

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). Les certificats présents sur ISE peuvent 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.

Export Cancel

 Conseil : n'oubliez pas le mot de passe.

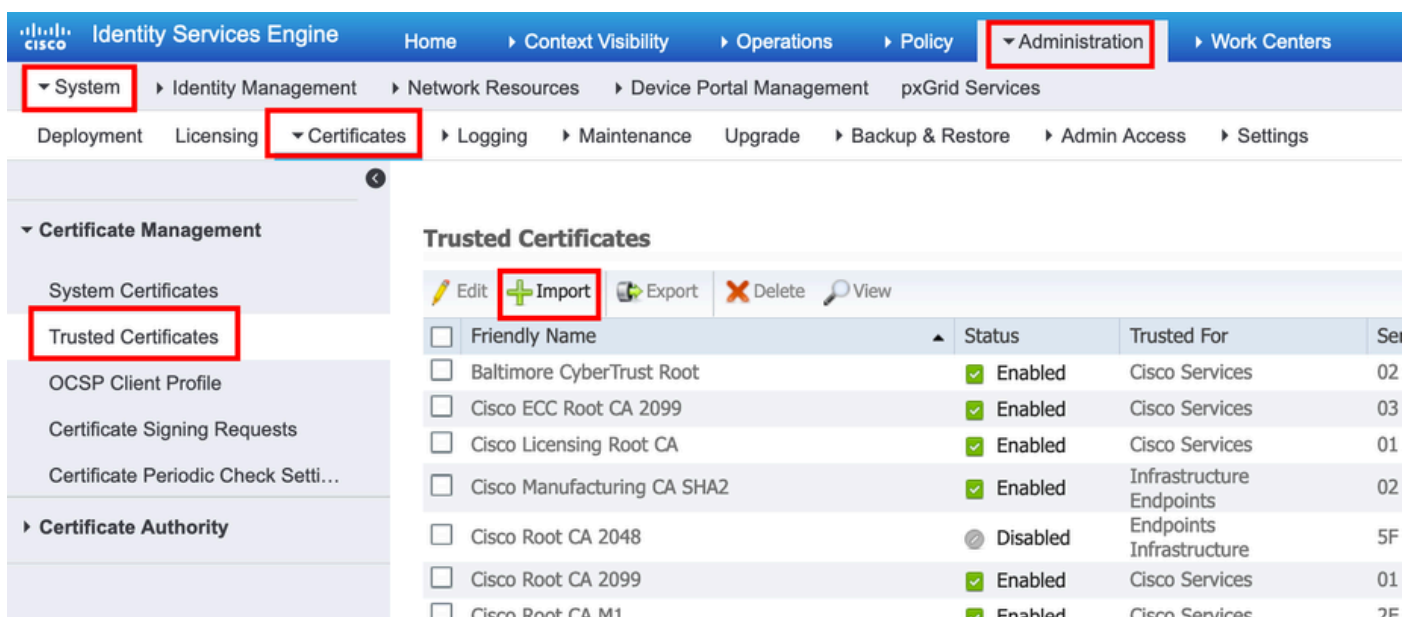
Importer le certificat dans ISE

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, importez le certificat racine et tous les autres certificats intermédiaires du certificat.

Accédez à Administration > System > Certificates > Certificate Management > Trusted Certificate, cliquez sur Import.



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is: Administration > System > Certificates > Trusted Certificates. The 'Import' button is highlighted with a red box. Below the navigation, the 'Trusted Certificates' table is visible, listing various certificates and their status.

Friendly Name	Status	Trusted For	Serial Number
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	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

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.

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

	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.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation bar at the top includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded, showing 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', and 'pxGrid Services'. The 'System' menu is further expanded to show 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Backup & Restore', 'Admin Access', and 'Settings'. The 'Certificates' menu is selected, and the 'Certificate Management' sidebar is visible, with 'System Certificates' highlighted. The main content area is titled 'Import Server Certificate' and contains the following fields and options:

- * Select Node: A dropdown menu with 'ise-1' selected.
- * Certificate File: A 'Browse...' button next to the file path 'Defaultselfsignedservercerti.pem'.
- * Private Key File: A 'Browse...' button next to the file path 'Defaultselfsignedservercerti.pvk'.
- Password: A password input field with a masked password '*****'.
- Friendly Name: A text input field containing 'ISE_Self_Signed'.
- Allow Wildcard Certificates: A checkbox with an information icon.
- Validate Certificate Extensions: A checkbox with an information icon.
- Usage: A section with several checkboxes:
 - 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 and Cancel buttons at the bottom.

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.