Erstellen von SAN-Zertifikaten für die Integration von IND und ISE pxGrid mit OpenSSL

Inhalt

Einleitung

Dieses Dokument beschreibt die Erstellung von SAN-Zertifikaten für die pxGrid-Integration zwischen Industrial Network Director (IND) und Identity Services Engine.

Hintergrundinformationen

Beim Erstellen von Zertifikaten in der Cisco ISE zur Verwendung mit pxGrid können kurze Hostnamen nicht in die ISE-GUI eingegeben werden, da die ISE nur den FQDN oder die IP-Adresse zulässt.

Zum Erstellen von Zertifikaten, die sowohl den Hostnamen als auch den FQDN enthalten, muss eine Zertifikatsanforderungsdatei außerhalb von ISE erstellt werden. Dies kann mithilfe von OpenSSL erfolgen, um eine Zertifikatssignaturanforderung (CSR) mit SAN-Feldeinträgen (Subject Alternative Name) zu erstellen.

Dieses Dokument enthält keine umfassenden Schritte, um die pxGrid-Kommunikation zwischen dem IND-Server und dem ISE-Server zu ermöglichen. Diese Schritte können verwendet werden, nachdem pxGrid konfiguriert wurde und bestätigt wurde, dass der Server-Hostname erforderlich ist. Wenn dieser Fehler in den Protokolldateien von ISE Profiler gefunden wird, erfordert die Kommunikation das Hostnamenzertifikat.

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

Schritte für die Erstbereitstellung von IND mit pxGrid-Kommunikation finden Sie unter https://www.cisco.com/c/dam/en/us/td/docs/switches/ind/install/IND_PxGrid_Registration_Guide_Final.pdf

Erforderliche Anwendungen

- Cisco Industrial Network Director (IND)
- Cisco Identity Services Engine (ISE)
- OpenSSL
    - In den meisten modernen Linux-Versionen, sowie MacOS, ist das OpenSSL-Paket standardmäßig installiert. Wenn Sie feststellen, dass keine Befehle verfügbar sind,

installieren Sie OpenSSL mithilfe der Paketverwaltungsanwendung Ihres Betriebssystems.
    - Informationen zu OpenSSL für Windows finden Sie unter https://wiki.openssl.org/index.php/Binaries

Zusätzliche Informationen

Für die Zwecke dieses Dokuments werden folgende Details verwendet:

- IND Server-Hostname: rch-mas-ind
- FQDN: rch-mas-ind.cisco.com
- OpenSSL-Konfiguration: rch-mas-ind.req
- Name der Zertifikatsanforderungsdatei: rch-mas-ind.csr
- Name der privaten Schlüsseldatei: rch-mas-ind.pem
- Name der Zertifikatsdatei: rch-mas-ind.cer

Prozessschritte

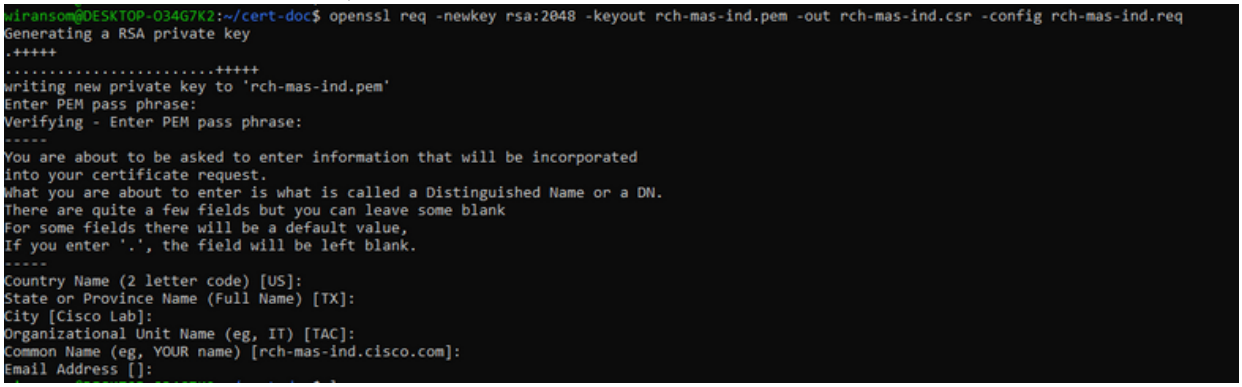
Zertifikat-CSR erstellen

1. Erstellen Sie auf einem System, auf dem OpenSSL installiert ist, eine Anforderungstextdatei für OpenSSL-Optionen, einschließlich SAN-Informationen.
    - Die meisten "_default"-Felder sind optional, da Antworten eingegeben werden können, während der OpenSSL-Befehl in Schritt #2 ausgeführt wird.
    - SAN-Details (DNS.1, DNS.2) sind erforderlich und müssen sowohl den kurzen DNS-Hostnamen als auch den FQDN des Servers enthalten. Bei Bedarf können weitere DNS-Namen hinzugefügt werden, z. B. DNS.3, DNS.4 usw.
    - Beispiel für eine Anforderungsdatei-Textdatei:

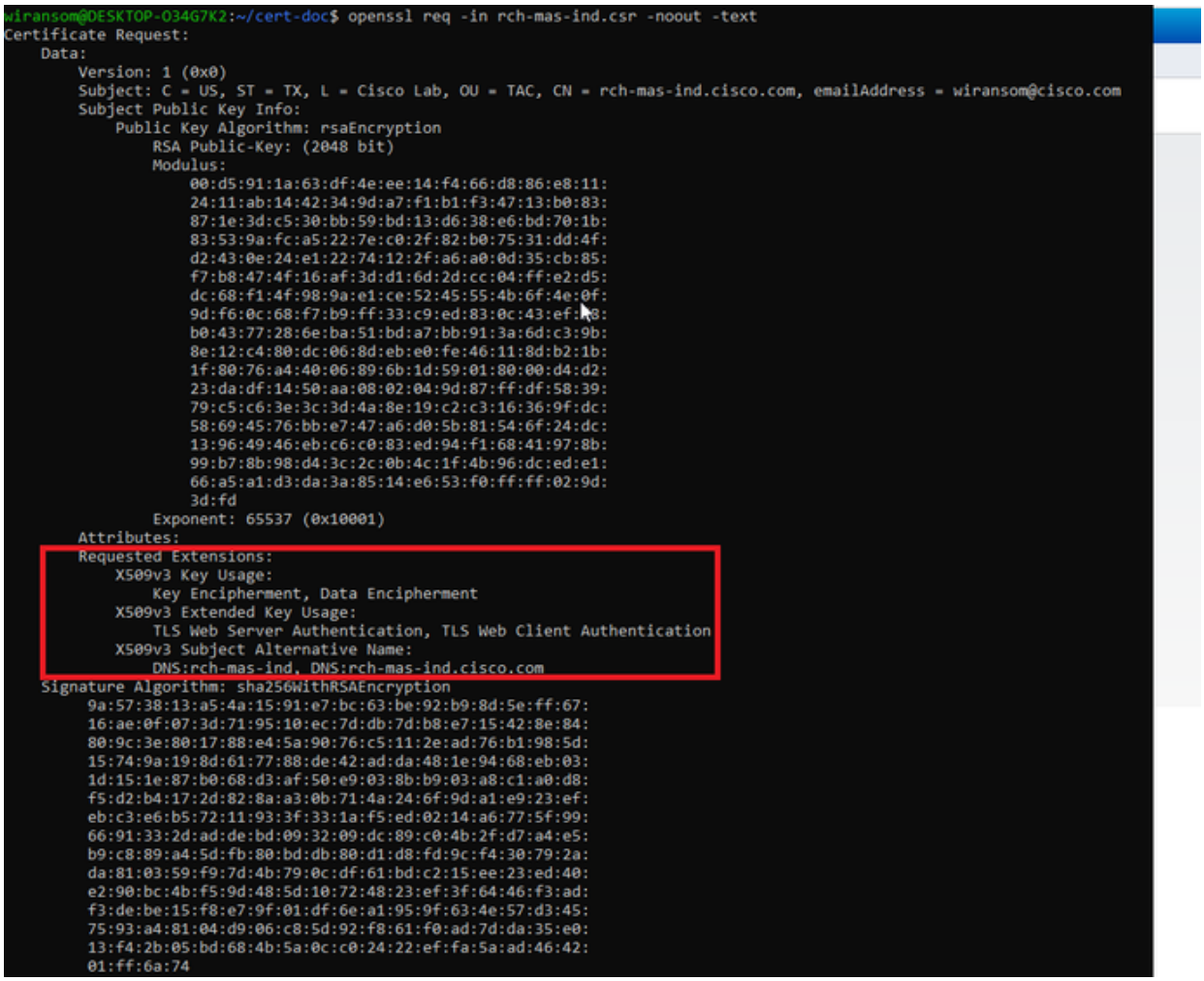
```
[Anforderung]
Distinguished_Name = Name
req_extensions = v3_req

[name]
countryName = Ländername (Code aus 2 Buchstaben)
countryName_default = USA
stateOrProvinceName = Bundesland/Kanton (vollständiger Name)
stateOrProvinceName_default = TX
localityName = Stadt
localityName_default = Cisco Lab
organizationalUnitName = Name der Organisationseinheit (z. B. IT)
organizationalUnitName_default = TAC
commonName = Allgemeiner Name (z. B. IHR Name)
commonName_max = 64
commonName_default = rch-mas-ind.cisco.com
```

```
emailAddress = E-Mail-Adresse
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. Verwenden Sie OpenSSL, um einen CSR mit dem kurzen DNS-Hostnamen im SAN-Feld zu erstellen. Erstellen Sie zusätzlich zur CSR-Datei eine private Schlüsseldatei.
   - Command:
     openssl req -newkey rsa:2048 -keyout <Server>.pem -out <Server>.csr -config <Server>.req
   - Geben Sie auf Aufforderung das gewünschte Kennwort ein. Vergessen Sie nicht, sich dieses Kennwort zu merken, da es in späteren Schritten verwendet wird.
   - Geben Sie eine gültige E-Mail-Adresse ein, wenn Sie dazu aufgefordert werden, oder lassen Sie das Feld leer, und drücken Sie die EINGABETASTE.



3. Überprüfen Sie bei Bedarf die Informationen in der CSR-Datei. Überprüfen Sie für ein SAN-Zertifikat "x509v3 Subject Alternative Name" (Alternativer Name des x509v3-Betreffs), wie in diesem Screenshot hervorgehoben.
   - Befehlszeile:
     openssl req -in <Server>.csr -noout -text



4. Öffnen Sie die CSR-Datei in einem Texteditor. Aus Sicherheitsgründen ist der Screenshot unvollständig und editiert. Die tatsächlich erzeugte CSR-Datei enthält mehr Zeilen.

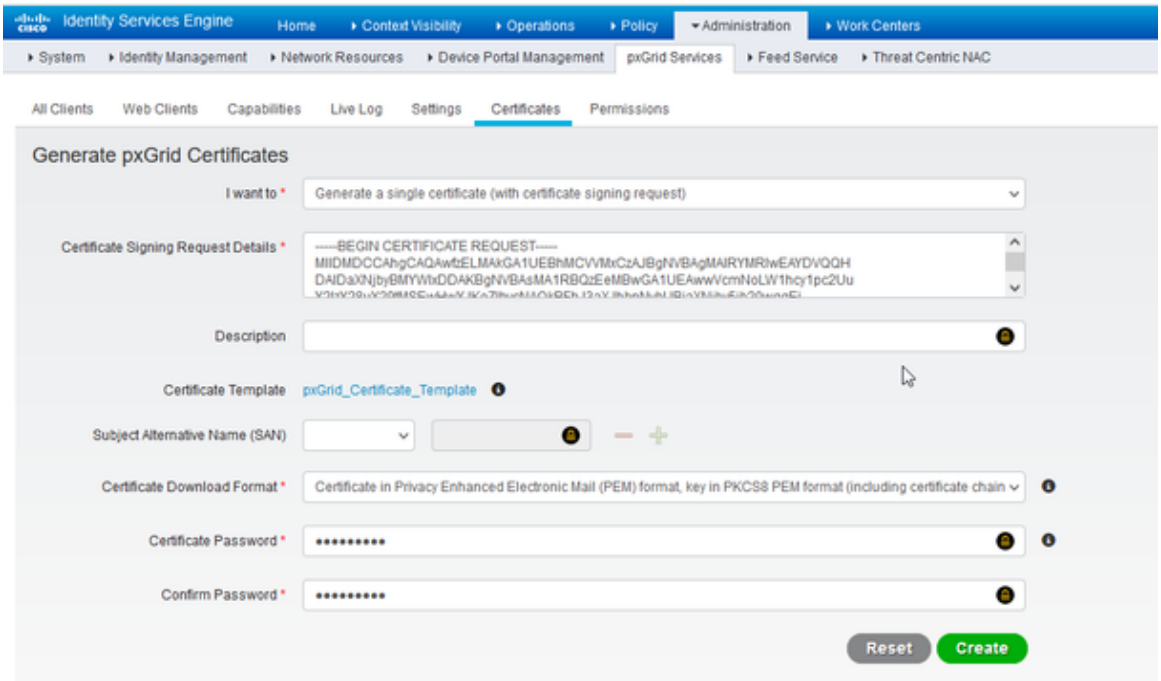
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDMDCCAhgCAQAwfzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAlRYMRIwEAYDVQQH
DAlDaXNjbyBMYWIxDDAKBgNVBAsMA1RBQzEeMBwGA1UEAwwVcmNoLW1hcy1pbmQu
Y2lzY28uY29tMSEwHwYJKoZIhvcNAQkBFhJ3aXJhbnNvbUBjaXNjby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVkRpj307uFPRm2IboESQRqxRC
NJ2n8bHzRxOwg4cePcUwu1m9E9Y45r1wG4NTmvylIn7AL4KwdTHdT9JDDiThInQS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

5. Kopieren Sie die Datei mit dem privaten Schlüssel (<server>.pem) auf Ihren PC, wie er in einem späteren Schritt verwendet wird.

Erstellung eines Zertifikats mit der Cisco ISE anhand der erstellten CSR-Dateiinformationen

In der ISE-GUI:

1. Entfernen Sie den vorhandenen pxGrid-Client.
    - Navigieren Sie zu Administration > pxGrid Services > All Clients.
    - Suchen Sie den vorhandenen Client-Hostnamen, und wählen Sie ihn aus (falls aufgeführt).
    - Wenn Sie gefunden und ausgewählt wurden, klicken Sie auf die Schaltfläche "Löschen", und wählen Sie "Auswahl löschen". Bei Bedarf bestätigen.
2. Neues Zertifikat erstellen.
    - Klicken Sie auf der Seite pxGrid-Dienste auf die Registerkarte Zertifikate.
    - Wählen Sie die Optionen aus:
        - "Ich möchte":
            - "Einzelnes Zertifikat generieren (mit Anforderung zum Signieren des Zertifikats)"
        - "Details der Zertifikatsignierungsanforderung:
            - Kopieren Sie die CSR-Details aus dem Texteditor, und fügen Sie sie ein. Achten Sie darauf, die BEGIN- und END-Zeilen einzuschließen.
        - "Format des Zertifikatsdownloads"
            - "Zertifikat im Privacy Enhanced Electronic Mail (PEM)-Format, Schlüssel im PKCS8 PEM-Format."
        - Geben Sie ein Zertifikatskennwort ein, und bestätigen Sie es.
        - Klicken Sie auf Erstellen.



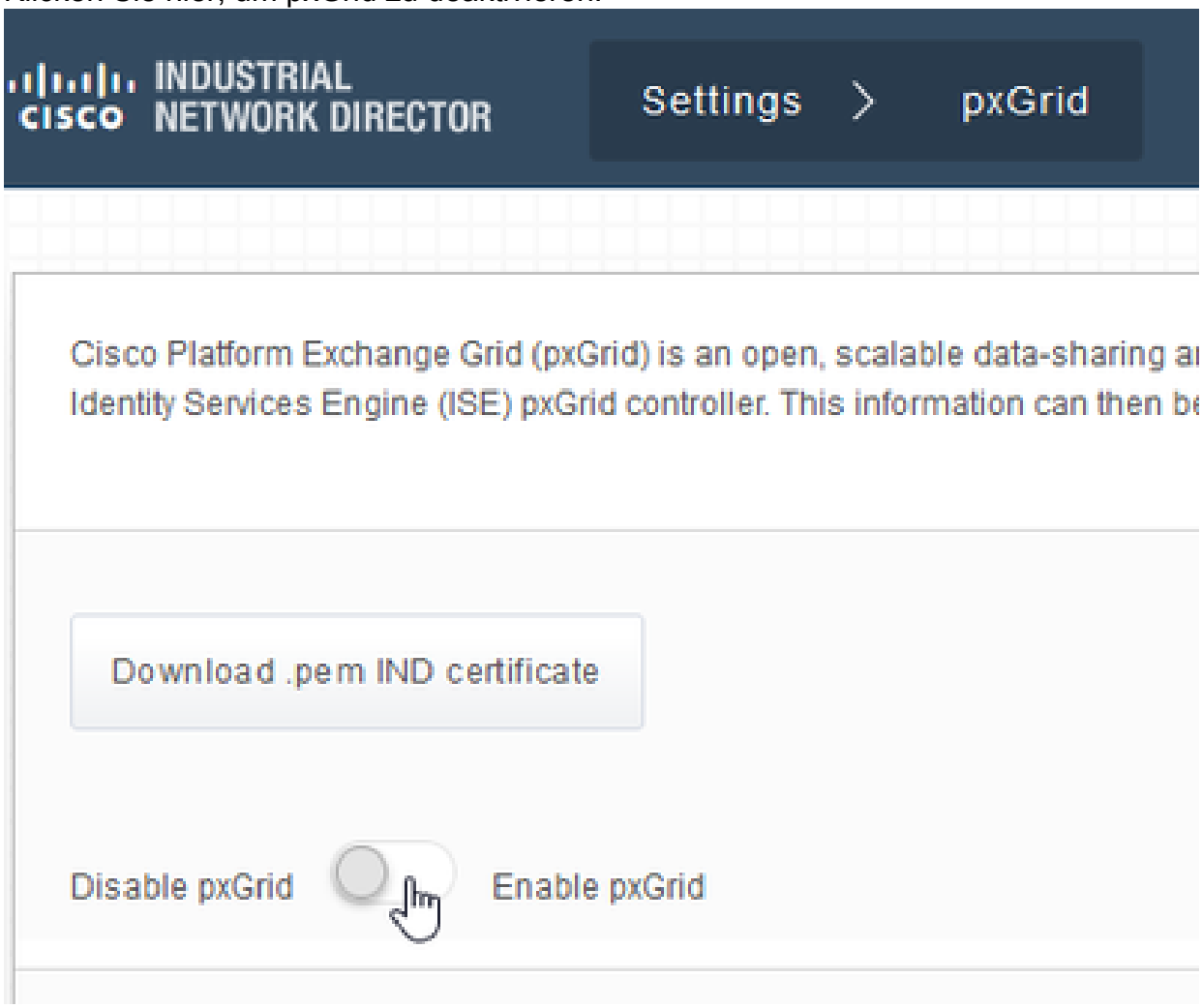
        - Dadurch wird eine ZIP-Datei erstellt und heruntergeladen, die die Zertifikatsdatei sowie zusätzliche Dateien für die Zertifikatskette enthält. Öffnen Sie die ZIP-Datei, und extrahieren Sie das Zertifikat.
            - Der Dateiname lautet normalerweise <IND server fqdn>.cer
            - In einigen Versionen der ISE lautet der Dateiname <IND fqdn>_<IND short name>.cer

Importieren Sie das neue Zertifikat in den IND-Server, und aktivieren Sie es für die

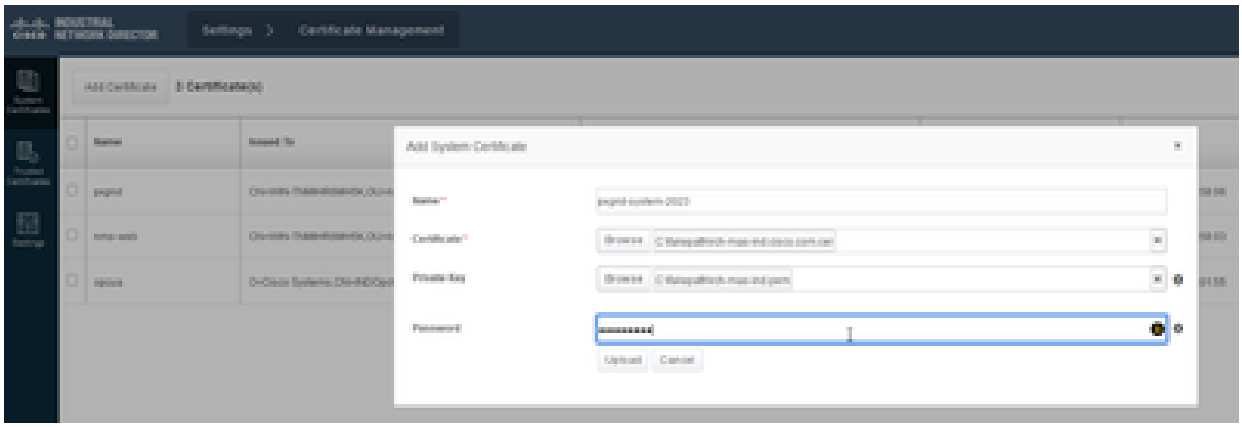
pxGrid-Verwendung.

In der IND-GUI:

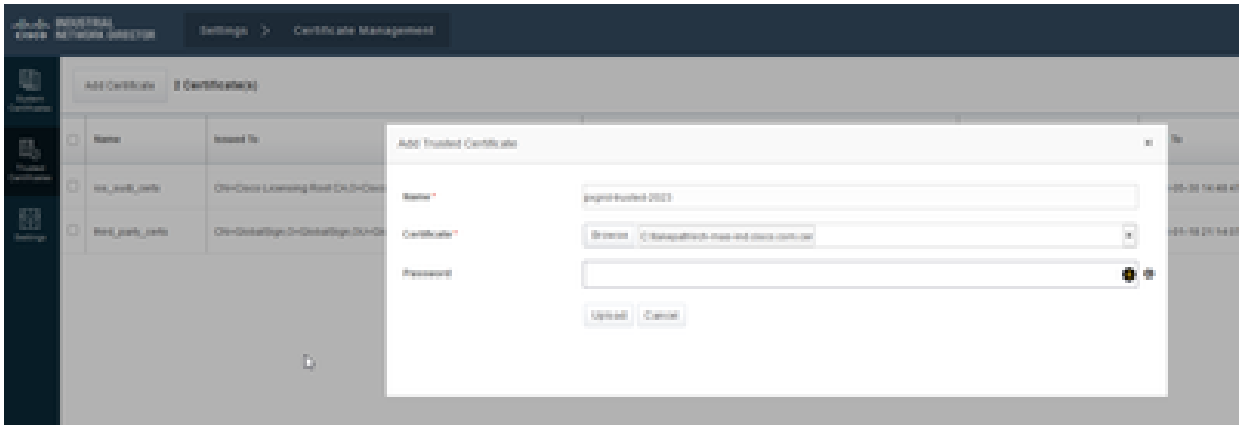
1. Deaktivieren Sie den pxGrid-Dienst, damit das neue Zertifikat importiert und als aktives Zertifikat festgelegt werden kann.
    - Navigieren Sie zu Einstellungen > pxGrid.
    - Klicken Sie hier, um pxGrid zu deaktivieren.



2. Importieren Sie das neue Zertifikat in Systemzertifikate.
    - Navigieren Sie zu Einstellungen > Zertifikatsverwaltung.
    - Klicken Sie auf "Systemzertifikate"
    - Klicken Sie auf "Zertifikat hinzufügen".
    - Geben Sie einen Zertifikatsnamen ein.
    - Klicken Sie links neben "Zertifikat" auf "Durchsuchen", und suchen Sie die neue Zertifikatsdatei.
    - Klicken Sie links neben "Zertifikat" auf "Durchsuchen", und suchen Sie nach dem privaten Schlüssel, der beim Erstellen der CSR-Anfrage gespeichert wurde.
    - Geben Sie das Kennwort ein, das Sie zuvor beim Erstellen des privaten Schlüssels und des CSR mit OpenSSL verwendet haben.
    - Klicken Sie auf "Hochladen".



3. Importieren Sie das neue Zertifikat als vertrauenswürdiges Zertifikat.
    - Navigieren Sie zu Einstellungen > Zertifikatsverwaltung, und klicken Sie auf "Vertrauenswürdige Zertifikate".
    - Klicken Sie auf "Zertifikat hinzufügen".
    - Geben Sie einen Zertifikatsnamen ein. Dabei muss es sich um einen anderen Namen als den in den Systemzertifikaten verwendeten handeln.
    - Klicken Sie links neben "Zertifikat" auf "Durchsuchen", und suchen Sie die neue Zertifikatsdatei.
    - Das Kennwortfeld kann leer gelassen werden.
    - Klicken Sie auf "Hochladen".



4. Legen Sie pxGrid so fest, dass das neue Zertifikat verwendet wird.
    - Navigieren Sie zu Einstellungen > Zertifikatsverwaltung, und klicken Sie auf "Einstellungen".
    - Falls noch nicht geschehen, wählen Sie "CA Certificate" unter "pxGrid".
    - Wählen Sie den Systemzertifikatnamen aus, der während des Zertifikatimports erstellt wurde.
    - Klicken Sie auf Speichern.

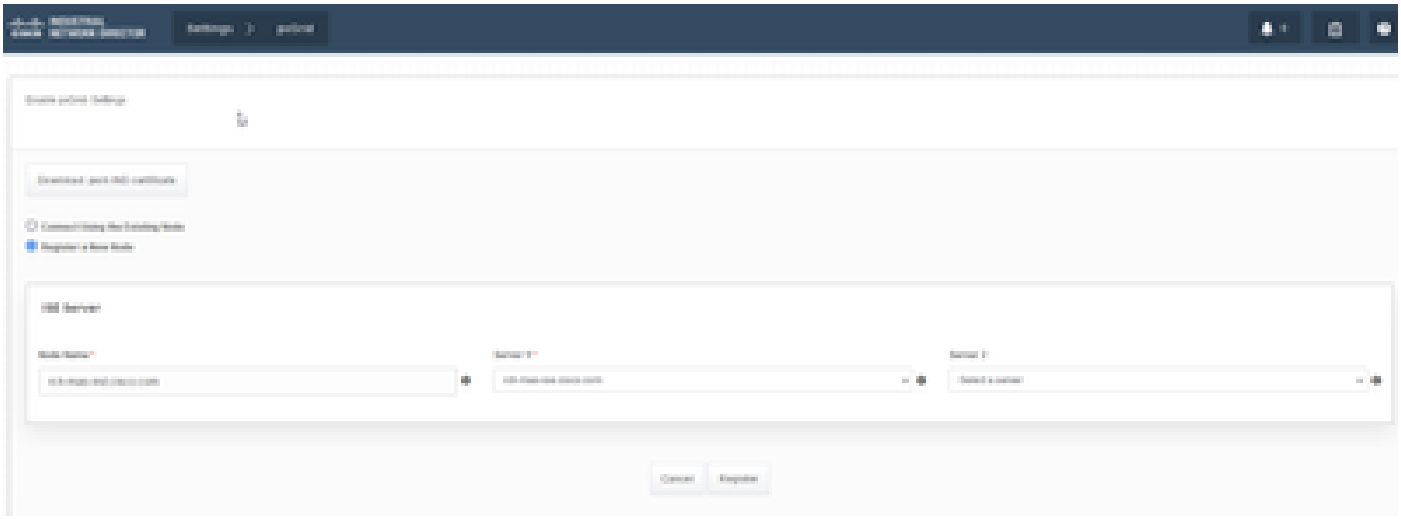
Aktivieren und Registrieren von pxGrid beim ISE-Server

In der IND-GUI:

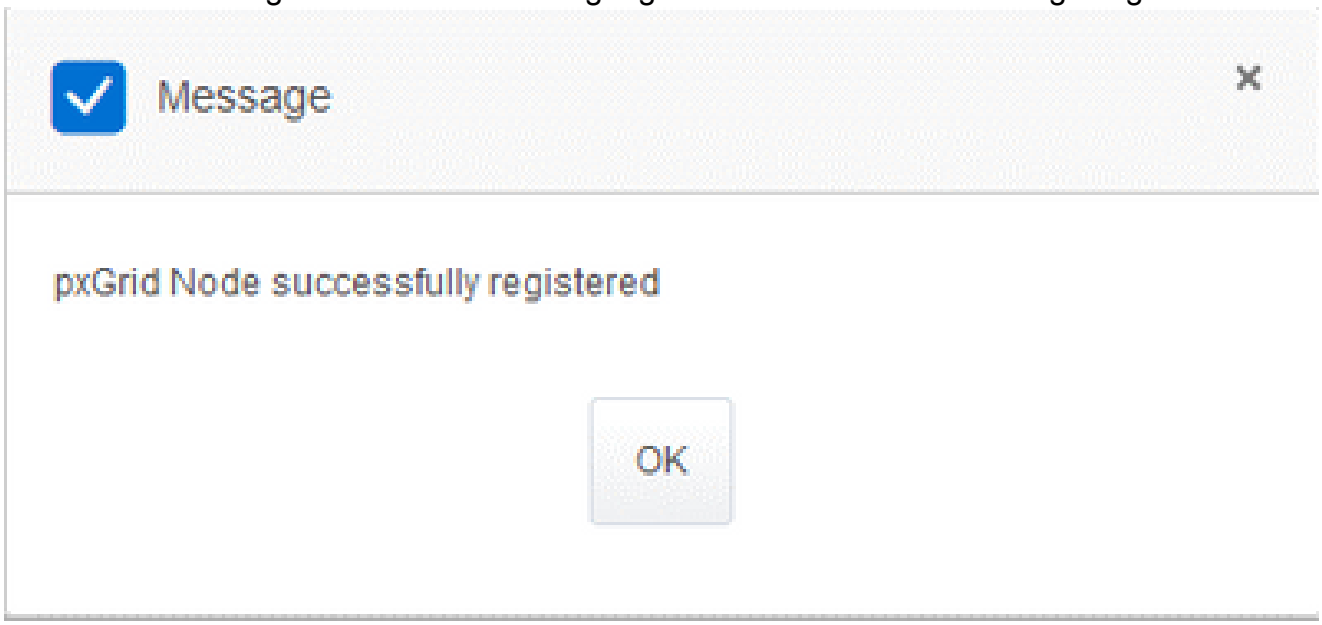
1. Navigieren Sie zu Einstellungen > pxGrid.
2. Klicken Sie auf den Schieberegler für pxGrid aktivieren.
3. Wenn Sie pxGrid nicht zum ersten Mal mit der ISE auf diesem IND-Server registrieren,

wählen Sie "Über den vorhandenen Knoten verbinden". Die IND-Knoten- und ISE-Serverinformationen werden automatisch ausgefüllt.

4. Um einen neuen IND-Server zu registrieren, um pxGrid zu verwenden, wählen Sie bei Bedarf "Einen neuen Knoten registrieren". Geben Sie den IND-Knotennamen ein, und wählen Sie bei Bedarf ISE-Server aus.
    - Wenn der ISE-Server nicht in den Dropdown-Optionen für Server 1 oder Server 2 aufgeführt ist, kann er mithilfe von Einstellungen > Policy Server als neuer pxGrid-Server hinzugefügt werden.



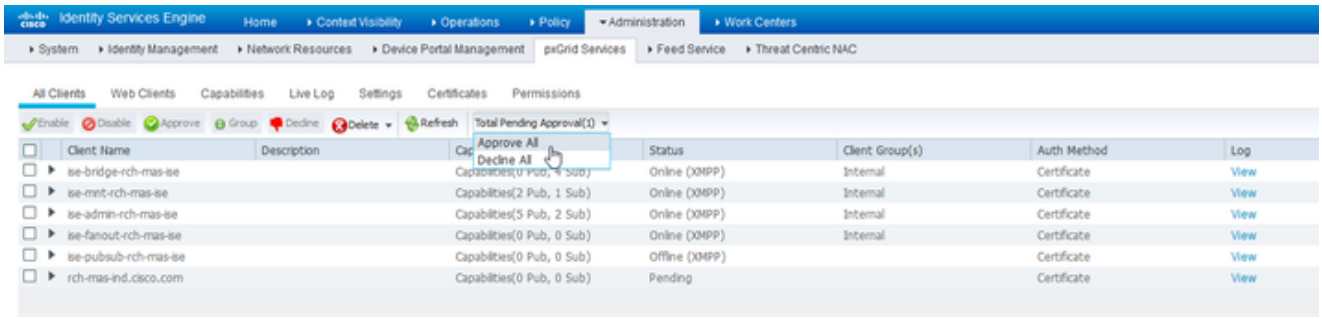
5. Klicken Sie auf Registrieren. Eine Bestätigung wird auf dem Bildschirm angezeigt.



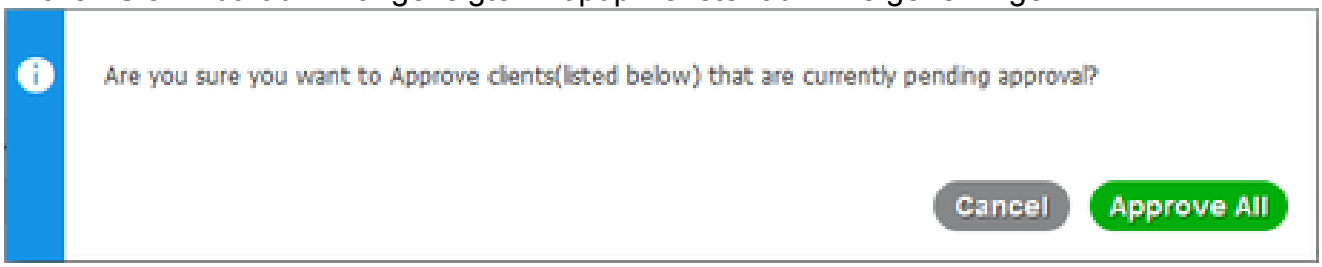
Registrierungsanforderung auf dem ISE-Server genehmigen

In der ISE-GUI:

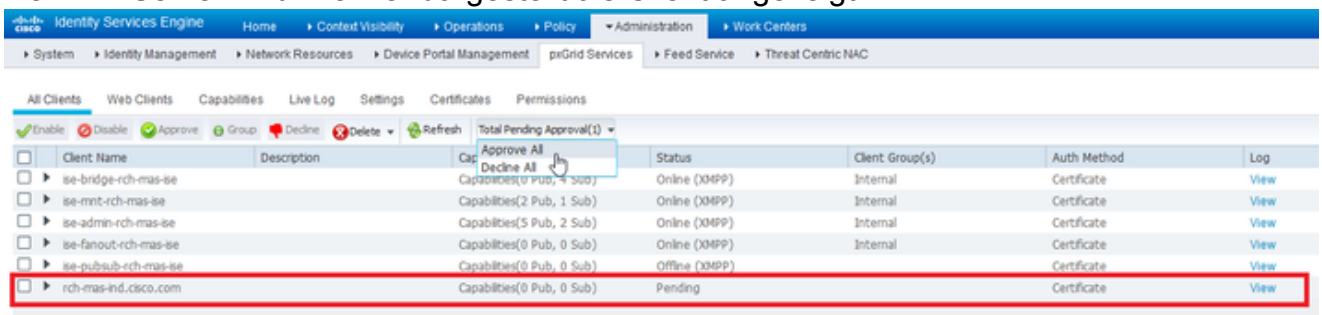
1. Navigieren Sie zu Administration > pxGrid Services > All Clients. Eine Anfrage mit ausstehender Genehmigung wird als "Gesamte ausstehende Genehmigung(1)" angezeigt.
2. Klicken Sie auf "Gesamt ausstehende Genehmigung(1)" und wählen Sie "Alle genehmigen".



3. Klicken Sie im daraufhin angezeigten Popup-Fenster auf "Alle genehmigen".



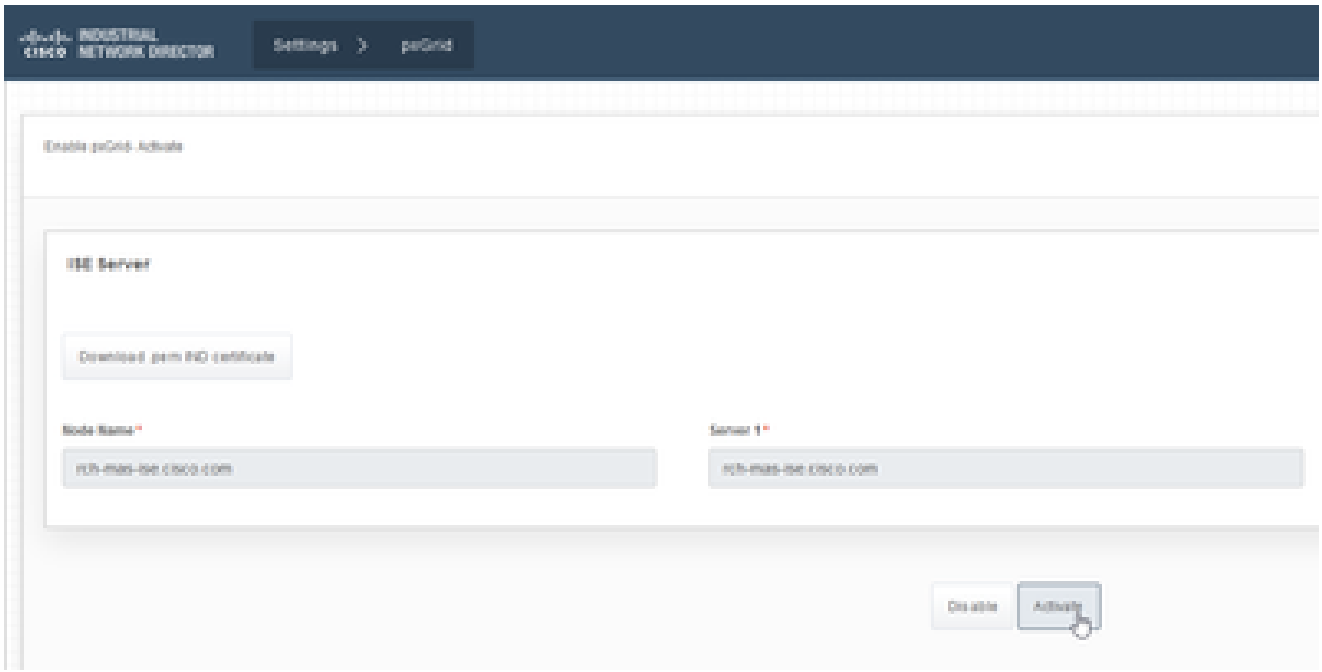
4. Der IND-Server wird wie hier dargestellt als Client angezeigt.



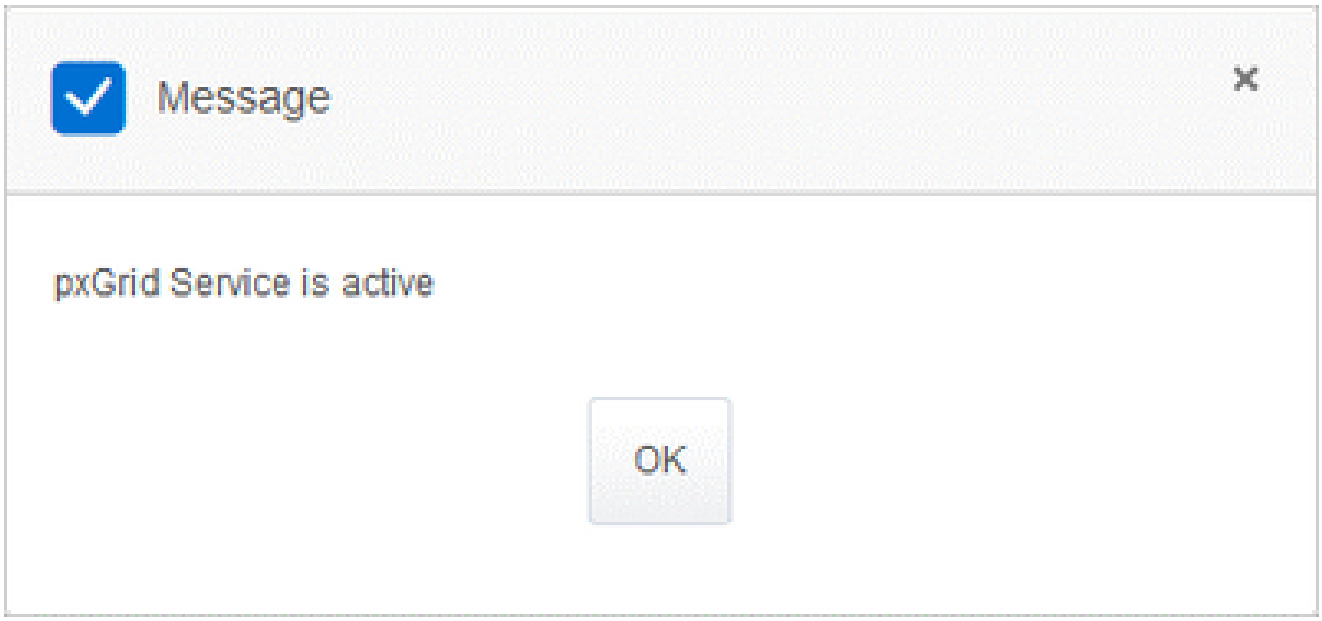
pxGrid-Dienst im IND-Server aktivieren

In der IND-GUI:

1. Navigieren Sie zu Einstellungen > pxGrid.
2. Klicke auf "Aktivieren".



3. Eine Bestätigung wird auf dem Bildschirm angezeigt.


Message
pxGrid Service is active
OK

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.