

Invoer- en uitvoercertificaten in ISE

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Certificaat exporteren in ISE](#)

[Het certificaat invoeren in ISE](#)

Inleiding

Dit document beschrijft hoe u de certificaten kunt importeren en exporteren in Cisco Identity Service Engine (ISE).

Achtergrondinformatie

ISE gebruikt certificaten voor verschillende doeleinden (Web UI, Web Portals, EAP, pxgrid). Een certificaat op ISE kan een van de volgende functies hebben:

- Admin: voor internodiecommunicatie en verificatie van het Admin-portal.
- EAP: Voor EAP-verificatie.
- RADIUS DTLS: voor RADIUS DTLS-serververificatie.
- Portal: om te communiceren tussen alle Cisco ISE-eindgebruikerportalen.
- PxGrid: Om te communiceren tussen de pxGrid controller.

Het is belangrijk om een reservekopie te maken van de certificaten die op ISE-knooppunten zijn geïnstalleerd. Wanneer u een back-up maakt van de configuratie, wordt een back-up gemaakt van de configuratiegegevens en het certificaat van de beheerknooppunt. Voor andere knooppunten wordt de back-up van certificaten echter afzonderlijk genomen.

Certificaat exporteren in ISE

Navigeren naar **Beheer > Systeem > Certificaten > Certificaatbeheer > Systeemcertificaat**. Breid het knooppunt uit, selecteer het certificaat en klik op **Exporteren**, zoals in de afbeelding:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration' (highlighted in red), and 'Work Centers'. Below this, a secondary navigation bar shows 'System' (highlighted in red), 'Identity Management', 'Network Resources', 'Device Portal Management', and 'pxGrid Services'. A third navigation bar includes 'Deployment', 'Licensing', 'Certificates' (highlighted in red), 'Logging', 'Maintenance', 'Upgrade', 'Backup & Restore', 'Admin Access', and 'Settings'. The left sidebar is titled 'Certificate Management' and contains 'System Certificates' (highlighted in red), 'Trusted Certificates', 'OCSP Client Profile', 'Certificate Signing Requests', and 'Certificate Periodic Check Setti...'. 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' (highlighted in red), 'Delete', and 'View'. A table lists certificates under 'ise-1':

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

Zoals in deze afbeelding wordt getoond, selecteert u het **Exportcertificaat** en de **persoonlijke sleutel**. Voer een minimaal 8 tekens in alfanumeriek wachtwoord in de lengte. Dit wachtwoord is vereist om het certificaat te kunnen herstellen.

The screenshot shows the 'Export Certificate' dialog box in ISE. The dialog title is 'Export Certificate'Default self-signed server certificate'. It shows two radio button options: 'Export Certificate Only' and 'Export Certificate and Private Key' (selected and highlighted in red). Below are input fields for '*Private Key Password' and '*Confirm Password'. A warning message states: 'Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.' At the bottom right, there are 'Export' and 'Cancel' buttons, with 'Export' highlighted in red.

Tip: Vergeet het wachtwoord niet.

Het certificaat invoeren in ISE

Er zijn twee stappen in het proces om het certificaat op ISE te importeren.

Stap 1. Zoek uit of het certificaat zelfondertekend is of door een derde partij ondertekend certificaat.

- Als het certificaat zelf is ondertekend, importeert u de openbare sleutel van het certificaat onder vertrouwde certificaten.
- Indien het certificaat is ondertekend door een certificeringsinstantie van een derde partij, Import Root en alle andere tussentijdse certificaten van het certificaat.

Navigeer naar **Beheer > Systeem > Certificaten > Certificaatbeheer > Trusted Certificate** en klik op **Importeren**, zoals in deze afbeelding wordt getoond.

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	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

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

Stap 2. Voer het echte certificaat in.

1. Zoals in deze afbeelding wordt getoond, navigeer dan naar **Beheer > Systeem > Certificaten > Certificaatbeheer** en klik op **Importeren**. Als de beheerdersrol is toegewezen aan het certificaat, wordt de service op het knooppunt opnieuw gestart.

The screenshot shows the Cisco Identity Services Engine Administration interface. The top navigation bar includes 'Administration', which is highlighted. Below it, the 'System' menu is expanded, showing 'Certificates'. The left sidebar has 'Certificate Management' expanded to 'System Certificates'. The main area is titled 'System Certificates' and contains a table of certificates. The 'Import' button is highlighted in red.

	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. Selecteer het knooppunt waarvoor u het certificaat wilt importeren.

3. Blader door de publieke en private sleutels.

4. Voer het wachtwoord voor de persoonlijke sleutel van het certificaat in en selecteer de gewenste rol.

5. Klik nu op **Indienen**, zoals in deze afbeelding wordt weergegeven.

- ▼ 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 Defaultselfsignedservercert.pem

* Private Key File Defaultselfsignedservercert.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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.