OpenSSLを使用したINDおよびISE pxGrid統合用のSAN証明書の作成

内容

概要

このドキュメントでは、Industrial Network Director(IND)とIdentity Services Engine間のpxGrid統合のためのSAN証明書を作成する方法について説明します。

背景説明

pxGridを使用するためにCisco ISEで証明書を作成する場合、ISEではFQDNまたはIPアドレスのみが許可されるため、サーバのショートホスト名をISE GUIに入力することはできません。

ホスト名およびFQDNを含む証明書を作成するには、証明書要求ファイルをISEの外部で作成する必要があります。これを行うには、OpenSSLを使用して、サブジェクト代替名(SAN)フィールドエントリで証明書署名要求(CSR)を作成します。

このドキュメントには、INDサーバとISEサーバ間のpxGrid通信を有効にするための包括的な手順は含まれていません。 これらの手順は、pxGridが設定され、サーバのホスト名が必要であることが確認された後で使用できます。 ISEプロファイラログファイルでこのエラーが見つかった場合、通信にはホスト名証明書が必要です。

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

pxGrid通信を使用したINDの初期導入手順については、https://www.cisco.com/c/dam/en/us/td/docs/switches/ind/install/IND_PxGrid_Registration_Guide_Final.pdf照してください。

必要なアプリケーション

- Cisco Industrial Network Director(IND)
- Cisco Identity Services Engine（ISE）
- OpenSSL
    - MacOSと同様に、最新のLinuxバージョンでは、OpenSSLパッケージがデフォルトでインストールされます。コマンドが使用できない場合は、オペレーティングシステムのパッケージ管理アプリケーションを使用してOpenSSLをインストールしてください。

- OpenSSL for Windowsの詳細については、https://wiki.openssl.org/index.php/Binariesを参照してください。

追加情報

このドキュメントでは、次の詳細を使用します。

- INDサーバのホスト名：rch-mas-ind
- FQDN:rch-mas-ind.cisco.com
- OpenSSLの設定：rch-mas-ind.req
- 証明書要求ファイル名：rch-mas-ind.csr
- 秘密キーのファイル名： rch-mas-ind.pem
- 証明書ファイル名：rch-mas-ind.cer

プロセスステップ

証明書CSRの作成

1. OpenSSLがインストールされているシステムで、SAN情報を含むOpenSSLオプションの要求テキストファイルを作成します。
   - ほとんどの「_default」フィールドはオプションです。これは、手順#2でOpenSSLコマンドを実行している間に回答を入力できるためです。
   - SANの詳細(DNS.1、DNS.2)が必要です。DNSの短いホスト名とサーバーのFQDNの両方を含める必要があります。必要に応じて、DNS.3、DNS.4などを使用して追加のDNS名を追加できます。
   - 要求ファイルのテキストファイルの例：

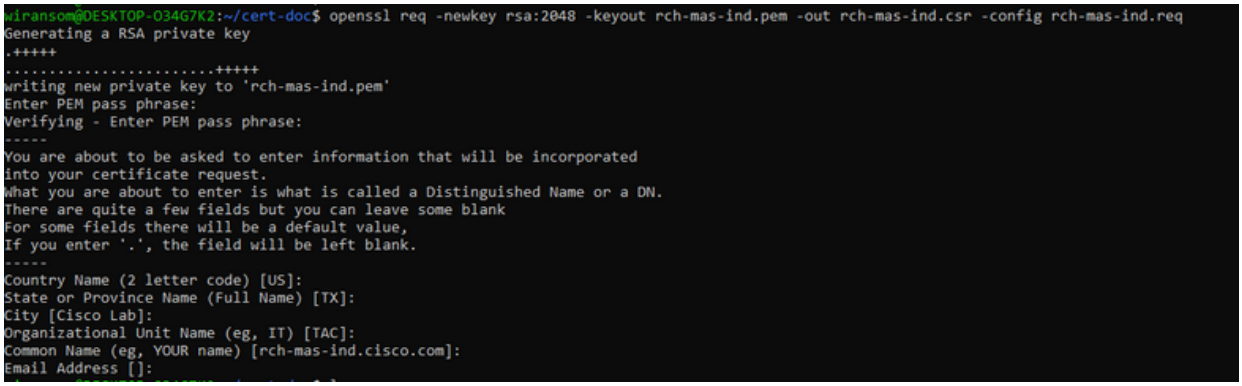
```
[req ]
distinguished_name =名前
req_extensions = v3_req

[name]
countryName =国名（2文字のコード）
countryName_default =米国
stateOrProvinceName =都道府県（フルネーム）
stateOrProvinceName_default = TX
localityName =市区町村
localityName_default =シスコラボ
organizationalUnitName =組織単位の名前（例、IT）
organizationalUnitName_default = TAC
commonName =共通名（例、自分の名前）
commonName_max = 64
commonName_default = rch-mas-ind.cisco.com
emailAddress =電子メールアドレス
emailAddress_max = 40
```

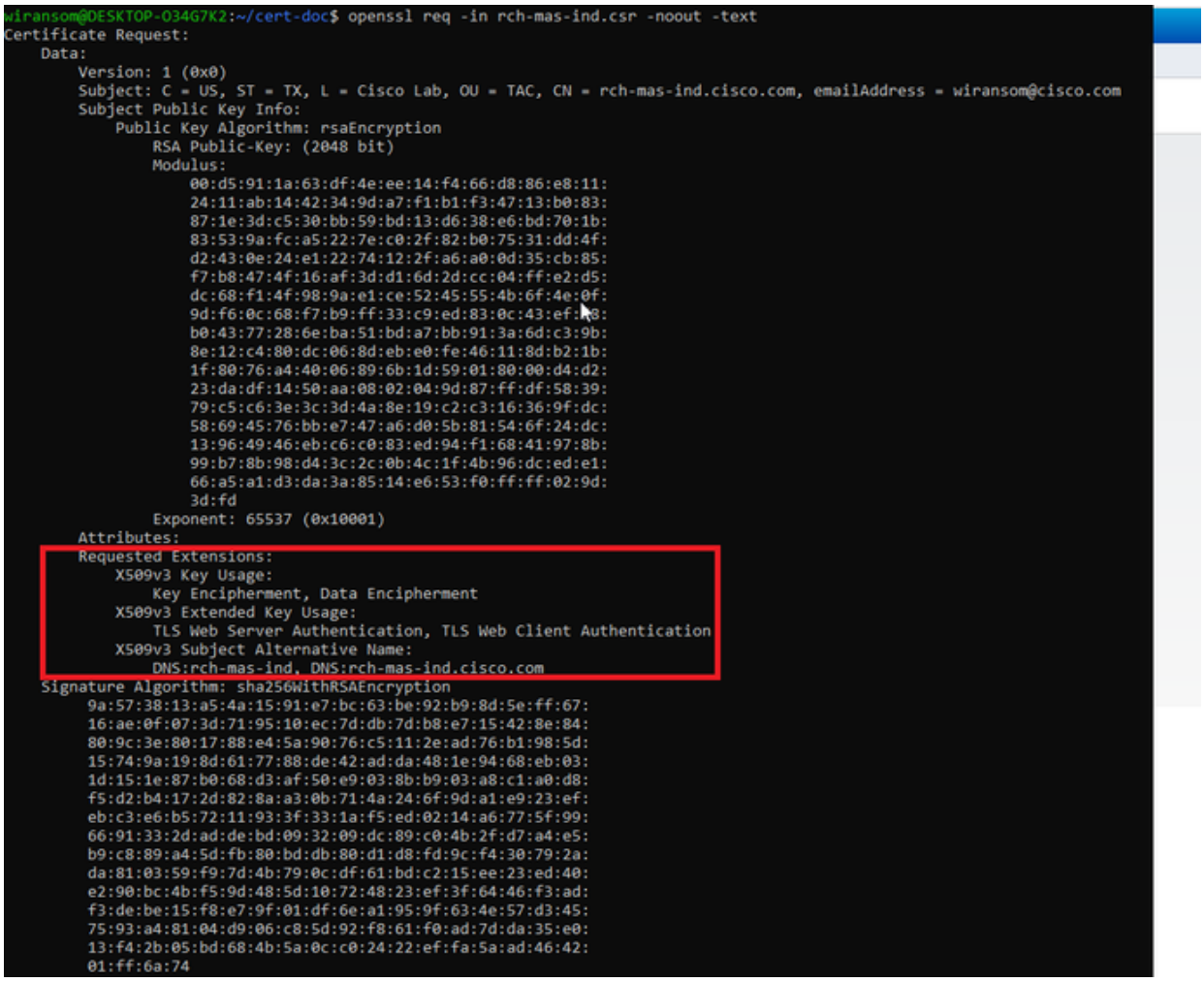
```
[v3_req]
keyUsage = keyEncipherment、dataEncipherment
拡張キー使用法= serverAuth、clientAuth
subjectAltName = @alt_names

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

2. OpenSSLを使用して、SANフィールドにDNS短いホスト名を持つCSRを作成します。 CSRファイルに加えて秘密キーファイルを作成します。
   - コマンド：
     openssl req -newkey rsa:2048 -keyout <サーバ>.pem -out <サーバ>.csr -config <サーバ>.req
   - プロンプトが表示されたら、任意のパスワードを入力します。 このパスワードは後の手順で使用するので、忘れないようにしてください。
   - プロンプトが表示されたら、有効な電子メールアドレスを入力するか、フィールドを空白のままにして、Enterキーを押します。



3. 必要に応じて、CSRファイル情報を確認します。SAN証明書の場合は、このスクリーンショットで強調表示されている「x509v3 Subject Alternative Name」を確認します。
   - コマンドライン:
     openssl req -in <サーバ>.csr -noout -text



4. テキストエディタでCSRファイルを開きます。 セキュリティ上の理由から、サンプルのスクリーンショットは不完全で編集されています。 実際に生成されたCSRファイルには、さらに多くの行が含まれています。

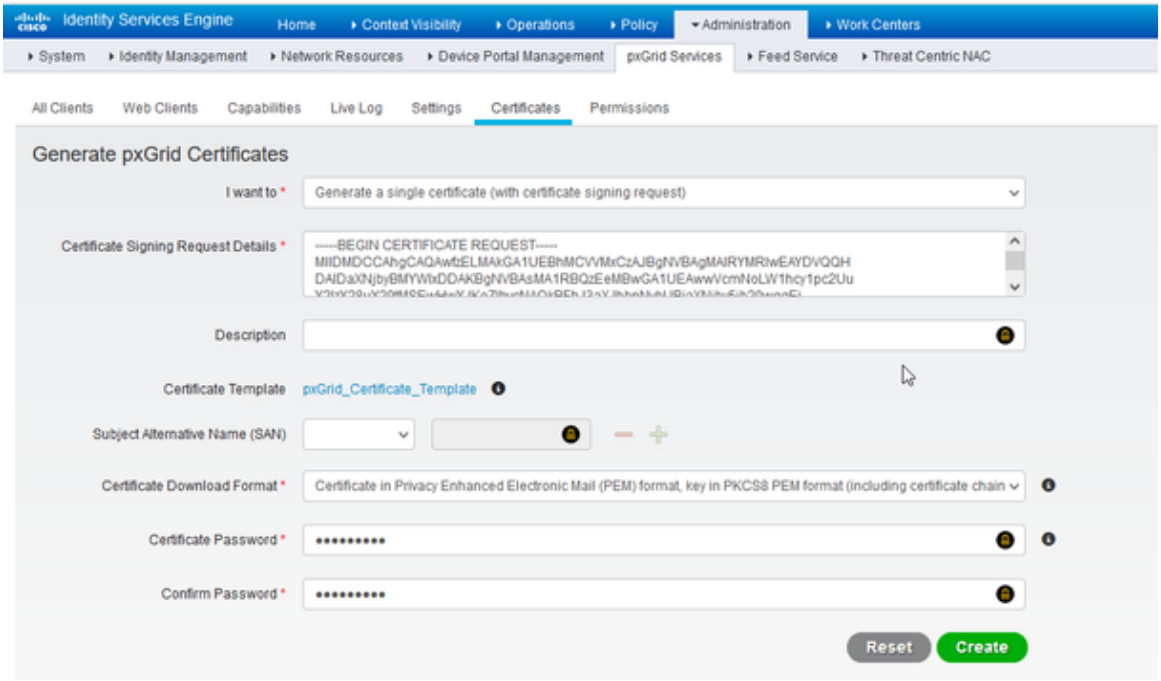
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDMDCCAhgCAQAwfzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAlRYMRIwEAYDVQQH
DAlDaXNjbyBMYWIxDDAKBgNVBAsMA1RBQzEeMBwGA1UEAwwVcmNoLW1hcy1pbmQu
Y2lzY28uY29tMSEwHwYJKoZIhvcNAQkBFhJ3aXJhbnNvbUBjaXNjby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVkRpj307uFPRm2IboESQRqxRC
NJ2n8bHzRxOwg4cePcUwu1m9E9Y45r1wG4NTmvylIn7AL4KwdTHdT9JDDiThInQS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

5. 秘密キーファイル(<server>.pem)は、後の手順で使用するときにPCにコピーします。

作成したCSRファイル情報を使用して、Cisco ISEで証明書を生成します

ISE GUI内：

1. 既存のpxGridクライアントを削除します。
    - Administration > pxGrid Services > All Clientsの順に移動します。
    - 既存のクライアントのホスト名がリストされている場合は、そのホスト名を検索して選択します。
    - 見つかり、選択されている場合は、[削除]ボタンをクリックし、[選択を削除]を選択します。 必要に応じて確認します。
2. 新しい証明書を作成します。
    - pxGridサービスページのCertificatesタブをクリックします。
    - 次のオプションを選択します。
        - 「実行したい」：
            - 「単一の証明書の生成（証明書署名要求を使用）」
        - 証明書署名要求の詳細：
            - テキストエディタからCSRの詳細をコピーして貼り付けます。 必ずBEGIN行とEND行を含めてください。
        - 「証明書のダウンロード形式」
            - 「Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format.」(プライバシー強化電子メール(PEM)形式の証明書、PKCS8 PEM形式のキー)
        - 証明書のパスワードを入力し、確認します。
        - [Create] ボタンをクリックします。

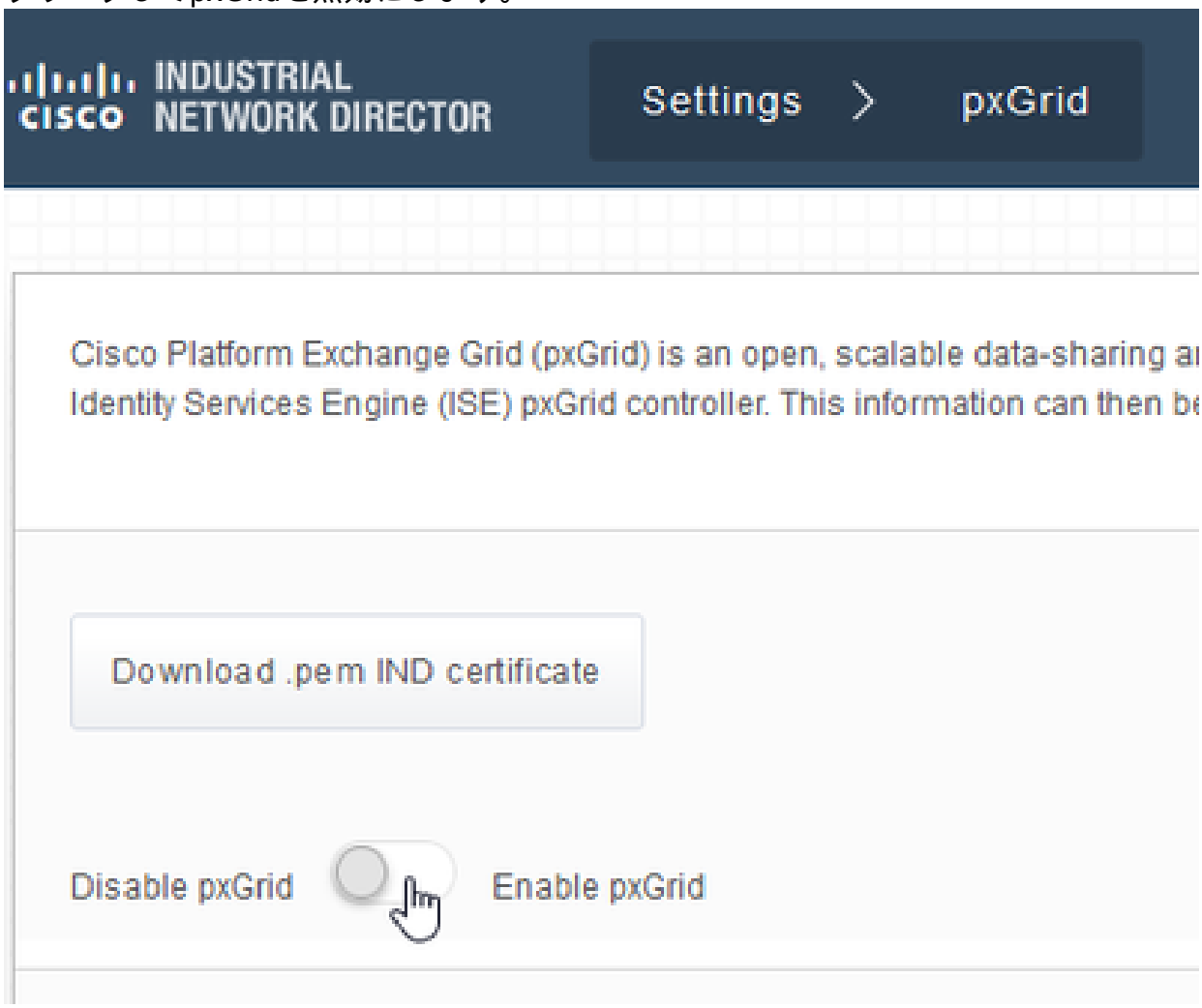


        - これにより、証明書ファイルと証明書チェーンの追加ファイルを含むZIPファイルが作成され、ダウンロードされます。ZIPファイルを開き、証明書を抽出します。
            - ファイル名は通常、<IND server fqdn>.cerです。
            - ISEのバージョンによっては、ファイル名は<IND fqdn>_<IND short name>.cerです。

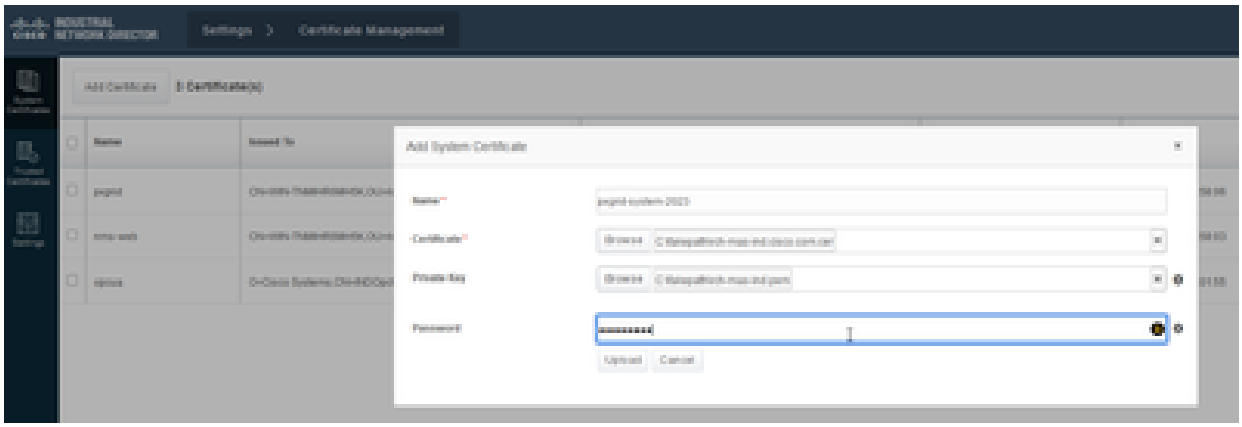
新しい証明書をINDサーバにインポートし、pxGridで使用できるようにします

IND GUI内：

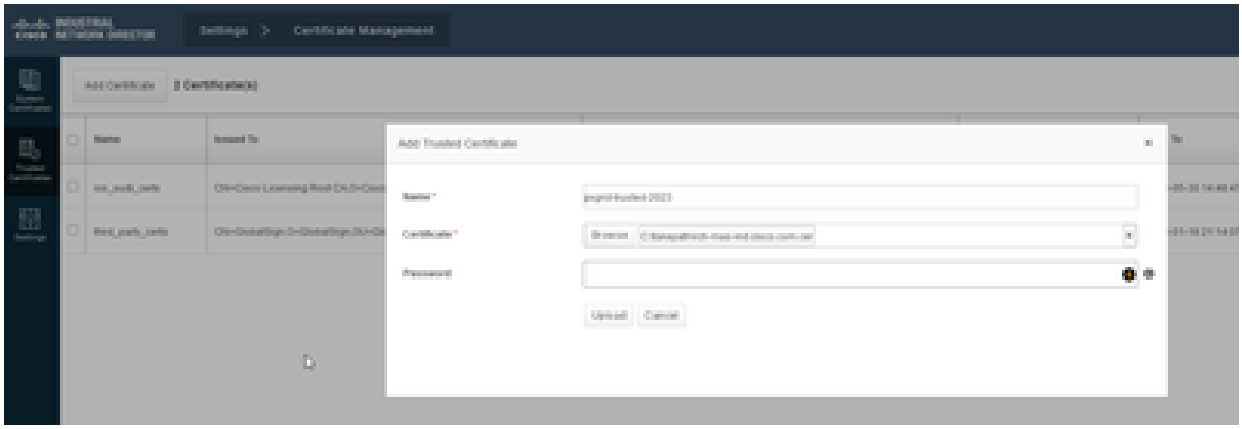
1. pxGridサービスを無効にして、新しい証明書をインポートし、アクティブな証明書として設定できるようにします。
   - Settings > pxGridの順に移動します。
   - クリックしてpxGridを無効にします。



2. 新しい証明書をシステム証明書にインポートします。
   - Settings > Certificate Managementの順に移動します。
   - [システム証明書]をクリックします。
   - [証明書の追加]をクリックします。
   - 証明書名を入力します。
   - 「証明書」の左にある「参照」をクリックし、新しい証明書ファイルを見つけます。
   - 「Certificate」の左側にある「Browse」をクリックし、CSRの作成時に保存した秘密キーを探します。
   - OpenSSLで秘密キーとCSRを作成するときに以前使用したパスワードを入力します。
   - 「アップロード」をクリックします。



3. 信頼できる証明書として新しい証明書をインポートします。
    - Settings > Certificate Managementに移動し、Trusted Certificatesをクリックします。
    - [証明書の追加]をクリックします。
    - 証明書名を入力します。これは、システム証明書で使用されている名前とは異なる名前にする必要があります。
    - 「証明書」の左にある「参照」をクリックし、新しい証明書ファイルを見つけます。
    - パスワードフィールドは空のままにしておくことができます。
    - 「アップロード」をクリックします。



4. 新しい証明書を使用するようにpxGridを設定します。
    - Settings > Certificate Managementに移動し、Settingsをクリックします。
    - まだ行っていない場合は、「pxGrid」の下の「CA証明書」を選択します。
    - 証明書のインポート中に作成されたシステム証明書名を選択します。
    - [Save] をクリックします。

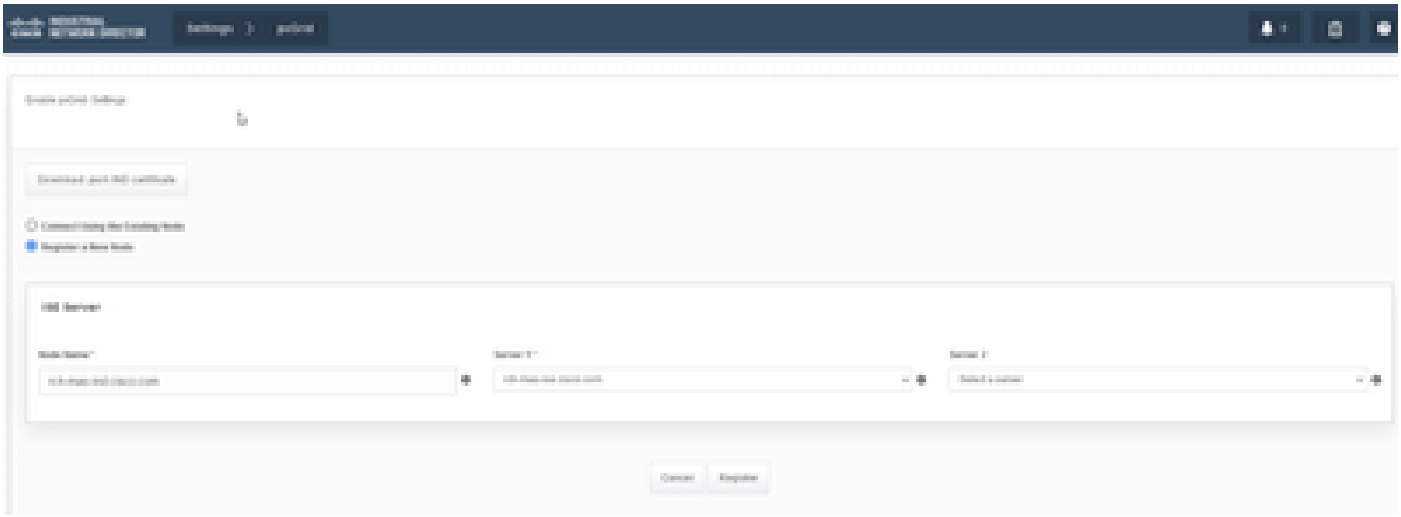
pxGridを有効にしてISEサーバに登録します。

IND GUI内：

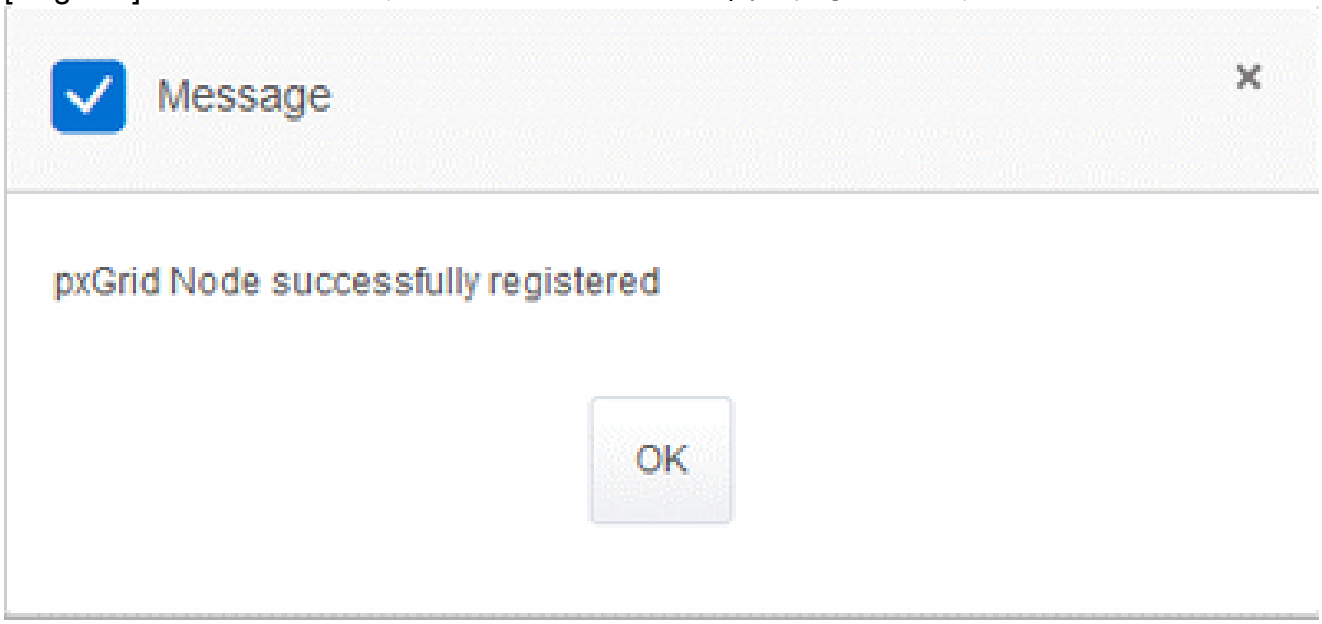
1. Settings > pxGridの順に移動します。
2. スライダをクリックしてpxGridを有効にします。
3. このINDサーバでpxGridをISEに初めて登録するときでない場合は、[Connect Using the Existing Node]を選択します。 INDノードとISEサーバ情報が自動的に入力されます。
4. pxGridを使用するために新しいINDサーバーを登録するには、必要に応じて「新規ノードの登録」を選択します。 INDノード名を入力し、必要に応じてISEサーバを選択

します。

- ISEサーバがサーバ1またはサーバ2のドロップダウンオプションに表示されない場合は、[設定] > [ポリシーサーバ]を使用して新しいpxGridサーバとして追加できます



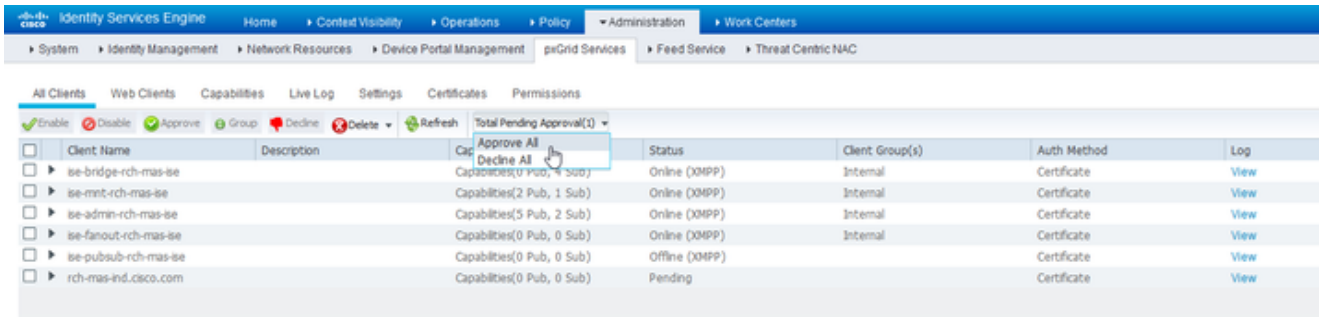
5. [Register] をクリックします。確認メッセージが画面に表示されます。



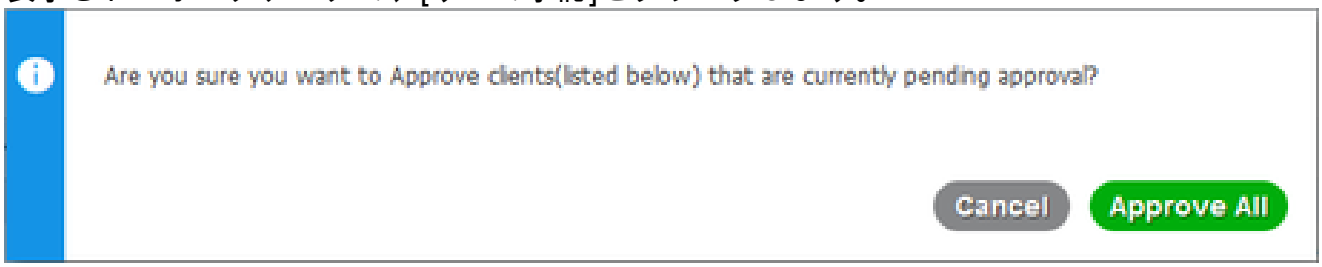
ISEサーバでの登録要求の承認

ISE GUI内：

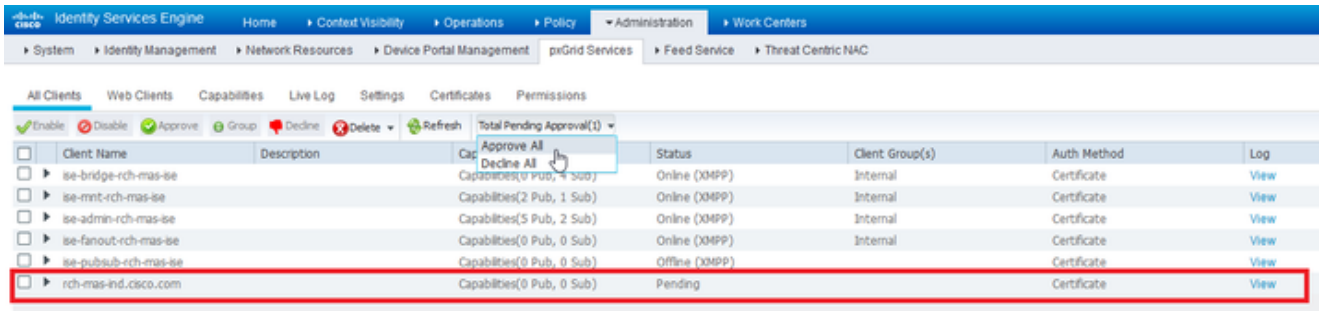
1. Administration > pxGrid Services > All Clientsの順に移動します。 承認保留中のリクエストには、「承認保留中の合計数(1)」と表示されます。
2. [承認待ちの合計数(1)]をクリックし、[すべて承認]を選択します。



3. 表示されるポップアップで、[すべて承認]をクリックします。



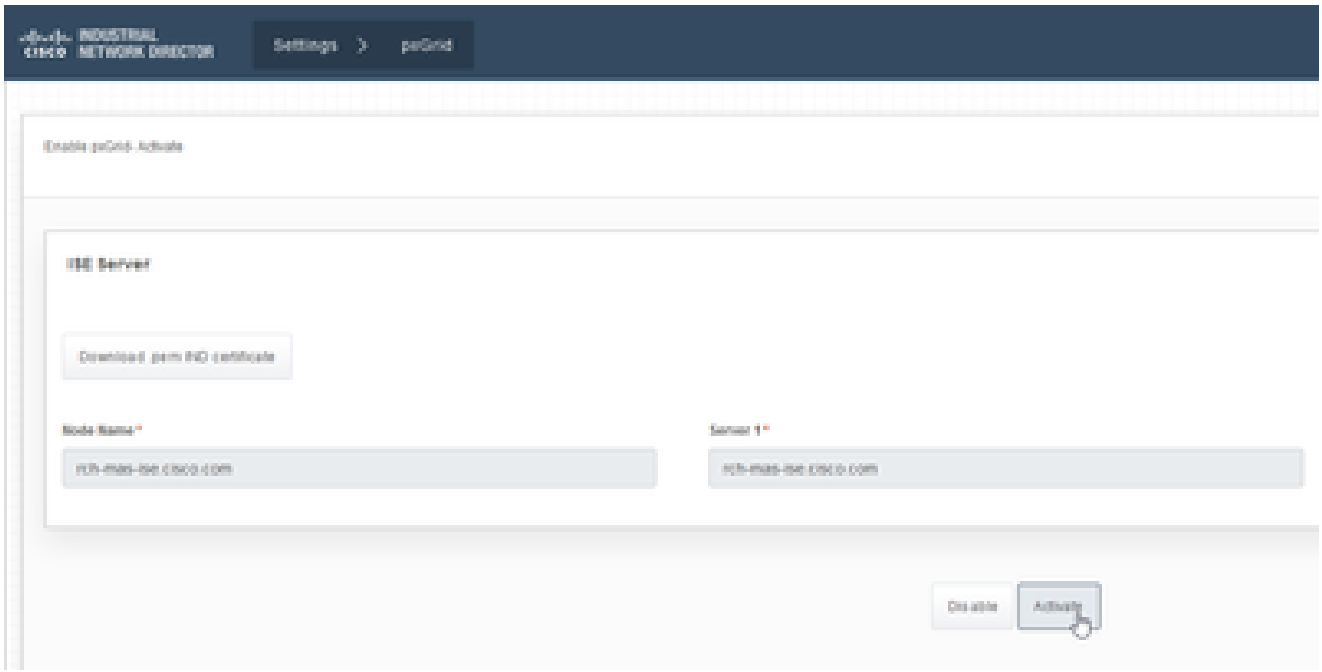
4. 次に示すように、INDサーバはクライアントとして表示されます。



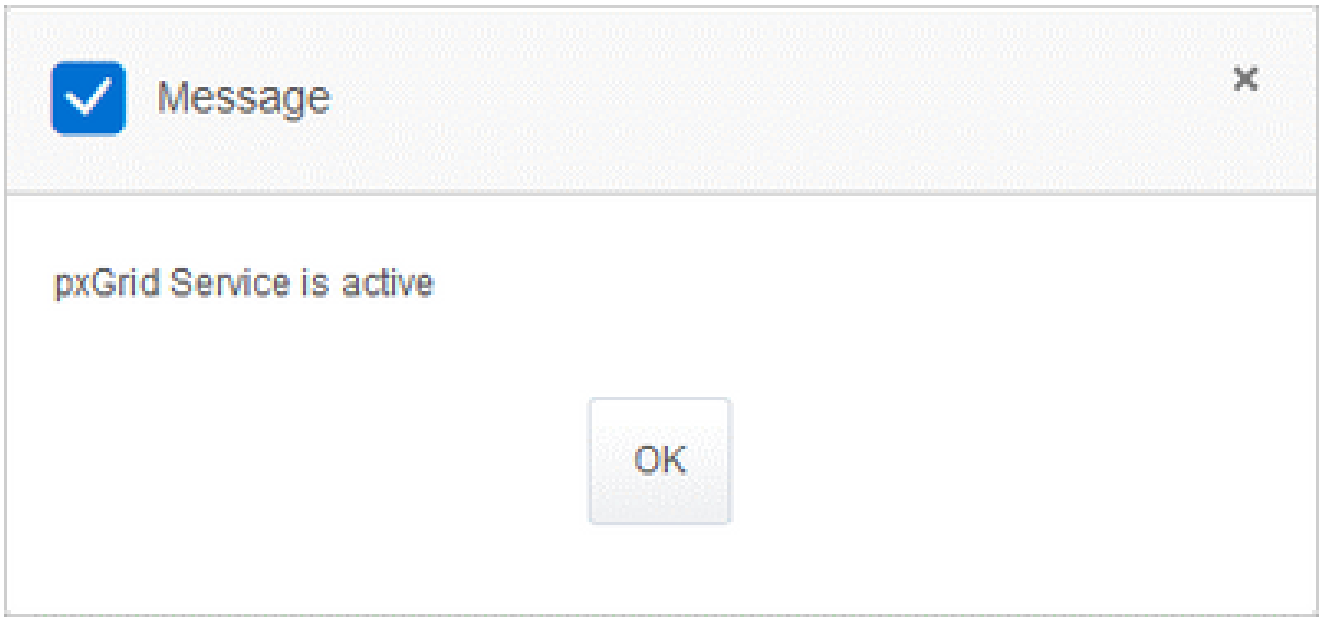
INDサーバでのpxGridサービスのアクティブ化

IND GUI内：

1. Settings > pxGridの順に移動します。
2. 「アクティブ化」をクリックします。



3. 確認メッセージが画面に表示されます。


Message
pxGrid Service is active
OK

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。