

# Importar y exportar certificados en ISE

## Contenido

[Introducción](#)

[Antecedentes](#)

[Exportar el certificado en ISE](#)

[Importar el certificado en ISE](#)

## Introducción

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

## Antecedentes

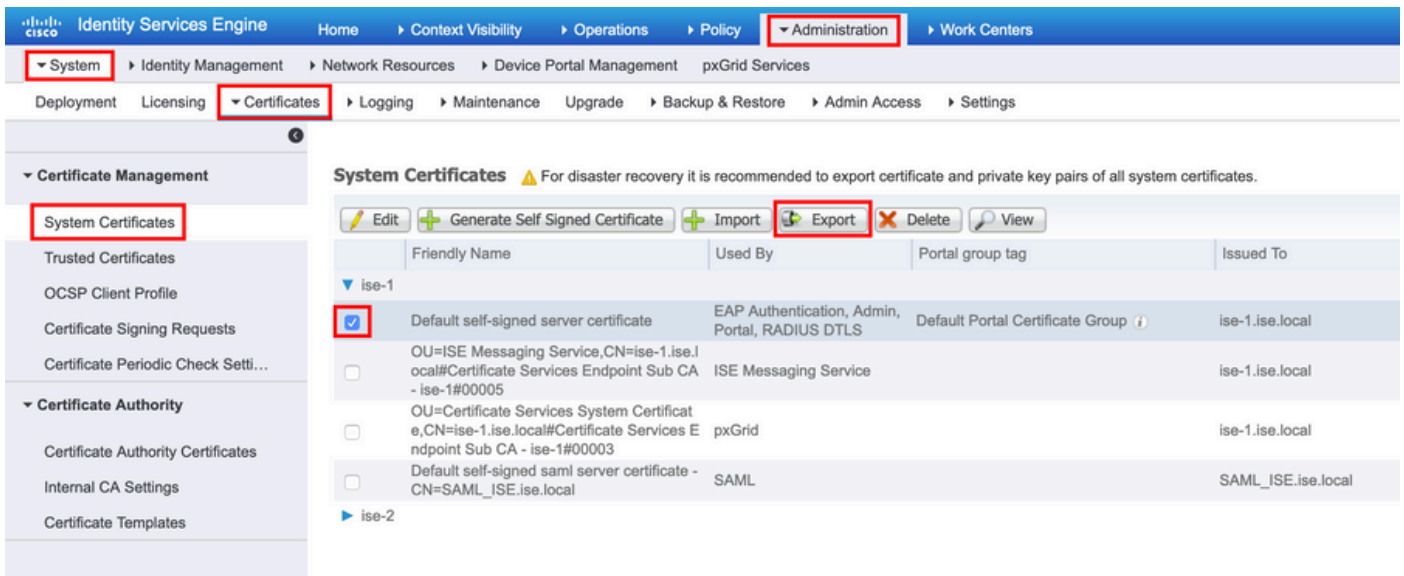
ISE utiliza certificados para diversos fines (interfaz de usuario web, portales web, EAP, pxgrid). El certificado presente en ISE puede tener una de estas funciones:

- 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.

**Trusted Certificates**

<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

**Import a new Certificate into the Certificate Store**

\* Certificate File  Defaultselfsignedservercert.pem

Friendly Name

**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

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.

The screenshot shows the Cisco Identity Services Engine Administration interface. The navigation menu includes 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', and 'pxGrid Services'. Under 'System', 'Certificates' is selected. The left sidebar shows 'Certificate Management' with 'System Certificates' highlighted. The main content area is titled 'System Certificates' and includes a warning: 'For disaster recovery it is recommended to export certificate and private key pairs of all system certificates'. Below this are buttons for 'Edit', 'Generate Self Signed Certificate', 'Import', 'Export', 'Delete', and 'View'. The 'Import' button is highlighted with a red box. A table lists certificates with columns for 'Friendly Name', 'Used By', and 'Portal group tag'. The table contains three entries under the 'ise-1' group:

	Friendly Name	Used By	Portal group tag
<input type="checkbox"/>	Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group ⓘ
<input type="checkbox"/>	OU=ISE Messaging Service,CN=ise-1.ise.local#Certificate Services Endpoint Sub CA - ise-1#00005	ISE Messaging Service	
<input type="checkbox"/>	OU=Certificate Services System Certificate,CN=ise-1.ise.local#Certificate Services Endpoint Sub CA - ise-1#00003	pxGrid	

Below the table, there is a section for 'ise-2'.

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.

- ▼ Certificate Management
  - System Certificates
  - Trusted Certificates
  - OCSP Client Profile
  - Certificate Signing Requests
  - Certificate Periodic Check Setti...
- ▶ Certificate Authority

### Import Server Certificate

\* Select Node

\* Certificate File  Defaultselfsignedservercerti.pem

\* Private Key File  Defaultselfsignedservercerti.pvk

Password

Friendly Name  ⓘ

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

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).