# Install, Renew, and Troubleshoot SSL Digital Certificates on Cisco ISE

## Contents



## Introduction

This document describes SSL certificate installation, renewal, and solutions to the most common issues observed on an Identity Services Engine.

## Prerequisites

### Requirements

Cisco recommends that you know Identity Service Engine GUI.

### Components Used

The information in this document is based on Cisco Identity Service Engine 3.x.

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.

### Background Information

This document provides the recommended steps and checklist of common issues to be verified and addressed before you begin to troubleshoot and call Cisco Technical Support.

A certificate is an electronic document that identifies an individual, a server, a company, or another entity and associates that entity with a public key.

A self-signed certificate is signed by its own creator. Certificates can be self-signed or digitally signed by an external Certificate Authority (CA).

A CA-signed digital certificate is considered an industry standard and more secure.

Certificates are used in a network to provide secure access.

Cisco ISE uses certificates for inter-node communication, and for communicating with external servers such as the Syslog server, feed server, and all the end-user portals (guest, sponsor, and personal devices portals).

Certificates identify a Cisco ISE node to an endpoint and secure the communication between that endpoint and the Cisco ISE node.

Certificates are used for all HTTPS communication and the Extensible Authentication Protocol (EAP) communication.

This document provides the recommended steps and checklist of common issues to be verified and addressed before you begin to troubleshoot and call Cisco Technical Support.

These solutions come directly from service requests that the Cisco Technical Support has solved. If your network is live, make sure that you understand the potential impact of the steps you take to address the issues.

## Configure

The following guides explain how to import and replace certificates:

### Importing a system certificate

https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/workflow/html/b_basic_setup_2_7.html#ID547

### Replacing an expired certificate

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/116977-technote-ise-cert-00.html#anc5

# Common Issues

## Scenario 1: Unable to replace an expiring Portal Certificate on an ISE node

### Error

While binding the new Portal Certificate with the CSR, the certificate bind process fails with the error shown below:

***Internal error. Ask your ISE administrator to check the logs for more details***

The most common reasons for this error are:

- The new certificate has the same subject name as the existing certificate

- Import a renewed certificate which is using the same private key of an existing certificate

### Solution

1. Temporarily assign the portal usage to another certificate on the same node
2. Delete the expiring Portal Certificate
3. Install the new Portal Certificate and then assign the portal usage

For example, if you wish to temporarily assign the portal usage to an existing certificate with EAP Authentication usage, follow the below steps:

**Step 1**. Select and Edit the certificate with EAP Authentication usage, add Portal role under Usage and Save

**Step 2.** Delete the expiring portal certificate

**Step 3.** Upload the new Portal Certificate without selecting any role (under Usage) and Submit

**Step 4.** Select and Edit the new Portal Certificate, assign Portal role under Usage and Save

## Scenario 2: Cannot generate two CSRs for the same ISE node with Multi-Use usage

### Error

New CSR creation for the same node with Multi-Use usage fails with the error:
***Another certificate with the same friendly name already exists. Friendly names must be unique.***

### Solution

CSR Friendly Names are hardcoded for each ISE node so it does not allow creating 2 CSRs for the same node with Multi-Use usage. The use case is on a specific node, there is one CA-signed certificate that is used for Admin and EAP authentication usage and another CA-signed certificate that is used for SAML and Portal usage and both certificates are going to expire.

In this scenario:

**Step 1.** Generate first CSR with Multi-Use usage

**Step 2.** Bind the CA-signed certificate with the first CSR and assign the Admin and EAP authentication role

**Step 3.** Generate a second CSR with Multi-Use usage

**Step 4.** Bind the CA-signed certificate with the second CSR and assign SAML and Portal role

## Scenario 3: Not able to bind the CA-signed certificate for portal usage or not being able to assign the portal tag to the certificate and getting an error

### Error

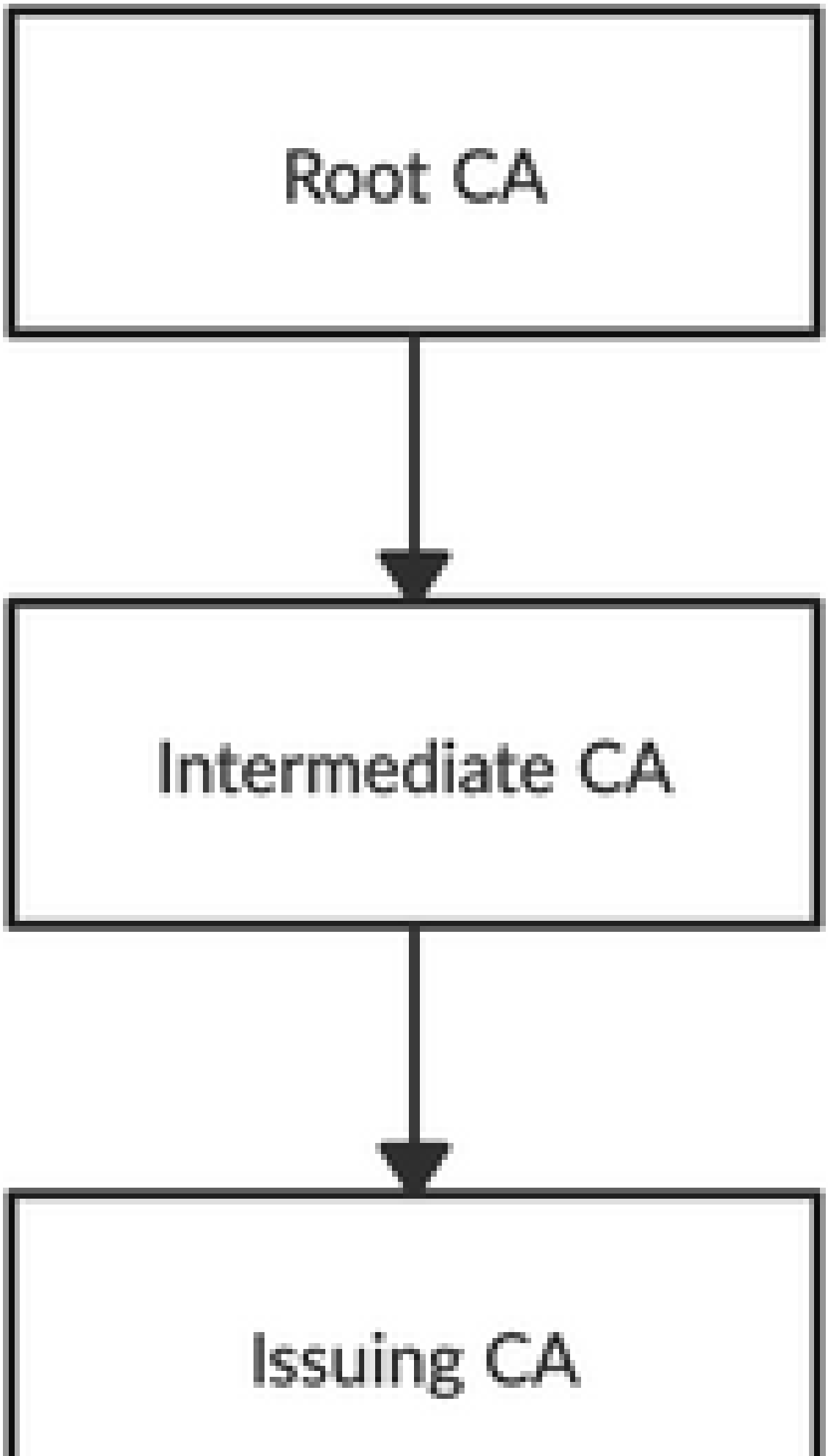
Binding a CA-signed certificate for portal usage throws the error:

There is one or more trusted certificate(s) which is part of the portal system certificate chain or selected with cert-based admin auth role with the same subject name but having a different serial number. Import/Update was aborted. For successful import/update, you need to either disable the cart-based admin auth role from a duplicate trusted certificate or change the portal role from the system certificate which contains the duplicate trusted certificate in its chain.

### Solution

Step 1. Check the certificate chain of the CA-signed certificate (for portal usage) and in the Trusted Certificates store, verify if you have any duplicate certificates from the certificate chain.
Step 2. Remove the duplicate certificate or uncheck the checkbox **Trust for certificate-based admin authentication** from the duplicate certificate.

For example, the CA-signed portal certificate has the below certificate chain:


Root CA
Intermediate CA
Issuing CA

***Disable or Delete or Trust Certificate is not allowed since it is being referenced by either in System Certificates AND/OR Secure Syslog Target under Remote Logging Targets.***

**Solution**

1. Verify that the expired default self-signed certificate is not associated with any existing Remote Logging Target. This can be verified under ***Administration > System > Logging > Remote Logging Targets > Select and Edit SecureSyslogCollector(s)***
2. Verify that the expired default self-signed certificate is not associated with any specific role (usage). this can be verified under ***Administration > System > Certificates > System Certificates***.

If the issue still persists, contact TAC.

## Scenario 5: Unable to bind CA signed pxGrid Certificate with the CSR on an ISE node

**Error**

While binding the new pxGrid Certificate with the CSR, the certificate bind process fails with the error:

***Certificate for pxGrid must contain both client and server authentication in the Extended Key Usage (EKU) extension.***

**Solution**

Ensure that the CA-signed pxGrid certificate must have both TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) and TLS Web Client Authentication (1.3.6.1.5.5.7.3.2) extended key usage because it is used for both client and server authentication (to secure communication between the pxGrid client and server)

Reference link: https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_011010.html

## Scenario 6: Unable to delete the expired default self-signed certificate from the Trusted Certificate Store due to existing LDAP or SCEP RA Profile configuration

**Error**

Deleting the expired default self-signed certificate from the Trusted Certificate store results in the error:

Trust Certificate could not be deleted because it's being referenced elsewhere, possibly from a SCEP RA Profile or an LDAP Identity Source

* Default self-signed server certificate

In order to delete the certificate(s), delete SCEP RA Profile or edit the LDAP Identity source to not use this Certificate.

**Solution**

1. Navigate to ***Administration > Identity Management > External Identity Sources > LDAP > Server Name > Connection***
2. Make sure LDAP Server Root CA is not using the "Default self-signed server certificate"
3. If LDAP server is not using the required certificate for a secure connection, navigate to ***Administration > System > Certificates > Certificate Authority > External CA Settings > SCEP RA Profiles***
4. Make sure any of the SCEP RA Profiles are not using default self-signed certificate

# Additional Resources

**How to Install a Wildcard Certificate**
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

**Manage ISE Certificates**
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

**Install a third-party CA Certificate on ISE**
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/200295-Install-a-3rd-party-CA-certificate-in-IS.html