使用OpenSSL为IND和ISE pxGrid集成创建SAN证书

目录

简介

本文档介绍如何为Industrial Network Director(IND)和身份服务引擎之间的pxGrid集成创建SAN证书。

背景信息

在Cisco ISE中为pxGrid使用创建证书时，无法将服务器短主机名输入到ISE GUI，因为ISE仅允许FQDN或IP地址。

要创建包含主机名和FQDN的证书，必须在ISE之外创建证书请求文件。可以使用OpenSSL创建证书签名请求(CSR)和主题备用名称(SAN)字段条目。

本文档不包括在IND服务器和ISE服务器之间启用pxGrid通信的全面步骤。 这些步骤可在配置pxGrid后使用，并确认需要服务器主机名。 如果在ISE分析器日志文件中发现此错误，则通信需要主机名证书。

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

通过pxGrid通信初始部署IND的步骤位于https://www.cisco.com/c/dam/en/us/td/docs/switches/ind/install/IND_PxGrid_Registration_Guide_Final.pdf

所需的应用程序

- 思科工业网络导向器(IND)
- 思科身份服务引擎(ISE)
- OpenSSL
  - 在大多数现代Linux版本以及MacOS中，默认情况下会安装OpenSSL软件包。如果您发现命令不可用，请使用操作系统的软件包管理应用程序安装OpenSSL。
  - 有关OpenSSL for Windows的信息，请访问https://wiki.openssl.org/index.php/Binaries

其他信息

本文档使用以下详细信息：

- IND服务器主机名：rch-mas-ind
- FQDN:rch-mas-ind.cisco.com
- OpenSSL配置：rch-mas-ind.req
- 证书请求文件名：rch-mas-ind.csr
- 私钥文件名：rch-mas-ind.pem
- 证书文件名：rch-mas-ind.cer

流程步骤

创建证书CSR

1. 在安装了OpenSSL的系统上，为OpenSSL选项（包括SAN信息）创建请求文本文件。
    - 大多数“_default”字段是可选的，因为在步骤10中运行OpenSSL命令时可以输入答#2。
    - SAN详细信息(DNS.1、DNS.2)是必需的，必须包括DNS短主机名和服务器的FQDN。如果需要，可以使用DNS.3、DNS.4等添加其他DNS名称。
    - 请求文件文本文件示例：

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

[姓名 ]
countryName =国家/地区名称（2个字母代码）
countryName_default =美国
stateOrProvinceName =省或省名称（全称）
stateOrProvinceName_default = TX
localityName =城市
localityName_default = Cisco Lab
organizationalUnitName =组织单位名称（例如，IT）
organizationalUnitName_default = TAC
commonName =通用名称（例如，您的名称）
commonName_max = 64
commonName_default = rch-mas-ind.cisco.com
emailAddress =电子邮件地址
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. 使用OpenSSL在SAN字段中创建具有DNS短主机名的CSR。除CSR文件外，创建私钥文件。
    - 命令:

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

- 出现提示时，输入您选择的密码。 请务必记住此密码，在后面的步骤中会用到它。
- 出现提示时，请输入有效的电子邮件地址，或将该字段留空，然后按<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. 如果需要，请验证CSR文件信息。对于SAN证书，请检查“x509v3 Subject Alternative Name”（x509v3主题备用名称），如本屏幕截图中所突出显示。
   - 命令行:

     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:
                    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
```

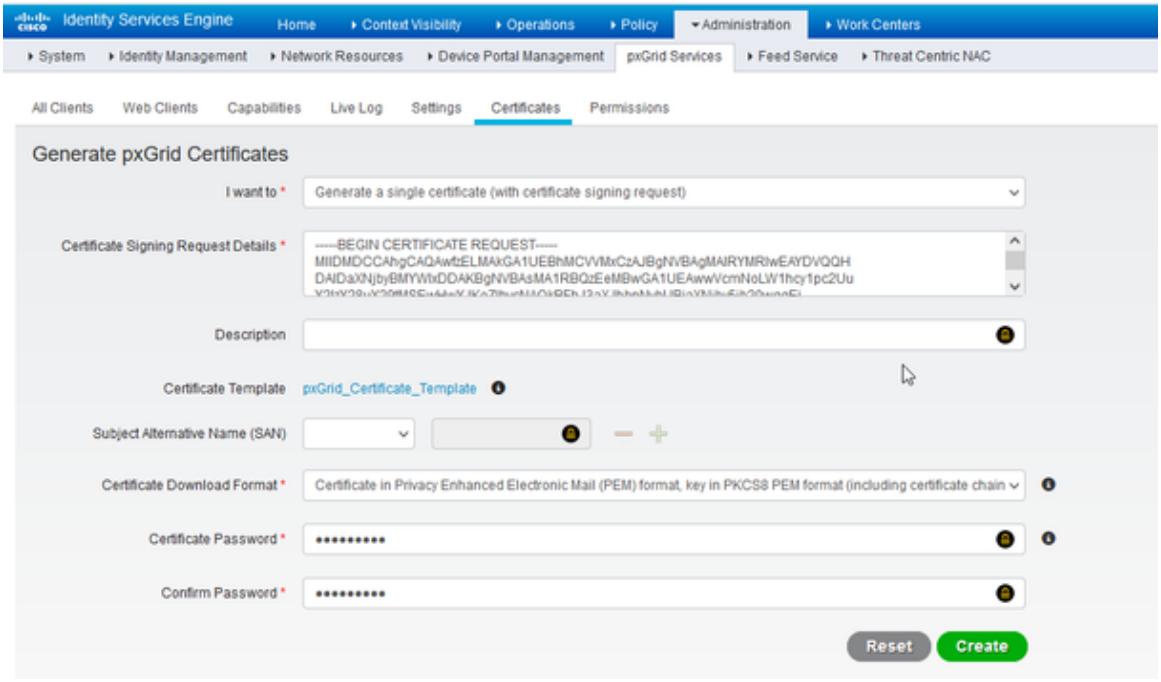
4. 在文本编辑器中打开CSR文件。 出于安全原因，示例屏幕截图不完整且经过编辑。 实际生成的CSR文件包含更多行。

5. 将私钥文件(<server>.pem)复制到您的PC，就像在后续步骤中所使用的一样。

使用思科ISE生成证书，使用创建的CSR文件信息

在ISE GUI中：

1. 删除现有的pxGrid客户端。
    - 导航到Administration > pxGrid Services > All Clients。
    - 查找并选择现有客户端主机名（如果列出），
    - 如果找到并选中，请点击Delete按钮，然后选择“Delete Selected”。 根据需要进行确认。
2. 创建新证书。
    - 点击pxGrid服务页面上的Certificates选项卡。
    - 选择以下选项：
        - “我想”：
            - "生成单个证书（包含证书签名请求）"
        - "证书签名请求详细信息：
            - 从文本编辑器中复制/粘贴CSR详细信息。 请务必包含BEGIN和END行。
        - "证书下载格式"
            - "隐私增强型电子邮件(PEM)格式的证书，PKCS8 PEM格式的密钥。"
        - 输入证书密码并确认。
        - 点击Create按钮。

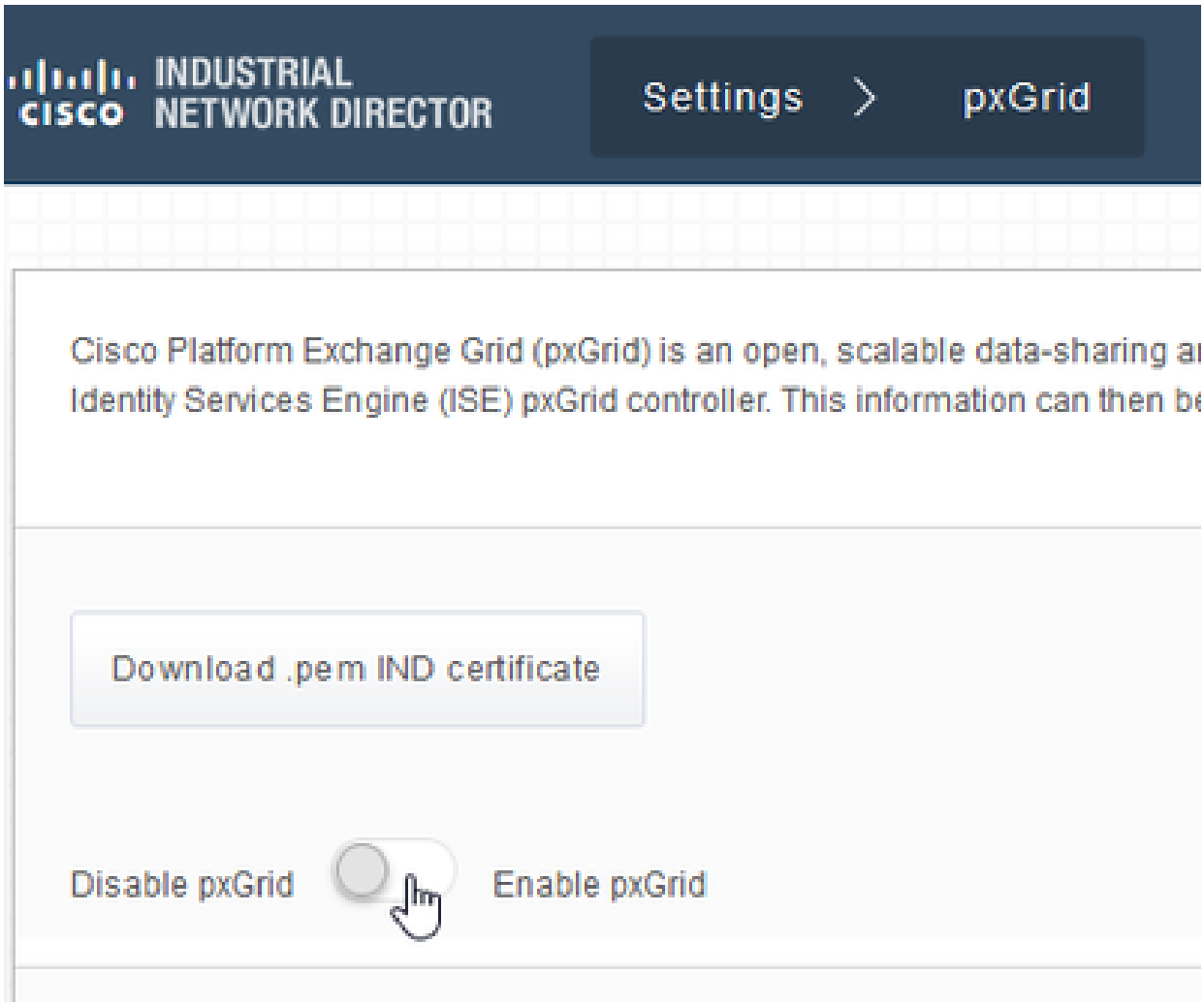


- 这将创建和下载包含证书文件以及证书链的其他文件的ZIP文件。打开ZIP并解压缩证书。
  - 文件名通常为<IND server fqdn>.cer
  - 在ISE的某些版本中，文件名是<IND fqdn>_<IND short name>.cer

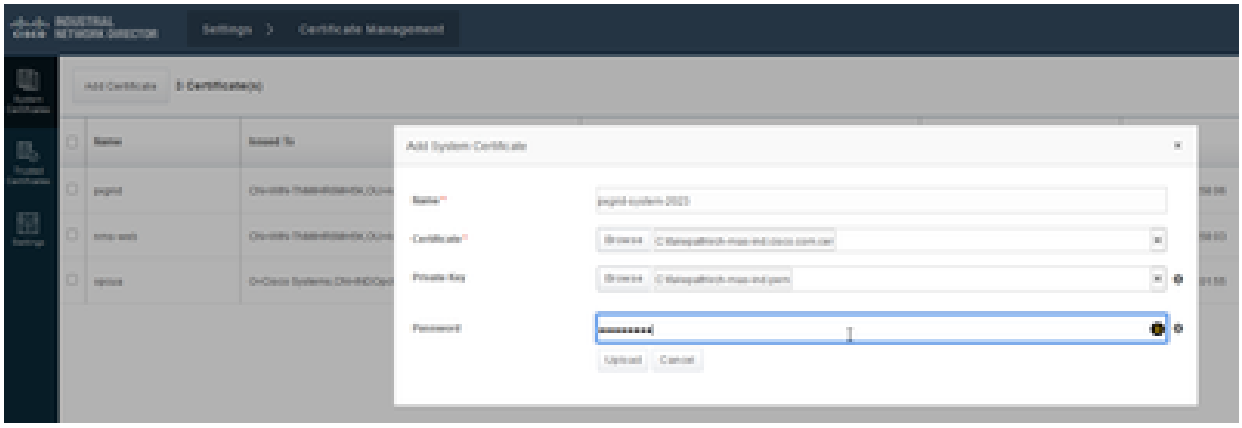
将新证书导入IND服务器，并启用它以供pxGrid使用

在IND GUI中：

1. 禁用pxGrid服务，以便可以导入新证书并将其设置为活动证书。
   - 导航到Settings（设置）> pxGrid。
   - 单击以禁用pxGrid。

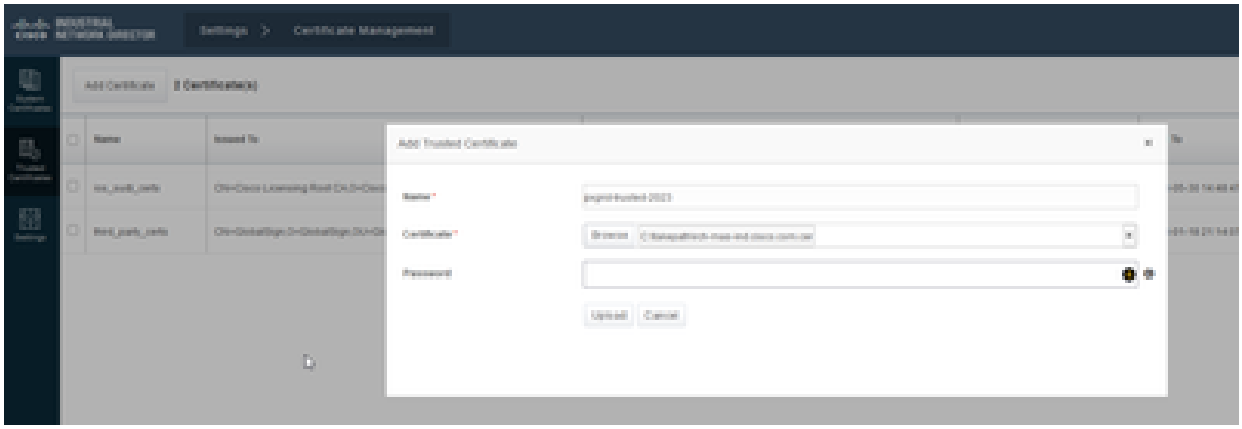


2. 将新证书导入系统证书。
   - 导航到Settings（设置）> Certificate Management（证书管理）。
   - 点击“System Certificates”（系统证书）
   - 点击“添加证书”。
   - 输入证书名称。
   - 单击“证书”左侧的“浏览”，然后找到新的证书文件。
   - 点击“证书”左侧的“浏览”，并找到创建CSR时保存的私钥。
   - 输入之前使用OpenSSL创建私钥和CSR时使用的密码。
   - 点击“上传”。



3. 将新证书导入为受信任证书。
   - 导航到Settings > Certificate Management，点击Trusted Certificates。

- 点击“添加证书”。
- 输入证书名称；该名称必须不同于系统证书上使用的名称。
- 点击“证书”左侧的“浏览”并找到新的证书文件。
- 密码字段可以留空。
- 点击“上传”。

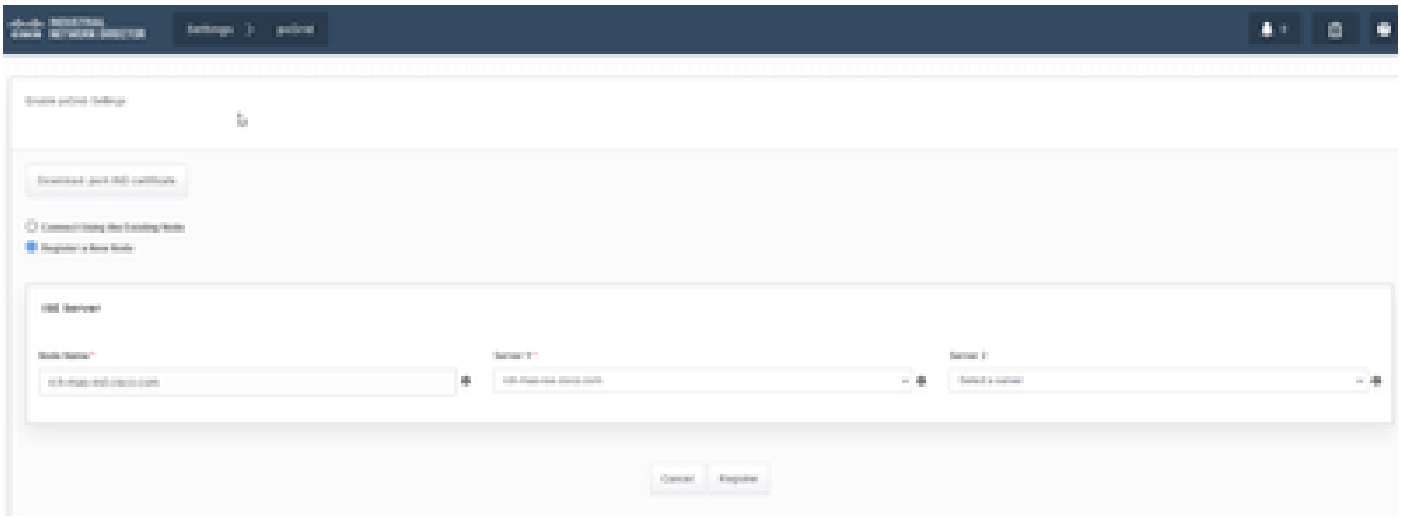


4. 设置pxGrid以使用新证书。
    - 导航到Settings（设置）> Certificate Management（证书管理），单击Settings（设置）。
    - 如果尚未完成，请选择“pxGrid”下的“CA证书”。
    - 选择在证书导入过程中创建的系统证书名称。
    - Click Save.

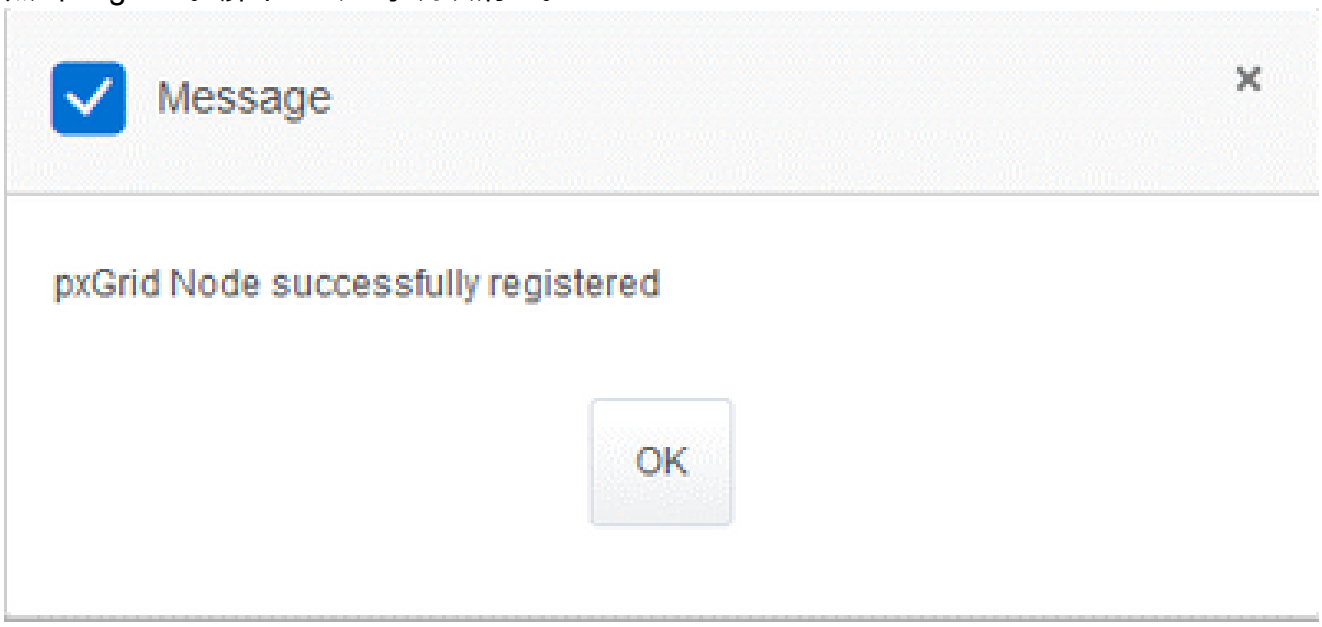
在ISE服务器中启用并注册pxGrid

在IND GUI中：

1. 导航到Settings（设置）> pxGrid。
2. 点击滑块以启用pxGrid。
3. 如果这不是第一次在此IND服务器上向ISE注册pxGrid，请选择“使用现有节点连接”。 会自动填充IND节点和ISE服务器信息。
4. 要注册新的IND服务器以使用pxGrid，如果需要，请选择“注册新节点”。 输入IND节点名称，并根据需要选择ISE服务器。
    - 如果ISE服务器未列在服务器1或服务器2的下拉选项中，可以使用Settings > Policy Server将其添加为新的pxGrid服务器



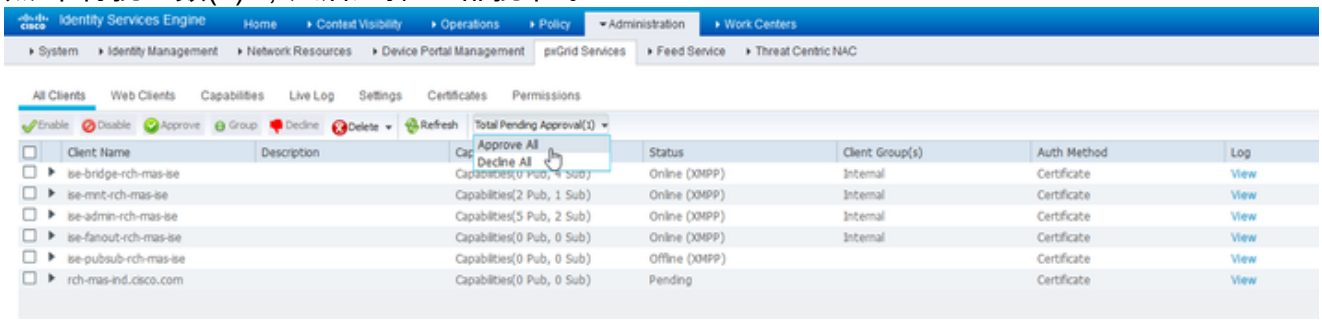
5. 点击Register。屏幕上会显示确认消息。



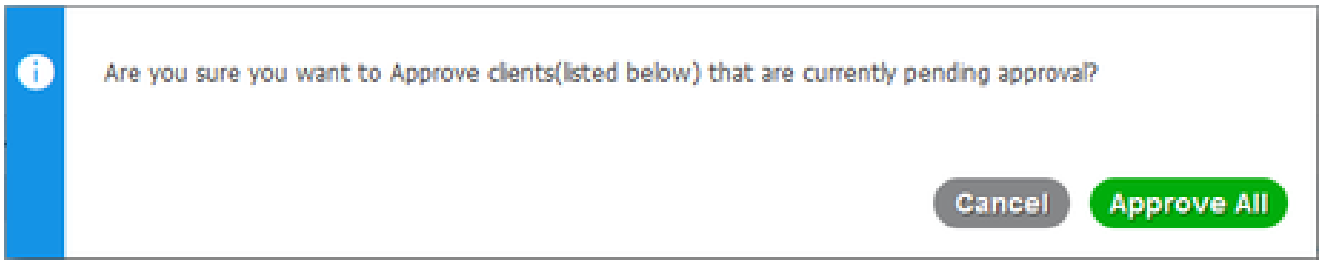
在ISE服务器中批准注册请求

在ISE GUI中：

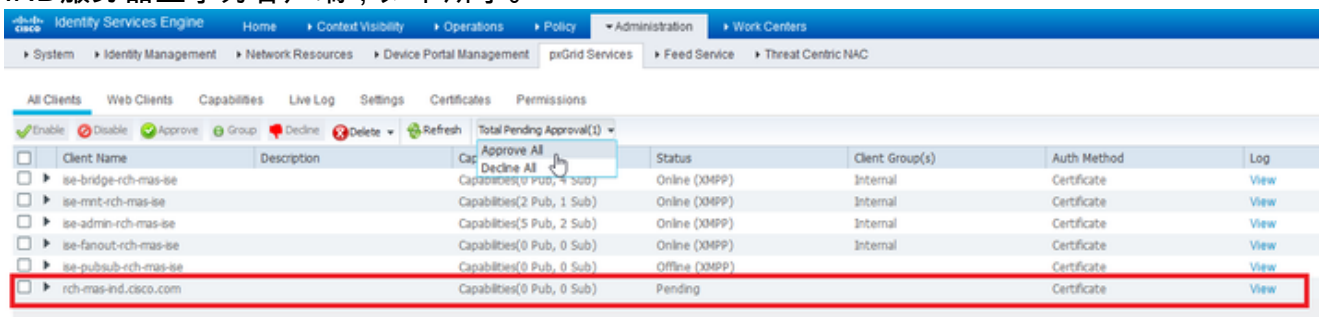
1. 导航到Administration > pxGrid Services > All Clients。 待批准请求显示为“待批准总数(1)”。
2. 点击“待批总数(1)”，然后选择“全部批准”。



3. 在显示的弹出窗口中，点击“全部批准”。



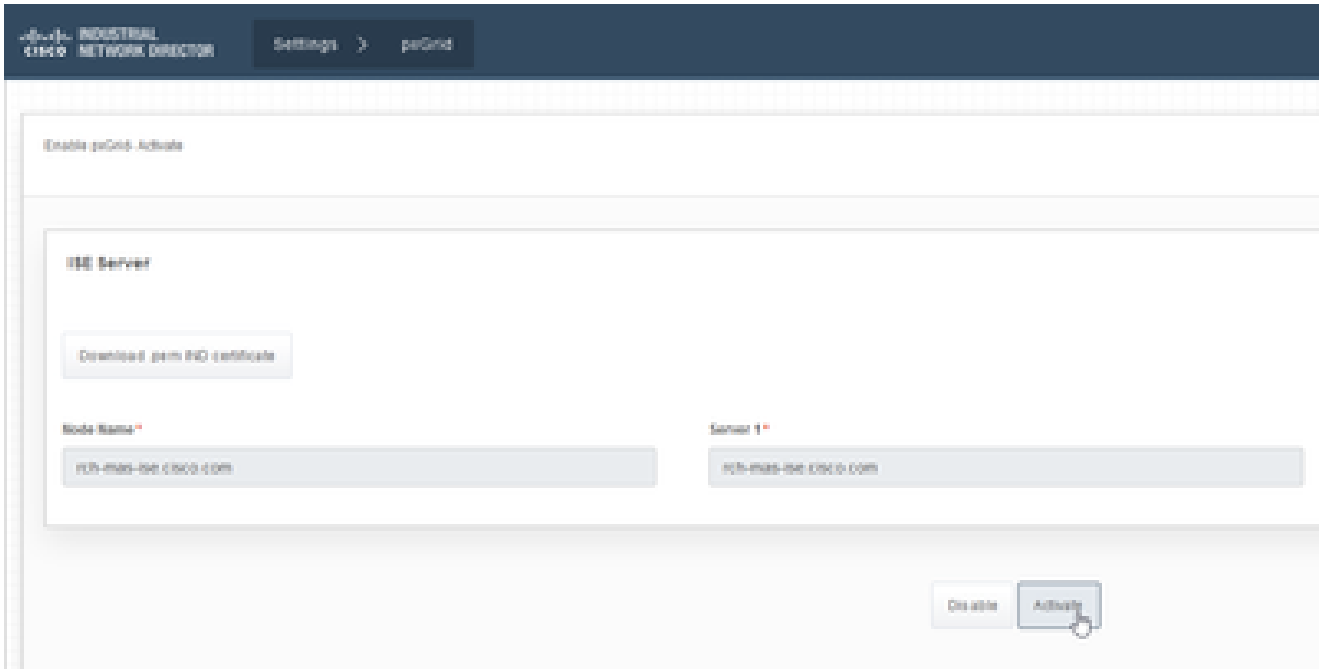
4. IND服务器显示为客户端，如下所示。



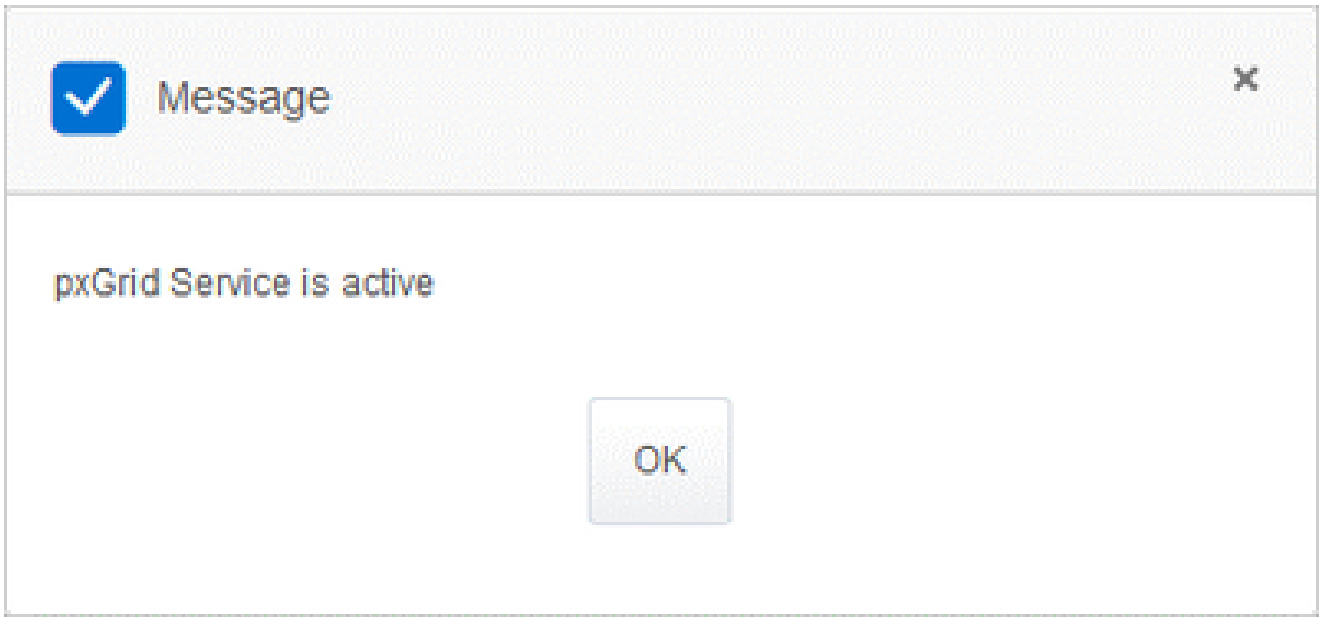
在IND服务器中激活pxGrid服务

在IND GUI中：

1. 导航到Settings（设置）> pxGrid。
2. 点击“激活”。



3. 屏幕上会显示确认消息。


Message
pxGrid Service is active
OK

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。