

Import and Export Certificates in ISE

Contents

[Introduction](#)

[Background Information](#)

[Export the Certificate in ISE](#)

[Import the Certificate in ISE](#)

Introduction

This document describes how to import and export the certificates in Cisco Identity Service Engine (ISE).

Background Information

ISE uses certificates for various purposes (Web UI, Web Portals, EAP, pxgrid). Certificates present on ISE can have one of these roles:

- Admin: For internode communication and authentication of the Admin portal.
- EAP: For EAP authentication.
- RADIUS DTLS: For RADIUS DTLS server authentication.
- Portal: In order to communicate among all Cisco ISE end-user portals.
- PxGrid: In order to communicate between the pxGrid controller.

Create a backup of certificates installed on ISE nodes. This saves the backup of configuration data, and certificate of the admin node is taken. However, for other nodes, the backup of certificates is taken individually.

Export the Certificate in ISE

Navigate to **Administration > System > Certificates > Certificate Management > System certificate**. Expand the **node**, select the **certificate**, and click **Export**, as shown in the image:

As shown in this image, select the **Export Certificate and Private Key**. Enter a minimum 8 character in length alpha-numeric password. This password is required to restore the certificate.

Export Certificate 'Default self-signed server certificate'

Export Certificate Only
 Export Certificate and Private Key

*Private Key Password

*Confirm Password

Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

Export Cancel

 **Tip:** Do not forget the password.

Import the Certificate in ISE

There are two steps involved to import the certificate on ISE.

Step 1. Determine if the certificate is self-signed or third party signed certificate.

- If the certificate is self-signed, import the public key of the certificate under trusted certificates.
- If the certificate is signed by some third-party certificate authority, import Root and all other intermediate certificates of the certificate.

Navigate to **Administration > System > Certificates > Certificate Management > Trusted Certificate**, click **Import**.

Identity Services Engine Home Context Visibility Operations Policy **Administration** Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services

Deployment Licensing **Certificates** Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

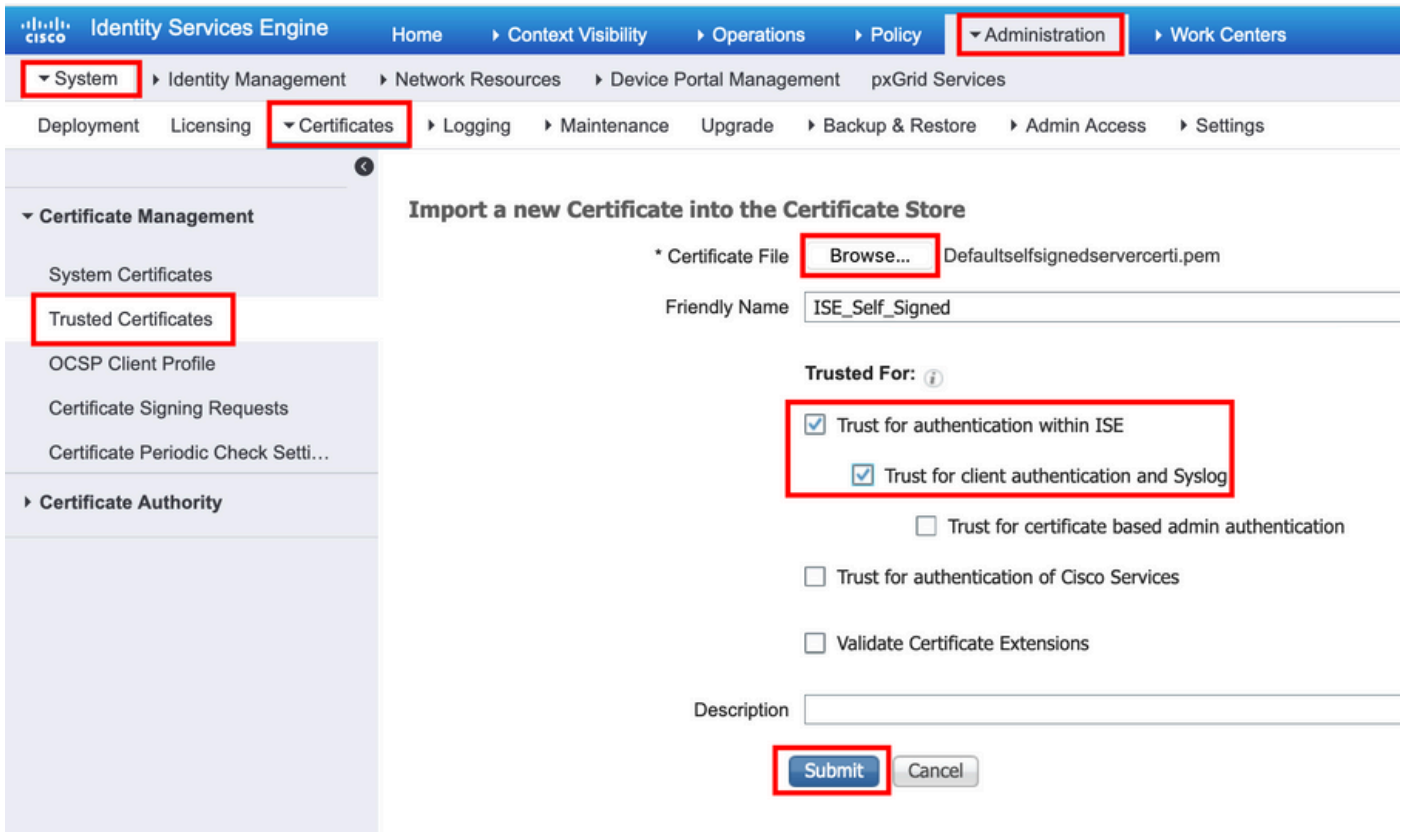
- System Certificates
- Trusted Certificates**
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Setti...

Certificate Authority

Trusted Certificates

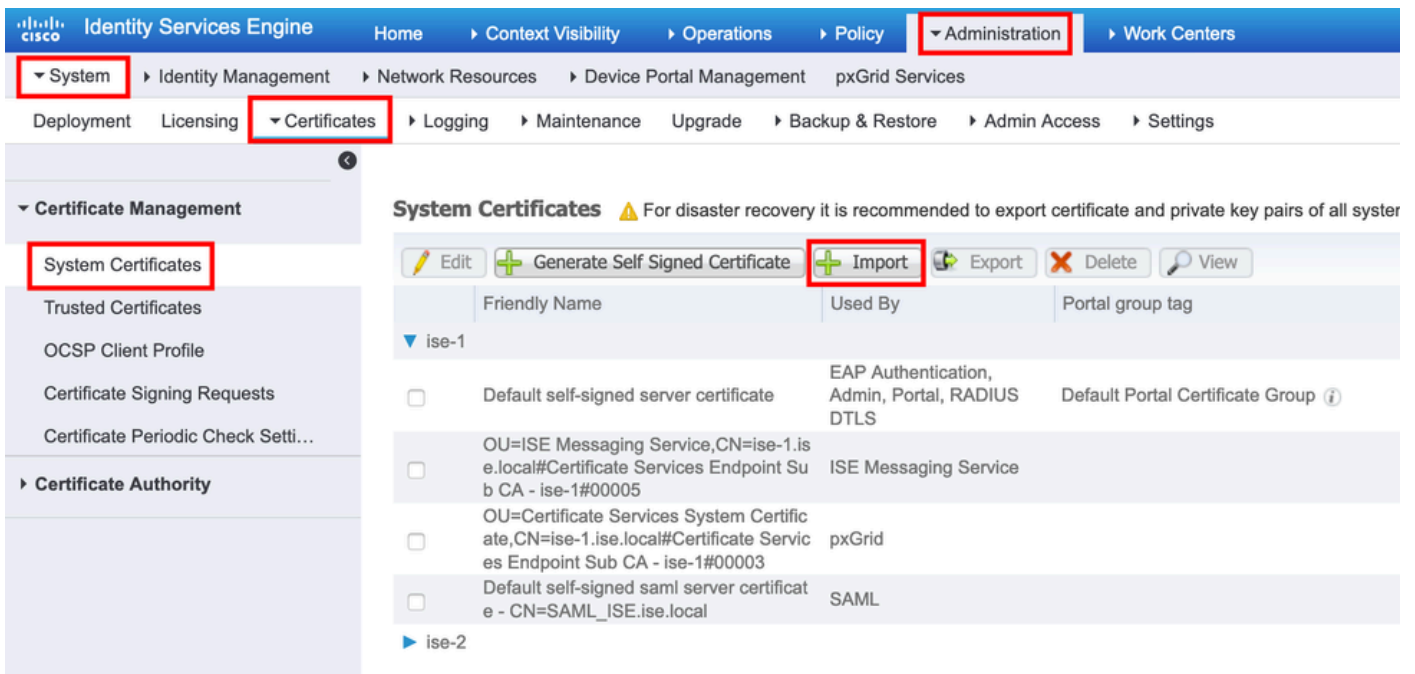
Edit **Import** Export Delete View

<input type="checkbox"/>	Friendly Name	Status	Trusted For	Se
<input type="checkbox"/>	Baltimore CyberTrust Root	Enabled	Cisco Services	02
<input type="checkbox"/>	Cisco ECC Root CA 2099	Enabled	Cisco Services	03
<input type="checkbox"/>	Cisco Licensing Root CA	Enabled	Cisco Services	01
<input type="checkbox"/>	Cisco Manufacturing CA SHA2	Enabled	Infrastructure Endpoints	02
<input type="checkbox"/>	Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F
<input type="checkbox"/>	Cisco Root CA 2099	Enabled	Cisco Services	01
<input type="checkbox"/>	Cisco Root CA M1	Enabled	Cisco Services	2F



Step 2. Import the actual certificate.

1. Navigate to **Administration > System > Certificates > Certificate Management**, click **Import**. If the admin role is assigned to the certificate, the service on the node restarts.



2. Select the node for which you want to import the certificate.

3. Browse the public and private keys.

4. Enter the password for the private key of the certificate and select the desired role.

5. Click **Submit**.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar shows 'System Certificates' under 'Certificate Management'. The main content area is titled 'Import Server Certificate' and contains the following fields and options:

- * Select Node: ise-1
- * Certificate File: Browse... (Defaultselfsignedservercert.pem)
- * Private Key File: Browse... (Defaultselfsignedservercert.pvk)
- Password: [Redacted]
- Friendly Name: ISE_Self_Signed
- Allow Wildcard Certificates:
- Validate Certificate Extensions:
- Usage section with the following roles:
 - Admin: Use certificate to authenticate the ISE Admin Portal
 - EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
 - RADIUS DTLS: Use certificate for the RADSec server
 - pxGrid: Use certificate for the pxGrid Controller
 - SAML: Use certificate for SAML Signing
 - Portal: Use for portal

A red box highlights the 'Submit' button at the bottom of the form.

Select Required Role