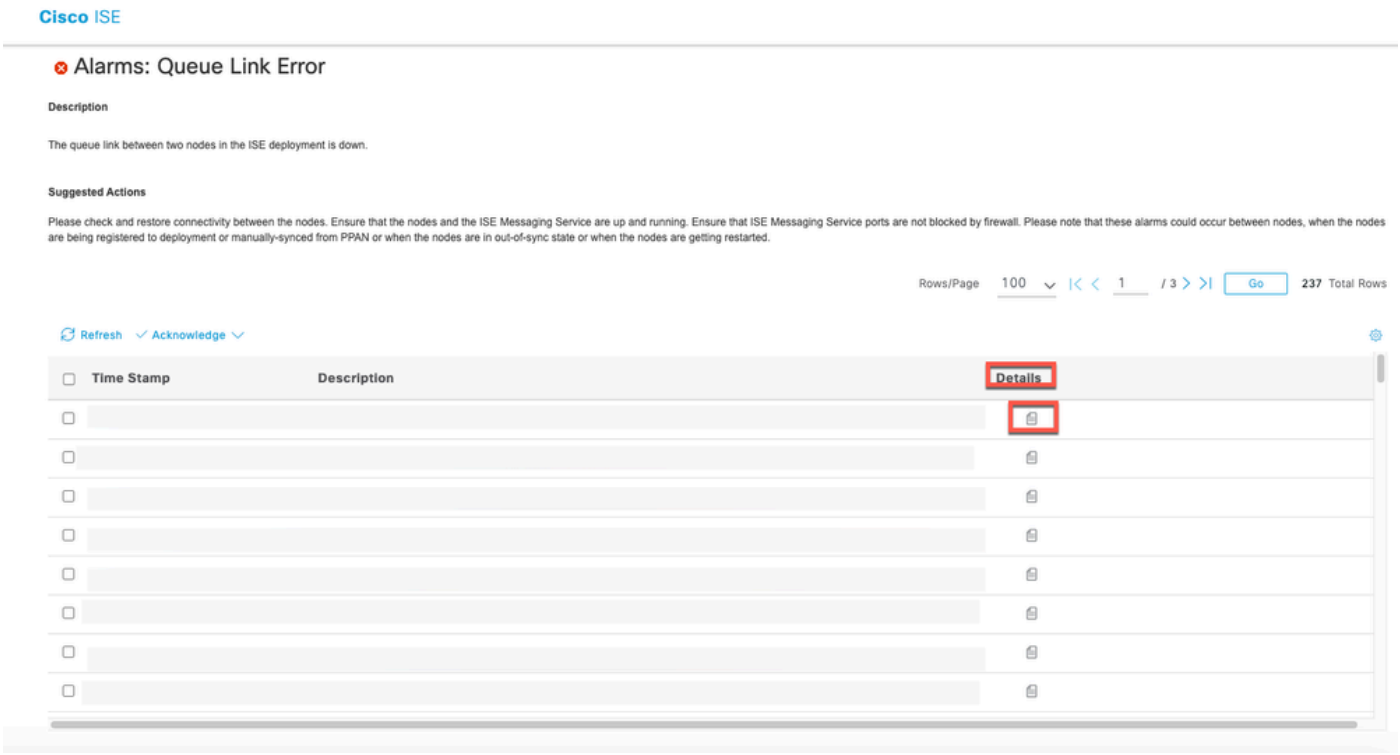
2. Queue link errors.

3. Health status is unavailable.

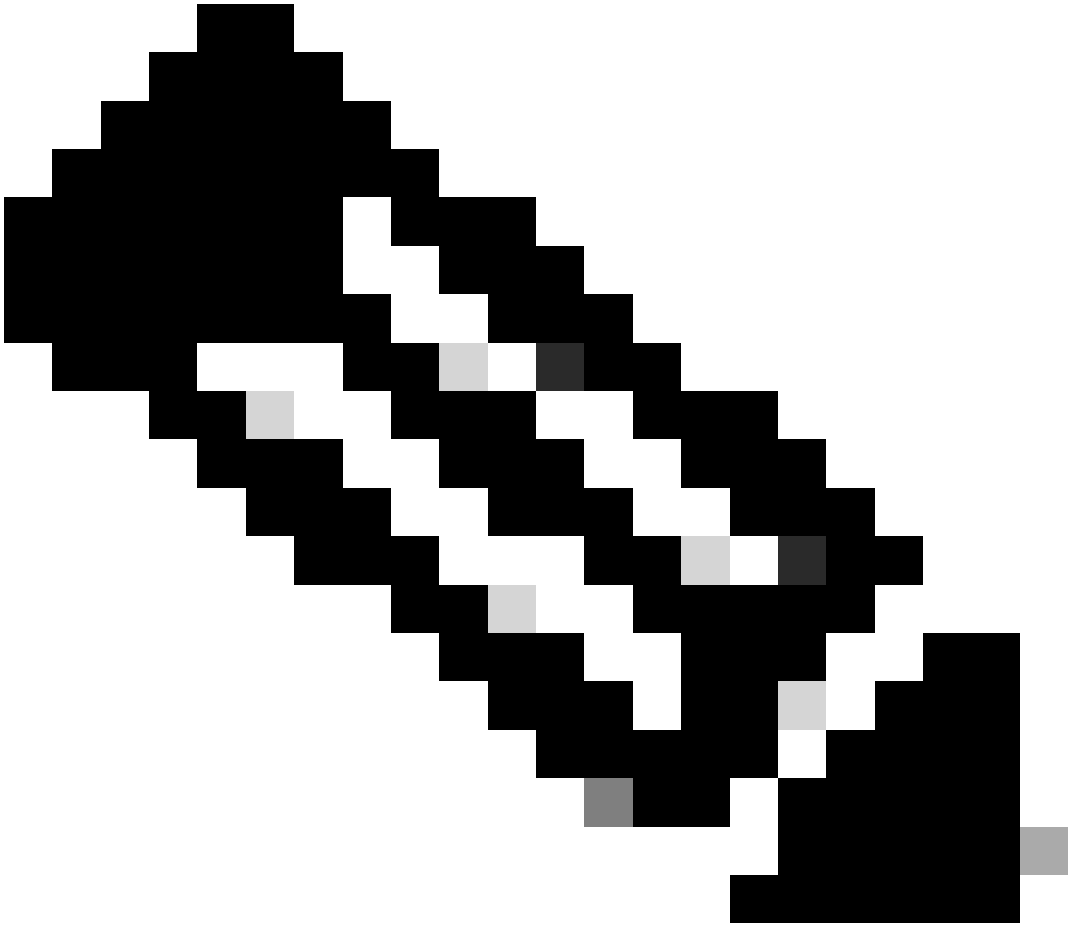
4. No date available in the system summary for some nodes.

Issues mentioned can be detected through ISE Dashbord. For the Queue Link Errors you would see an alarm under alarm section. The section for the System Summary would not show any data if there is and issue.

All Issues mentioned can be fixed by Regenerateing ISE internal Root CA. Specially for the Queue Link Errors in case the alarm comes for (Unknow_Ca). If you still counter the issue, Pleaes Open TAC Support Case for farther assistance.



Queue Link Alarm Example



Note: If you run into any issues after a Successful Upgrade. Please Open a TAC case using the Keyword for the new issue. Please do not use the Upgrade Keyword. Upgrade keyword must be used only when you face issues with the Actual Upgrade Process.

Authentication Issues after the upgrade

After a successul upgrade you could run into Authentication issue. Pleaes verify and Check:

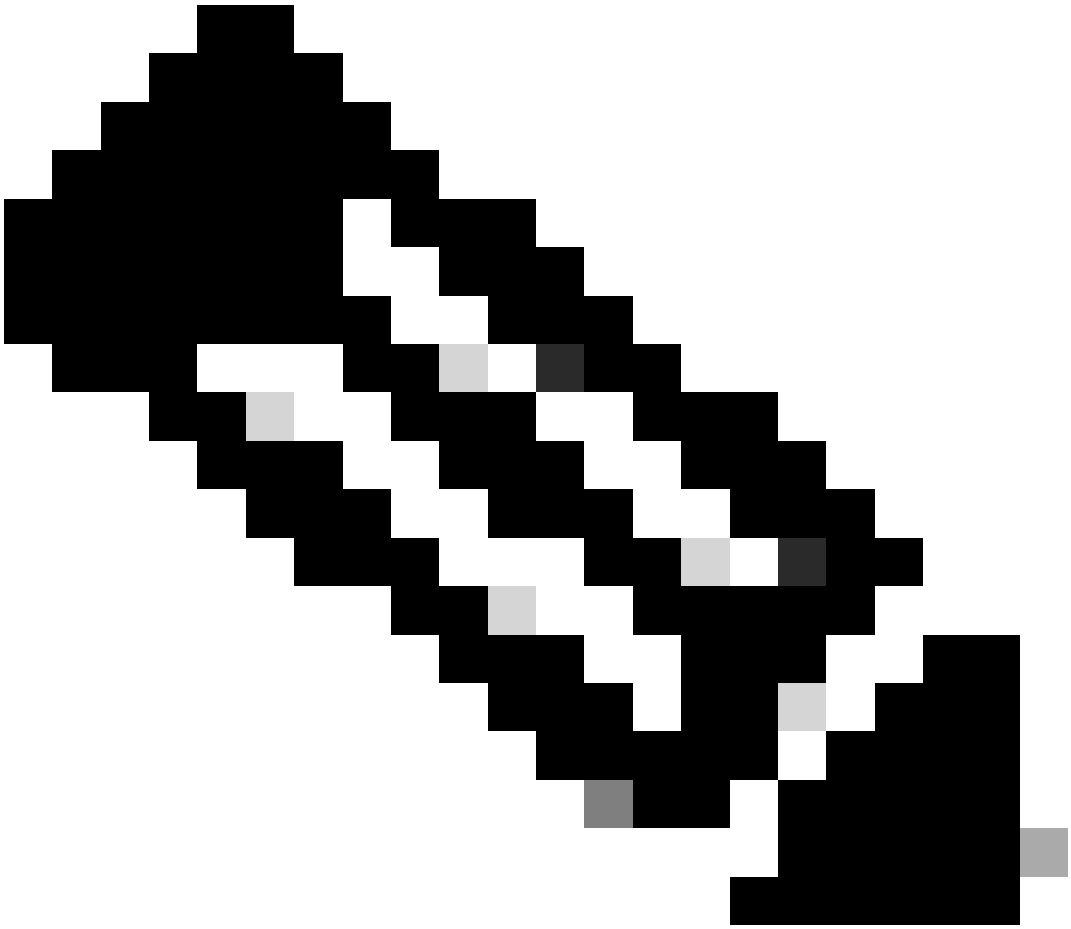
- Raduis Live Logs report Details. check the Failure Reason, Suggested Resolution and Root Cause. See Example:

Authentication Details

Source Timestamp	
Received Timestamp	
Policy Server	
Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile
Resolution	Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule-results.
Root cause	Selected Authorization Profile contains ACCESS_REJECT attribute
Username	
Endpoint Id	
Calling Station Id	
IPv4 Address	
Authentication Identity Store	
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Network Device	
Device Type	All Device Types#Fortigate Firewalls
Location	All Locations
NAS Port Type	Virtual
Authorization Profile	DenyAccess
Response Time	27 milliseconds

Radius Live Logs Report Example

- Authentication can fail after upgrade 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.
- If you still facing issues and you need to Open a TAC Case, Please make to Complete Tasks:



Note: Please use the Authentication Keyword when you open a case for the Authentication issue. Do not use the same case which is opened for the Upgrade.

---

1. Pick one machine that is experincing the issue for troubleshooting.

2. Note the time stamp for testing.

3. Note the MAC Address for the testing device.

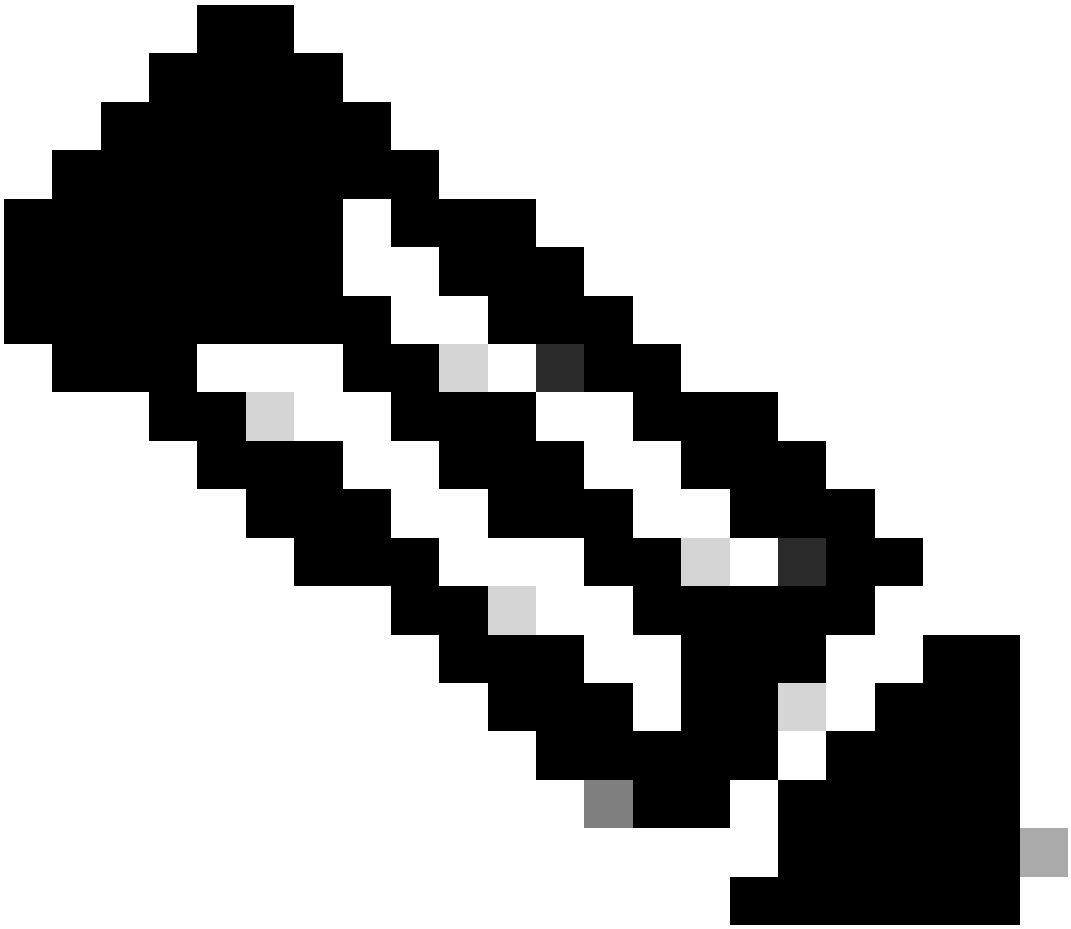
4. recreate the issue.

5. Collect Radius Live logs details. Make sure the time stamp matches.

6. if you are using AnyConnect, Collect DART Bundle from the end user mahcine.

7. Generate a Support Bundle from the PSN hundling the authentication requests.

8. Upload all information to your case.



Note: Various issues on ISE require different sets of logs to troubleshoot. A full list of needed debugs must be provided by the TAC engineer.

Related Information

- **Cisco Technical Support & Downloads**