Créer des certificats SAN pour l'intégration IND et ISE pxGrid à l'aide d'OpenSSL

Table des matières

Introduction

Ce document décrit comment créer des certificats SAN pour l'intégration pxGrid entre Industrial Network Director (IND) et Identity Services Engine.

Informations générales

Lors de la création de certificats dans Cisco ISE pour l'utilisation de pxGrid, les noms d'hôte courts du serveur ne peuvent pas être entrés dans l'interface utilisateur graphique ISE, car ISE autorise uniquement le nom de domaine complet ou l'adresse IP.

Pour créer des certificats qui incluent le nom d'hôte ainsi que le nom de domaine complet, un fichier de demande de certificat doit être créé en dehors d'ISE. Cela peut être fait à l'aide d'OpenSSL pour créer une demande de signature de certificat (CSR) avec des entrées de champ Autre nom du sujet (SAN).

Ce document ne comprend pas d'étapes complètes pour activer la communication pxGrid entre le serveur IND et le serveur ISE. Ces étapes peuvent être utilisées après la configuration de pxGrid, et il a été confirmé que le nom d'hôte du serveur est requis. Si cette erreur est détectée dans les fichiers journaux du profileur ISE, la communication nécessite le certificat de nom d'hôte.

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

Les étapes du déploiement initial d'IND avec la communication pxGrid sont disponibles à l'adresse https://www.cisco.com/c/dam/en/us/td/docs/switches/ind/install/IND_PxGrid_Registration_Guide_Final.pdf

Applications requises

- Cisco Industrial Network Director (IND)
- Cisco Identity Services Engine (ISE)
- OpenSSL
    - Dans la plupart des versions Linux modernes, ainsi que MacOS, le package OpenSSL est installé par défaut. Si vous constatez que les commandes ne sont pas disponibles, installez OpenSSL à l'aide de l'application de gestion des packages de votre système

d'exploitation.
    - Pour plus d'informations sur OpenSSL pour Windows, consultez la page https://wiki.openssl.org/index.php/Binaries

Additional Information

Pour les besoins de ce document, ces détails sont utilisés :

- Nom d'hôte du serveur IND : rch-mas-ind
- Nom de domaine complet : rch-mas-ind.cisco.com
- Configuration OpenSSL : rch-mas-ind.req
- Nom du fichier de demande de certificat : rch-mas-ind.csr
- Nom du fichier de clé privée : rch-mas-ind.pem
- Nom du fichier de certificat : rch-mas-ind.cer

Étapes du processus

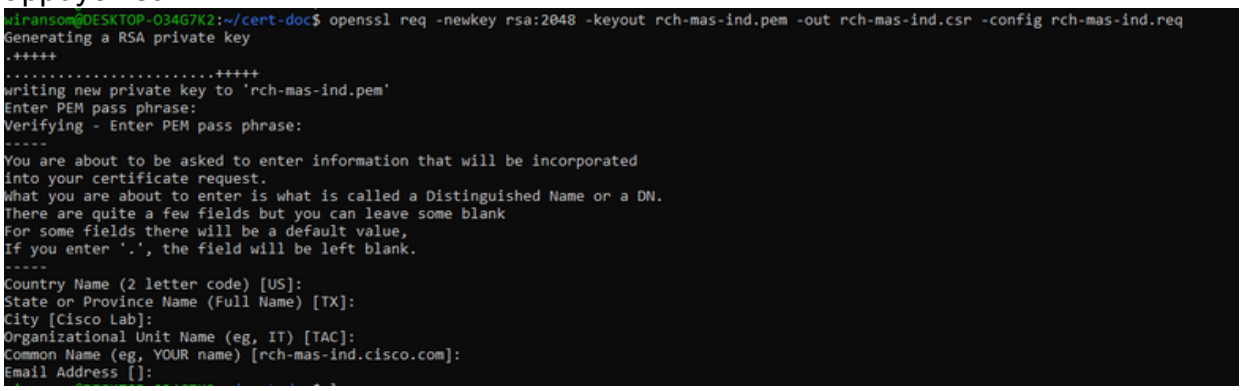
Créer le certificat CSR

1. Sur un système sur lequel OpenSSL est installé, créez un fichier texte de demande pour les options OpenSSL, y compris les informations SAN.
    - La plupart des champs « par défaut » sont facultatifs, car les réponses peuvent être saisies lors de l'exécution de la commande OpenSSL à l'étape #2.
    - Les détails SAN (DNS.1, DNS.2) sont requis et doivent inclure à la fois le nom d'hôte court DNS et le nom de domaine complet du serveur. Des noms DNS supplémentaires peuvent être ajoutés si nécessaire, à l'aide de DNS.3, DNS.4, etc.
    - Exemple de fichier texte de demande :

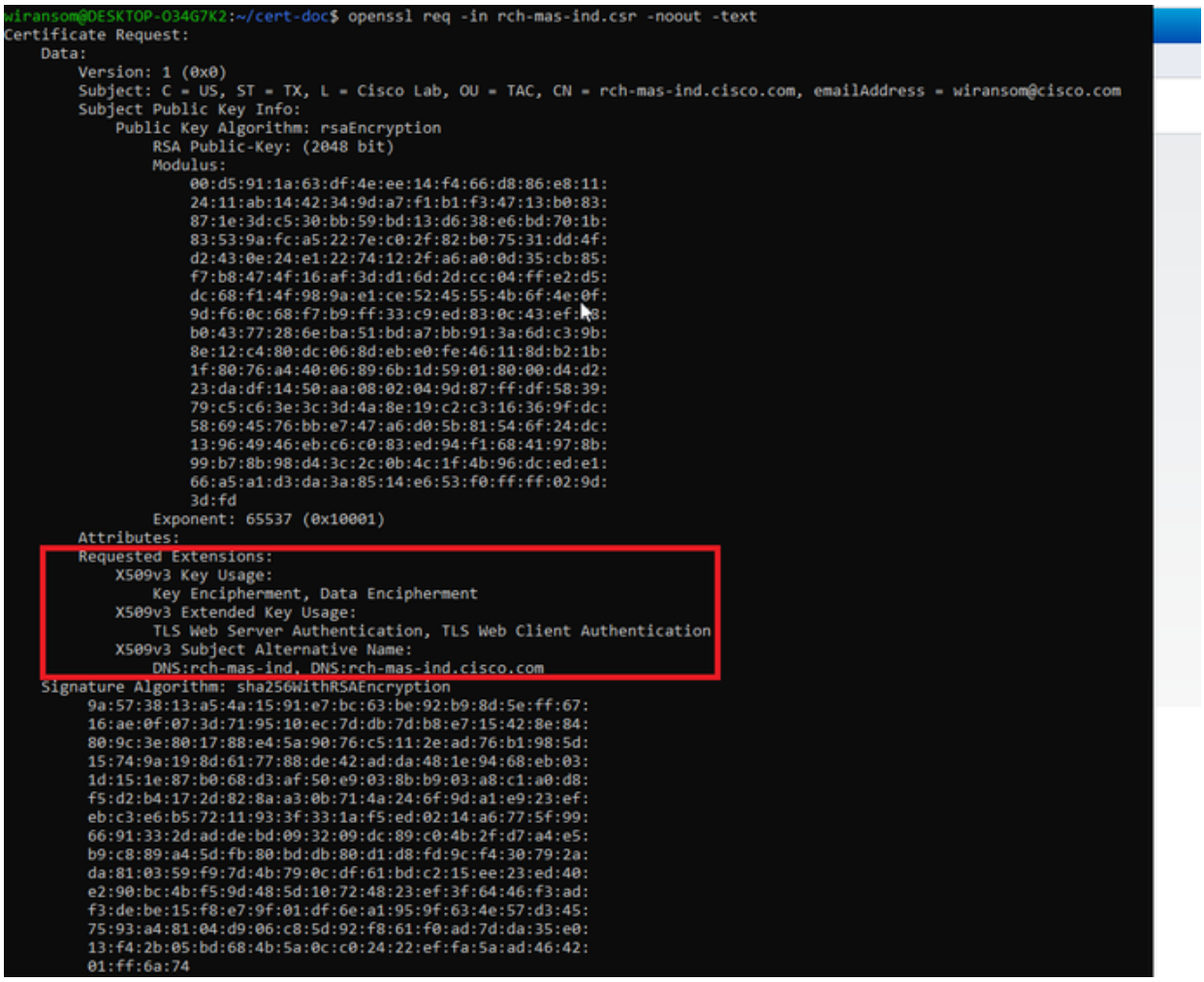
```
[obligatoire]
nom_unique = nom
req_extensions = v3_req

[nom]
countryName = Nom du pays (code à 2 lettres)
countryName_default = États-Unis
stateOrProvinceName = Nom de l'État ou de la province (Nom complet)
stateOrProvinceName_default = TX
localityName = Ville
localityName_default = Laboratoire Cisco
organizationUnitName = Nom de l'unité d'organisation (par exemple, IT)
NomUnitéOrganisation_par défaut = TAC
commonName = Nom commun (par exemple, VOTRE nom)
commonName_max = 64
commonName_default = rch-mas-ind.cisco.com
emailAddress = Adresse e-mail
```

```
AdresseEmail_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. Utilisez OpenSSL pour créer un CSR avec un nom d'hôte court DNS dans le champ SAN. Créez un fichier de clé privée en plus du fichier CSR.
    - commande :
      openssl req -newkey rsa : 2048 -keyout <serveur>.pem -out <serveur>.csr -config <serveur>.req
    - Lorsque vous y êtes invité, entrez le mot de passe de votre choix. Veillez à mémoriser ce mot de passe, tel qu'il sera utilisé dans les étapes ultérieures.
    - Entrez une adresse e-mail valide lorsque vous y êtes invité ou laissez le champ vide et appuyez sur <ENTRÉE>.



3. Si vous le souhaitez, vérifiez les informations du fichier CSR. Pour obtenir un certificat SAN, recherchez « Autre nom du sujet x509v3 », comme indiqué dans cette capture d'écran.
    - Ligne de commande :
      openssl req -in <serveur>.csr -noout -text



4. Ouvrez le fichier CSR dans un éditeur de texte. Pour des raisons de sécurité, l'exemple de capture d'écran est incomplet et modifié. Le fichier CSR généré contient davantage de lignes.

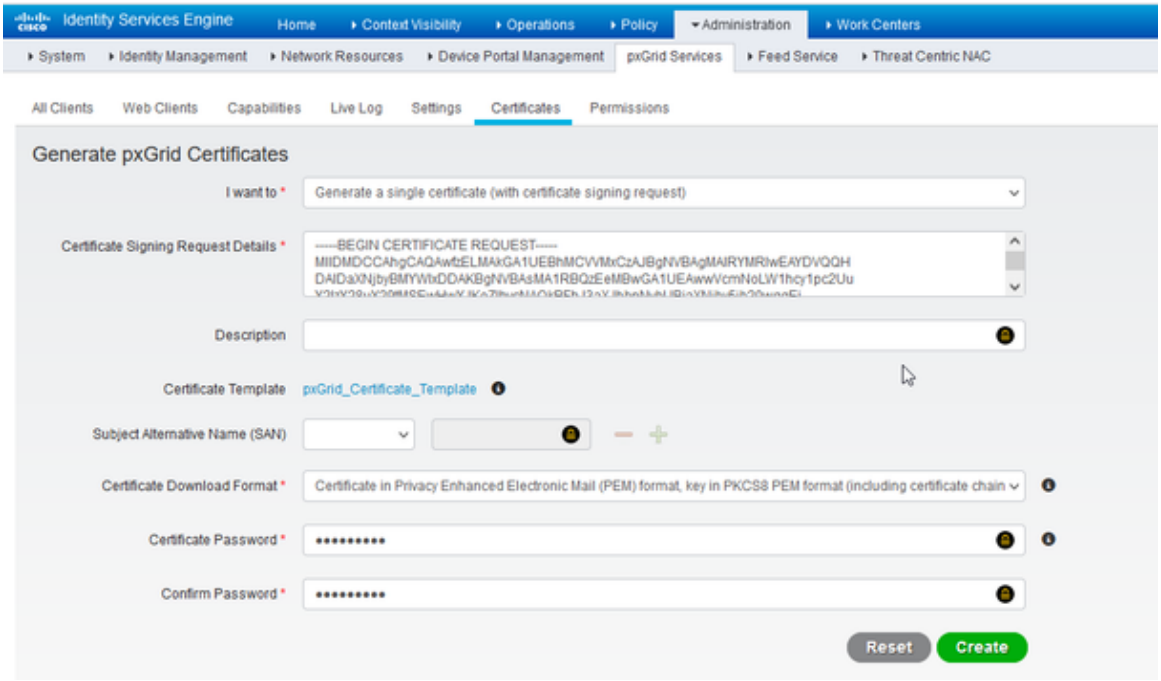
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDMDCCAhgCAQAwfzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAlRYMRIwEAYDVQQH
DAlDaXNjbyBMYWIxDDAKBgNVBAsMA1RBQzEeMBwGA1UEAwwVcmNoLW1hcy1pbmQu
Y2lzY28uY29tMSEwHwYJKoZIhvcNAQkBFhJ3aXJhbnNvbUBjaXNjby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVkRpj307uFPRm2IboESQRqxRC
NJ2n8bHzRxOwg4cePcUwu1m9E9Y45r1wG4NTmvylIn7AL4KwdTHdT9JDDiThInQS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

5. Copiez le fichier de clé privée (<server>.pem) sur votre PC tel qu'il est utilisé dans une étape ultérieure.

Utilisez Cisco ISE pour générer un certificat, en utilisant les informations du fichier CSR créé

Dans l'interface utilisateur graphique ISE :

1. Supprimer le client pxGrid existant.
    - Accédez à Administration > pxGrid Services > All Clients.
    - Recherchez et sélectionnez le nom d'hôte du client existant, le cas échéant,
    - S'il est trouvé et sélectionné, cliquez sur le bouton Supprimer, puis choisissez « Supprimer la sélection ». Confirmez si nécessaire.
2. Créez le nouveau certificat.
    - Cliquez sur l'onglet Certificats de la page des services pxGrid.
    - Choisissez les options suivantes :
        - « Je veux » :
            - « Générer un certificat unique (avec demande de signature de certificat) »
        - « Détails de la demande de signature de certificat :
            - Copiez/collez les détails CSR à partir de l'éditeur de texte. Veillez à inclure les lignes BEGIN et END.
        - « Format de téléchargement du certificat »
            - « Certificat au format PEM (Privacy Enhanced Electronic Mail), clé au format PEM PKCS8. »
        - Entrez un mot de passe de certificat et confirmez-le.
        - Cliquez sur le bouton Créer.

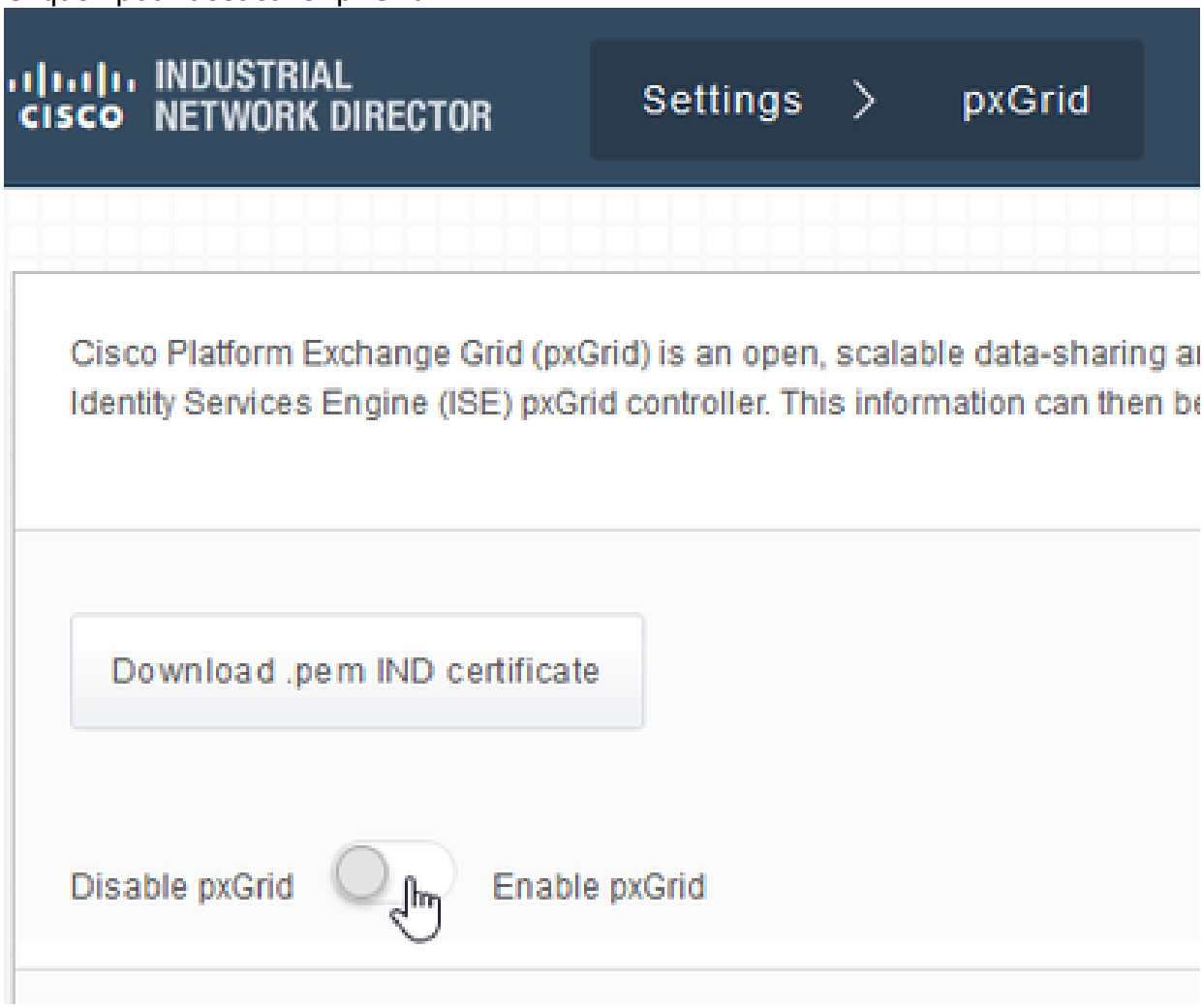


        - Ceci crée et télécharge un fichier ZIP qui contient le fichier de certificat ainsi que des fichiers supplémentaires pour la chaîne de certificats. Ouvrez le fichier ZIP et extrayez le certificat.
            - Le nom de fichier est normalement <IND server fqdn>.cer
            - Dans certaines versions d'ISE, le nom de fichier est <IND fqdn>_<IND short name>.cer

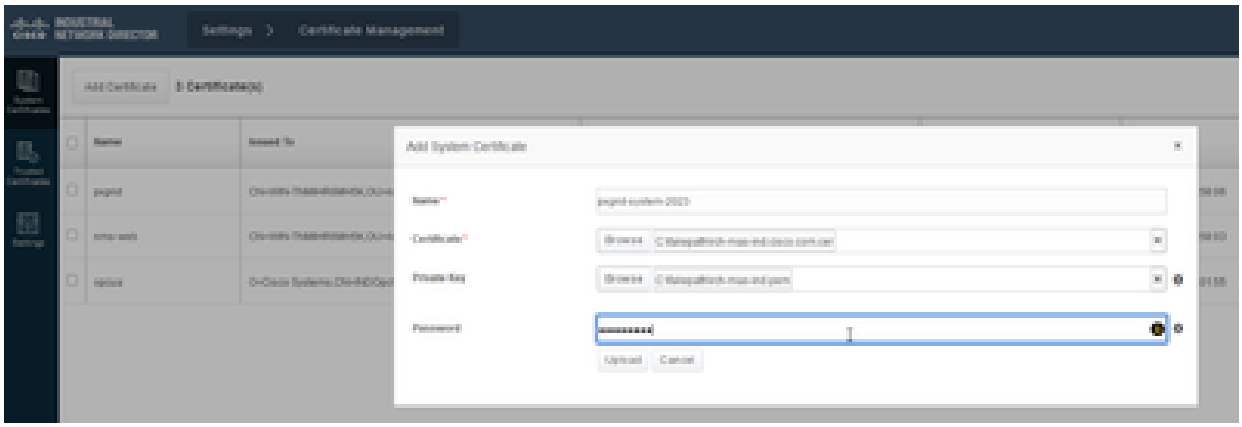
Importez le nouveau certificat dans le serveur IND et activez-le pour une utilisation pxGrid

Dans l'interface utilisateur graphique IND :

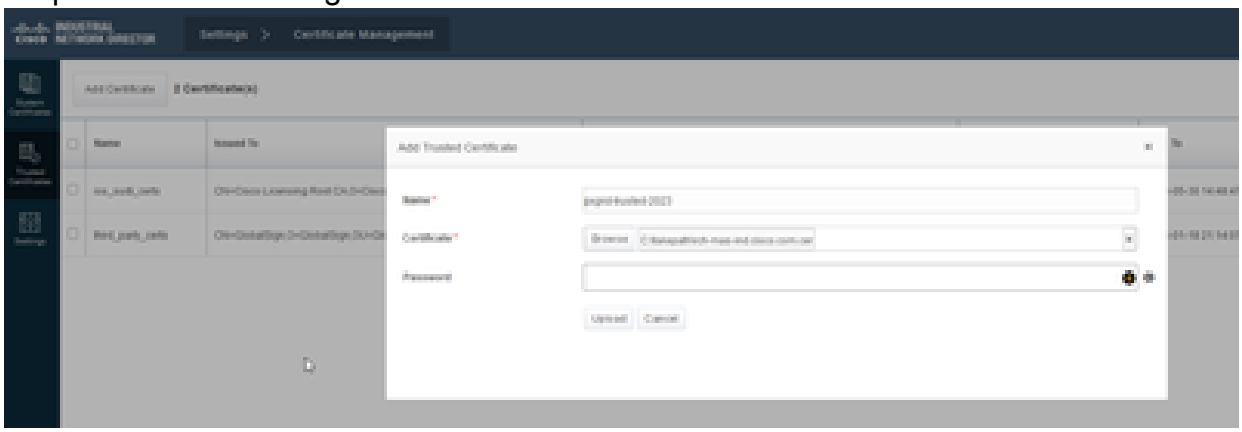
1. Désactivez le service pxGrid, afin que le nouveau certificat puisse être importé et défini comme certificat actif.
    - Accédez à Settings > pxGrid.
    - Cliquez pour désactiver pxGrid.



2. Importez le nouveau certificat dans Certificats système.
    - Accédez à Paramètres > Gestion des certificats.
    - Cliquez sur « Certificats système »
    - Cliquez sur « Ajouter un certificat ».
    - Entrez un nom de certificat.
    - Cliquez sur « Parcourir » à gauche de « Certificat » et localisez le nouveau fichier de certificat.
    - Cliquez sur « Parcourir » à gauche de « Certificat » et localisez la clé privée enregistrée lors de la création du CSR.
    - Saisissez le mot de passe précédemment utilisé lors de la création de la clé privée et du CSR avec OpenSSL.
    - Cliquez sur « Télécharger ».



3. Importez le nouveau certificat en tant que certificat sécurisé.
    - Accédez à Paramètres > Gestion des certificats, cliquez sur « Certificats approuvés ».
    - Cliquez sur « Ajouter un certificat ».
    - Entrez un nom de certificat ; il doit s'agir d'un nom différent de celui utilisé sur les certificats système.
    - Cliquez sur « Parcourir » à gauche de « Certificat » et localisez le nouveau fichier de certificat.
    - Le champ Mot de passe peut rester vide.
    - Cliquez sur « Télécharger ».



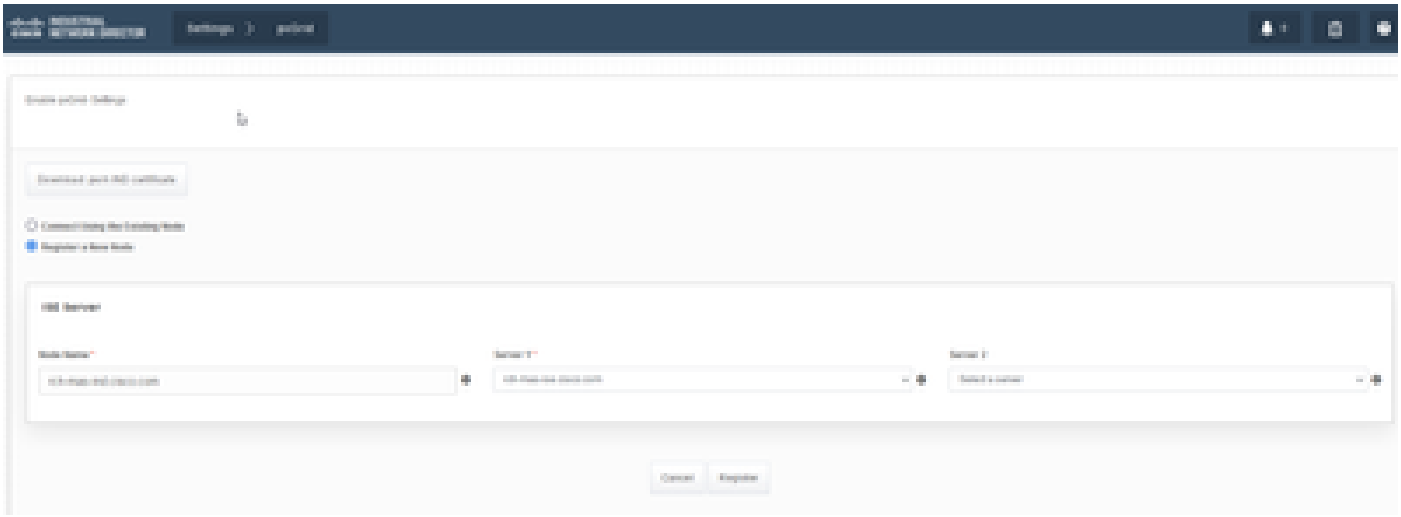
4. Configurez pxGrid pour utiliser le nouveau certificat.
    - Accédez à Paramètres > Gestion des certificats, cliquez sur « Paramètres ».
    - Si ce n'est pas déjà fait, sélectionnez « Certificat CA » sous « pxGrid ».
    - Sélectionnez le nom du certificat système créé lors de l'importation du certificat.
    - Cliquez sur Save.

Activer et enregistrer pxGrid auprès du serveur ISE

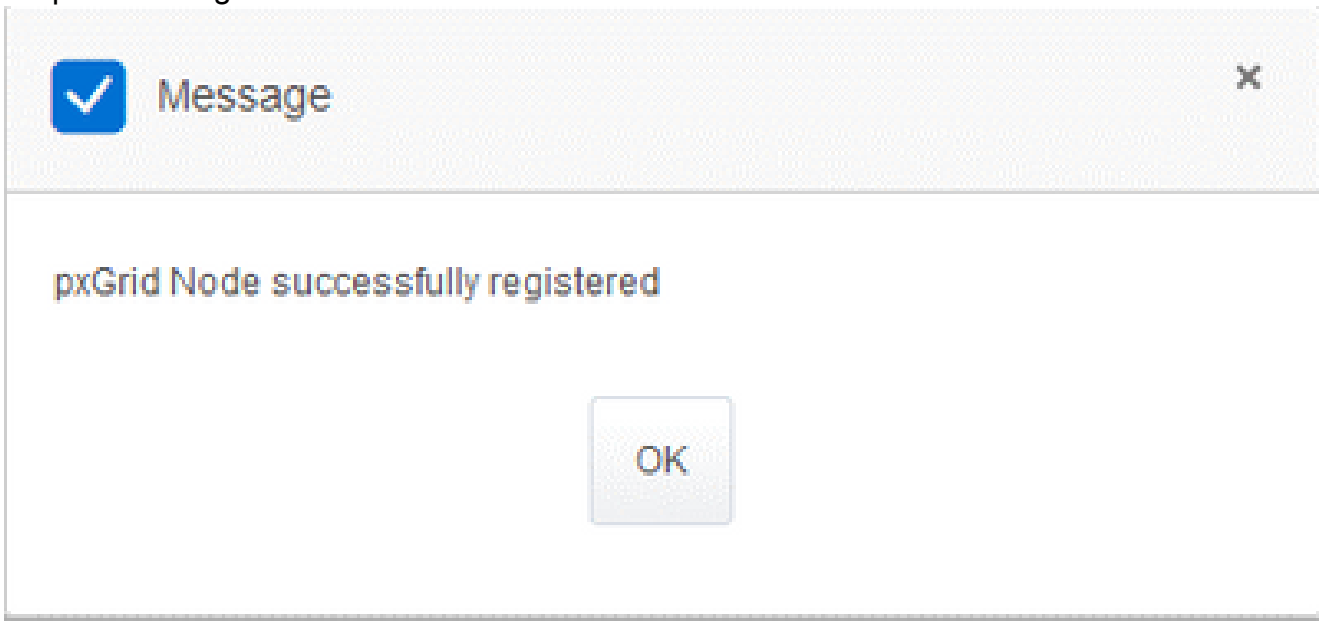
Dans l'interface utilisateur graphique IND :

1. Accédez à Settings > pxGrid.
2. Cliquez sur le curseur pour activer pxGrid.
3. Si ce n'est pas la première fois que vous enregistrez pxGrid avec ISE sur ce serveur IND, sélectionnez « Connect Using the Existing Node » (Connexion à l'aide du noeud existant). Les informations relatives au noeud IND et au serveur ISE sont automatiquement renseignées.

4. Pour enregistrer un nouveau serveur IND afin d'utiliser pxGrid, si nécessaire, sélectionnez « Register a New Node ». Entrez le nom du noeud IND et sélectionnez les serveurs ISE selon vos besoins.
    - Si le serveur ISE n'est pas répertorié dans les options déroulantes pour Server 1 ou Server 2, il peut être ajouté en tant que nouveau serveur pxGrid à l'aide de Paramètres > Serveur de stratégie



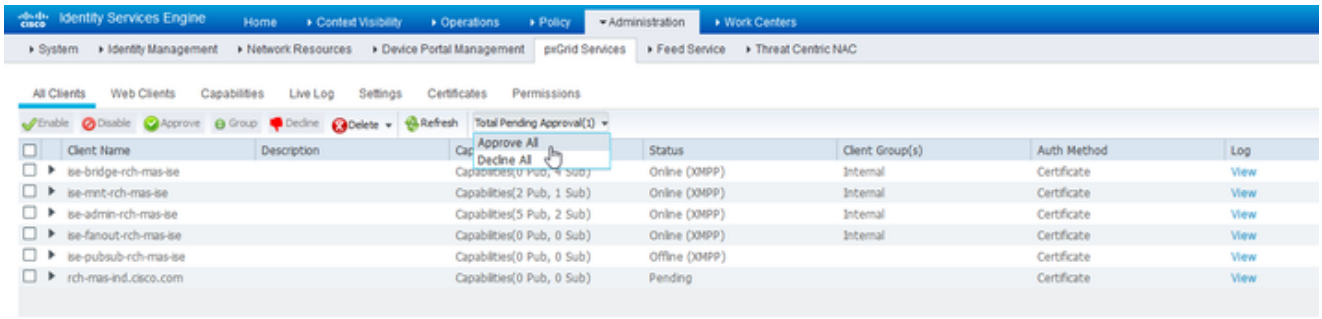
5. Cliquez sur Register. Une confirmation s'affiche à l'écran.



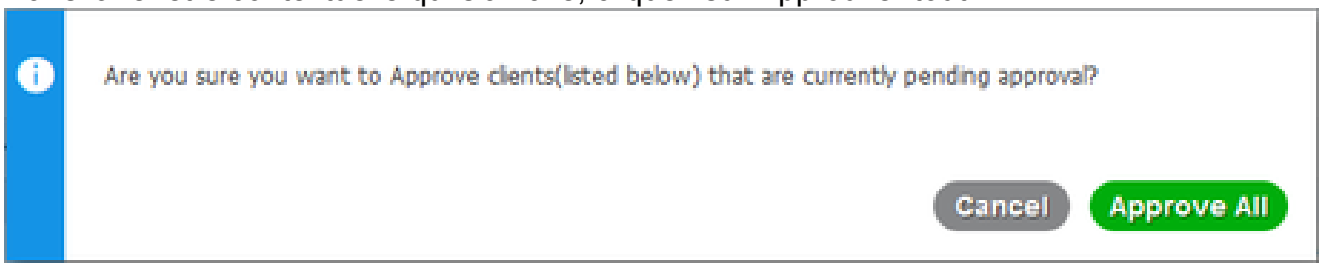
Approuver la demande d'enregistrement dans le serveur ISE

Dans l'interface utilisateur graphique ISE :

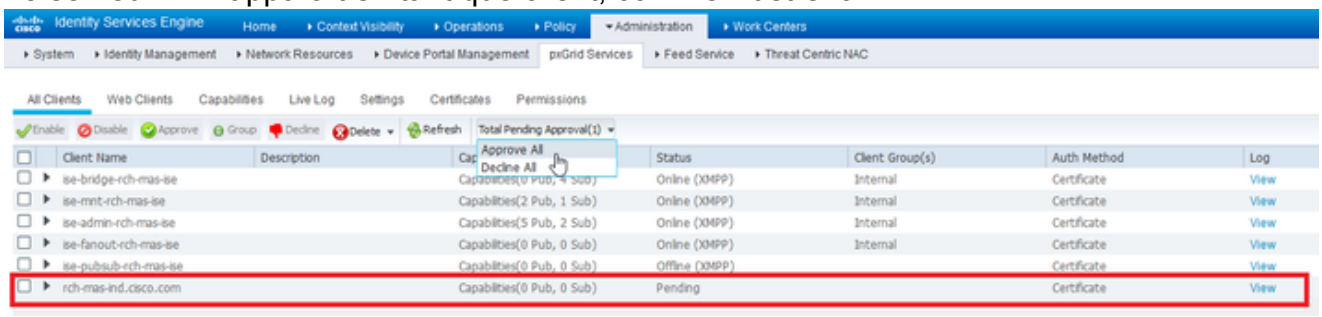
1. Accédez à Administration > pxGrid Services > All Clients. Une demande en attente d'approbation s'affiche sous la forme « Total en attente d'approbation(1) ».
2. Cliquez sur « Approbation totale en attente(1) » et sélectionnez « Approuver tout ».



3. Dans la fenêtre contextuelle qui s'affiche, cliquez sur Approuver tout.



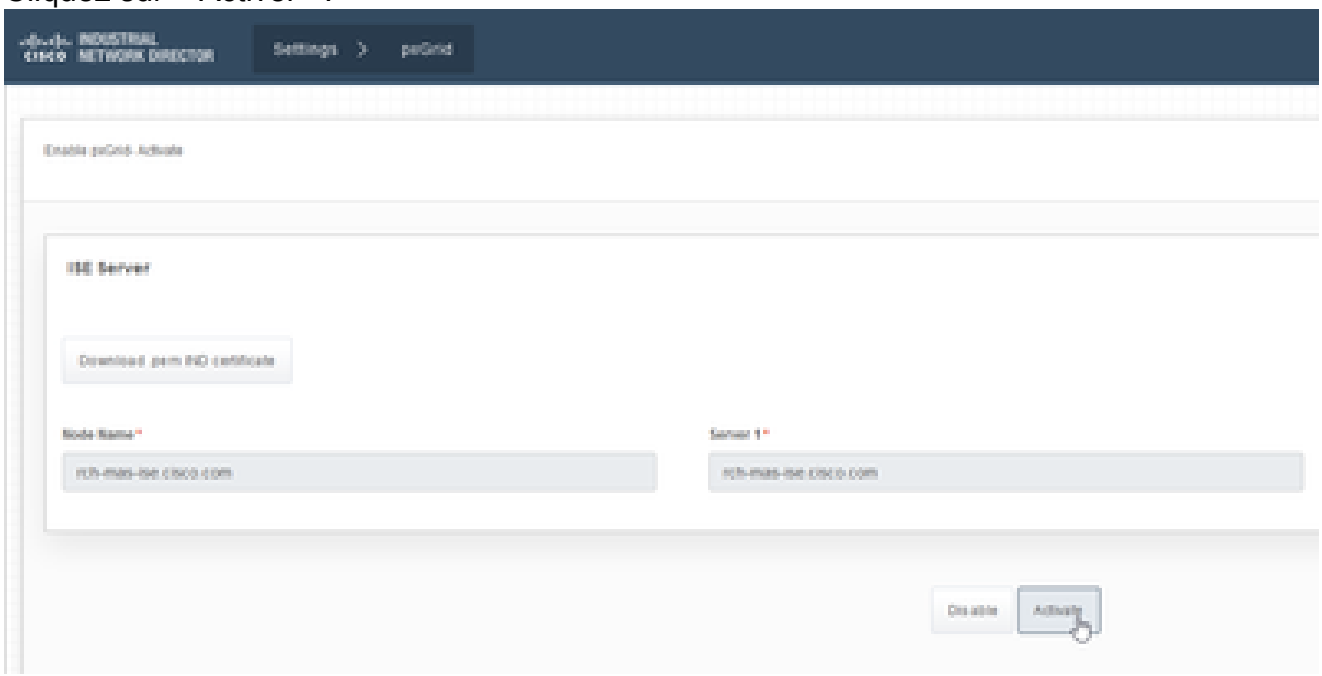
4. Le serveur IND apparaît en tant que client, comme illustré ici.



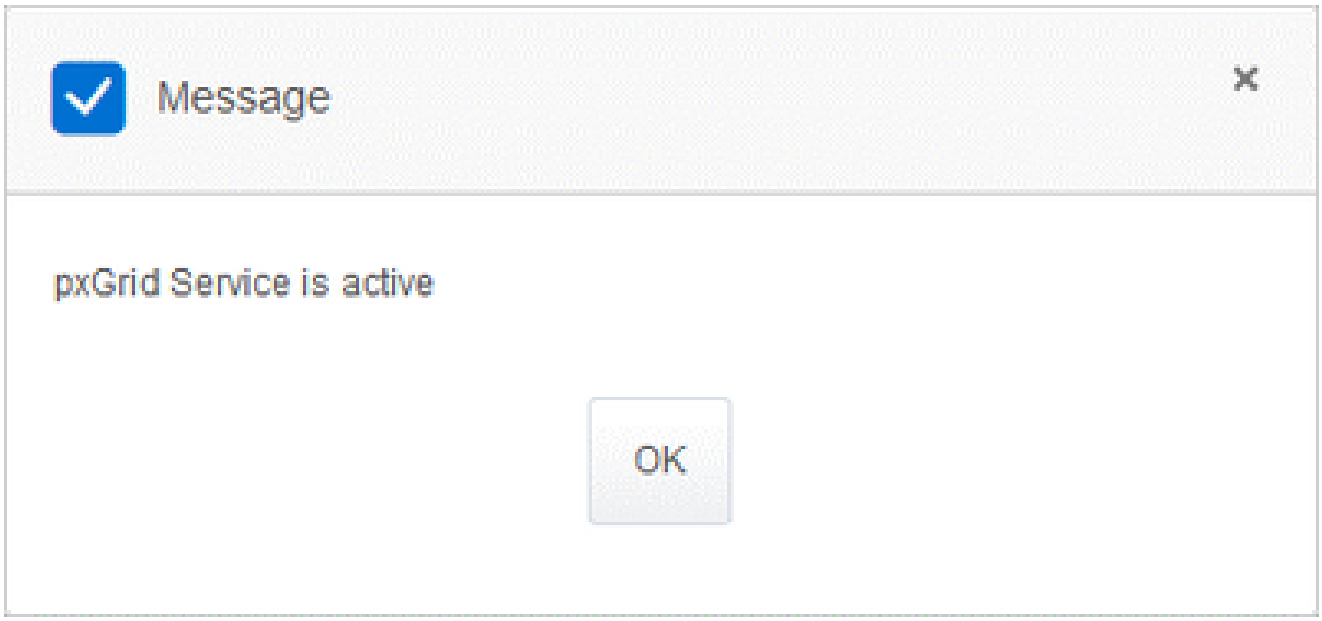
Activer le service pxGrid dans le serveur IND

Dans l'interface utilisateur graphique IND :

1. Accédez à Settings > pxGrid.
2. Cliquez sur « Activer ».



3. Une confirmation s'affiche à l'écran.


Message
pxGrid Service is active
OK

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.