Importar y exportar certificados en ISE

Contenido

Introducción

Este documento describe cómo importar y exportar los certificados en Cisco Identity Service Engine (ISE).

Antecedentes

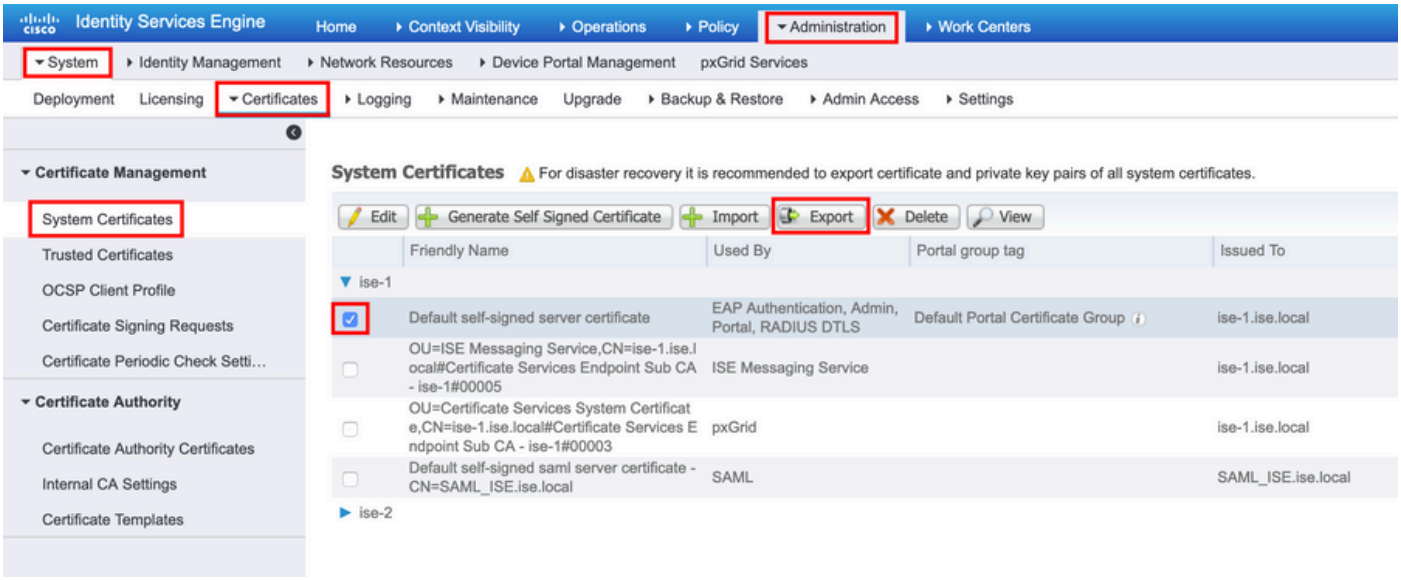
ISE utiliza certificados para diversos fines (interfaz de usuario web, portales web, EAP, pxgrid). El certificado presente en ISE puede tener una de estas funciones:

- Admin: para la comunicación entre nodos y la autenticación del portal de administración.
- EAP: para autenticación EAP.
- RADIUS DTLS: para la autenticación del servidor RADIUS DTLS.
- Portal: para establecer comunicación entre todos los portales de usuarios finales de Cisco ISE.
- PxGrid: Para establecer comunicación entre el controlador pxGrid.

Es importante realizar una copia de seguridad de los certificados instalados en los nodos ISE. Al realizar la copia de seguridad de la configuración, se realiza la copia de seguridad de los datos de configuración y el certificado del nodo de administración. Sin embargo, para otros nodos, la copia de seguridad de los certificados se realiza de forma individual.

Exportar el certificado en ISE

Vaya a **Administración > Sistema > Certificados > Administración de certificados > Certificado del sistema. Expanda el nodo, seleccione el certificado y haga clic en Exportar**, como se muestra en la imagen:



Como se muestra en esta imagen, seleccione **Export Certificate and Private Key (Exportar certificado y clave privada).** Introduzca una contraseña alfanumérica de al menos 8 caracteres. Esta contraseña es necesaria para restaurar el certificado.

Sugerencia: no olvide la contraseña.

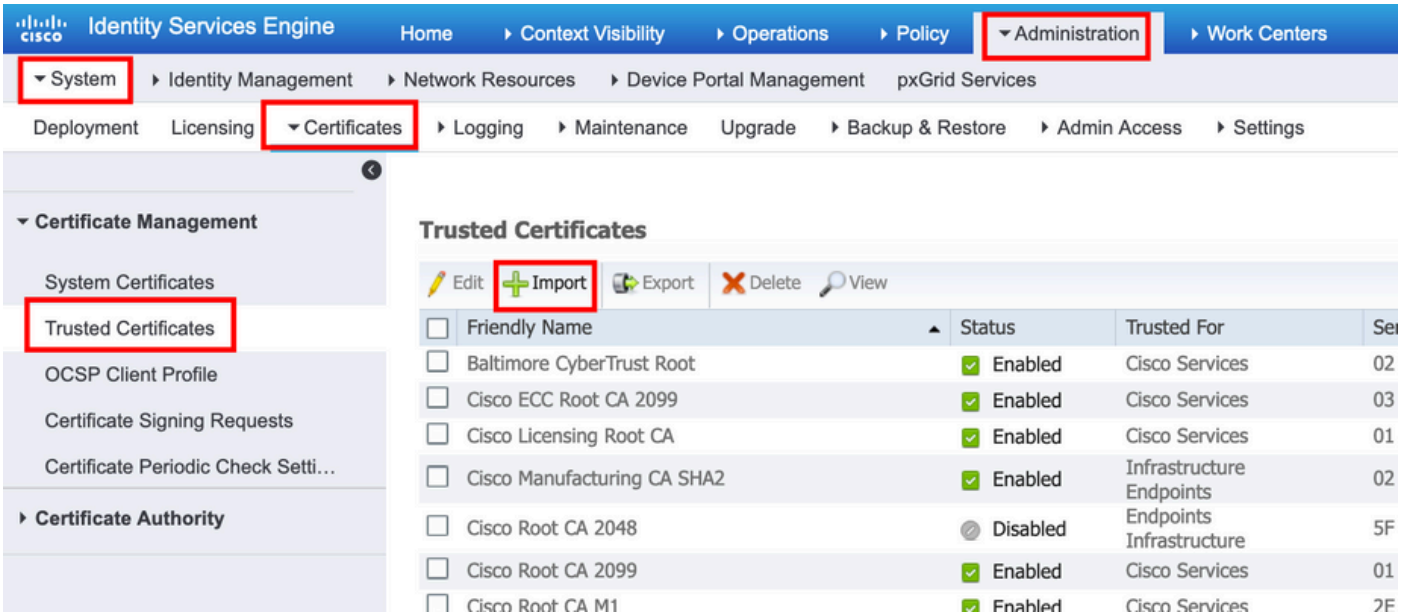
Importar el certificado en ISE

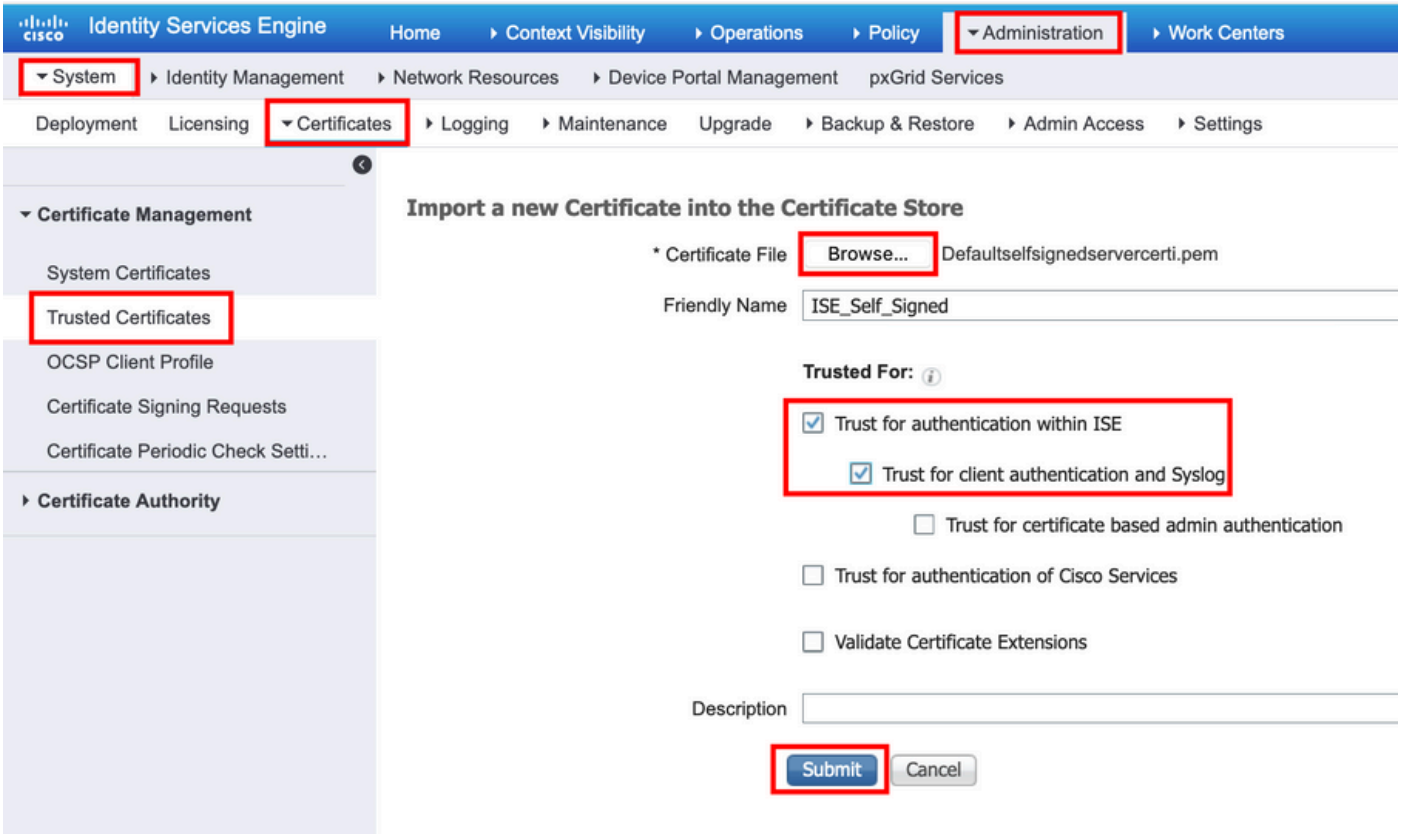
Hay dos pasos necesarios para importar el certificado en ISE.

Paso 1. Averigüe si el certificado está firmado por usted mismo o por un tercero.

- Si el certificado está autofirmado, importe la clave pública del certificado en certificados de confianza.
- Si el certificado está firmado por alguna autoridad de certificación de terceros, Importar raíz y todos los demás certificados intermedios del certificado.

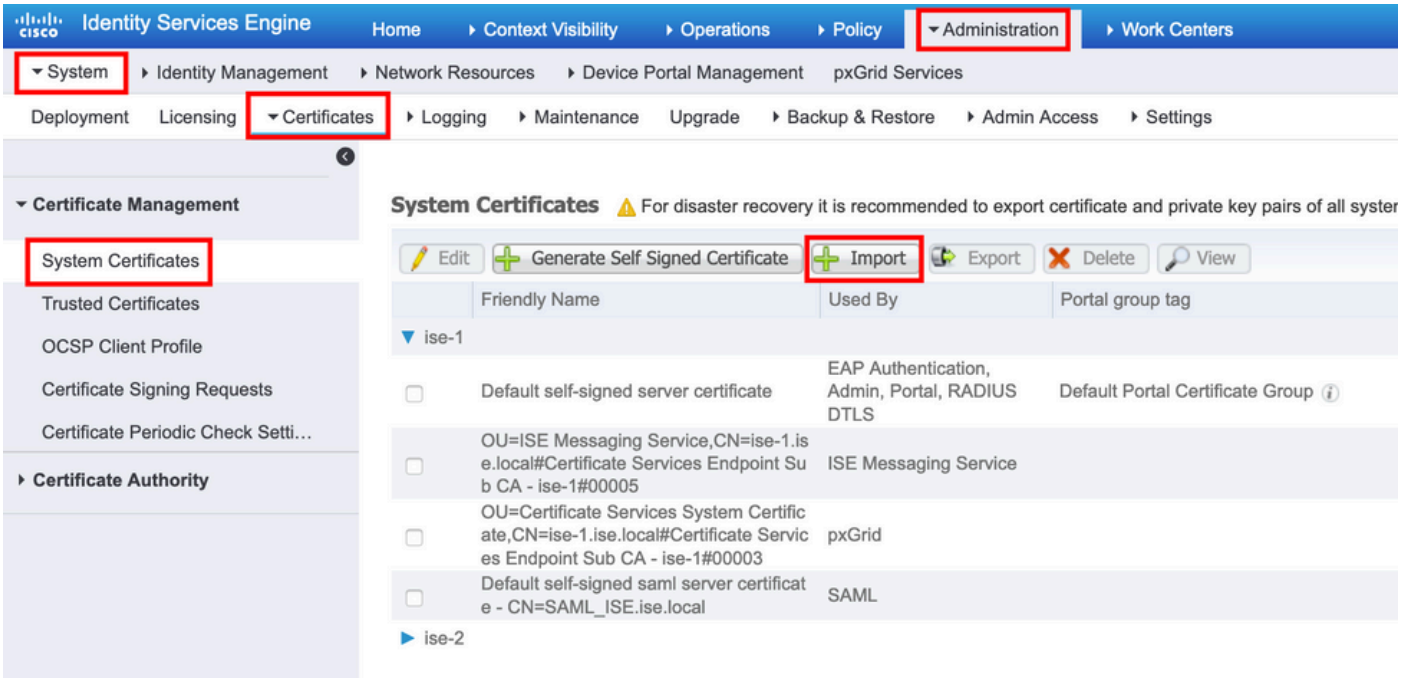
Vaya a **Administration > System > Certificates > Certificate Management > Trusted Certificate**, haga clic en **Import**, como se muestra en esta imagen.





Paso 2. Importe el certificado real.

1. Como se muestra en esta imagen, navegue hasta **Administración > Sistema > Certificados > Administración de certificados,** haga clic en **Importar**. Si el rol de administrador está asignado al certificado, se reiniciará el servicio en el nodo.

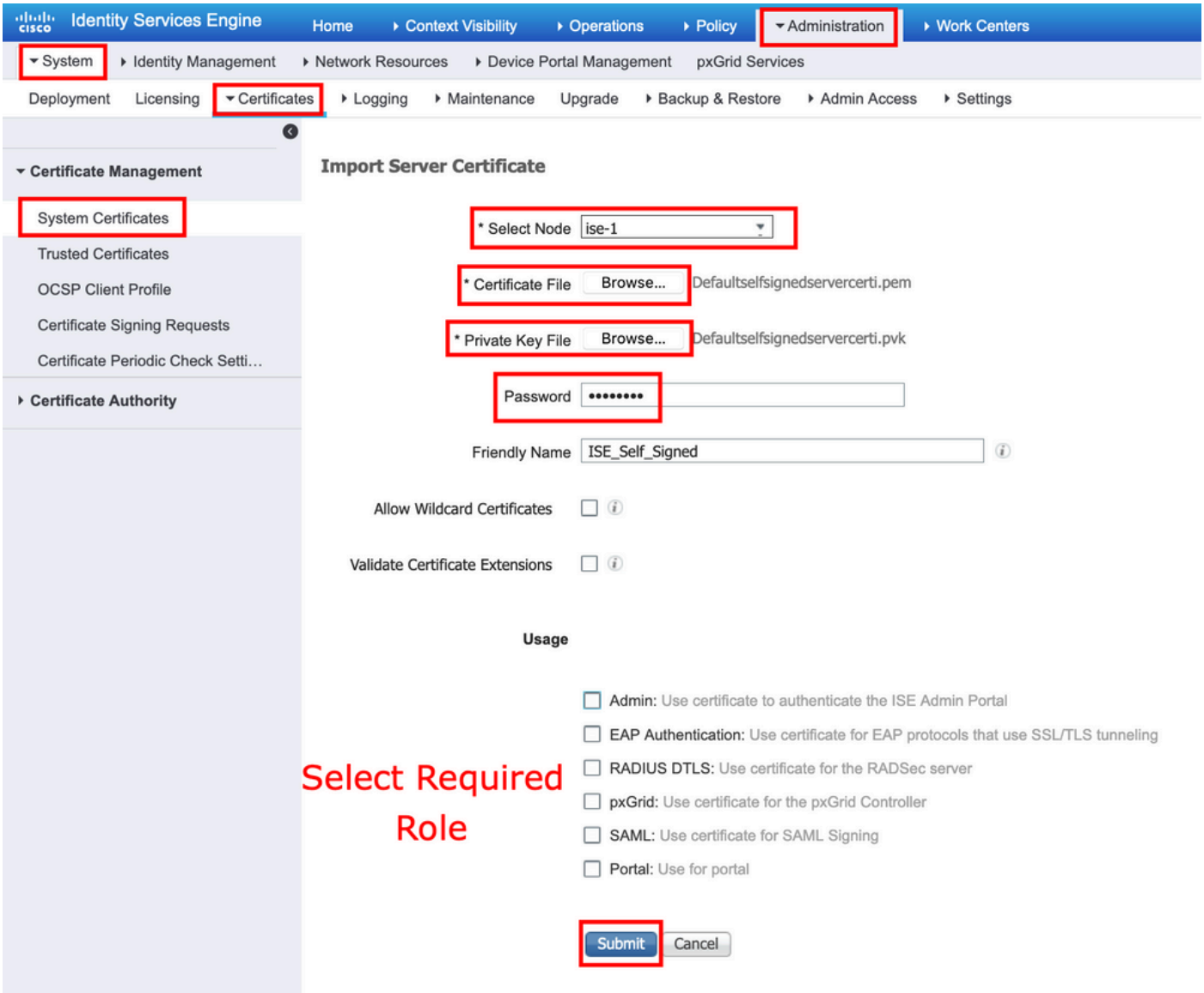


2. Seleccione el nodo para el que desea importar el certificado.

3. Examine las claves pública y privada.

4. Introduzca la contraseña de la clave privada del certificado y seleccione el rol deseado.

5. Ahora haga clic en **Enviar**, como se muestra en esta imagen.


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
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
Select Required Role
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
Submit
Cancel

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).