Import and Export Certificates in ISE

Contents

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). Certificate present on ISE can have one of these roles:

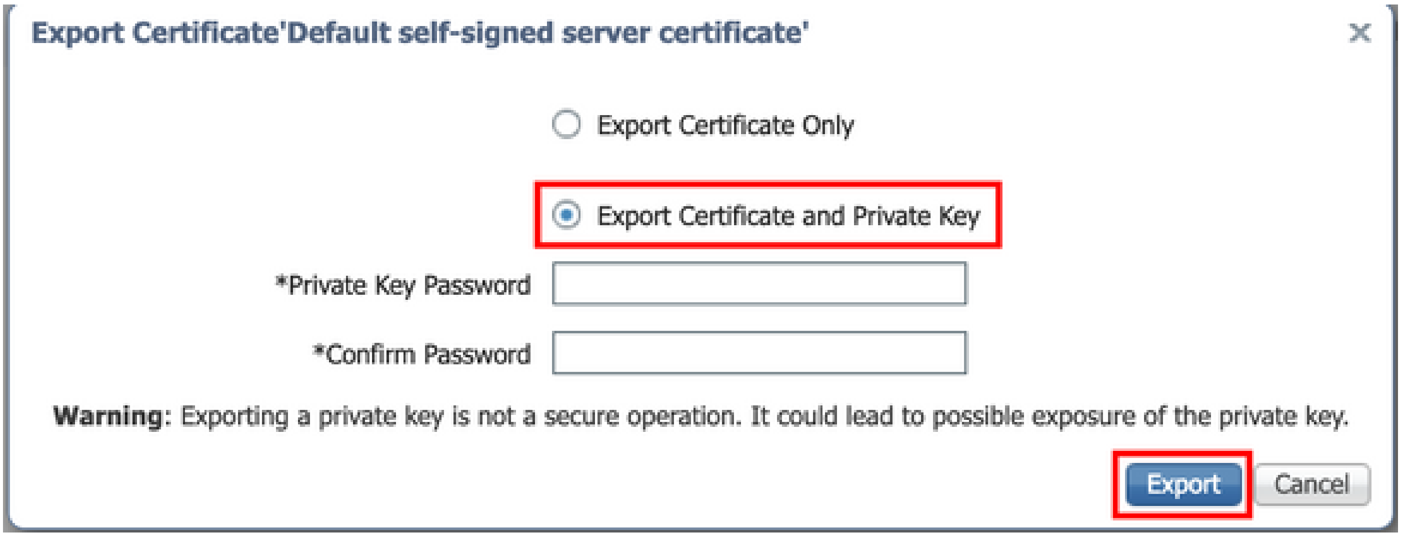
- Admin: For internode communication and authentication of the Admin portal.
- EAP: For EAP authentication.
- RADIUS DTLS: For RADIUS DTLS server authentication.
- Portal: In order to communicate among all Cisco ISE end-user portals.
- PxGrid: In order to communicate between the pxGrid controller.

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.

Tip: Do not forget the password.

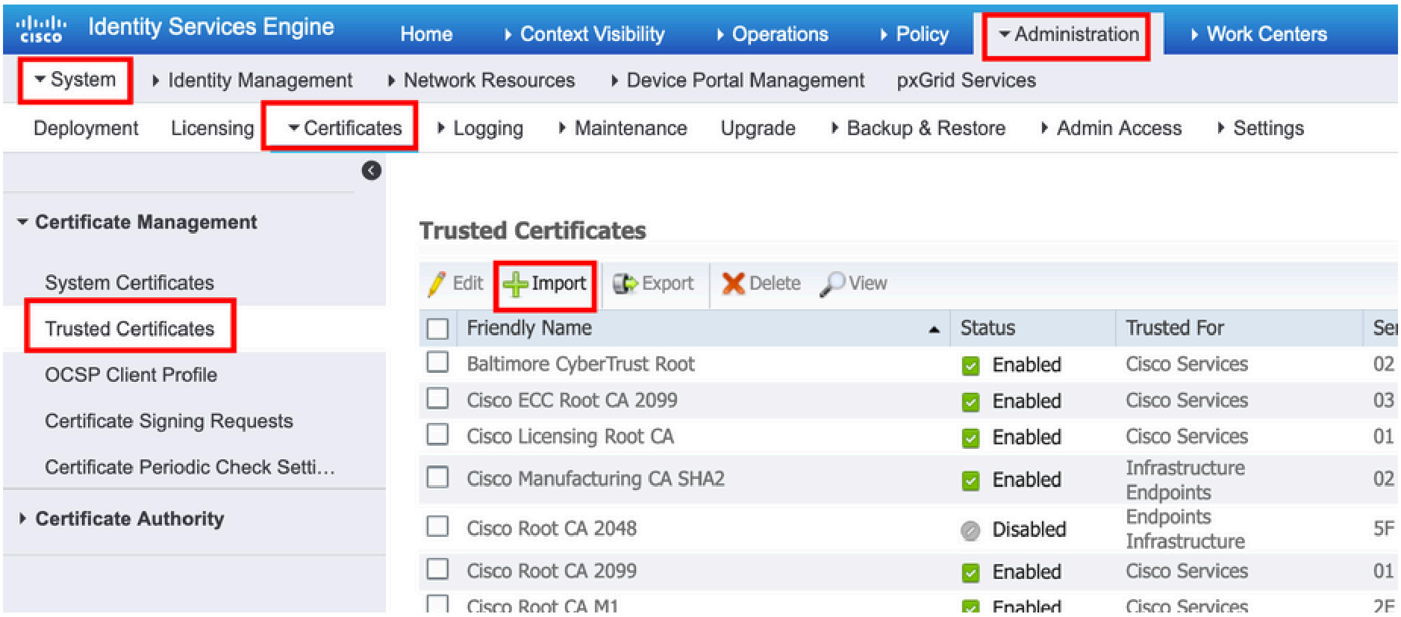
Import the Certificate in ISE

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.

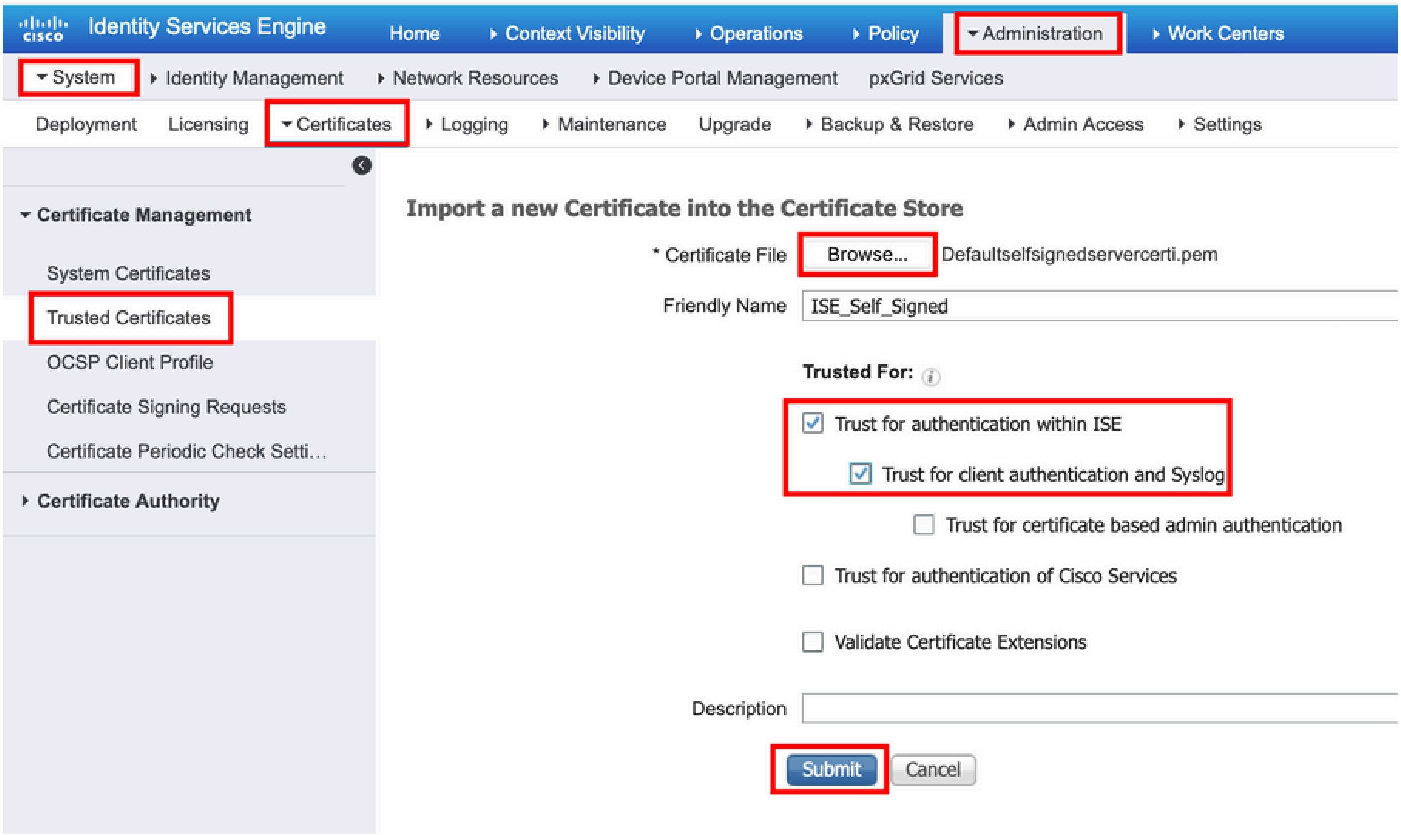
- If the certificate is self-signed, import the public key of the certificate under trusted certificates.
- If the certificate is signed by some third-party certificate authority, Import Root and all other intermediate certificates of the certificate.

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



Trusted Certificates

□	Friendly Name	Status	Trusted For	Ser
□	Baltimore CyberTrust Root	✓ Enabled	Cisco Services	02
□	Cisco ECC Root CA 2099	✓ Enabled	Cisco Services	03
□	Cisco Licensing Root CA	✓ Enabled	Cisco Services	01
□	Cisco Manufacturing CA SHA2	✓ Enabled	Infrastructure Endpoints	02
□	Cisco Root CA 2048	⊘ Disabled	Endpoints Infrastructure	5F
□	Cisco Root CA 2099	✓ Enabled	Cisco Services	01
□	Cisco Root CA M1	✓ Enabled	Cisco Services	2E



Import a new Certificate into the Certificate Store

* Certificate File: Defaultselfsignedservercerti.pem

Friendly Name: ISE_Self_Signed

Trusted For:

☑ Trust for authentication within ISE

☑ Trust for client authentication and Syslog

☐ Trust for certificate based admin authentication

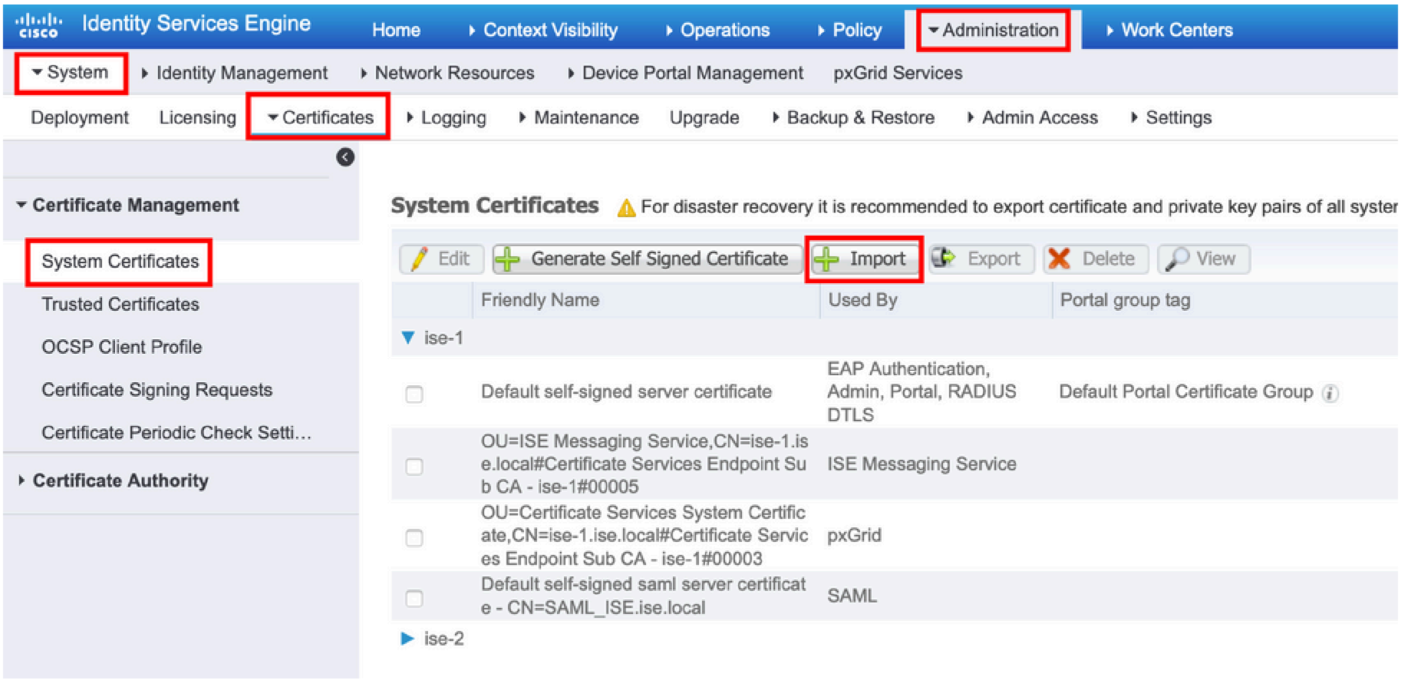
☐ Trust for authentication of Cisco Services

☐ Validate Certificate Extensions

Description:

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.



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all syster

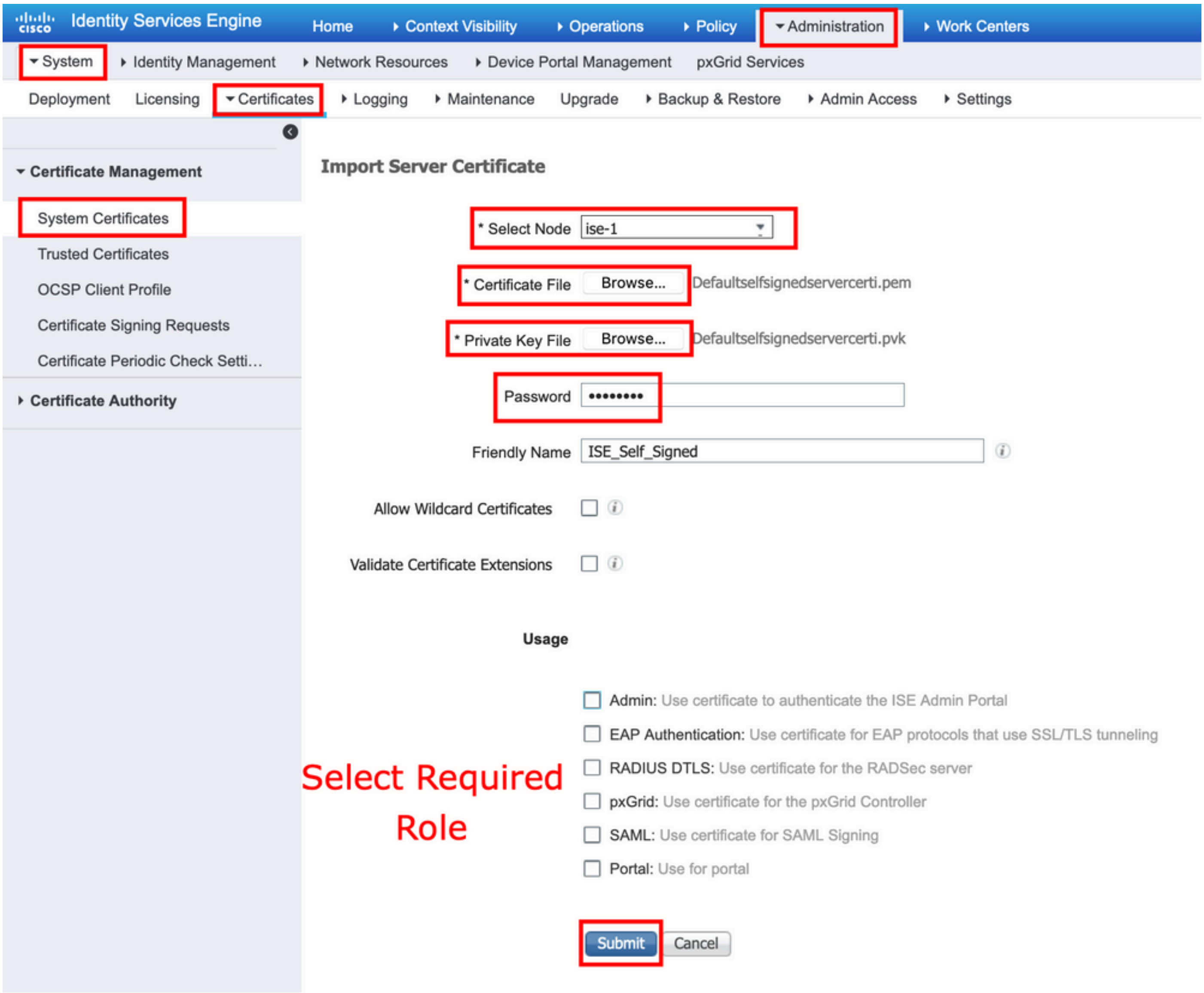
	Friendly Name	Used By	Portal group tag
▼ ise-1			
☐	Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group
☐	OU=ISE Messaging Service,CN=ise-1.ise.local#Certificate Services Endpoint Sub CA - ise-1#00005	ISE Messaging Service	
☐	OU=Certificate Services System Certificate,CN=ise-1.ise.local#Certificate Services Endpoint Sub CA - ise-1#00003	pxGrid	
☐	Default self-signed saml server certificate - CN=SAML_ISE.ise.local	SAML	
▶ ise-2			

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**.



Import Server Certificate

* Select Node: ise-1

* Certificate File: Browse... Defaultselfsignedservercerti.pem

* Private Key File: Browse... Defaultselfsignedservercerti.pvk

Password: ••••••••

Friendly Name: ISE_Self_Signed

Allow Wildcard Certificates □

Validate Certificate Extensions □

Usage

- □ 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

Select Required Role

Submit   Cancel