Criar certificados SAN para integração de IND e ISE pxGrid usando OpenSSL

Contents

Introdução

Este documento descreve como criar certificados SAN para integração pxGrid entre o Industrial Network Diretor (IND) e o Identity Services Engine.

Informações de Apoio

Ao criar certificados no Cisco ISE para uso do pxGrid, os nomes de host curtos do servidor não podem ser inseridos na GUI do ISE, pois o ISE permite apenas o FQDN ou o endereço IP.

Para criar certificados que incluam o nome do host e o FQDN, um arquivo de solicitação de certificado deve ser criado fora do ISE. Isso pode ser feito usando o OpenSSL para criar uma CSR (Solicitação de Assinatura de Certificado) com entradas do campo SAN (Nome Alternativo do Assunto).

Este documento não inclui etapas abrangentes para ativar a comunicação pxGrid entre o servidor IND e o servidor ISE. Essas etapas podem ser usadas após a configuração do pxGrid e após a confirmação de que o nome de host do servidor é necessário. Se esse erro for encontrado nos arquivos de log do ISE Profiler, a comunicação exigirá o certificado do nome de host.

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

As etapas para a implantação inicial do IND com comunicação pxGrid podem ser encontradas em https://www.cisco.com/c/dam/en/us/td/docs/switches/ind/install/IND_PxGrid_Registration_Guide_Final.pdf

Aplicativos necessários

- Diretor de rede industrial da Cisco (IND)
- Cisco Identity Services Engine (ISE)
- OpenSSL
    - Na maioria das versões modernas do Linux, assim como do MacOS, o pacote OpenSSL é instalado por padrão. Se você achar que os comandos não estão disponíveis, instale o OpenSSL usando o aplicativo de gerenciamento de pacotes do seu sistema operacional.

- Informações sobre o OpenSSL para Windows podem ser encontradas em https://wiki.openssl.org/index.php/Binaries

Informações adicionais

Para os fins deste documento, estes detalhes são usados:

- IND Nome do host do servidor: rch-mas-ind
- FQDN: rch-mas-ind.cisco.com
- Configuração do OpenSSL: rch-mas-ind.req
- Nome do arquivo de solicitação de certificado: rch-mas-ind.csr
- Nome do arquivo de chave privada: rch-mas-ind.pem
- Nome do arquivo de certificado: rch-mas-ind.cer

Etapas do processo

Criar o certificado CSR

1. Em um sistema com o OpenSSL instalado, crie um arquivo de texto de solicitação para as opções do OpenSSL, incluindo informações de SAN.
   - A maioria dos campos "_default" é opcional, pois as respostas podem ser inseridas durante a execução do comando OpenSSL na etapa #2.
   - Os detalhes da SAN (DNS.1, DNS.2) são obrigatórios e devem incluir o nome de host DNS curto e o FQDN do servidor. Nomes de DNS adicionais podem ser adicionados, se necessário, usando DNS.3, DNS.4, etc.
   - Exemplo de arquivo de texto de solicitação:

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

[nome]
countryName = Nome do país (código de 2 letras)
countryName_default = EUA
stateOrProvinceName = Nome do estado ou província (Nome completo)
stateOrProvinceName_default = TX
localityName = Cidade
localityName_default = Laboratório da Cisco
Nome da unidade organizacional = Nome da unidade organizacional (por exemplo, TI)
Nome_da_Unidade_organizacional = TAC
commonName = Nome comum (por exemplo, SEU nome)
commonName_max = 64
commonName_default = rch-mas-ind.cisco.com
emailAddress = Endereço de e-mail
emailAddress_max = 40
```

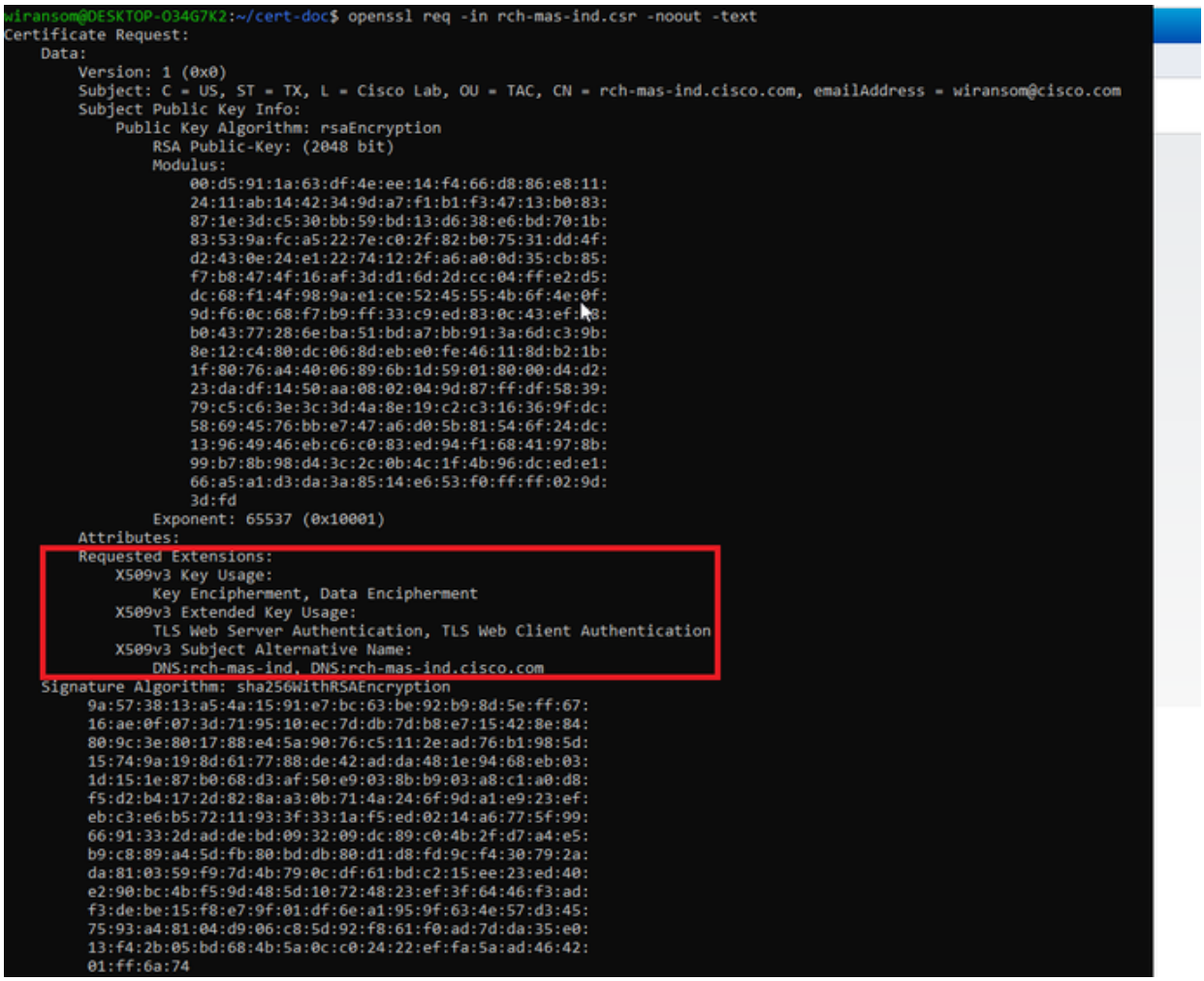
```
[v3_req]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @alt_names

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

2. Use o OpenSSL para criar o CSR com o nome de host DNS curto no campo SAN. Crie um arquivo de chave privada além do arquivo CSR.
    - Comando:
      openssl req -newkey rsa:2048 -keyout <servidor>.pem -out <servidor>.csr -config <servidor>.req
    - Quando solicitado, insira uma senha de sua escolha. Lembre-se dessa senha, pois ela será usada em etapas posteriores.
    - Insira um endereço de e-mail válido quando solicitado ou deixe o campo em branco e pressione <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. Se desejar, verifique as informações do arquivo CSR. Para obter um certificado de SAN, procure "x509v3 Subject Alternative Name" (Nome alternativo do assunto x509v3), conforme destacado nesta captura de tela.
    - Linha de comando:
      openssl req -in <servidor>.csr -noout -text



4. Abra o arquivo CSR em um editor de texto. Por motivos de segurança, a captura de tela de exemplo está incompleta e editada. O arquivo CSR gerado real contém mais linhas.

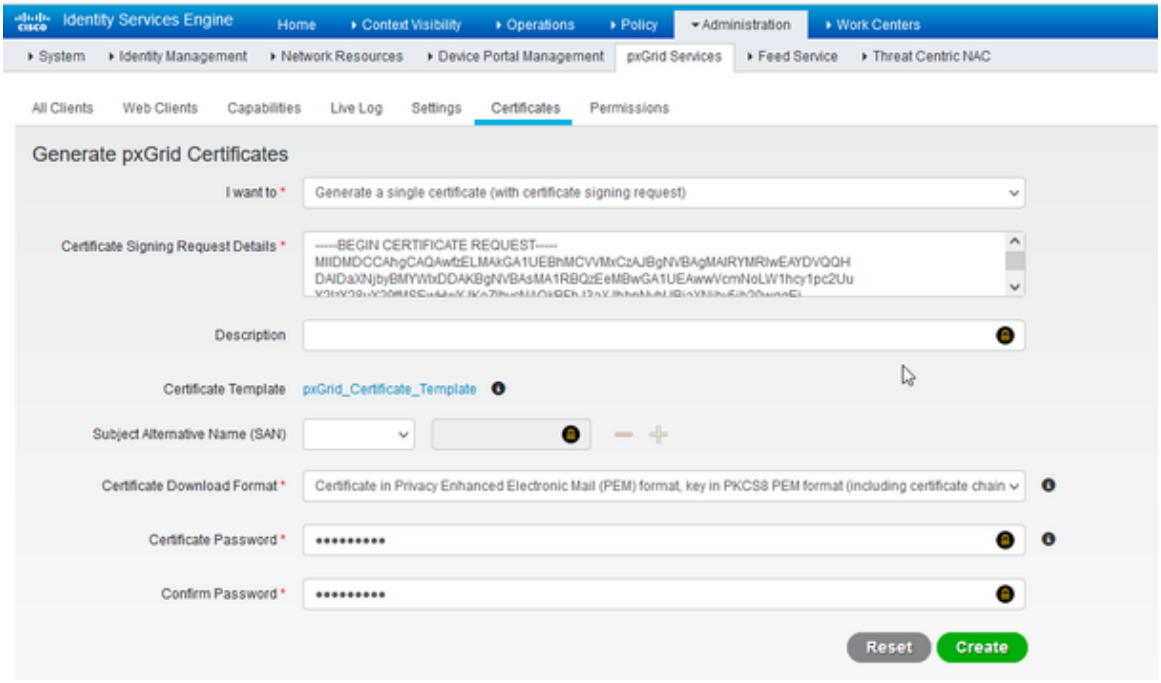
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDMDCCAhgCAQAwfzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAlRYMRIwEAYDVQQH
DAlDaXNjbyBMYWIxDDAKBgNVBAsMA1RBQzEeMBwGA1UEAwwVcmNoLW1hcy1pbmQu
Y2lzY28uY29tMSEwHwYJKoZIhvcNAQkBFhJ3aXJhbnNvbUBjaXNjby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVkRpj307uFPRm2IboESQRqxRC
NJ2n8bHzRxOwg4cePcUwu1m9E9Y45r1wG4NTmvylIn7AL4KwdTHdT9JDDiThInQS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

5. Copie o arquivo de chave privada (<servidor>.pem) para o seu PC como ele será usado em uma etapa posterior.

Usar o Cisco ISE para gerar um certificado, usando as informações do arquivo CSR criado

Na GUI do ISE:

1. Remova o cliente pxGrid existente.
    - Navegue até Administração > serviços do pxGrid > Todos os clientes.
    - Localize e selecione o nome de host do cliente existente, se listado,
    - Se encontrado e selecionado, clique no botão Excluir e escolha "Excluir selecionado". Confirme conforme necessário.
2. Crie o novo certificado.
    - Clique na guia Certificados na página de serviços do pxGrid.
    - Escolha as opções:
        - "Desejo":
            - "Gerar um único certificado (com solicitação de assinatura de certificado)"
        - "Detalhes da Solicitação de Assinatura de Certificado:
            - Copie/cole os detalhes de CSR do editor de texto. Certifique-se de incluir as linhas BEGIN e END.
        - "Certificate Download Format" (Formato de download de certificado)
            - "Certificado no formato Privacy Enhanced Electronic Mail (PEM), chave no formato PKCS8 PEM."
        - Insira uma senha de certificado e confirme-a.
        - Clique no botão Criar.

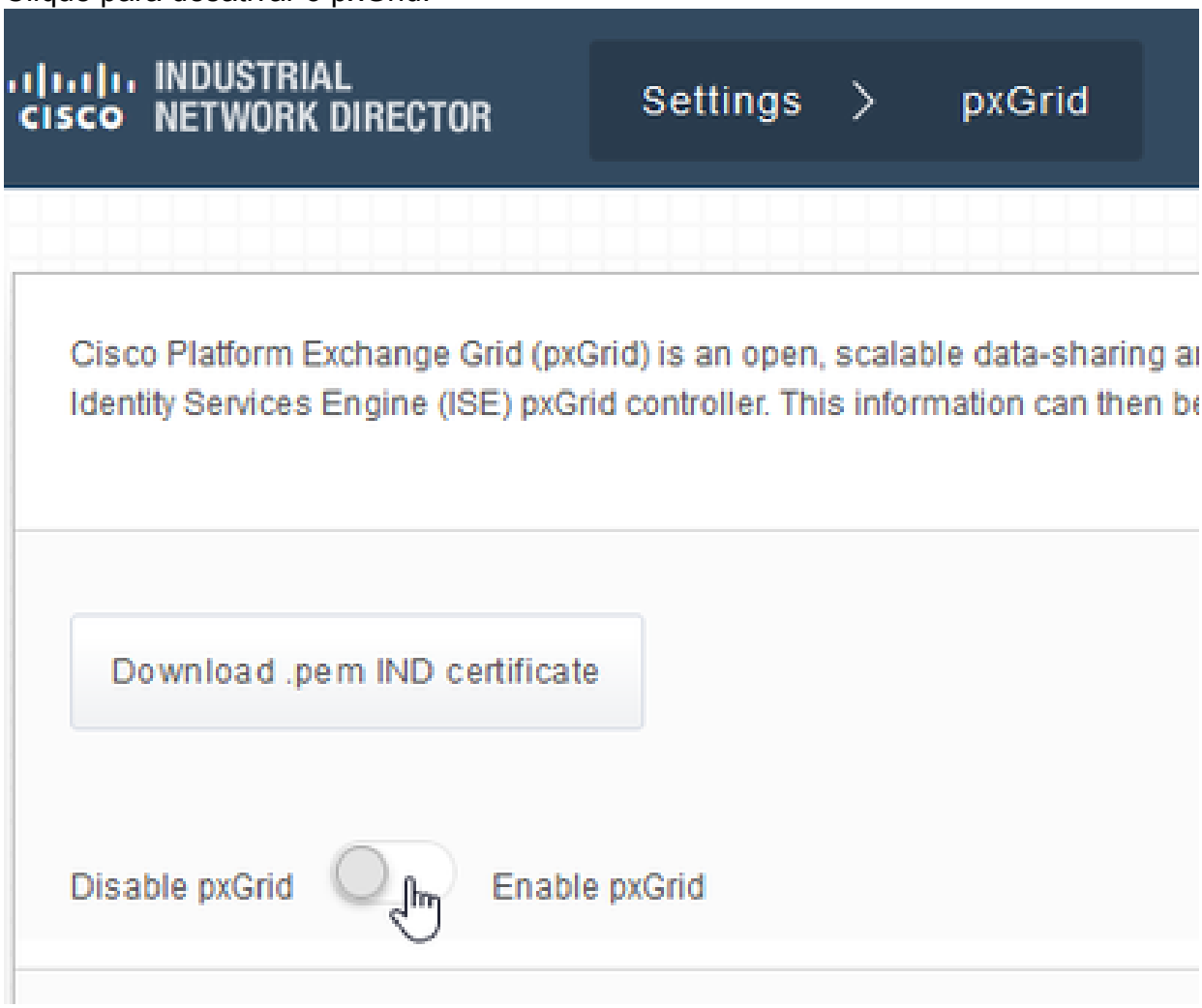


        - Isso cria e baixa um arquivo ZIP que contém o arquivo de certificado, bem como arquivos adicionais para a cadeia de certificados. Abra o ZIP e extraia o certificado.
            - O nome do arquivo é normalmente <IND server fqdn>.cer
            - Em algumas versões do ISE, o nome do arquivo é <IND fqdn>_<IND short name>.cer

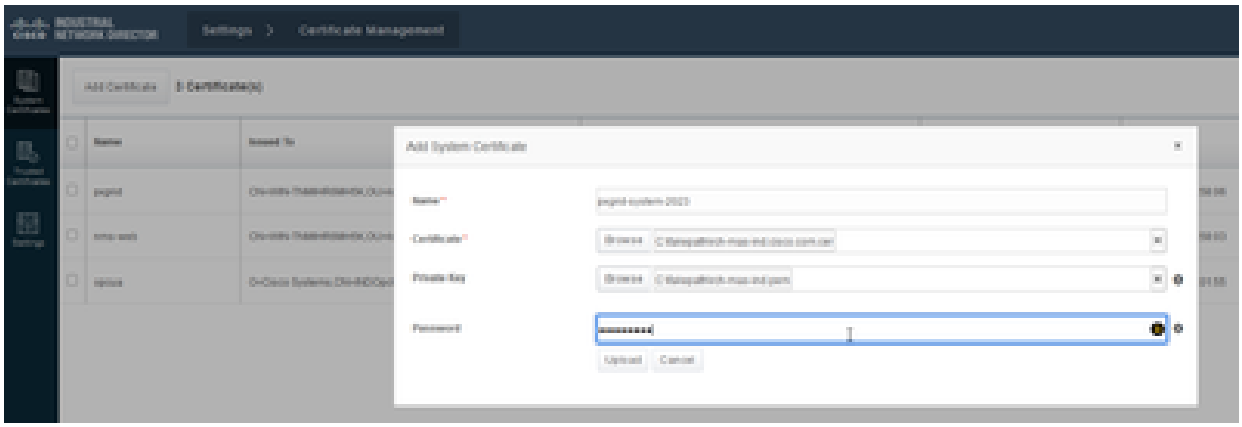
Importe o novo certificado para o servidor IND e habilite-o para uso do pxGrid

Na GUI do IND:

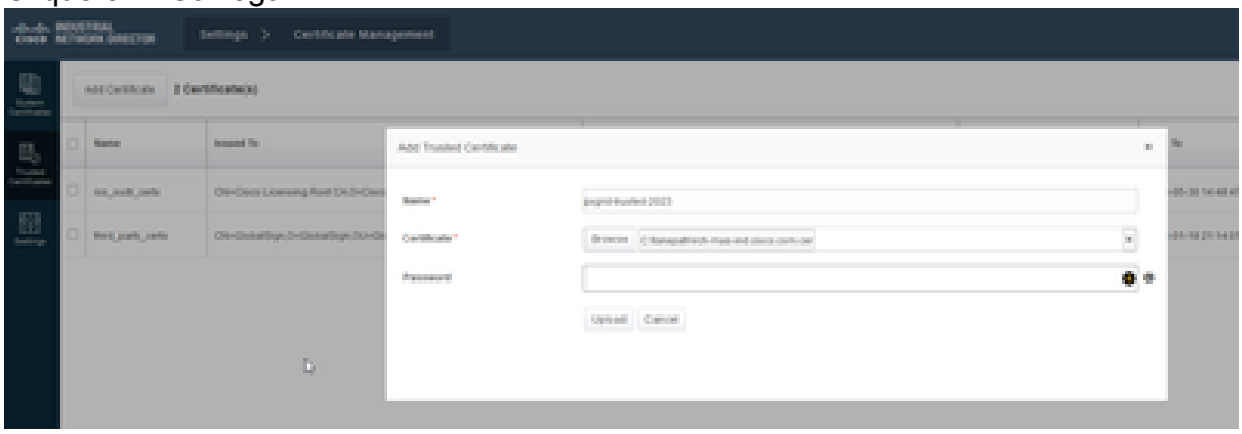
1. Desabilite o serviço pxGrid para que o novo certificado possa ser importado e definido como o certificado ativo.
    - Navegue até Configurações > pxGrid.
    - Clique para desativar o pxGrid.



2. Importe o novo certificado para Certificados do Sistema.
    - Navegue até Configurações > Gerenciamento de certificados.
    - Clique em "Certificados do sistema"
    - Clique em "Adicionar certificado".
    - Insira um nome de certificado.
    - Clique em "Procurar" à esquerda de "Certificado" e localize o novo arquivo de certificado.
    - Clique em "Procurar" à esquerda de "Certificado" e localize a chave privada salva ao criar o CSR.
    - Insira a senha usada anteriormente ao criar a chave privada e CSR com OpenSSL.
    - Clique em "Carregar".



3. Importe o novo certificado como um certificado confiável.
    - Navegue para Configurações > Gerenciamento de Certificados e clique em "Certificados de Confiabilidade".
    - Clique em "Adicionar certificado".
    - Insira um nome de certificado; esse deve ser um nome diferente do usado em Certificados do Sistema.
    - Clique em "Procurar" à esquerda de "Certificado" e localize o novo arquivo de certificado.
    - O campo da senha pode ser deixado em branco.
    - Clique em "Carregar".



4. Defina pxGrid para usar o novo certificado.
    - Navegue até Configurações > Gerenciamento de certificados e clique em "Configurações".
    - Se ainda não tiver feito isso, selecione "CA Certificate" em "pxGrid".
    - Selecione o nome do certificado do sistema criado durante a importação do certificado.
    - Click Save.

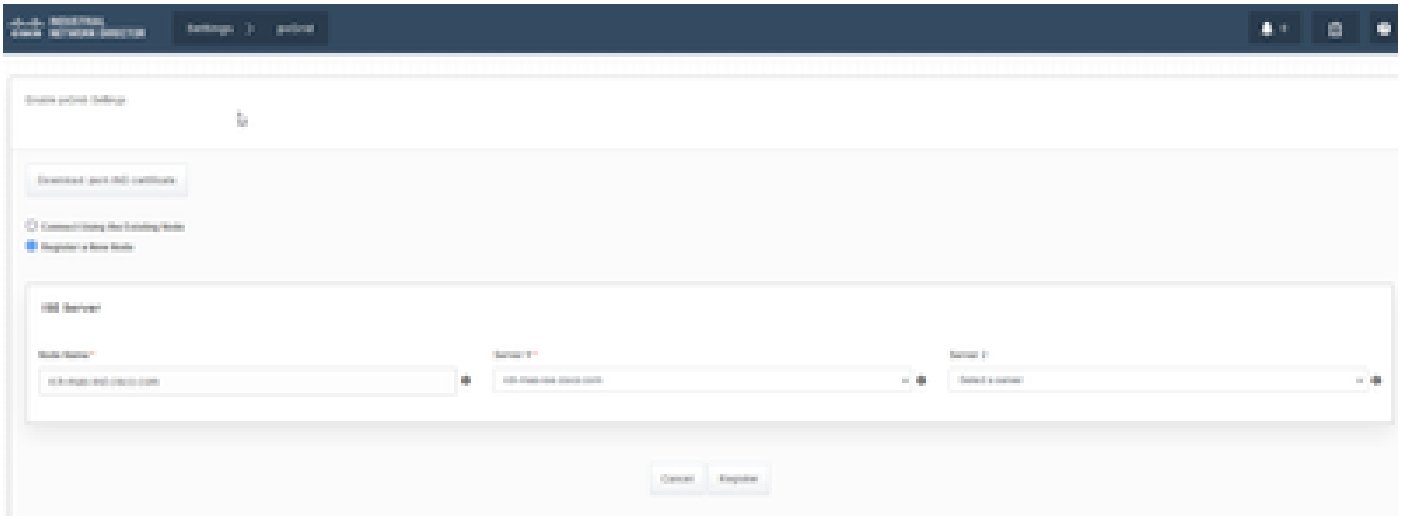
Habilitar e registrar o pxGrid com o servidor ISE

Na GUI do IND:

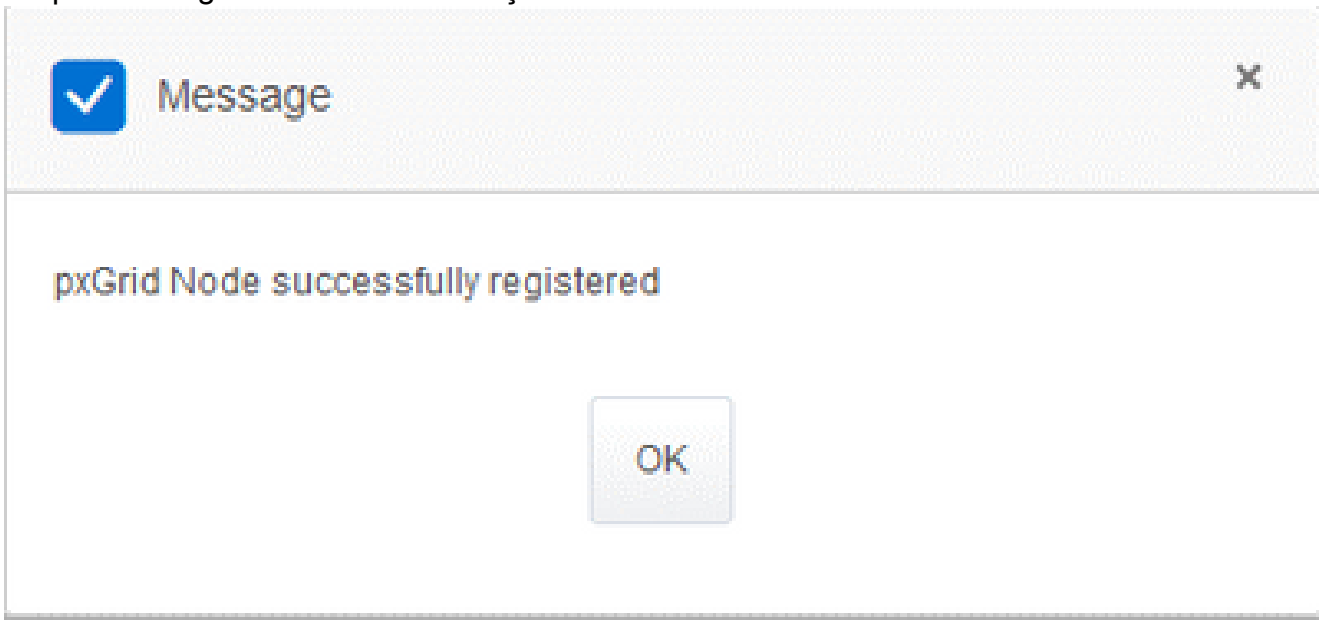
1. Navegue até Configurações > pxGrid.
2. Clique no controle deslizante para Ativar pxGrid.
3. Se esta não for a primeira vez que o pxGrid é registrado com o ISE neste servidor IND, escolha "Conectar usando o nó existente". As informações do nó IND e do

servidor ISE são preenchidas automaticamente.

4. Para registrar um novo servidor IND para usar o pxGrid, se necessário, escolha "Registrar um Novo Nó". Insira o nome do nó IND e escolha os servidores ISE conforme necessário.
    - Se o servidor ISE não estiver listado nas opções suspensas do Servidor 1 ou Servidor 2, ele poderá ser adicionado como um novo servidor pxGrid usando Configurações > Servidor de políticas



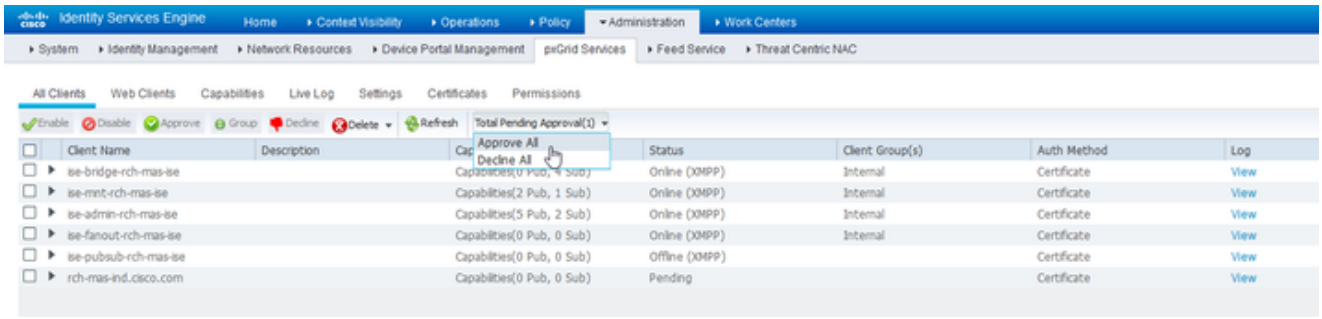
5. Clique em Registrar. Uma confirmação é mostrada na tela.



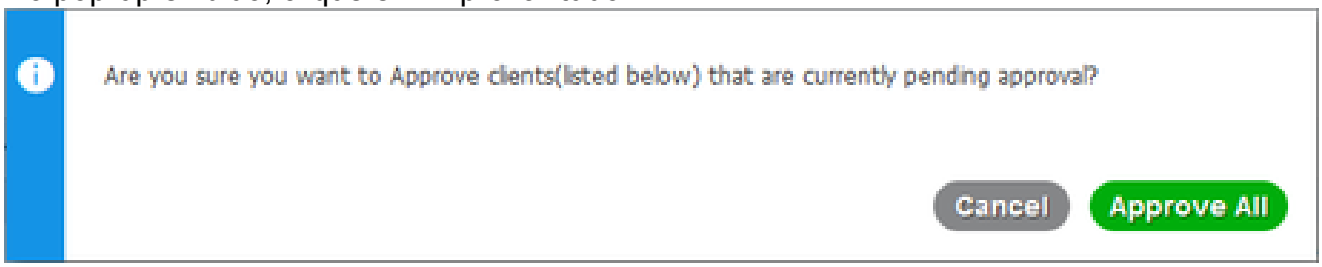
Aprovar solicitação de registro no servidor ISE

Na GUI do ISE:

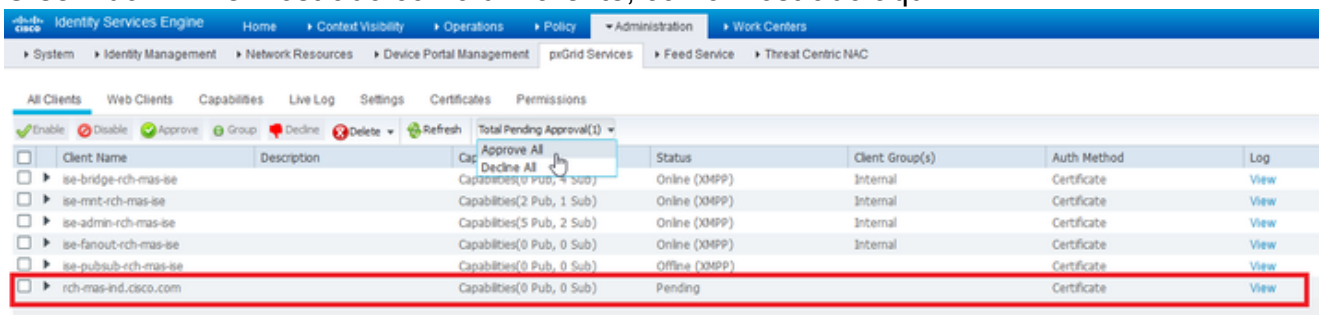
1. Navegue até Administração > serviços do pxGrid > Todos os clientes. Uma solicitação com aprovação pendente mostra "Total com aprovação pendente(1)".
2. Clique em "Total de Aprovações Pendentes(1)" e selecione "Aprovar Tudo".



3. No pop-up exibido, clique em "Aprovar tudo".



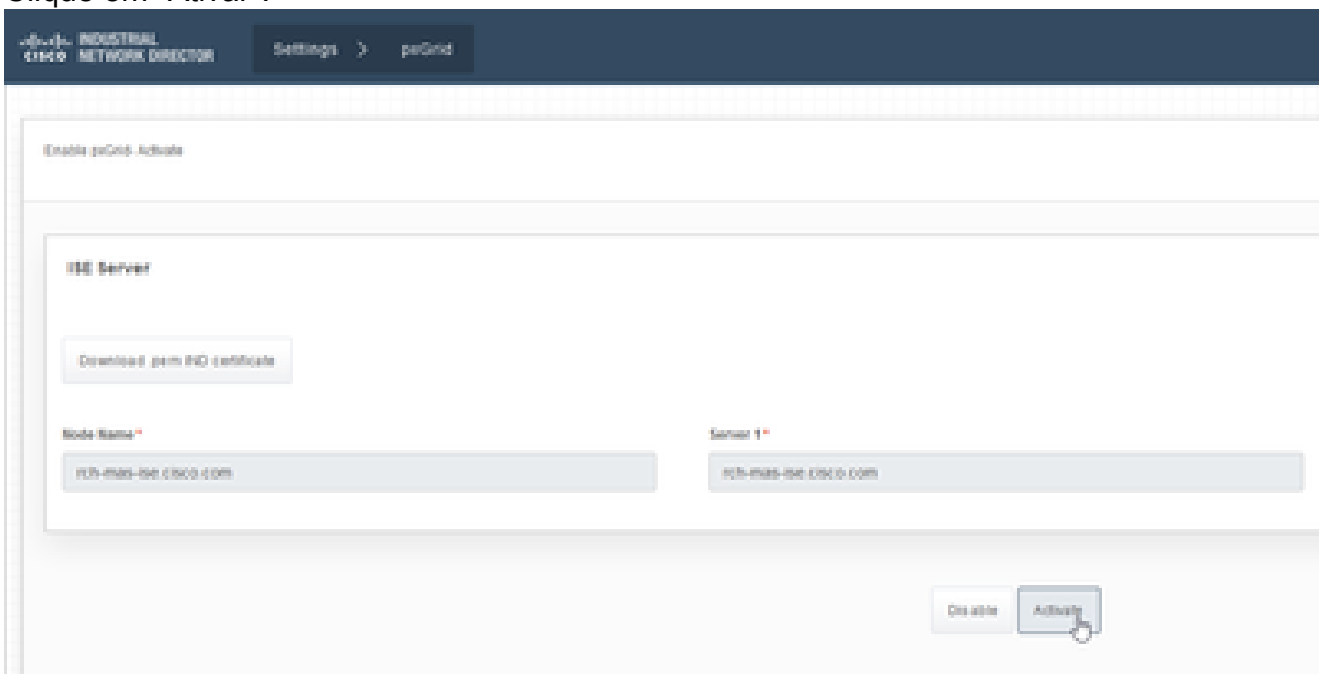
4. O servidor IND é mostrado como um cliente, como mostrado aqui.



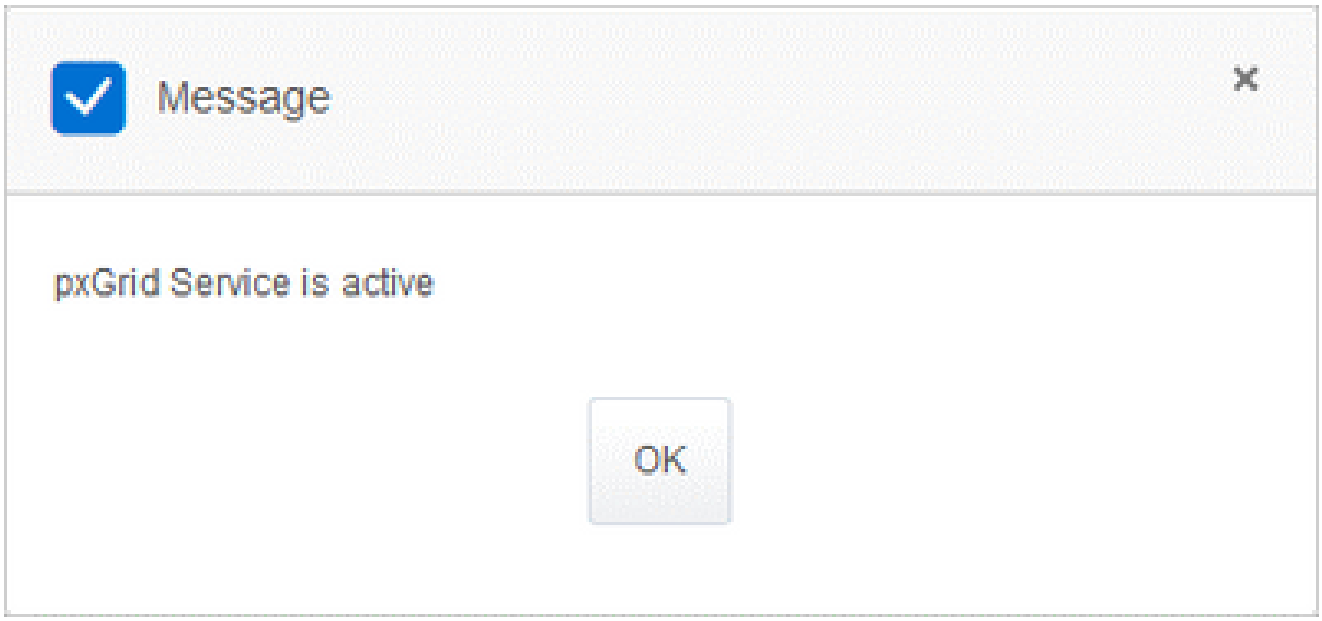
Ativar o serviço pxGrid no servidor IND

Na GUI do IND:

1. Navegue até Configurações > pxGrid.
2. Clique em "Ativar".



3. Uma confirmação é mostrada na tela.


Message
pxGrid Service is active
OK

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.