Create SAN Certificates for IND and ISE pxGrid Integration Using OpenSSL

Contents

Introduction

This document describes how to create SAN certificates for pxGrid integration between Industrial Network Director (IND) and Identity Services Engine.

Background Information

When creating certificates in Cisco ISE for pxGrid use, server short hostnames cannot be entered into the ISE GUI as ISE allows only the FQDN or IP address.

To create certificates that include the hostname as well as FQDN, a certificate request file must be created outside of ISE. This can be done using OpenSSL to create a Certificate Signing Request (CSR) with Subject Alternative Name (SAN) field entries.

This document does not include comprehensive steps to enable pxGrid communication between the IND server and the ISE server. These steps can be used after pxGrid has been configured, and it has been confirmed that the server hostname is required. If this error is found in the ISE Profiler log files, communication requires the hostname certificate.

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

Steps for initial deployment of IND with pxGrid communication can be found at https://www.cisco.com/c/dam/en/us/td/docs/switches/ind/install/IND_PxGrid_Registration_Guide_Final.pdf

Applications Required

- Cisco Industrial Network Director (IND)
- Cisco Identity Services Engine (ISE)
- OpenSSL
  - In most modern Linux versions, as well as MacOS, the OpenSSL package is installed by default. If you find that commands are not available, please install OpenSSL using your operating system’s package management application.
  - Information about OpenSSL for Windows can be found at https://wiki.openssl.org/index.php/Binaries

Additional Information

For the purpose of this document, these details are used:

- IND Server hostname: rch-mas-ind
- FQDN: rch-mas-ind.cisco.com
- OpenSSL configuration: rch-mas-ind.req
- Certificate request file name: rch-mas-ind.csr
- Private key file name: rch-mas-ind.pem
- Certificate file name: rch-mas-ind.cer

Process Steps

Create the certificate CSR

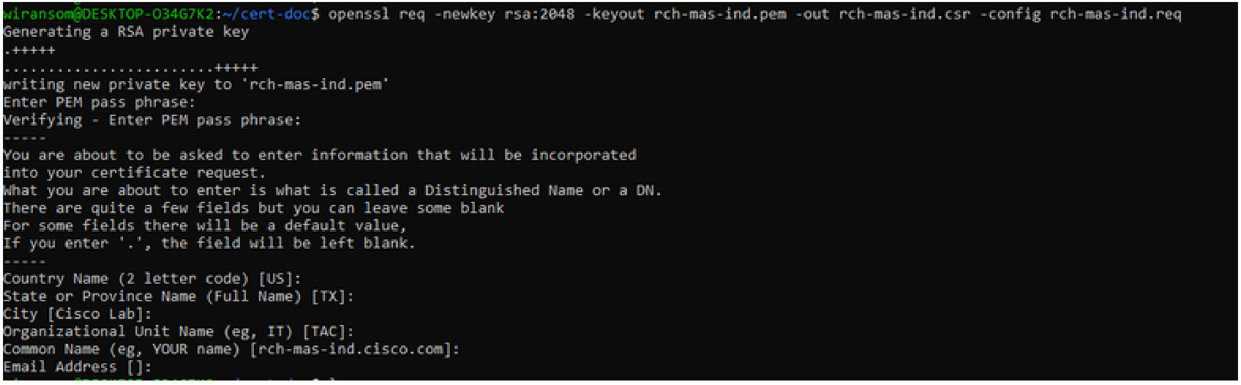
1. On a system with OpenSSL installed, create a request text file for OpenSSL options including SAN information.
   - Most “_default” fields are optional, as answers can be entered while running the OpenSSL command in step #2.
   - SAN details (DNS.1, DNS.2) are required and must include both the DNS short hostname, and server’s FQDN. Additional DNS names can be added if needed, using DNS.3, DNS.4, and so on.
   - Example request file text file:

```
[req]
distinguished_name = name
req_extensions = v3_req

[name]
countryName = Country Name (2 letter code)
countryName_default = US
stateOrProvinceName = State or Province Name (Full Name)
stateOrProvinceName_default = TX
localityName = City
localityName_default = Cisco Lab
organizationalUnitName = Organizational Unit Name (eg, IT)
organizationalUnitName_default = TAC
commonName = Common Name (eg, YOUR name)
commonName_max = 64
commonName_default = rch-mas-ind.cisco.com
emailAddress = Email Address
emailAddress_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. Use OpenSSL to create CSR with DNS short hostname in SAN field. Create a private key file in addition to CSR file.
   - Command:

```
openssl req -newkey rsa:2048 -keyout <server>.pem -out <server>.csr -config <server>.req
```

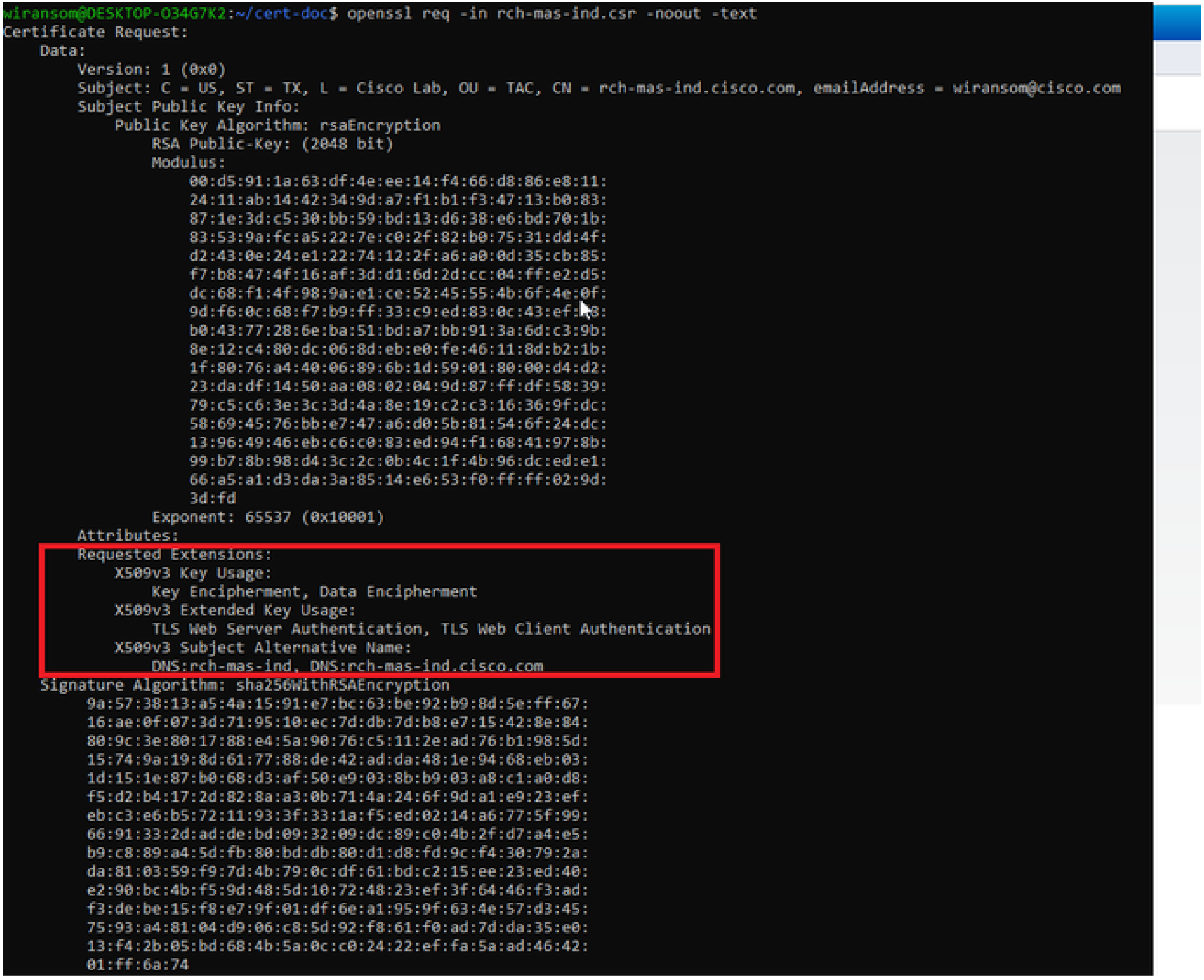
- When prompted, enter a password of your choice. Be sure to remember this password, as it is used in later steps.
- Enter a valid email address when prompted or leave the field blank and press <ENTER>.



```
wiransom@DESKTOP-O34G7K2:~/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 []:
```

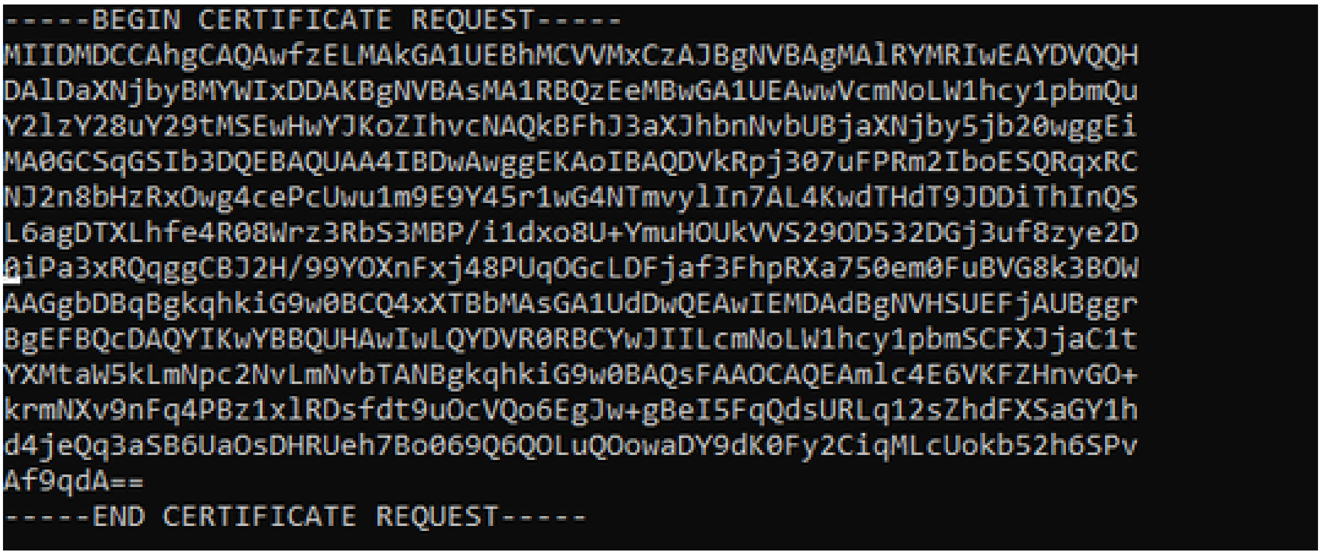
3. If desired, verify the CSR file information. For a SAN certificate, check for “x509v3 Subject Alternative Name” as highlighted in this screenshot.
    - Command line:

      openssl req -in <server>.csr -noout -text



```
wiransom@DESKTOP-O34G7K2:~/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:[illegible]8:
                    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 the CSR file in a text editor. For security reasons, the sample screenshot is incomplete and edited. The actual generated CSR file contains more lines.



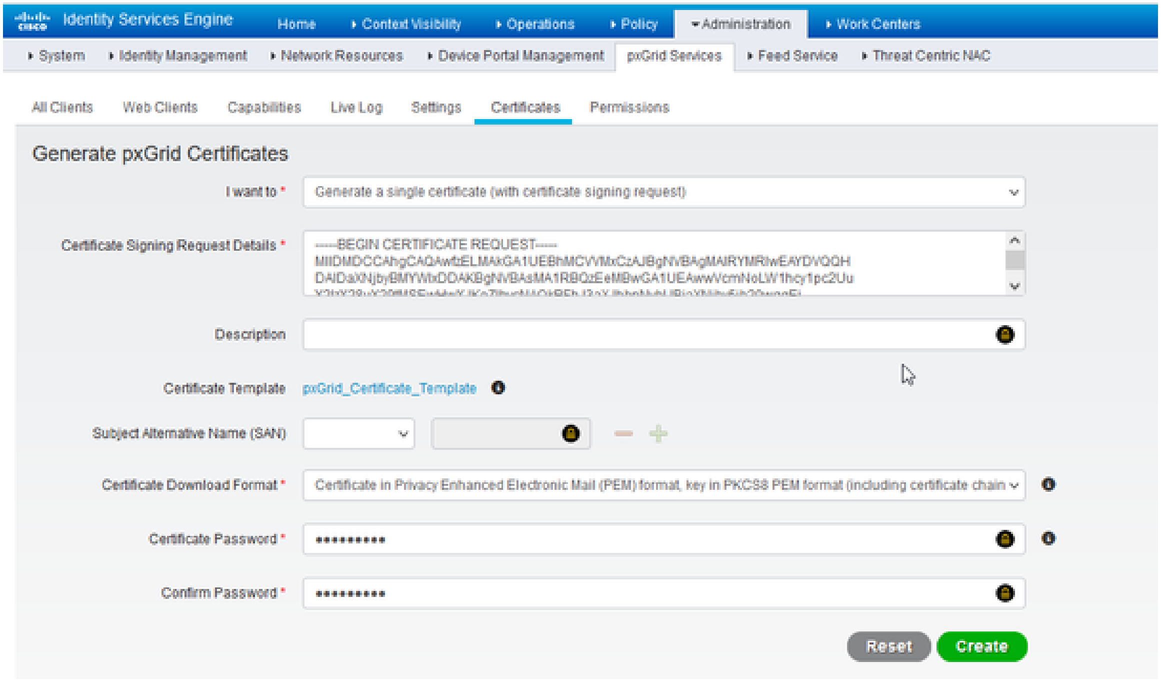
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDMDCCAhgCAQAwfzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAlRYMRIwEAYDVQQH
DAlDaXNjbyBMYWIxDDAKBgNVBAsMA1RBQzEeMBwGA1UEAwwVcmNoLW1hcy1pbmQu
Y2lzY28uY29tMSEwHwYJKoZIhvcNAQkBFhJ3aXJhbnNvbUBjaXNjby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVkRpj307uFPRm2IboESQRqxRC
NJ2n8bHzRxOwg4cePcUwu1m9E9Y45r1wG4NTmvylIn7AL4KwdTHdT9JDDiThInQS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

5. Copy the private key file (<server>.pem) to your PC as it is used in a later step.

Use Cisco ISE to generate a certificate, using the created CSR file information

Within the ISE GUI:

1. Remove the existing pxGrid client.
    - Navigate to Administration > pxGrid Services > All Clients.
    - Find and select the existing client hostname, if listed,
    - If found and selected, click the Delete button, and choose “Delete Selected.” Confirm as needed.
2. Create the new certificate.
    - Click on the Certificates tab on the pxGrid services page.
    - Choose the options:
        - “I want to”:
            - “Generate a single certificate (with certificate signing request)”
        - “Certificate Signing Request Details:
            - Copy/paste the CSR details from the text editor. Be sure to include the BEGIN and END lines.
        - “Certificate Download Format”
            - “Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format.”
        - Enter a certificate password and confirm it.
        - Click the Create button.



Generate pxGrid Certificates

I want to * Generate a single certificate (with certificate signing request)

Certificate Signing Request Details *

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDMDCCAhgCAQAwfzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAlRYMRIwEAYDVQQH
DAlDaXNjbyBMYWIxDDAKBgNVBAsMA1RBQzEeMBwGA1UEAwwVcmNoLW1hcy1pc2Uu
```

Description

Certificate Template pxGrid_Certificate_Template

Subject Alternative Name (SAN)

Certificate Download Format * Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain

Certificate Password * •••••••••

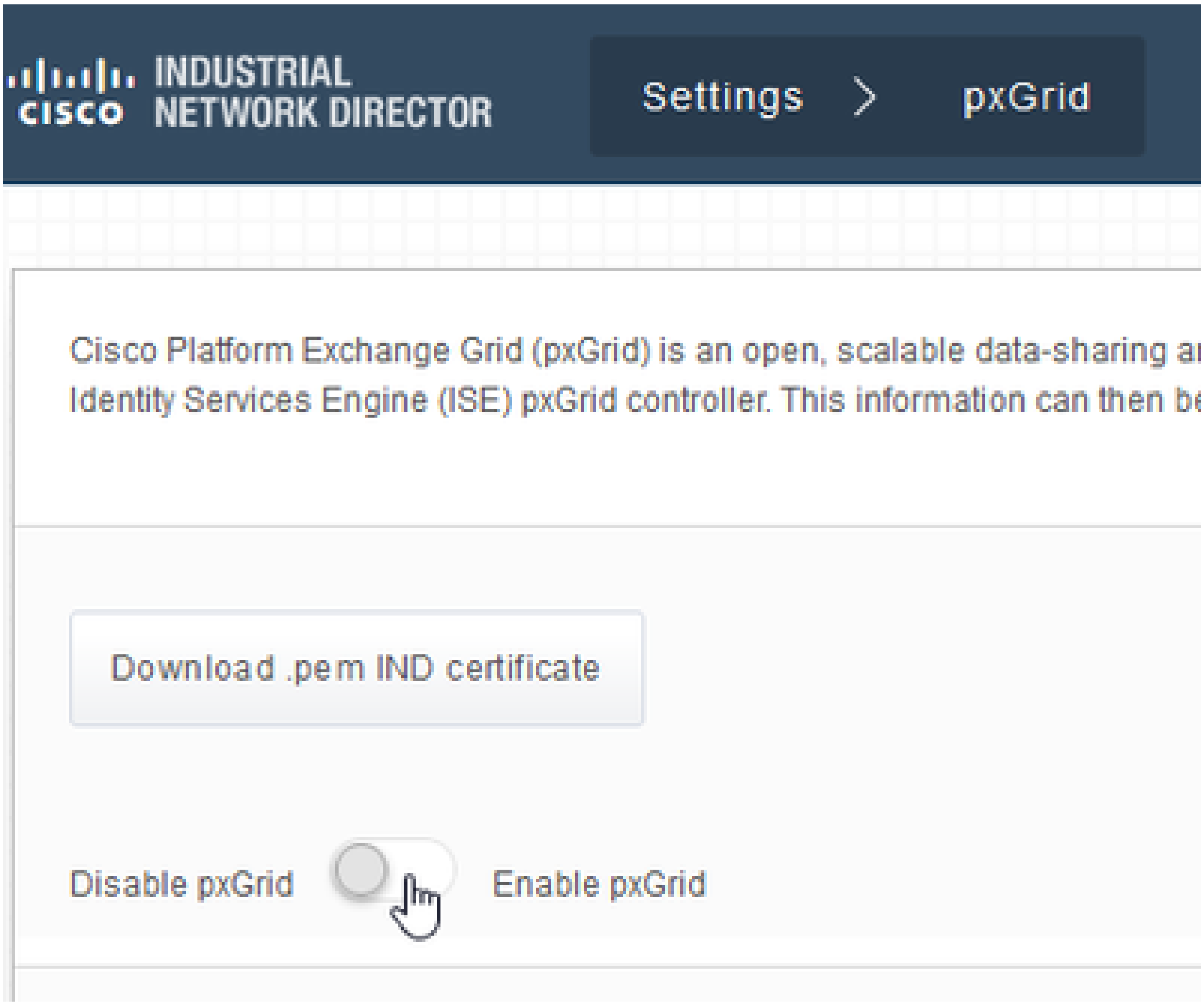
Confirm Password * •••••••••

- This creates and downloads a ZIP file that contains the certificate file as well as additional files for the certificate chain. Open the ZIP and extract the certificate.
  - The filename is normally <IND server fqdn>.cer
  - In some versions of ISE, the filename is <IND fqdn>_<IND short name>.cer

Import the new certificate into the IND server, and enable it for pxGrid use

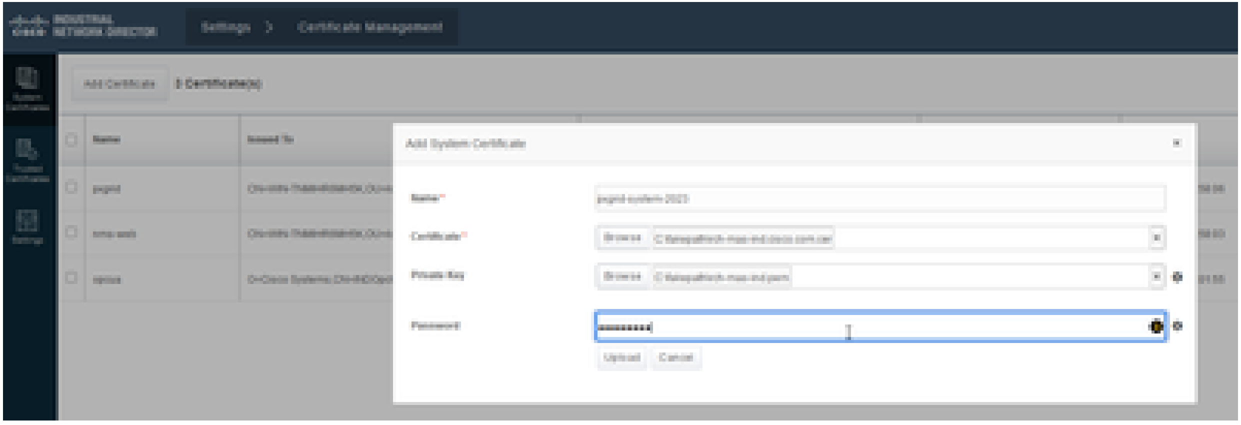
Within the IND GUI:

1. Disable the pxGrid service, so the new certificate can be imported and set as the active certificate.
   - Navigate to Settings > pxGrid.
   - Click to disable pxGrid.



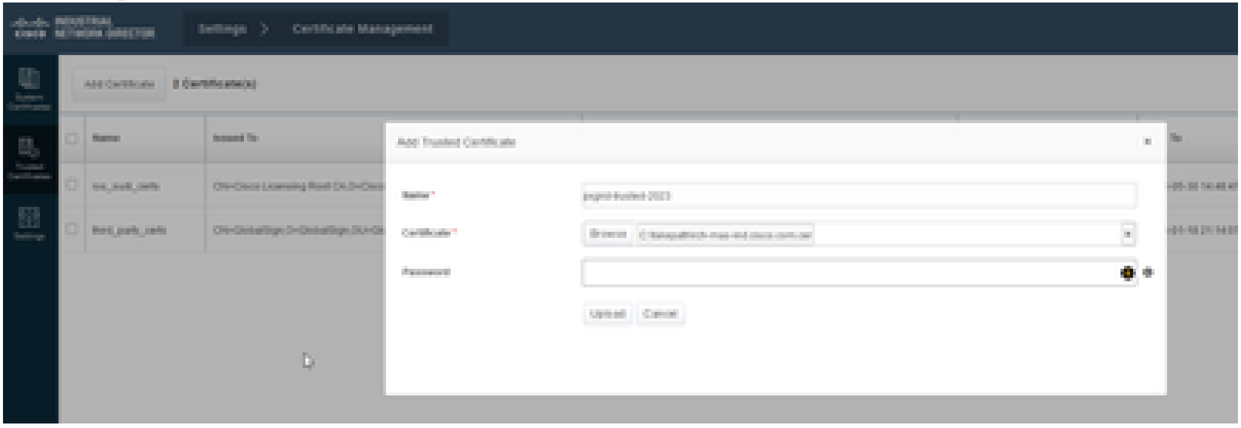
Cisco Platform Exchange Grid (pxGrid) is an open, scalable data-sharing a
Identity Services Engine (ISE) pxGrid controller. This information can then b

2. Import the new certificate into System Certificates.
    - Navigate to Settings > Certificate Management.
    - Click onto “System Certificates”
    - Click “Add Certificate.”
    - Enter a certificate name.
    - Click “Browse” to the left of “Certificate”, and locate the new certificate file.
    - Click “Browse” to the left of “Certificate”, and locate the private key saved when creating the CSR.
    - Enter the password previously used when creating the private key and CSR with OpenSSL.
    - Click “Upload.”



3. Import the new certificate as a trusted certificate.
    - Navigate to Settings > Certificate Management, click on “Trusted Certificates.”
    - Click “Add Certificate.”

- Enter a certificate name; this must be a different name than the one used on System Certificates.
- Click “Browse” to the left of “Certificate” and locate the new certificate file.
- The password field can be left empty.
- Click “Upload.”

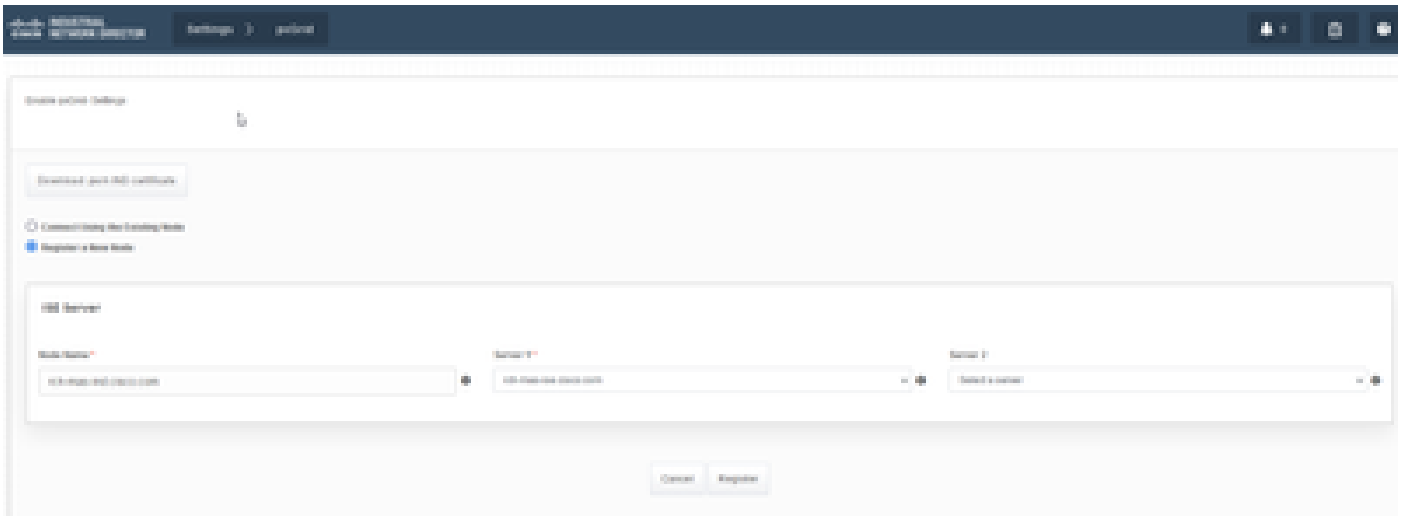


4. Set pxGrid to use the new certificate.
   - Navigate to Settings > Certificate Management, click on “Settings.”
   - If not already done, select “CA Certificate” under “pxGrid.”
   - Select the system certificate name created during the certificate import.
   - Click Save.

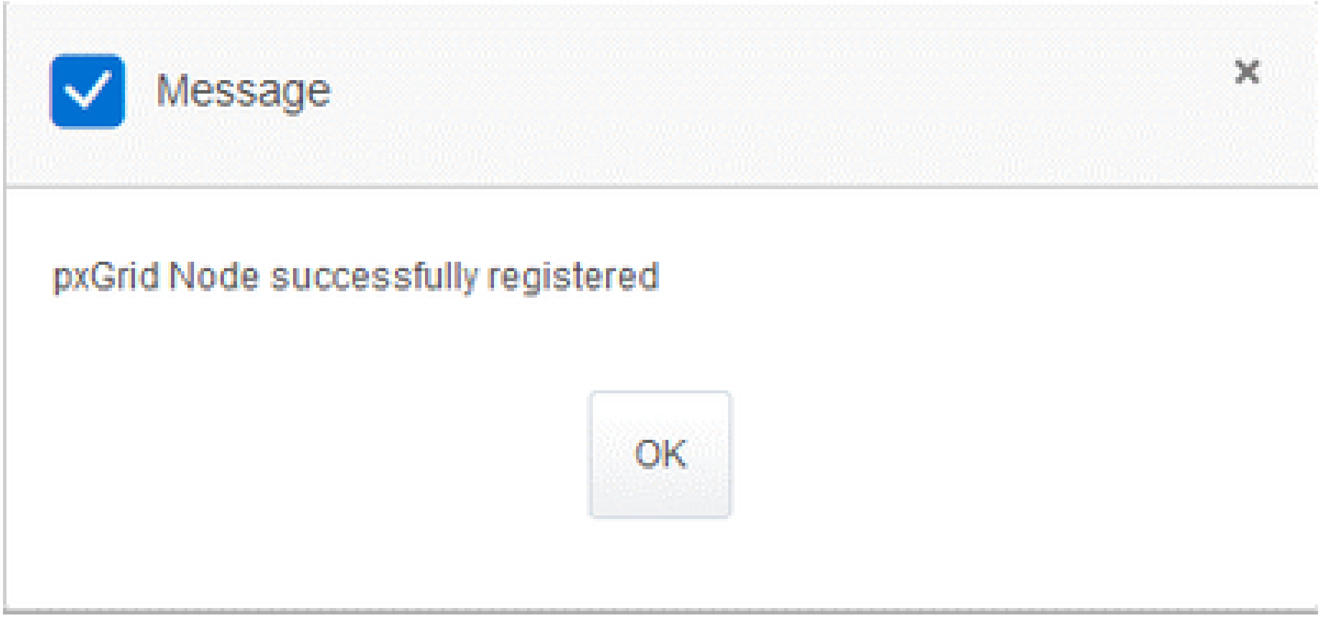
Enable and register pxGrid with the ISE server

Within the IND GUI:

1. Navigate to Settings > pxGrid.
2. Click the slider to Enable pxGrid.
3. If this is not the first time registering pxGrid with ISE on this IND server, choose “Connect Using the Existing Node.” The IND node and ISE server information automatically populates.
4. To register a new IND server to use pxGrid, if needed, choose “Register a New Node”. Enter the IND node name and choose ISE servers as needed.
   - If the ISE server is not listed within the dropdown options for Server 1 or Server 2, it can be added as a new pxGrid server using Settings > Policy Server



5. Click Register. A confirmation is shown on-screen.

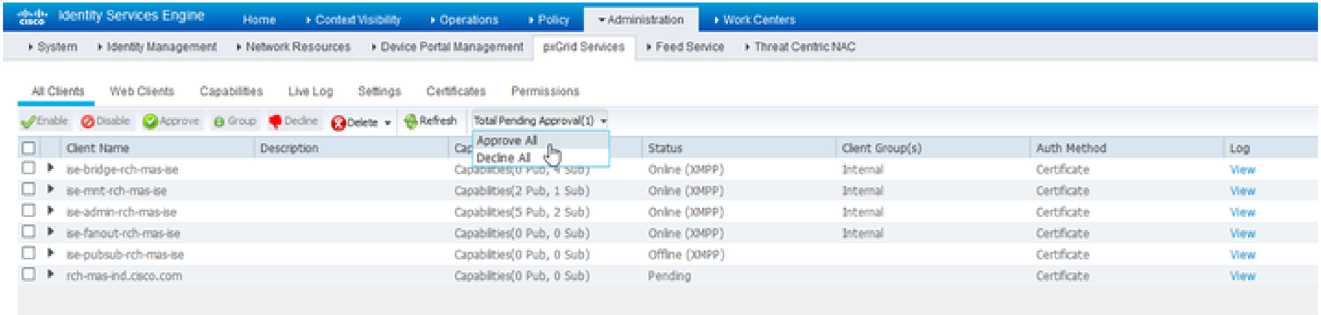


pxGrid Node successfully registered

Approve registration request in ISE server

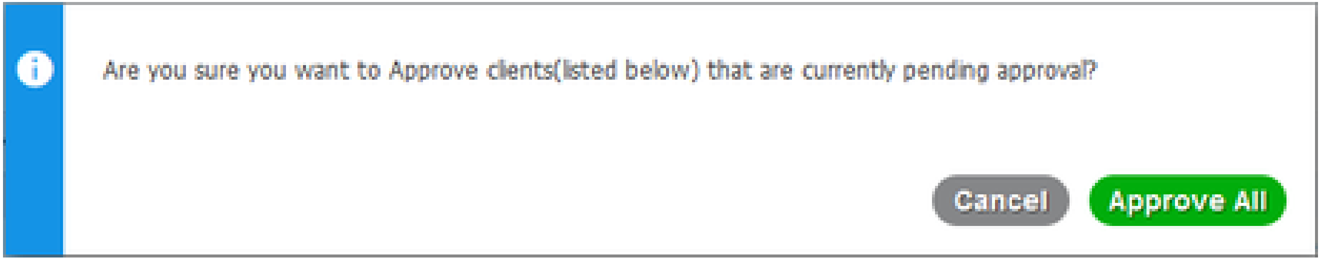
Within the ISE GUI:

1. Navigate to Administration > pxGrid Services > All Clients. A request Pending Approval shows as “Total Pending Approval(1).”
2. Click on “Total Pending Approval(1)” and select “Approve All.”



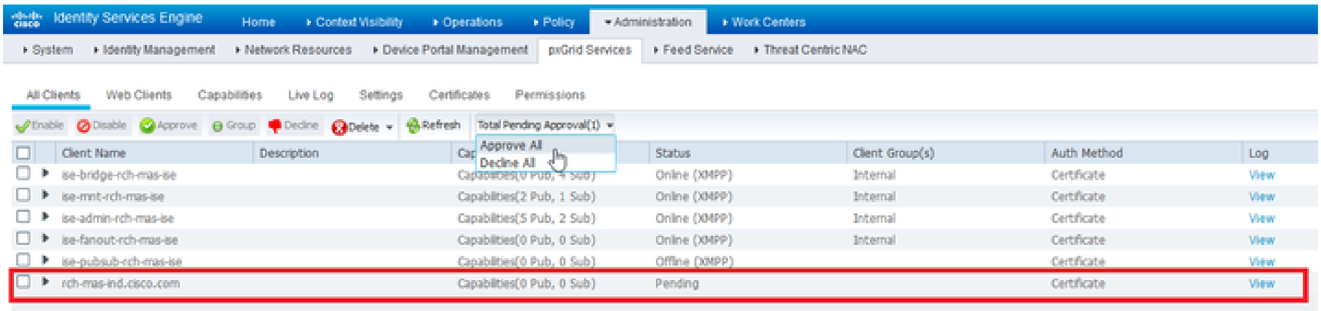
Client Name	Description	Cap	Status	Client Group(s)	Auth Method	Log
ise-bridge-rch-mas-ise		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View
ise-mnt-rch-mas-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View
ise-admin-rch-mas-ise		Capabilities(5 Pub, 2 Sub)	Online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

3. On the pop-up that appears, click “Approve All.”



Are you sure you want to Approve clients(listed below) that are currently pending approval?

4. The IND server shows as a client, as shown here.

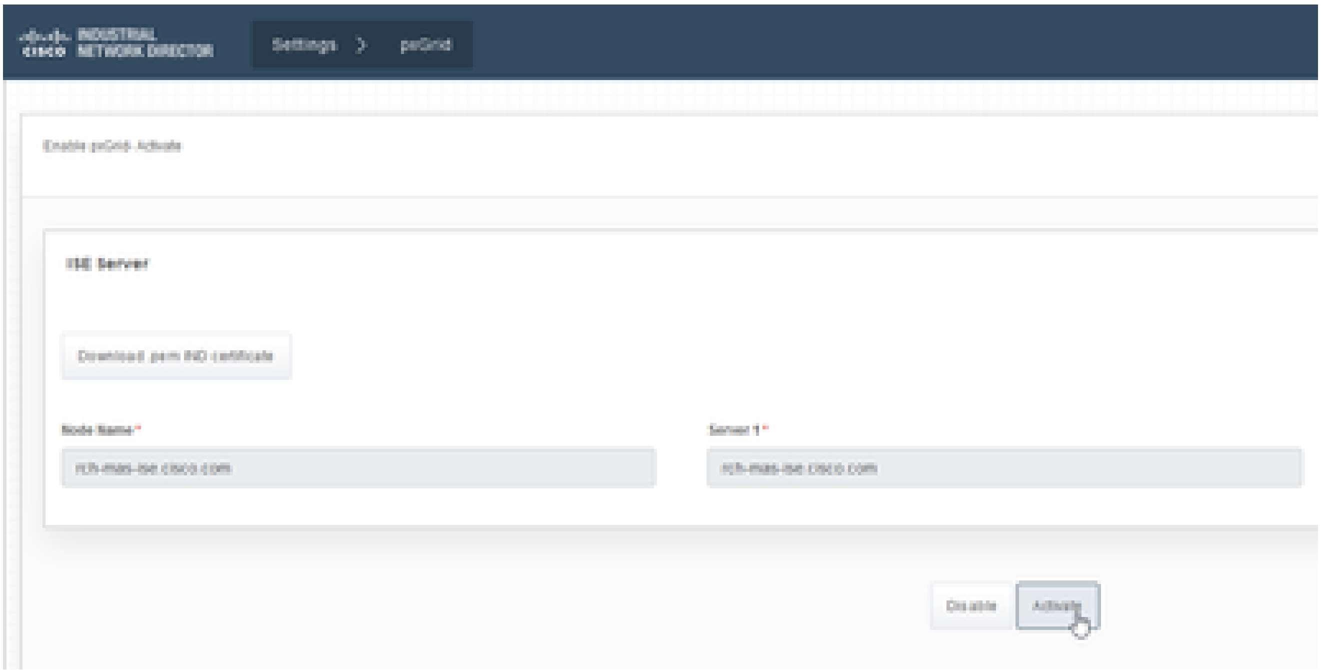


Client Name	Description	Cap	Status	Client Group(s)	Auth Method	Log
ise-bridge-rch-mas-ise		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View
ise-mnt-rch-mas-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View
ise-admin-rch-mas-ise		Capabilities(5 Pub, 2 Sub)	Online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

Activate pxGrid service in IND server

Within the IND GUI:

1. Navigate to Settings > pxGrid.
2. Click on “Activate.”



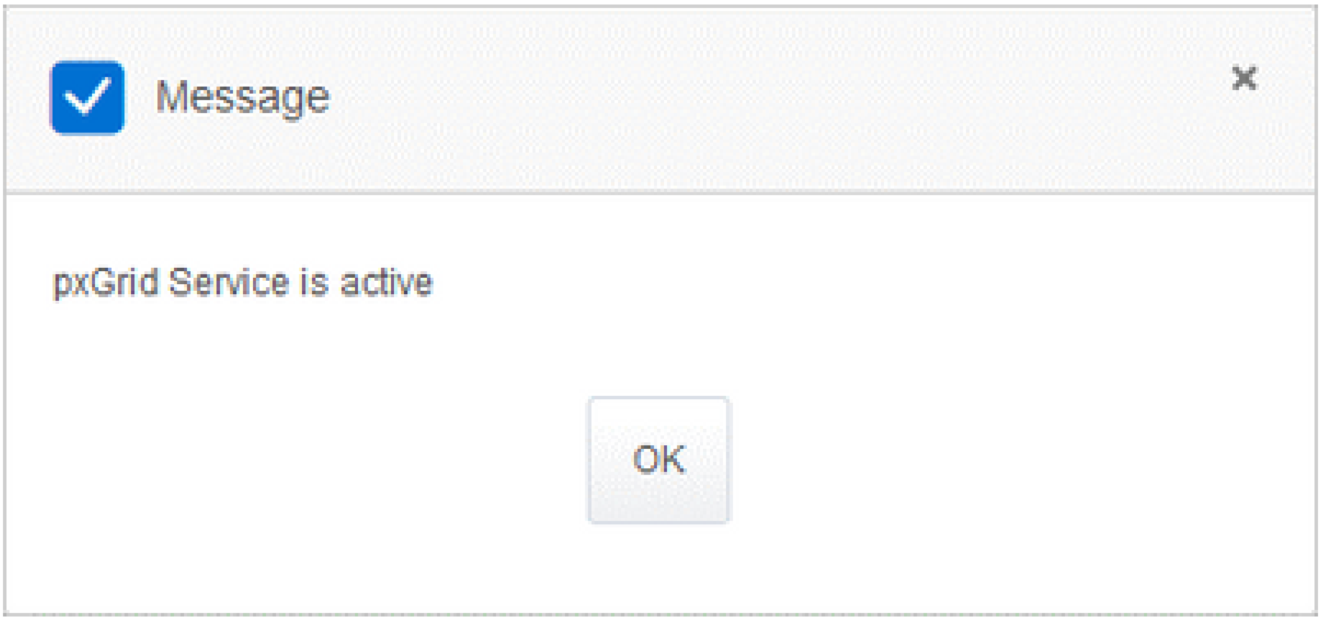
Enable pxGrid- Activate

ISE Server

Node Name*: rch-mas-ise.cisco.com

Server 1*: rch-mas-ise.cisco.com

3. A confirmation is shown on-screen.



pxGrid Service is active