

Importer et exporter des certificats dans ISE

Table des matières

[Introduction](#)

[Informations générales](#)

[Exporter le certificat dans ISE](#)

[Importer le certificat dans ISE](#)

Introduction

Ce document décrit comment importer et exporter les certificats dans Cisco Identity Service Engine (ISE).

Informations générales

ISE utilise des certificats à des fins diverses (interface utilisateur Web, portails Web, EAP, pxgrid). Le certificat présent sur ISE peut avoir l'un des rôles suivants :

- Admin : pour la communication entre les noeuds et l'authentification du portail Admin.
- EAP : pour authentification EAP.
- RADIUS DTLS : pour l'authentification du serveur RADIUS DTLS.
- Portail : afin de communiquer entre tous les portails d'utilisateurs finaux Cisco ISE.
- PxGrid : afin de communiquer entre le contrôleur pxGrid.

Créez une sauvegarde des certificats installés sur les noeuds ISE. Ceci enregistre la sauvegarde des données de configuration et le certificat du noeud admin est pris. Toutefois, pour les autres noeuds, la sauvegarde des certificats est effectuée individuellement.

Exporter le certificat dans ISE

Accédez à Administration > System > Certificates > Certificate Management > System certificate. Développez le noeud, sélectionnez le certificat, puis cliquez sur Export, comme indiqué dans l'image :

Comme l'illustre cette image, sélectionnez Export Certificate and Private Key. Entrez un mot de passe alphanumérique comportant au moins 8 caractères. Ce mot de passe est requis pour restaurer le certificat.

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.

Conseil : n'oubliez pas le mot de passe.

Importer le certificat dans ISE

Deux étapes sont nécessaires pour importer le certificat sur ISE.

Étape 1. Déterminez si le certificat est auto-signé ou signé par un tiers.

- Si le certificat est auto-signé, importez la clé publique du certificat sous certificats approuvés.
- Si le certificat est signé par une autorité de certification tierce, Import Root et tous les autres certificats intermédiaires du certificat.

Accédez à Administration > System > Certificates > Certificate Management > Trusted Certificate, cliquez sur 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	Sei
<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

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 a new Certificate into the Certificate Store

* Certificate File **Browse...** Defaultselfsignedservercert.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

Submit Cancel

Étape 2. Importer le certificat réel.

1. Accédez à Administration > Système > Certificats > Gestion des certificats, cliquez sur Importer. Si le rôle admin est attribué au certificat, le service sur le noeud redémarre.

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

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates

Edit Generate Self Signed Certificate **Import** Export Delete View

	Friendly Name	Used By	Portal group tag
ise-1			
<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	
<input type="checkbox"/>	Default self-signed saml server certificate - CN=SAML_ISE.ise.local	SAML	
ise-2			

2. Sélectionnez le noeud pour lequel vous souhaitez importer le certificat.

3. Parcourez les clés publique et privée.

4. Entrez le mot de passe de la clé privée du certificat et sélectionnez le rôle souhaité.

5. Cliquez sur Soumettre.

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...** Defaultselfsignedservercert.pem

* Private Key File **Browse...** Defaultselfsignedservercert.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

Submit Cancel

Select Required Role

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.