Invoer- en uitvoercertificaten in ISE

Inhoud

Inleiding

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

Achtergrondinformatie

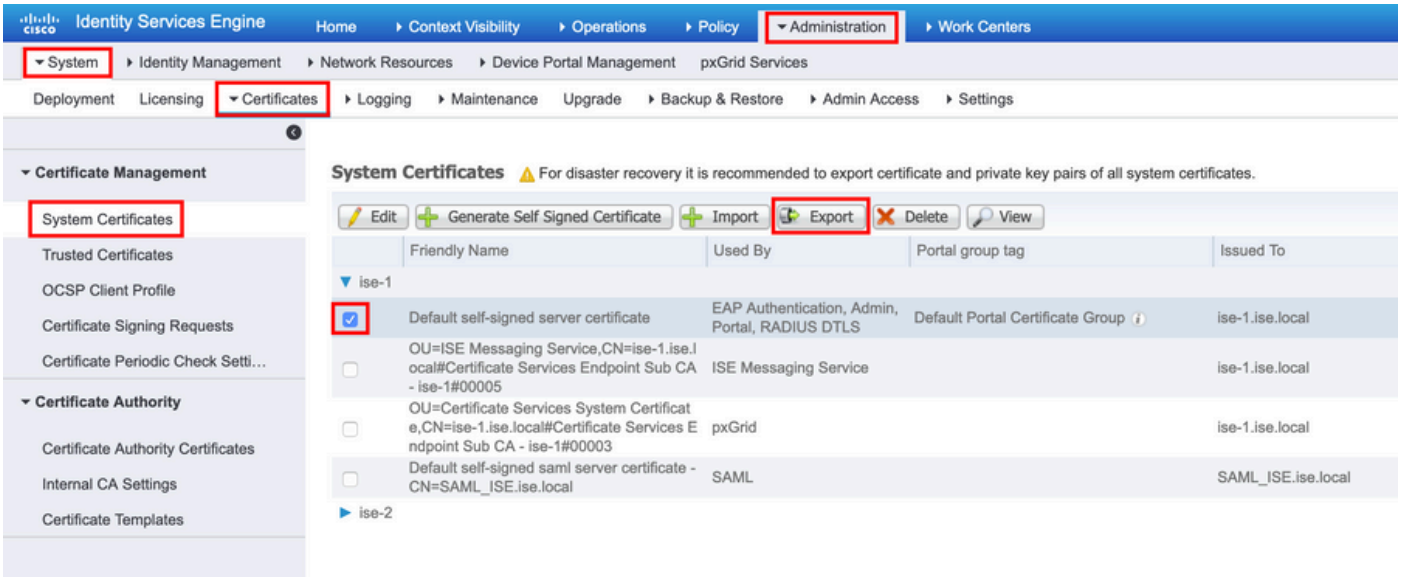
ISE gebruikt certificaten voor verschillende doeleinden (Web UI, Web Portals, EAP, pxgrid). Een certificaat op ISE kan een van de volgende functies hebben:

- 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:



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.

Tip: Vergeet het wachtwoord niet.

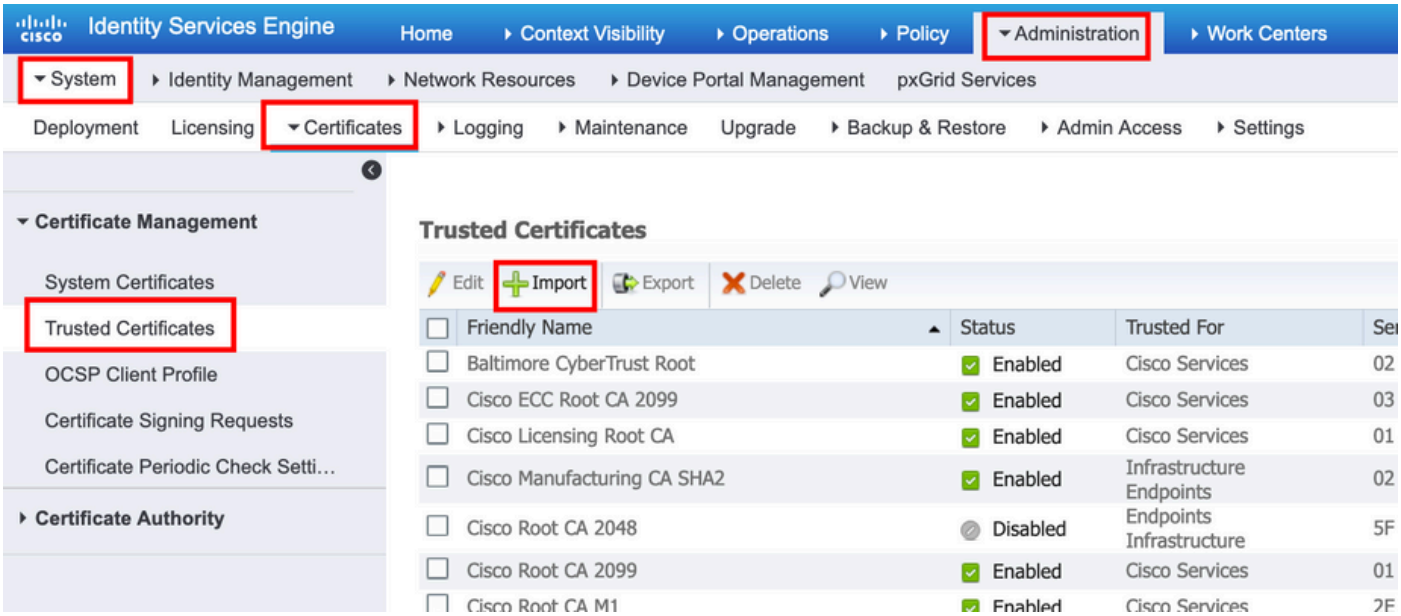
Het certificaat invoeren in ISE

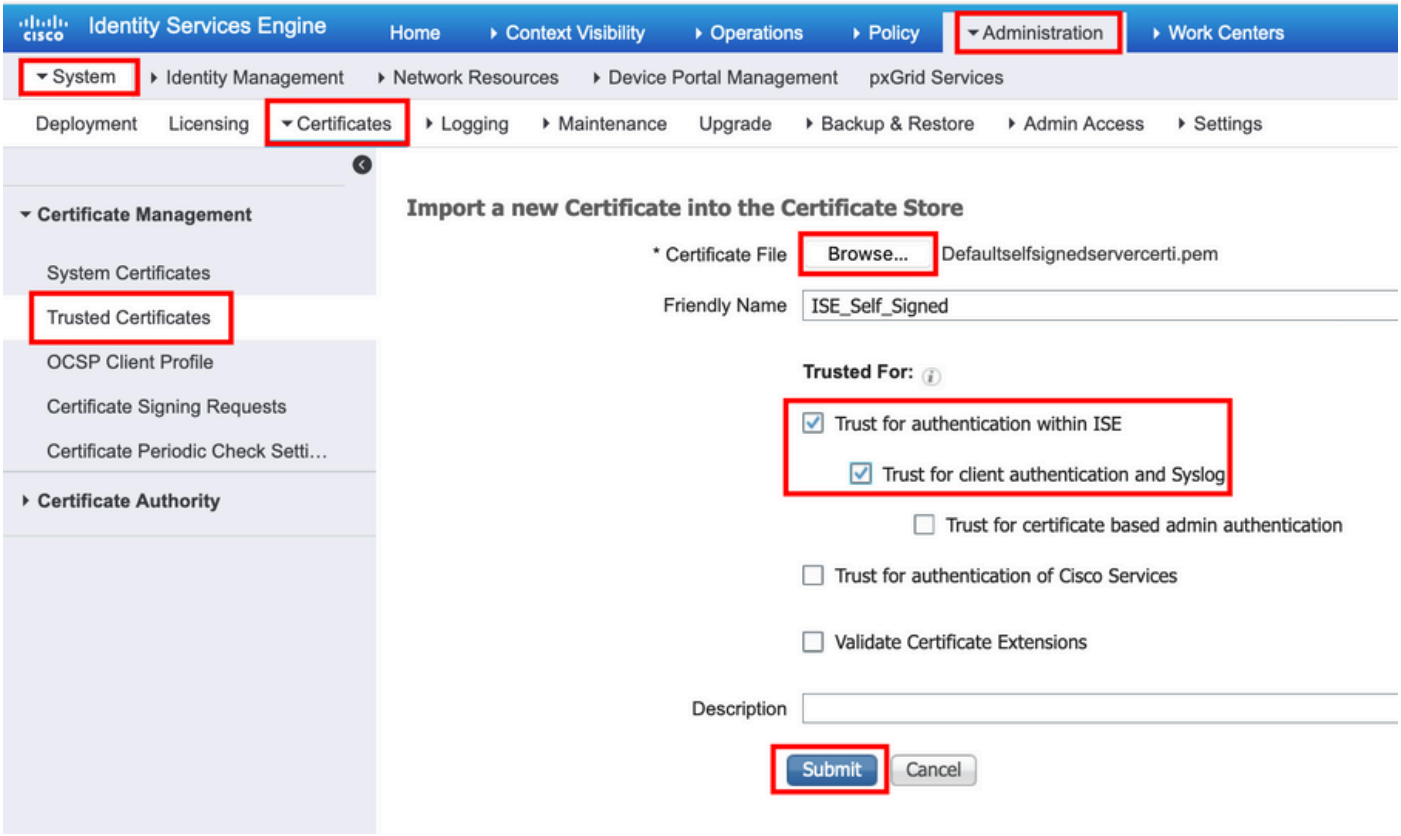
Er zijn twee stappen in het proces om het certificaat op ISE te importeren.

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.

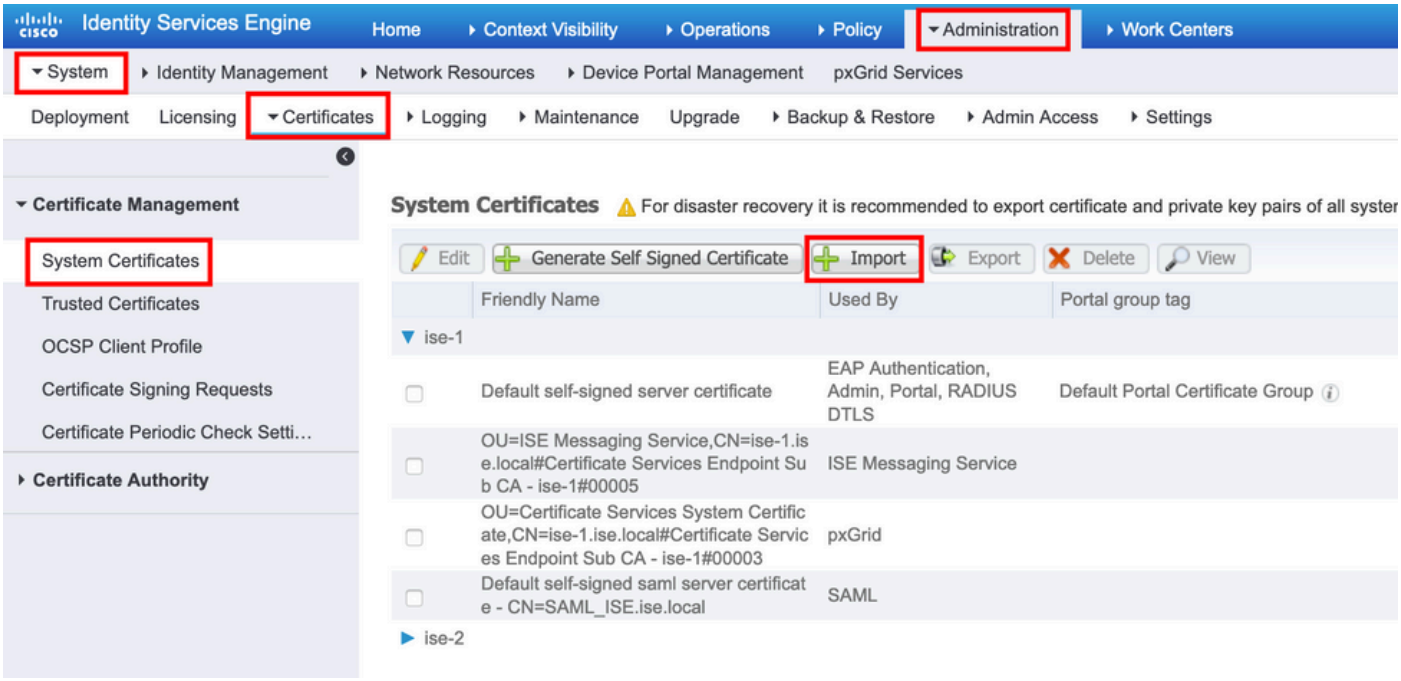
Navigeer naar **Beheer > Systeem > Certificaten > Certificaatbeheer > Trusted Certificate en** klik op **Importeren**, zoals in deze afbeelding wordt getoond.





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.

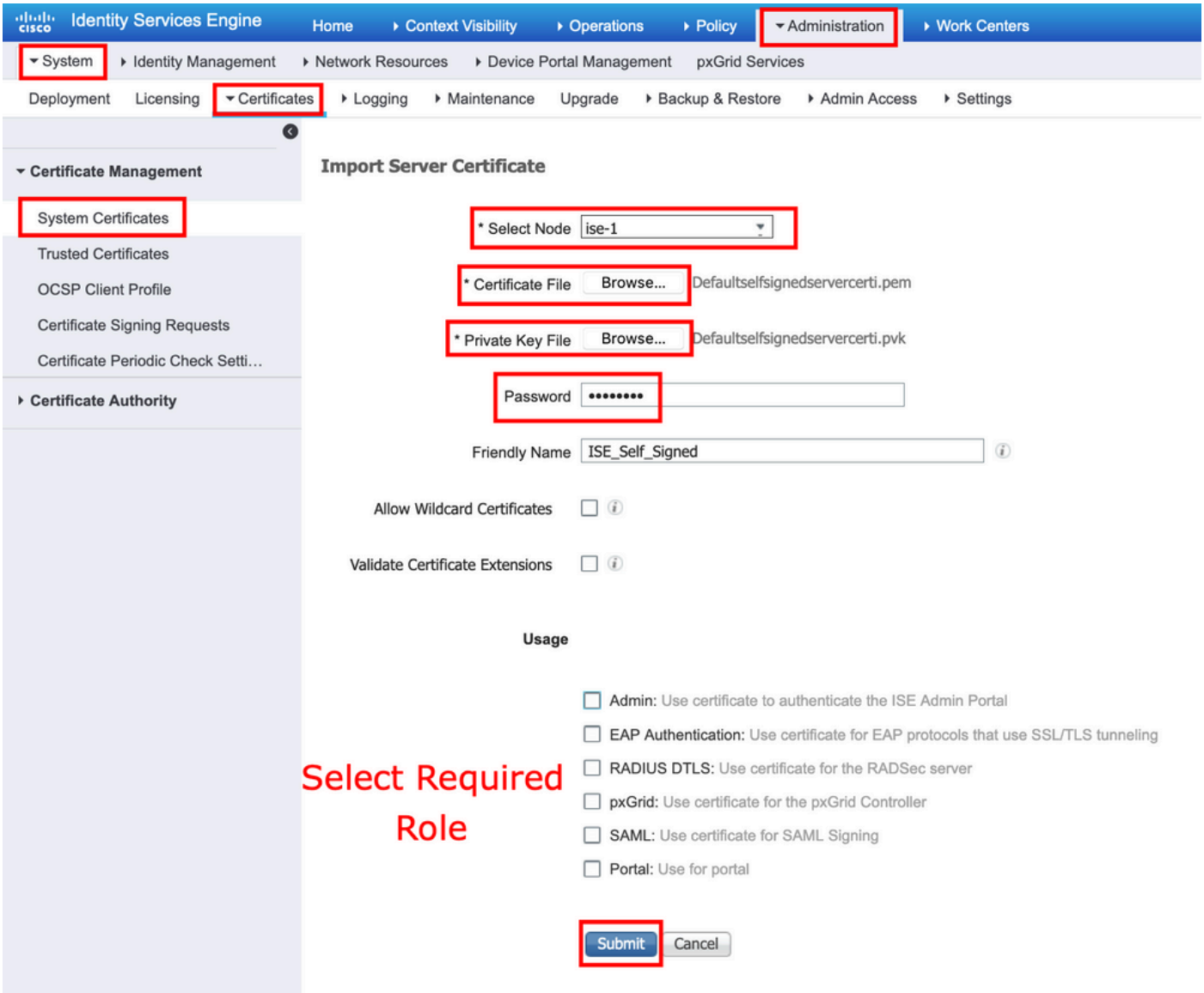


2. Selecteer het knooppunt waarvoor u het certificaat wilt importeren.

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.


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

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.