

# 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 match
```

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](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]
keyUsage = 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>.

```
hlransom@DESKTOP-03467K2:~/cert-doc$ openssl req -newkey rsa:2048 -keyout rch-mas-ind.pem -out rch-mas-ind.csr -config rch-mas-ind.req
Generating a RSA private key
.+++++
.....+++++
writing new private key to 'rch-mas-ind.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (Full Name) [TX]:
City [Cisco Lab]:
Organizational Unit Name (eg, IT) [TAC]:
Common Name (eg, YOUR name) [rch-mas-ind.cisco.com]:
Email Address []:
```

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

```
wiransom@DESKTOP-03467K2:~/cert-doc$ openssl req -in rch-mas-ind.csr -noout -text
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = US, ST = TX, L = Cisco Lab, OU = TAC, CN = rch-mas-ind.cisco.com, emailAddress = wiransom@cisco.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:d5:91:1a:63:df:4e:ee:14:f4:66:d8:86:e8:11:
        24:11:ab:14:42:34:9d:a7:f1:b1:f3:47:13:b0:83:
        87:1e:3d:c5:30:bb:59:bd:13:d6:38:e6:bd:70:1b:
        83:53:9a:fc:a5:22:7e:c0:2f:82:b0:75:31:dd:4f:
        d2:43:0e:24:e1:22:74:12:2f:a6:a0:0d:35:cb:85:
        f7:b8:47:4f:16:af:3d:d1:6d:2d:cc:04:ff:e2:d5:
        dc:68:f1:4f:98:9a:e1:ce:52:45:55:4b:6f:4e:0f:
        9d:f6:0c:68:f7:b9:ff:33:c9:ed:83:0c:43:ef:83:
        b0:43:77:28:6e:ba:51:bd:a7:bb:91:3a:6d:c3:9b:
        8e:12:c4:80:dc:06:8d:eb:e0:fe:46:11:8d:b2:1b:
        1f:80:76:a4:40:06:89:6b:1d:59:01:80:00:d4:d2:
        23:da:df:14:50:aa:08:02:04:9d:87:ff:df:58:39:
        79:c5:c6:3e:3c:3d:4a:8e:19:c2:c3:16:36:9f:dc:
        58:69:45:76:bb:e7:47:a6:d0:5b:81:54:6f:24:dc:
        13:96:49:46:eb:c6:c0:83:ed:94:f1:68:41:97:8b:
        99:b7:8b:98:d4:3c:2c:0b:4c:1f:4b:96:dc:ed:e1:
        66:a5:a1:d3:da:3a:85:14:e6:53:f0:ff:ff:02:9d:
        3d:fd
      Exponent: 65537 (0x10001)
  Attributes:
    Requested Extensions:
      X509v3 Key Usage:
        Key Encipherment, Data Encipherment
      X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
      X509v3 Subject Alternative Name:
        DNS:rch-mas-ind, DNS:rch-mas-ind.cisco.com
  Signature Algorithm: sha256WithRSAEncryption
    9a:57:38:13:a5:4a:15:91:e7:bc:63:be:92:b9:8d:5e:ff:67:
    16:ae:0f:07:3d:71:95:10:ec:7d:db:7d:b8:e7:15:42:8e:84:
    80:9c:3e:80:17:88:e4:5a:90:76:c5:11:2e:ad:76:b1:98:5d:
    15:74:9a:19:8d:61:77:88:de:42:ad:da:48:1e:94:68:eb:03:
    1d:15:1e:87:b0:68:d3:af:50:e9:03:8b:b9:03:a8:c1:a0:d8:
    f5:d2:b4:17:2d:82:8a:a3:0b:71:4a:24:6f:9d:a1:e9:23:ef:
    eb:c3:e6:b5:72:11:93:3f:33:1a:f5:ed:02:14:a6:77:5f:99:
    66:91:33:2d:ad:de:bd:09:32:09:dc:89:c0:4b:2f:d7:a4:e5:
    b9:c8:89:a4:5d:fb:80:bd:db:80:d1:d8:fd:9c:f4:30:79:2a:
    da:81:03:59:f9:7d:4b:79:0c:df:61:bd:c2:15:ee:23:ed:40:
    e2:90:bc:4b:f5:9d:48:5d:10:72:48:23:ef:3f:64:46:f3:ad:
    f3:de:be:15:f8:e7:9f:01:df:6e:a1:95:9f:63:4e:57:d3:45:
    75:93:a4:81:04:d9:06:c8:5d:92:f8:61:f0:ad:7d:da:35:e0:
    13:f4:2b:05:bd:68:4b:5a:0c:c0:24:22:ef:fa:5a:ad:46:42:
    01:ff:6a:74
```

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-----
MIIDMCCAhgCAQAwfzELMAkGA1UEBhMCVVMxGzAJBgNVBAGMA1RYMRiWEAYDVQQH
DA1DaXNjbyBMYWIXDDAKBgNVBAsMA1RBQzEeMBwGA1UEAwwVcmNoLW1hcy1pbmQu
Y21zY28uY29tMSEwHwYJKoZIhvcNAQkBFHJ3aXJhbnNvbUBjaXNjby5jb20wggiEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVkRpj307uFPRm2IboESQRqxRC
NJ2n8bHzRxOwg4cePcUwu1m9E9Y45r1wG4NTmvy1In7AL4KwdTHdT9JDDiThInQS
L6agDTXLhfe4R08Wrz3RbS3MBP/i1dxo8U+YmuHOUkVVS290D532DGj3uf8zye2D
0iPa3xRQqggCBJ2H/99Y0XnFxj48PUqOGcLDFjaf3FhpRXa750em0FuBVG8k3BOW
AAGgbDBqBgkqhkiG9w0BCQ4xXTBbMAsGA1UdDwQEAwIEMDAdBgNVHSUEFjAUBggr
BgEFBQcDAQYIKwYBBQUHAwIwLQYDVR0RBCYwJiILcmNoLW1hcy1pbmSCFXJjaC1t
YXMtaw5kLmNpc2NvLmNvbTANBgkqhkiG9w0BAQsFAAOCAQEAm1c4E6VKFZHnvGO+
krmNXv9nFq4PBz1x1RDsfdt9u0cVQo6EgJw+gBeI5FqQdsURLq12sZhdFXSaGY1h
d4jeQq3aSB6Ua0sDHRUeh7Bo069Q6QOLuQOowaDY9dK0Fy2CiQmLcUokb52h6SPv
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.

The screenshot shows the 'Generate pxGrid Certificates' form in the ISE GUI. The form includes the following fields and options:

- I want to \***: A dropdown menu with the selected option 'Generate a single certificate (with certificate signing request)'.
- Certificate Signing Request Details \***: A text area containing a Base64-encoded CSR: 

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIDMCAhgcAQAwfzELMAkGA1UEBhMCVWxkCzAJBgNVBAGMAiRYMRwEAYDVQQH  
DAIDaXNjbjBMYWVhDDAKBgNVBAsMA1RBQzEeMBwGA1UEAwwVcmNoLW10c2J1  
Y3RvY29uY3R0MDCChAkwYwZBbnRlMA0GCSqGSIb3DQEBAQUAA4IBDwAwEgQ  
-----
```
- Description**: An empty text field.
- Certificate Template**: A dropdown menu with the selected option 'pxGrid\_Certificate\_Template'.
- Subject Alternative Name (SAN)**: A dropdown menu with an empty text field and '+' and '-' icons.
- Certificate Download Format \***: A dropdown menu with the selected option 'Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)'.
- Certificate Password \***: A password field with masked characters (dots).
- Confirm Password \***: A password field with masked characters (dots).

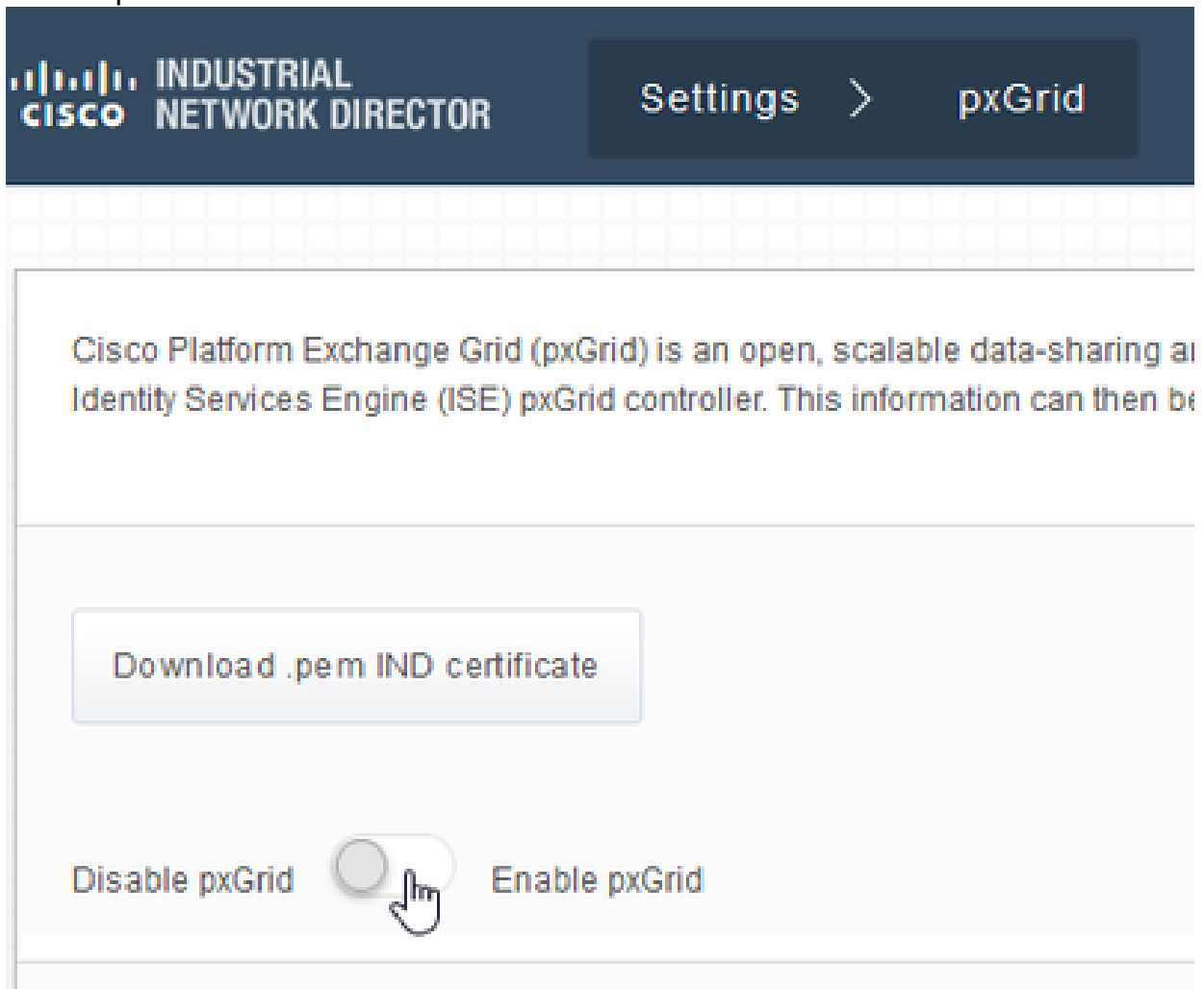
At the bottom right of the form, there are two buttons: 'Reset' and 'Create'.

- 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

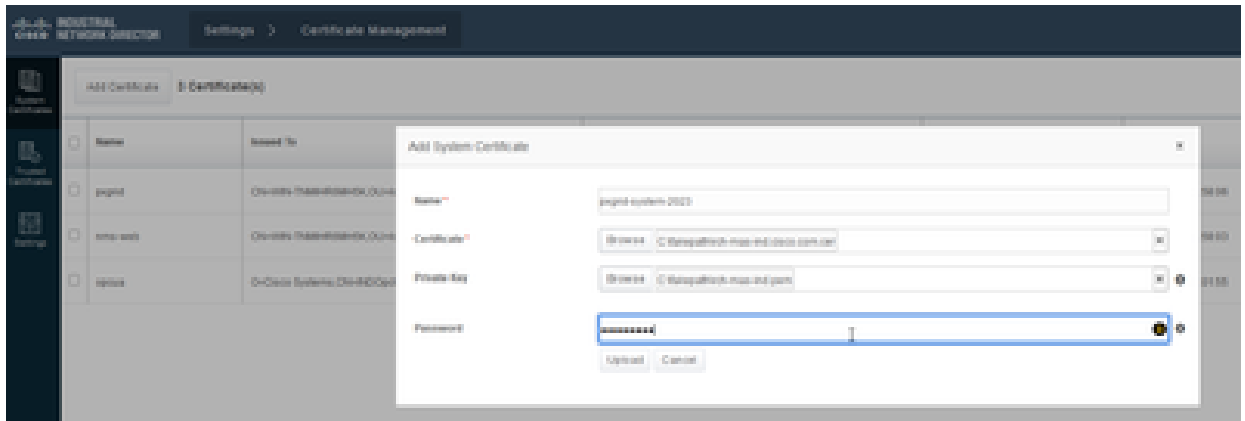
Binnen de IND GUI:

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.



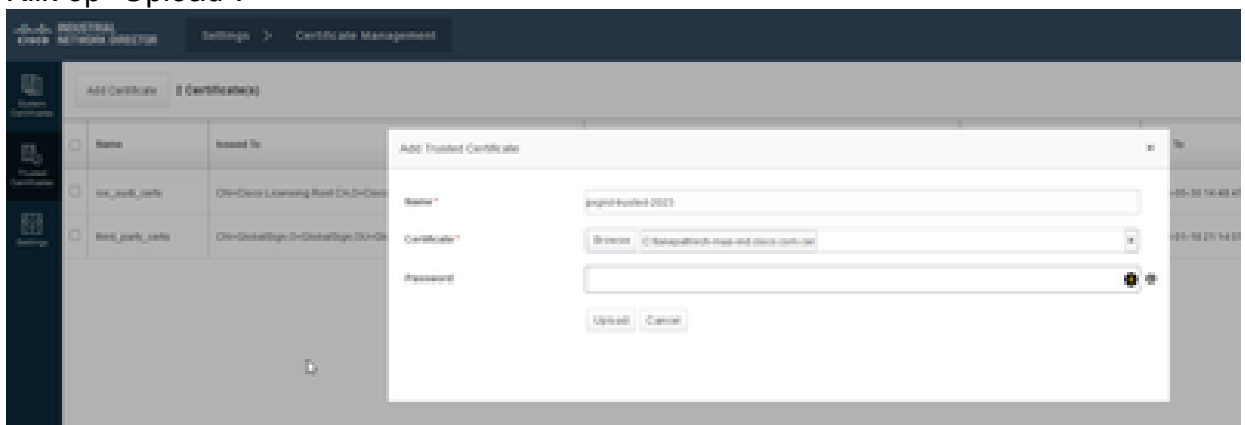
2. Importeer het nieuwe certificaat in systeemcertificaten.
  - Ga naar Instellingen > Certificaatbeheer.
  - Klik op "Systeemcertificaten"
  - Klik op "Certificaat toevoegen".
  - Voer een certificaatnaam in.
  - Klik op "Bladeren" links van "Certificaat" en zoek het nieuwe certificaatbestand.
  - Klik 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 certificaatimport is gemaakt.
- Klik op Save (Opslaan).

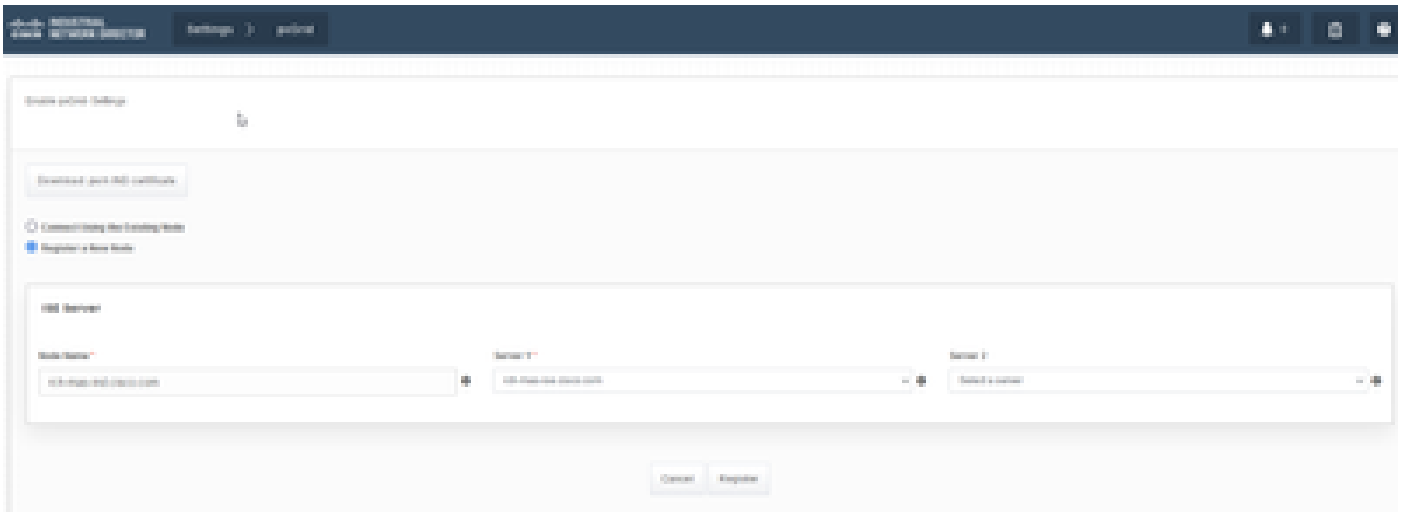
## PxGrid inschakelen en registreren met de ISE-server

Binnen de IND GUI:

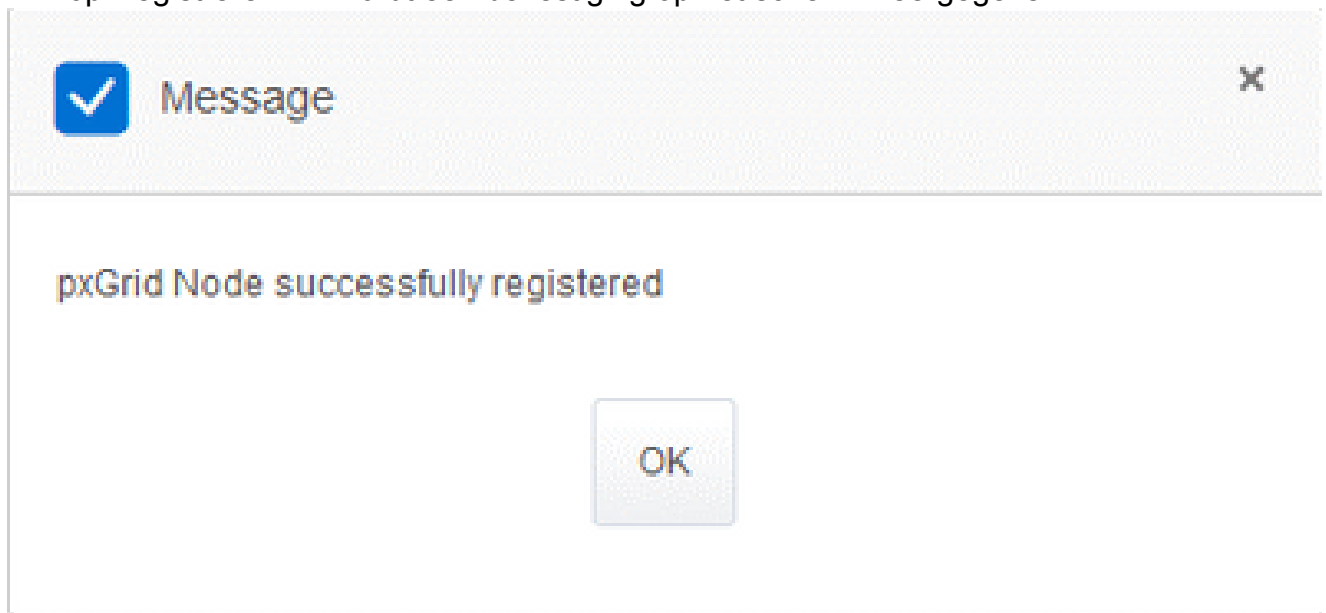
1. Ga naar Instellingen > PxGrid.
2. Klik op de schuifschakelaar om pxGrid in te schakelen.
3. Als dit niet de eerste keer is dat PxGrid met ISE wordt geregistreerd op deze IND-server, kies dan "Verbinden met behulp van het bestaande knooppunt". De informatie over de IND-knooppunt en de ISE-server wordt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



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



## Registratieaanvraag goedkeuren op ISE-server

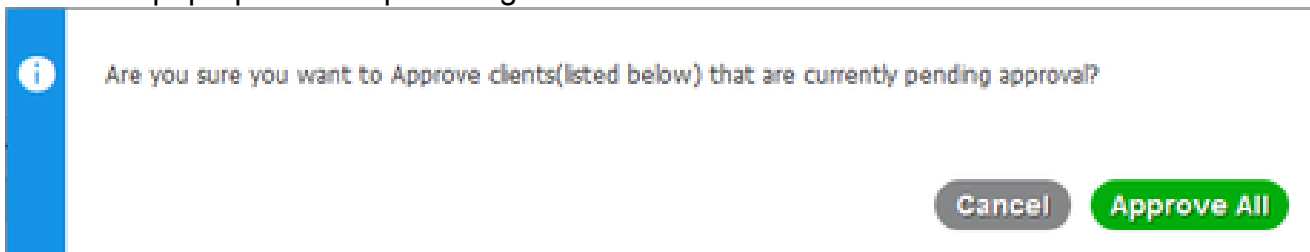
Binnen de ISE GUI:

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."



Client Name	Description	Cap	Status	Client Group(s)	Auth Method	Log
se-bridge-rch-mas-ise		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View
se-mnt-rch-mas-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View
se-admin-rch-mas-ise		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View
se-fanout-rch-mas-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
se-pubsub-rch-mas-ise		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View
rch-mas-nd.cisco.com		Capabilities(0 Pub, 0 Sub)	Pending		Certificate	View

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



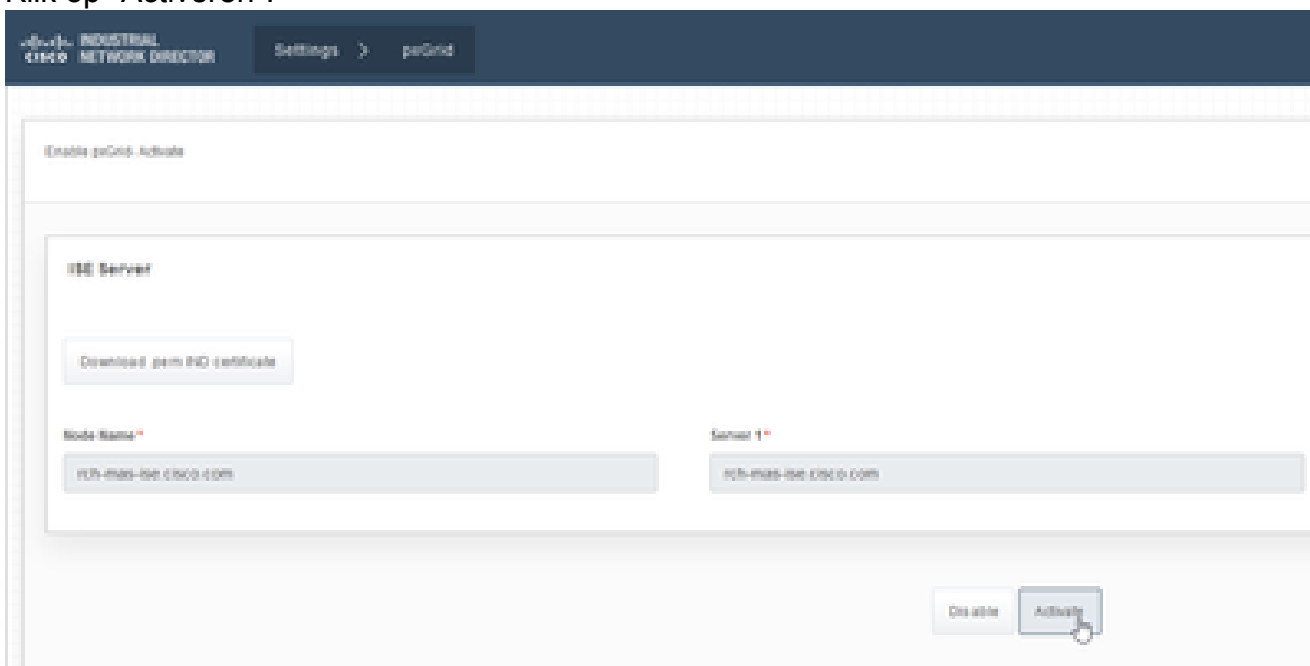
4. De IND server toont als client, zoals hier getoond.

Client Name	Description	Cap	Status	Client Group(s)	Auth Method	Log
se-bridge-rch-mas-ise		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View
se-mnt-rch-mas-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View
se-admin-rch-mas-ise		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View
se-fanout-rch-mas-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
se-pubsub-rch-mas-ise		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View
rch-mas-nd.cisco.com		Capabilities(0 Pub, 0 Sub)	Pending		Certificate	View

## 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.