# SAN-certificaten voor IND en ISE-pxGrid-integratie maken met OpenSSL

## Inhoud

## Inleiding

Dit document beschrijft hoe u SAN-certificaten kunt maken voor pxGrid-integratie tussen Industrial Network Director (IND) en Identity Services Engine.

## Achtergrondinformatie

Wanneer u certificaten maakt in Cisco ISE voor pxGrid-gebruik, kunnen korte serverhostnamen niet in de ISE GUI worden ingevoerd omdat ISE alleen het FQDN- of IP-adres toestaat.

Om certificaten te maken die zowel de hostnaam als FQDN bevatten, moet een certificaataanvraagbestand buiten ISE worden gemaakt. Dit kan worden gedaan met OpenSSL om een certificaatondertekeningsaanvraag (CSR) met de veldingangen Onderwerp Alternatieve naam (SAN) te maken.

Dit document bevat geen uitgebreide stappen om pxGrid-communicatie tussen de IND-server en de ISE-server mogelijk te maken.  Deze stappen kunnen worden gebruikt nadat pxGrid is geconfigureerd en is bevestigd dat de server hostname is vereist.  Als deze fout wordt gevonden in de ISE Profiler logbestanden, vereist communicatie het hostname certificaat.

```
Unable to get sync statusjava.security.cert.CertificateException: No subject alternative DNS name matcht
```

Stappen voor de eerste inzet van IND met pxGrid-communicatie zijn te vinden op https://www.cisco.com/c/dam/en/us/td/docs/switches/ind/install/IND_PxGrid_Registration_Guide_Final.pdf

## Vereiste toepassingen

- Cisco Industrial Network Director (IND)
- Cisco Identity Services Engine (ISE)
- OpenSSL
    - In de meeste moderne Linux-versies, evenals MacOS, wordt het OpenSSL-pakket standaard geïnstalleerd. Als u merkt dat er geen opdrachten beschikbaar zijn, installeert u OpenSSL met behulp van de pakketbeheerapplicatie van uw besturingssysteem.

- Informatie over OpenSSL voor Windows is te vinden op https://wiki.openssl.org/index.php/Binaries

# Aanvullende informatie

Voor de toepassing van dit document worden deze gegevens gebruikt:

- IND Server hostnaam: rch-mas-ind
- FQDN: rch-mas-ind.cisco.com
- OpenSSL-configuratie: rch-mas-ind.req
- Bestandsnaam certificaataanvraag: rch-mas-ind.csr
- Private key bestandsnaam: rch-mas-ind.pem
- Naam certificaatbestand: rch-mas-ind.cer

# Processtappen

## CSR-certificaat maken

1. Maak op een systeem waarop OpenSSL is geïnstalleerd een tekstbestand met de vraag naar OpenSSL-opties, inclusief SAN-informatie.
   - De meeste "_default"-velden zijn optioneel, omdat er antwoorden kunnen worden ingevoerd terwijl de OpenSSL-opdracht wordt uitgevoerd in stap #2.
   - SAN-gegevens (DNS.1, DNS.2) zijn vereist en moeten zowel de DNS-korte hostnaam als de FQDN-naam van de server bevatten. Indien nodig kunnen extra DNS-namen worden toegevoegd met behulp van DNS.3, DNS.4, enzovoort.
   - Voorbeeld tekstbestand voor verzoek:

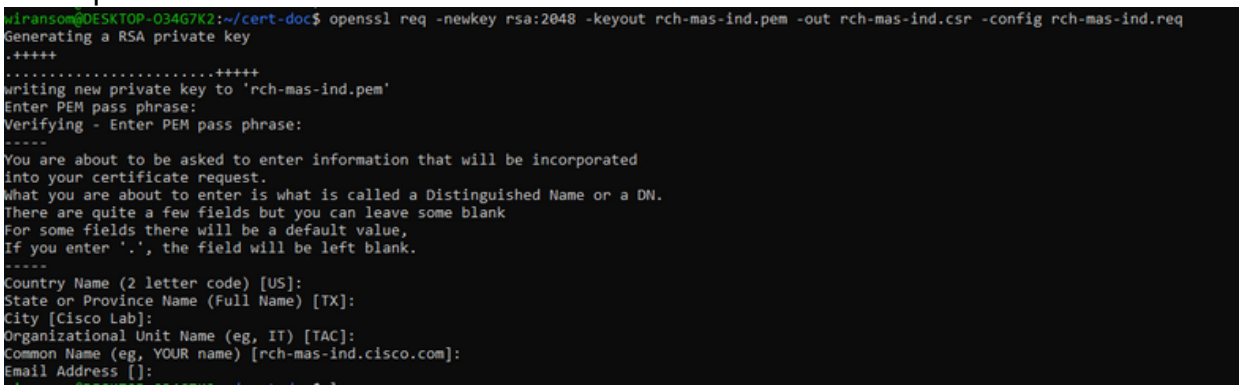
```
[Req]
voornaam_naam = naam
req_extensions = v3_req

[naam]
LandNaam = Landnaam (2-lettercode)
countryName_default = US
staatOfProvinceName = staat of provincie (volledige naam)
stateOrProvinceName_default = TX
plaatsNaam = stad
localityName_default = Cisco Lab
organisatorischeUnitName = Organisatorische Eenheidsnaam (bijv. IT)
organisatieUnitName_default = TAC
commonName = algemene naam (bijvoorbeeld, UW naam)
vaakNaam_max = 64
commonName_default = rch-mas-ind.cisco.com
e-mailadres = e-mailadres
e-mailadres_max = 40
```

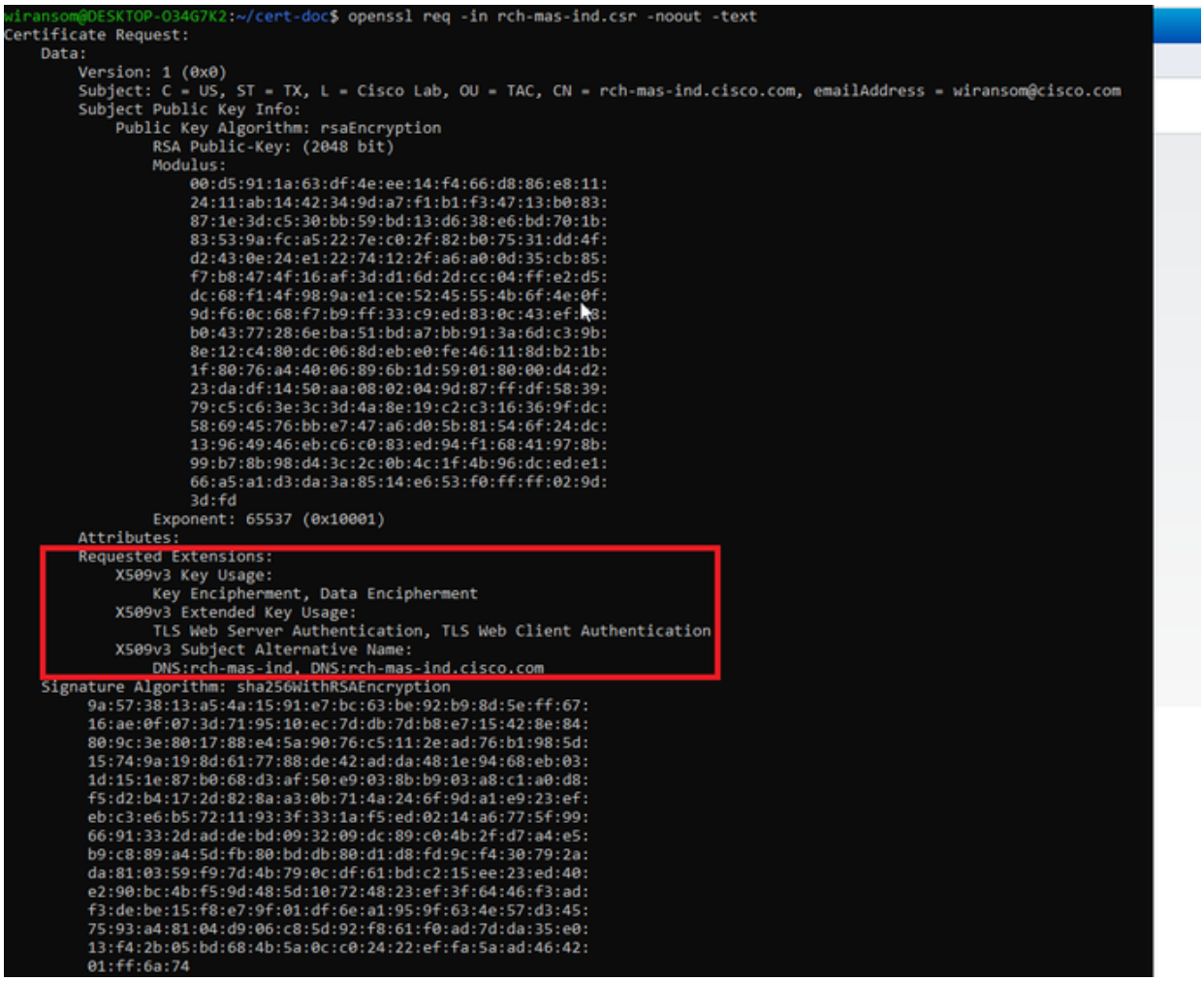
```
[v3_req]
keyGebruik = keyEncipherment, dataEncipherment
ExtendedKeyUsage = serverAuth, clientAuth
subjectAltName = @alt_names

[alt_names]
DNS.1 = rch-mas-ind
DNS.2 = rch-mas-ind.cisco.com
```

2. Gebruik OpenSSL om CSR met DNS korte hostnaam in SAN-veld te maken. Maak een privé-sleutelbestand naast het CSR-bestand.
    - Opdracht:
      openssl req -newkey rsa:2048 -keyout <server>.pem -out <server>.csr -config <server>.req
    - Voer desgevraagd een wachtwoord naar keuze in.  Vergeet niet dit wachtwoord te onthouden, aangezien het in de volgende stappen wordt gebruikt.
    - Voer een geldig e-mailadres in wanneer dit wordt gevraagd of laat het veld leeg en druk op <ENTER>.




3. Controleer desgewenst de CSR-bestandsinformatie. Voor een SAN-certificaat controleert u op "x509v3 Onderwerp Alternatieve Naam" zoals aangegeven in deze screenshot.
    - Opdrachtregel:
      openssl-req -in <server>.csr -no-text




4. Open het CSR-bestand in een teksteditor.  Om veiligheidsredenen is de screenshot van de steekproef onvolledig en bewerkt.  Het eigenlijke gegenereerde CSR-bestand bevat meer regels.

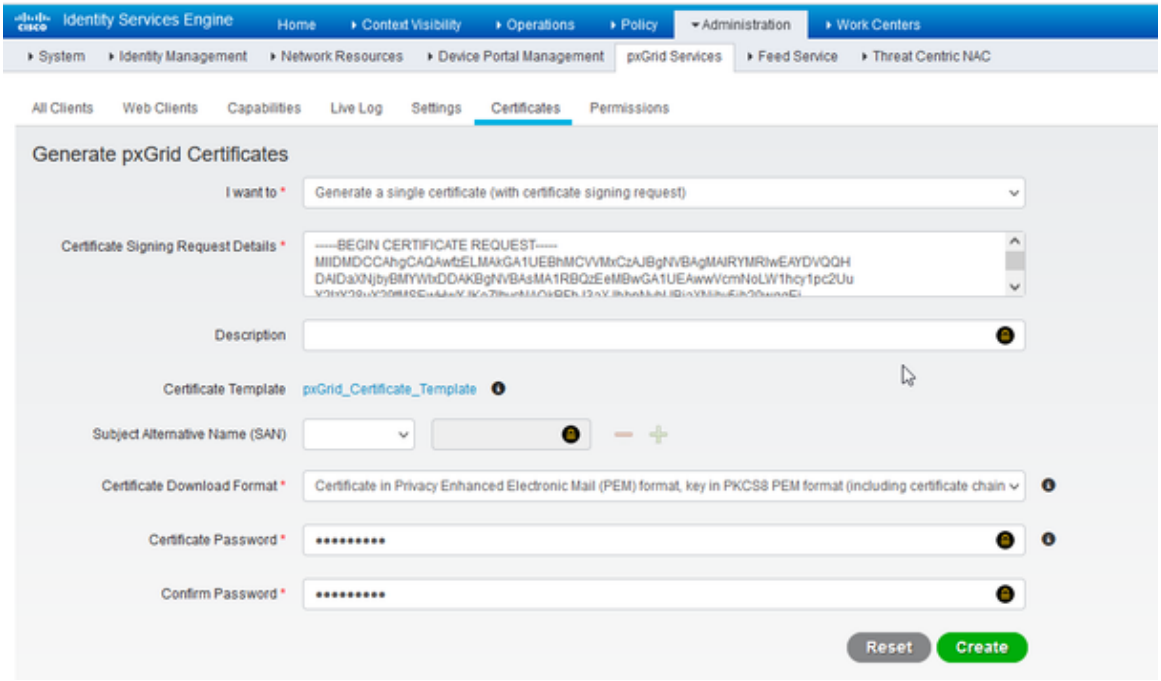
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDMDCCAhgCAQAwfzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAlRYMRIwEAYDVQQH
DAlDaXNjbyBMYWIxDDAKBgNVBAsMA1RBQzEeMBwGA1UEAwwVcmNoLW1hcy1pbmQu
Y2lzY28uY29tMSEwHwYJKoZIhvcNAQkBFhJ3aXJhbnNvbUBjaXNjby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVkRpj307uFPRm2IboESQRqxRC
NJ2n8bHzRxOwg4cePcUwu1m9E9Y45r1wG4NTmvylIn7AL4KwdTHdT9JDDiThInQS
L6agDTXLhfe4R08Wrz3RbS3MBP/i1dxo8U+YmuHOUkVVS29OD532DGj3uf8zye2D
0iPa3xRQqggCBJ2H/99YOXnFxj48PUqOGcLDFjaf3FhpRXa750em0FuBVG8k3BOW
AAGgbDBqBgkqhkiG9w0BCQ4xXTBbMAsGA1UdDwQEAwIEMDAdBgNVHSUEFjAUBggr
BgEFBQcDAQYIKwYBBQUHAwIwLQYDVR0RBCYwJIILcmNoLW1hcy1pbmSCFXJjaC1t
YXMtaW5kLmNpc2NvLmNvbTANBgkqhkiG9w0BAQsFAAOCAQEAmlc4E6VKFZHnvGO+
krmNXv9nFq4PBz1xlRDsfdt9uOcVQo6EgJw+gBeI5FqQdsURLq12sZhdFXSaGY1h
d4jeQq3aSB6UaOsDHRUeh7Bo069Q6QOLuQOowaDY9dK0Fy2CiqMLcUokb52h6SPv
Af9qdA==
-----END CERTIFICATE REQUEST-----
```

5. Kopieer het privé-sleutelbestand (<server>.pem) naar uw pc zoals het in een latere stap wordt gebruikt.

## Gebruik Cisco ISE om een certificaat te genereren met behulp van de gemaakte CSR-bestandsinformatie

Binnen de ISE GUI:

1. Verwijder de bestaande pxGrid-client.
    - Ga naar Beheer > PxGrid-services > Alle clients.
    - Zoek en selecteer de bestaande client hostnaam, indien vermeld,
    - Indien gevonden en geselecteerd, klik op de knop Verwijderen en kies "Geselecteerde verwijderen". Bevestig indien nodig.
2. Maak het nieuwe certificaat aan.
    - Klik op het tabblad Certificaten op de pxGrid-servicepagina.
    - Kies de opties:
        - "Ik wil":
            - "Genereer één certificaat (met verzoek om certificaatondertekening)"
        - "Details van aanvraag certificaat-ondertekening:
            - Kopieer/plak de CSR-gegevens uit de teksteditor. Vergeet niet de begin- en eindlijnen op te nemen.
        - "Formaat certificaat downloaden"
            - "Certificaat in Privacy Enhanced Electronic Mail (PEM)-formaat, sleutel in PKCS8 PEM-formaat."
        - Voer een certificaatwachtwoord in en bevestig het.
        - Klik op de knop Aanmaken.

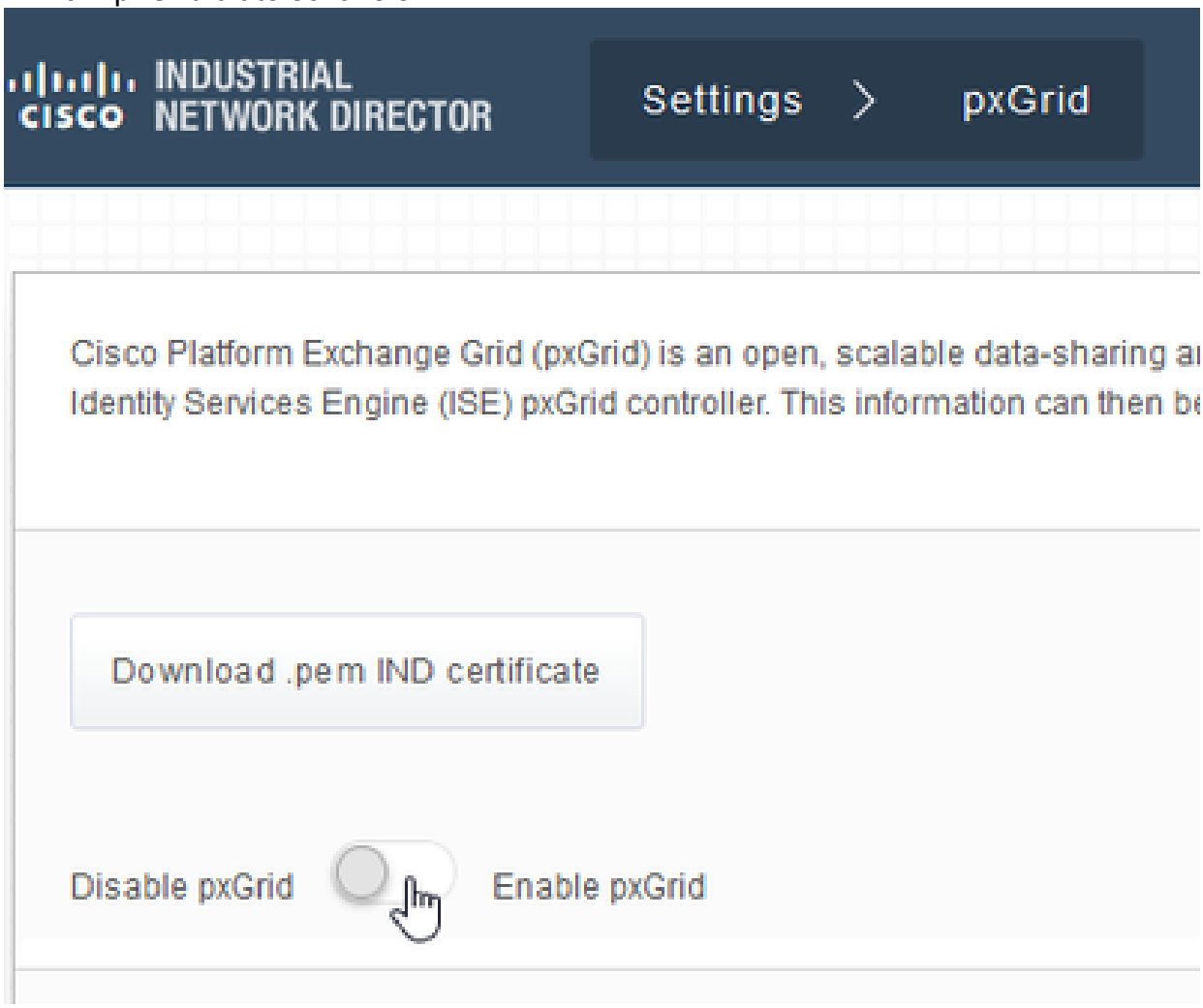



        - Dit maakt en downloadt een ZIP-bestand dat het certificaatbestand bevat, evenals aanvullende bestanden voor de certificaatketen. Open de ZIP en haal het certificaat eruit.
            - De bestandsnaam is normaal <IND server fqdn>.cer
            - In sommige versies van ISE is de bestandsnaam <IND fqdn>_<IND short name>.cer

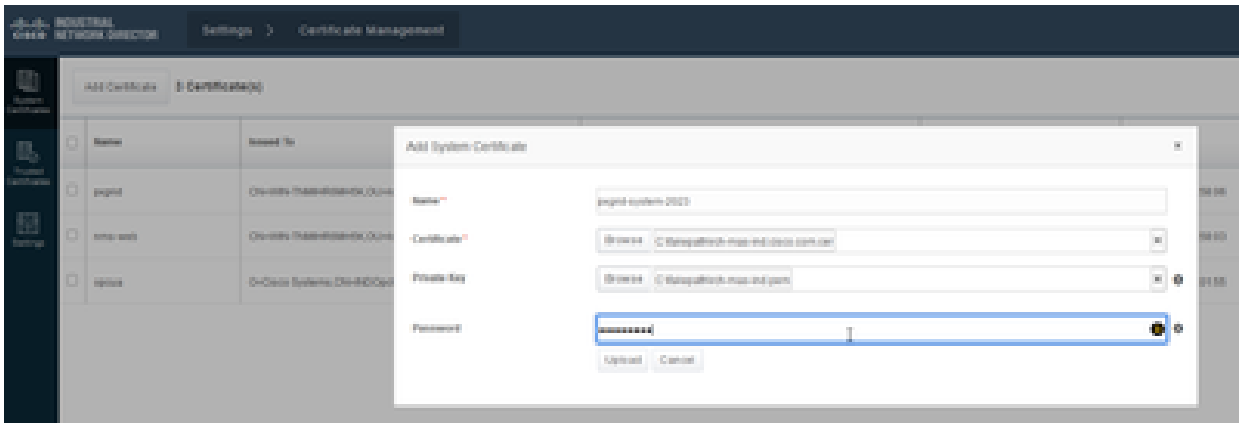
## Importeer het nieuwe certificaat in de IND-server en schakel het in voor pxGrid-gebruik

Binnen de IND GUI:

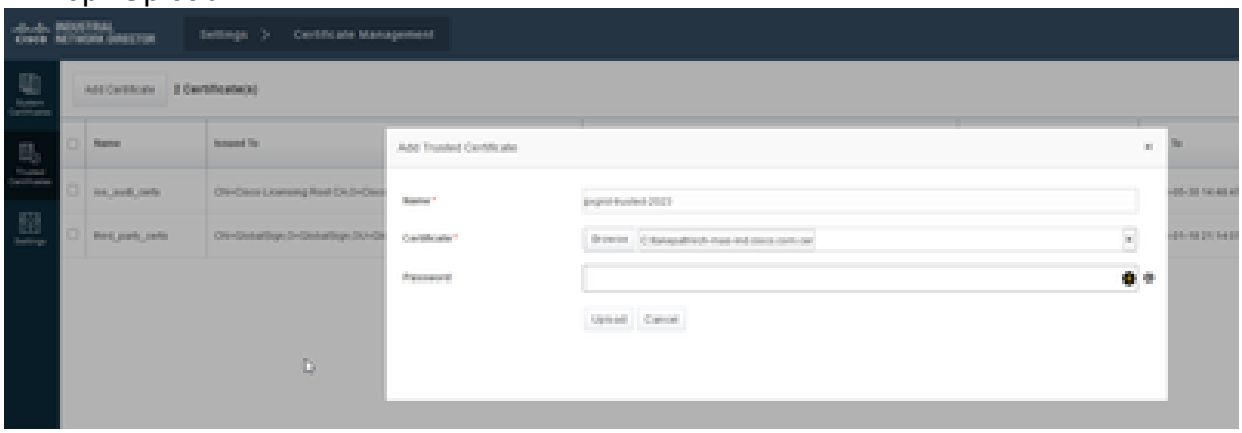
1. Schakel de pxGrid-service uit, zodat het nieuwe certificaat kan worden geïmporteerd en ingesteld als het actieve certificaat.
    - Ga naar Instellingen > PxGrid.
    - Klik om pxGrid uit te schakelen.




2. Importeer het nieuwe certificaat in systeemcertificaten.
    - Ga naar Instellingen > Certificaatbeheer.
    - Klik op "Systeemcertificaten"
    - Klik op "Certificaat toevoegen".
    - Voer een certificaatnaam in.
    - Klik op "Bladeren" links van "Certificaat" en zoek het nieuwe certificaatbestand.
    - Klik op "Bladeren" links van "Certificaat" en zoek de privésleutel die is opgeslagen bij het maken van de MVO.
    - Voer het wachtwoord in dat eerder is gebruikt bij het maken van de persoonlijke sleutel en CSR met OpenSSL.
    - Klik op "Upload".



3. Importeer het nieuwe certificaat als een vertrouwd certificaat.
    - Ga naar Instellingen > Certificaatbeheer en klik op "Trusted Certificates".
    - Klik op "Certificaat toevoegen".
    - Voer een certificaatnaam in. Dit moet een andere naam zijn dan de naam die op systeemcertificaten wordt gebruikt.
    - Klik op "Bladeren" links van "Certificaat" en zoek het nieuwe certificaatbestand.
    - Het wachtwoordveld kan leeggelaten worden.
    - Klik op "Upload".



4. Stel pxGrid in om het nieuwe certificaat te gebruiken.
    - Ga naar Instellingen > Certificaatbeheer en klik op "Instellingen".
    - Als u dat nog niet hebt gedaan, selecteert u "CA-certificaat" onder "PxGrid".
    - Selecteer de naam van het systeemcertificaat die tijdens de certificaatinvoer is gemaakt.
    - Klik op Save (Opslaan).

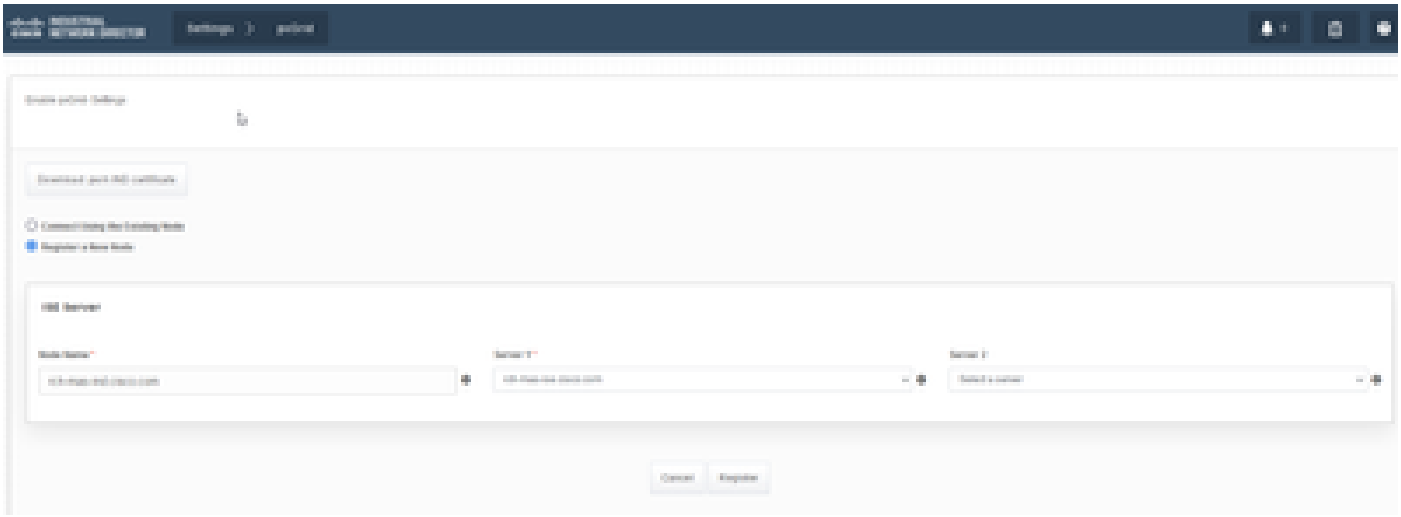
## PxGrid inschakelen en registreren met de ISE-server

Binnen de IND GUI:

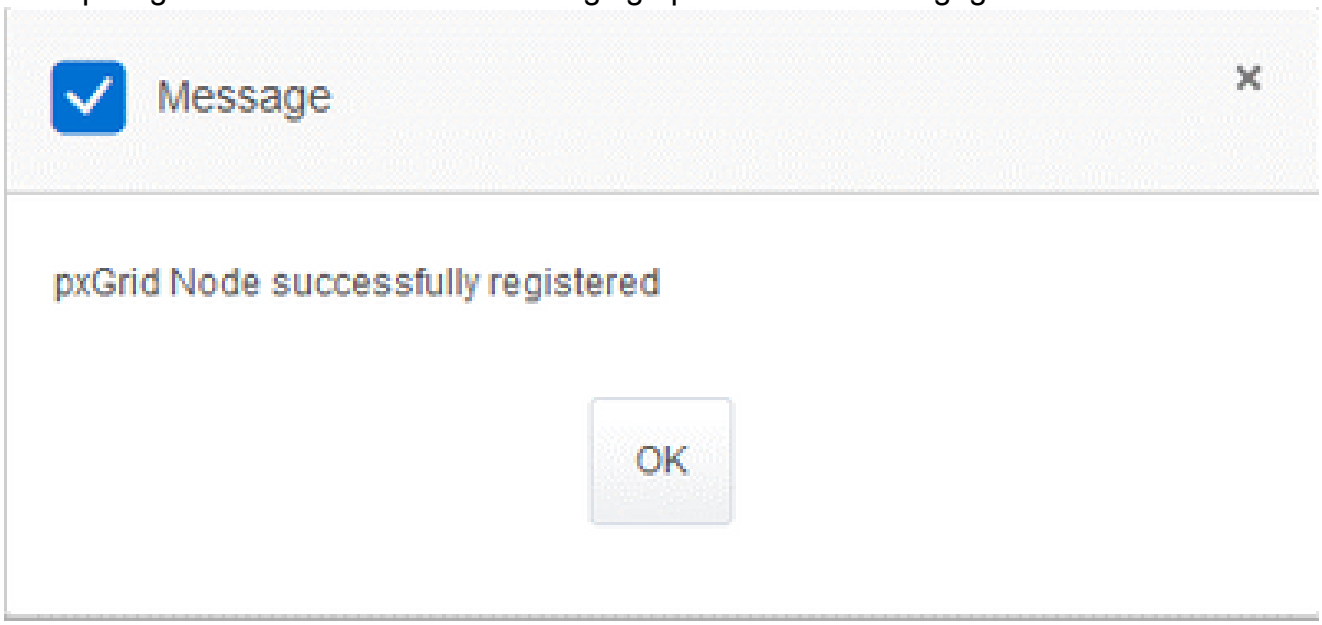
1. Ga naar Instellingen > PxGrid.
2. Klik op de schuifschakelaar om pxGrid in te schakelen.
3. Als dit niet de eerste keer is dat PxGrid met ISE wordt geregistreerd op deze IND-server, kies dan "Verbinden met behulp van het bestaande knooppunt". De informatie over de IND-knooppunt en de ISE-server wordt automatisch ingevuld.
4. Om een nieuwe IND server te registreren om pxGrid te gebruiken, indien nodig, kies

"Registreer een nieuw knooppunt". Voer de naam van de IND-knooppunt in en kies indien nodig ISE-servers.

- Als de ISE-server niet in de vervolgkeuzemogelijkheden voor Server 1 of Server 2 staat vermeld, kan deze als nieuwe pxGrid-server worden toegevoegd met Instellingen > Beleidsserver



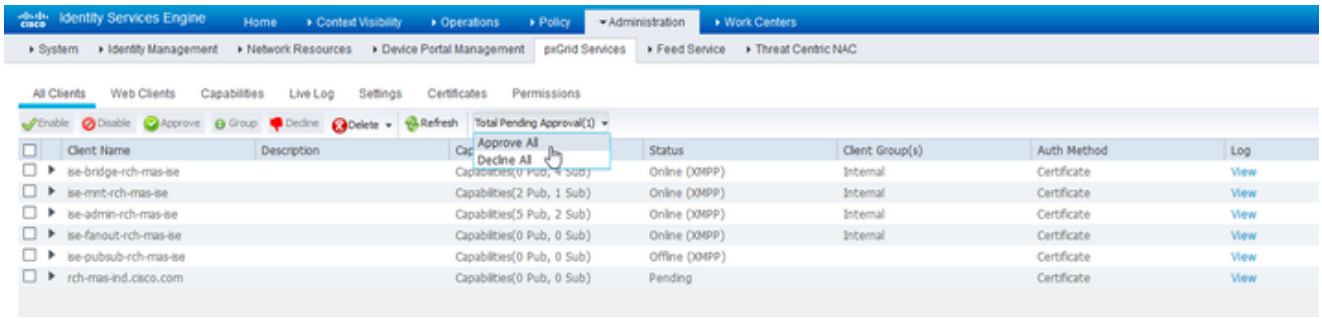
5. Klik op Registreren. Er wordt een bevestiging op het scherm weergegeven.



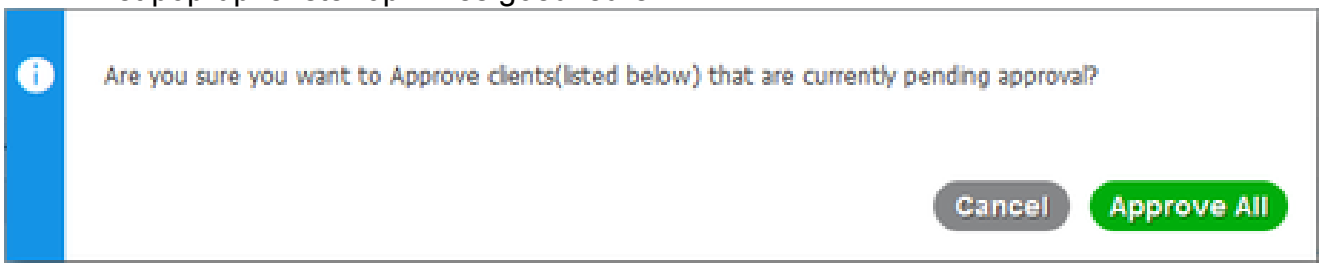

## Registratieaanvraag goedkeuren op ISE-server

Binnen de ISE GUI:

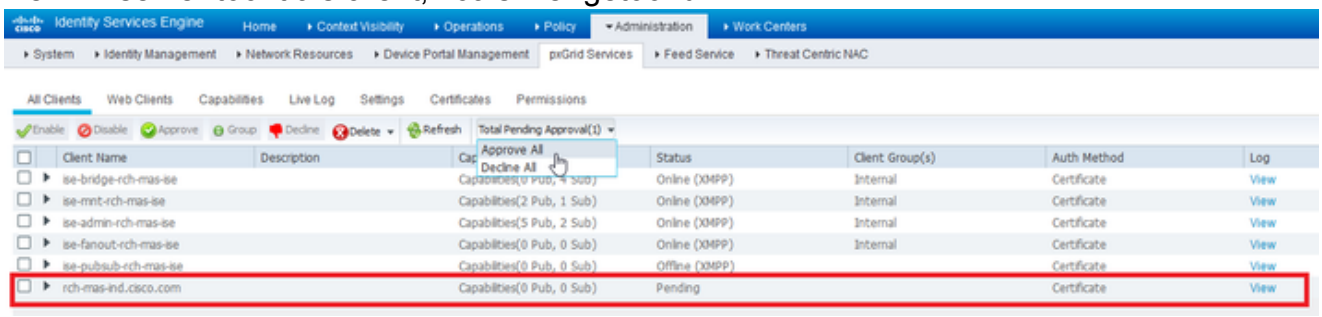
1. Ga naar Beheer > PxGrid-services > Alle clients. Een aanvraag in behandeling toont als "Totaal in behandeling zijnde goedkeuring(1)."
2. Klik op "Total Pending Approval(1)" en selecteer "Approve All."




3. Klik in het pop-upvenster op "Alles goedkeuren".



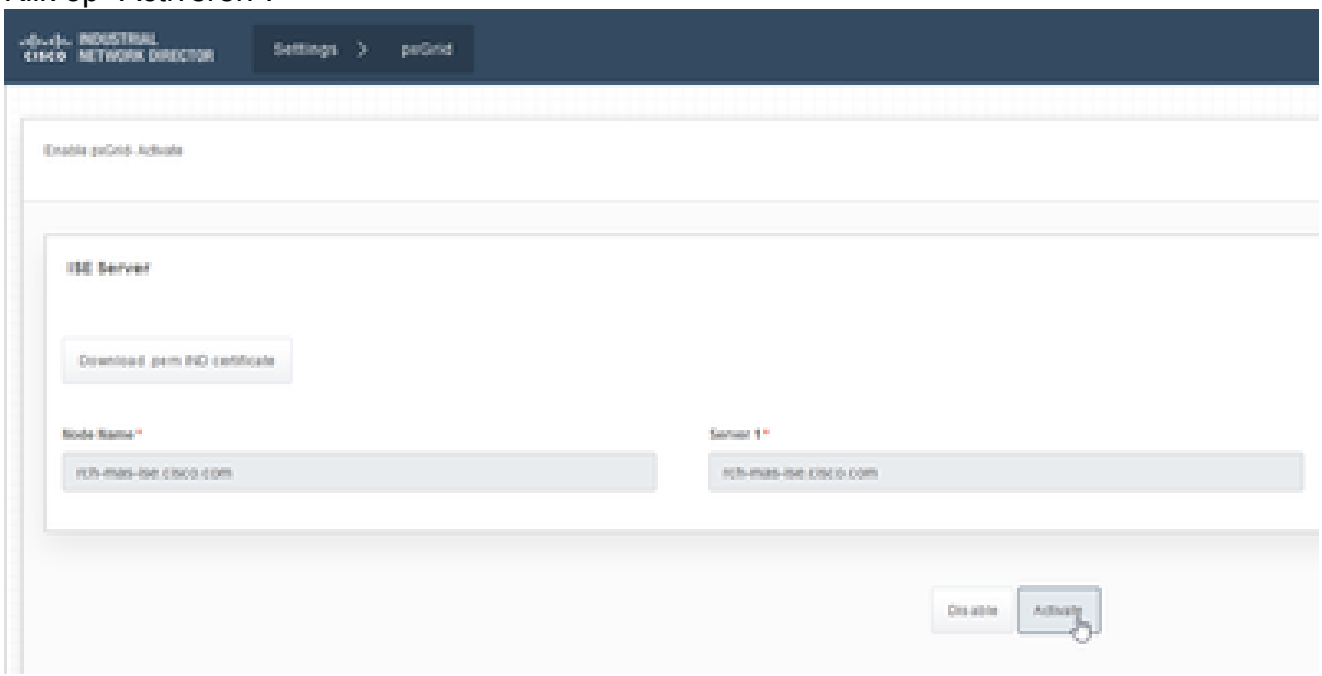

4. De IND server toont als client, zoals hier getoond.



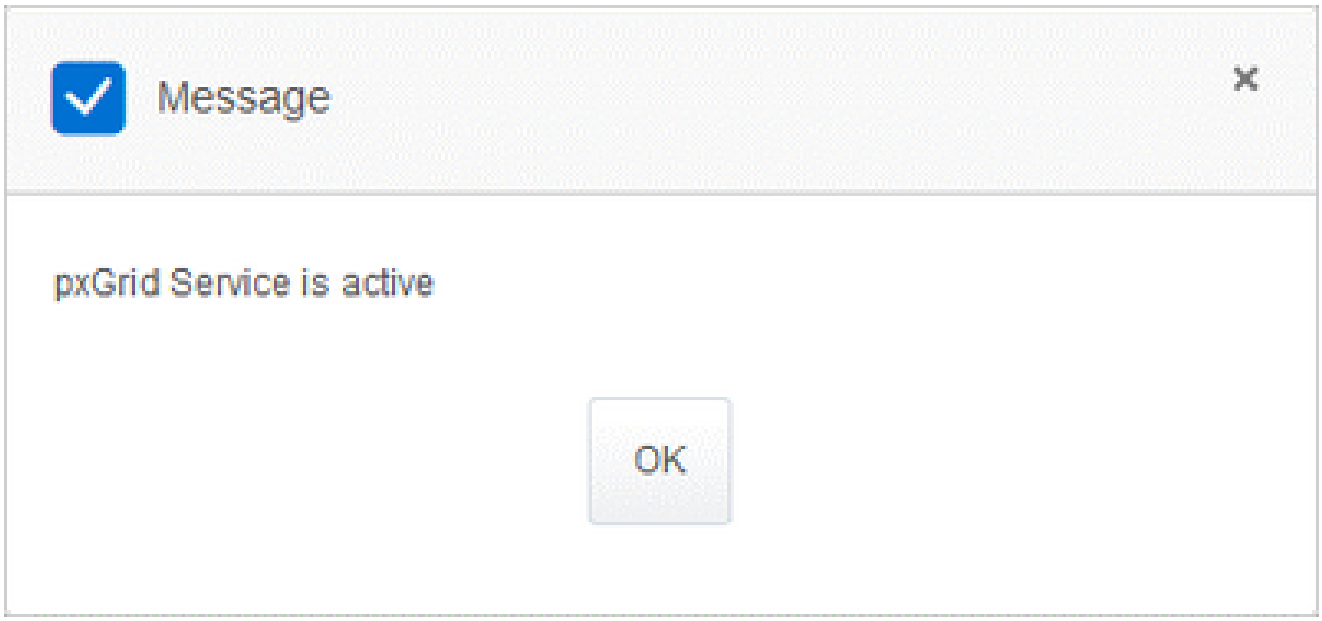

## Activeer de pxGrid-service op de IND-server

Binnen de IND GUI:

1. Ga naar Instellingen > PxGrid.
2. Klik op "Activeren".




3. Er wordt een bevestiging op het scherm weergegeven.


Message
pxGrid Service is active
OK

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.