使用OpenSSL為IND和ISE pxGrid整合建立SAN證書

目錄

簡介

本文檔介紹如何為Industrial Network Director(IND)和Identity Services Engine之間的pxGrid整合建立SAN證書。

背景資訊

在Cisco ISE中為pxGrid使用建立證書時，無法將伺服器短主機名輸入到ISE GUI中，因為ISE僅允許FQDN或IP地址。

若要建立包含主機名和FQDN的證書，必須在ISE之外建立證書請求檔案。可以使用OpenSSL建立證書簽名請求(CSR)以及使用者替代名稱(SAN)欄位條目。

本文檔不包括在IND伺服器和ISE伺服器之間啟用pxGrid通訊的全面步驟。 在配置pxGrid並確認需要伺服器主機名後，可以使用這些步驟。 如果在ISE探查器日誌檔案中發現此錯誤，通訊需要主機名證書。

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

有關使用pxGrid通訊的IND初始部署步驟，請訪問 https://www.cisco.com/c/dam/en/us/td/docs/switches/ind/install/IND_PxGrid_Registration_Guide_Final.pdf

需要的應用程式

- Cisco Industrial Network Director(IND)
- 思科身分識別服務引擎(ISE)
- OpenSSL
  - 在多數現代Linux版本以及MacOS中，OpenSSL包是預設安裝的。如果您發現命令不可用，請使用作業系統的軟體包管理應用程式安裝OpenSSL。
  - 有關OpenSSL for Windows的資訊，請訪問https://wiki.openssl.org/index.php/Binaries

其他資訊

就本檔案而言，使用下列詳細資訊：

- IND伺服器主機名：rch-mas-ind
- FQDN:rch-mas-ind.cisco.com
- OpenSSL配置：rch-mas-ind.req
- 證書請求檔名： rch-mas-ind.csr
- 私鑰檔名：rch-mas-ind.pem
- 證書檔名： rch-mas-ind.cer

流程步驟

建立證書CSR

1. 在安裝了OpenSSL的系統上，為OpenSSL選項（包括SAN資訊）建立一個請求文本檔案。
    - 大多數「_default」欄位是可選的，因為可以在步驟10中運行OpenSSL命令時輸入答#2。
    - SAN詳細資訊(DNS.1、DNS.2)是必需的，必須包括DNS短主機名以及伺服器的FQDN。如果需要，可以使用DNS.3、DNS.4等新增其他DNS名稱。
    - 請求檔案文本檔案示例：

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

[名稱]
countryName =國家/地區名稱（2個字母代碼）
countryName_default =美國
stateOrProvinceName =州或省名稱（全稱）
stateOrProvinceName_default = TX
localityName =城市
localityName_default = Cisco Lab
organizationalUnitName =組織單位名稱（例如IT）
organizationalUnitName_default = TAC
commonName =公用名（例如，您的姓名）
commonName_max = 64
commonName_default = rch-mas-ind.cisco.com
emailAddress =電子郵件地址
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欄位中建立具有DNS短主機名的CSR。除CSR檔案外，再建立私密金鑰

檔案。

- 指令:

  openssl req -newkey rsa:2048 -keyout <server>.pem -out <server>.csr -config <server>.req
- 出現提示時，輸入您選擇的密碼。 請務必記住此密碼，如同在後續步驟中使用。
- 出現提示時輸入有效的電子郵件地址，或將該欄位留空，然後按<ENTER>鍵。

```
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，請驗證CSR檔案資訊。對於SAN證書，請檢查「x509v3 Subject Alternative Name」（x509v3主題備用名稱），如本螢幕快照中突出顯示。

- 命令列：

  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
```

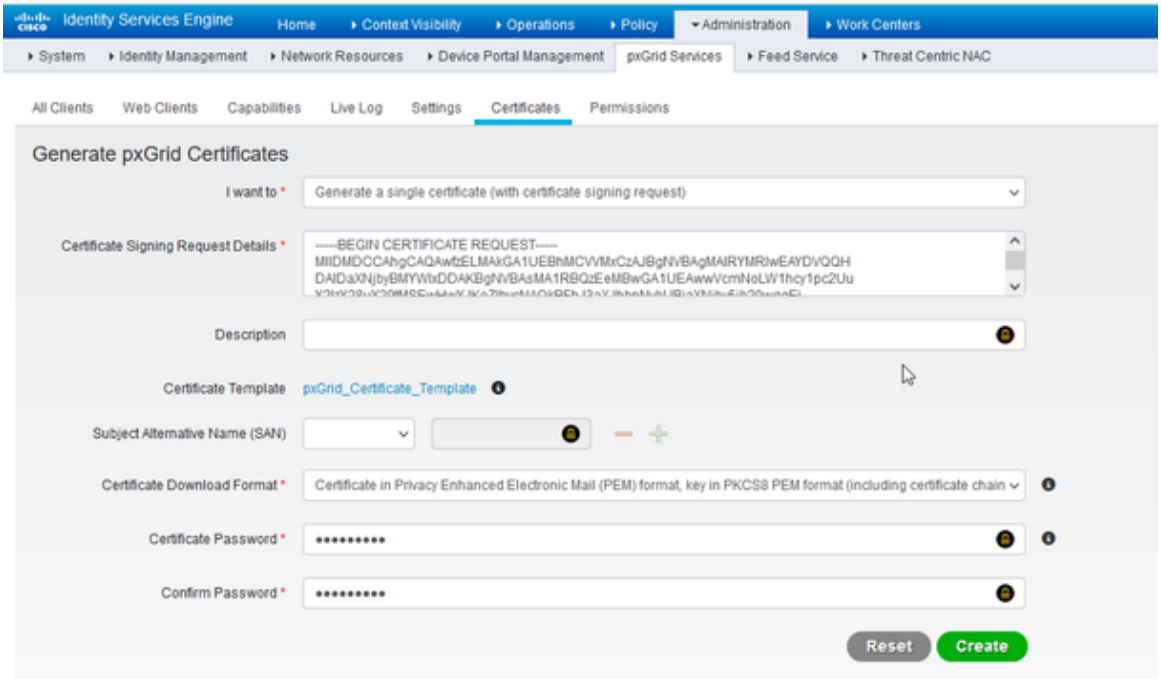
4. 在文本編輯器中開啟CSR檔案。 出於安全原因，示例螢幕截圖不完整且經過編輯。 實際產生的CSR檔案包含更多行。

5. 將私鑰檔案(<server>.pem)複製到PC，就像在後續步驟中所使用的一樣。

使用思科ISE生成證書，使用建立的CSR檔案資訊

在ISE GUI中：

1. 刪除現有的pxGrid客戶端。
    - 導航到Administration > pxGrid Services > All Clients。
    - 查詢並選擇現有的客戶機主機名（如果列出），
    - 如果找到並選定，請按一下「刪除」按鈕，然後選擇「刪除選定項」。 根據需要進行確認。
2. 建立新證書。
    - 按一下pxGrid服務頁面上的「證書」(Certificates)頁籤。
    - 選擇選項：
        - 「我想」：
            - "生成單個證書（包含證書簽名請求）"
        - "證書簽名請求詳細資訊：
            - 從文字編輯器複製/貼上CSR詳細資訊。 務必包括BEGIN和END行。
        - "證書下載格式"
            - "隱私增強型電子郵件(PEM)格式的證書，PKCS8 PEM格式的金鑰。"
        - 輸入證書密碼並加以確認。
        - 按一下「建立」按鈕。

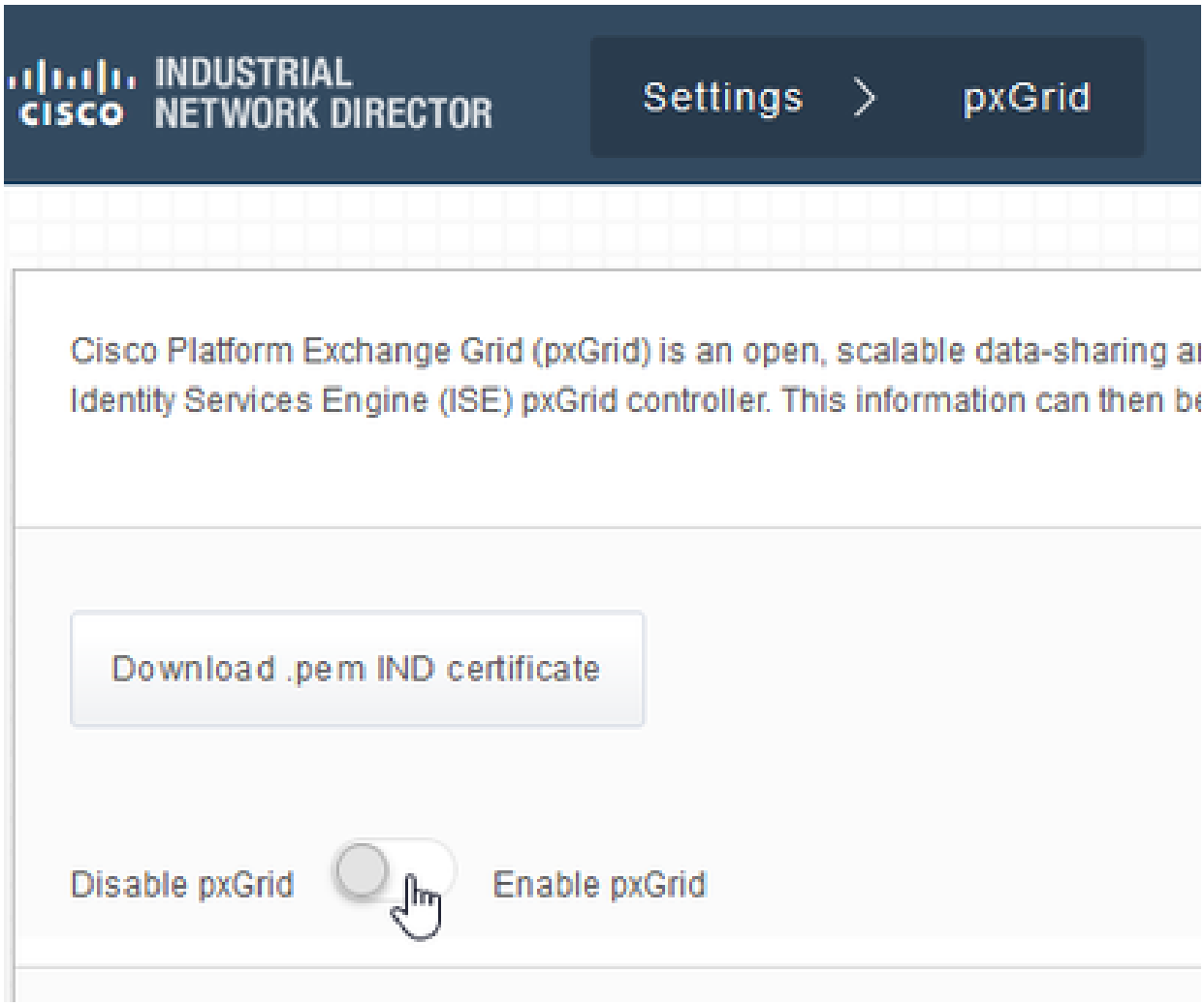


- 這會建立和下載包含憑證檔案以及憑證鏈結的其他檔案的ZIP檔案。開啟ZIP並解壓縮憑證。
  - 檔名通常為<IND server fqdn>.cer
  - 在ISE的某些版本中，檔名是<IND fqdn>_<IND短名稱>.cer

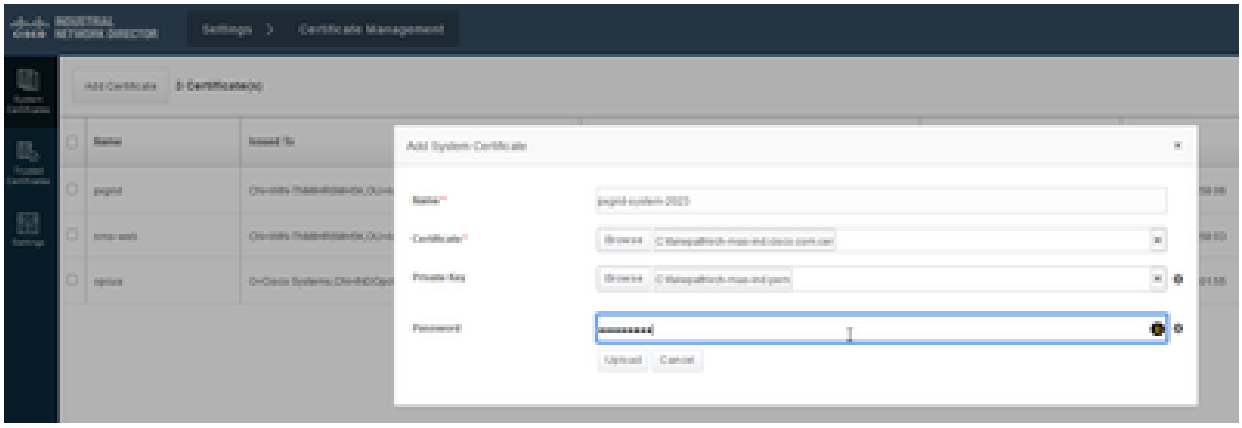
將新證書匯入到IND伺服器，並將其啟用以供pxGrid使用

在IND GUI中：

1. 禁用pxGrid服務，以便可以匯入新證書並將其設定為活動證書。
   - 導航到Settings > pxGrid。
   - 按一下可禁用pxGrid。

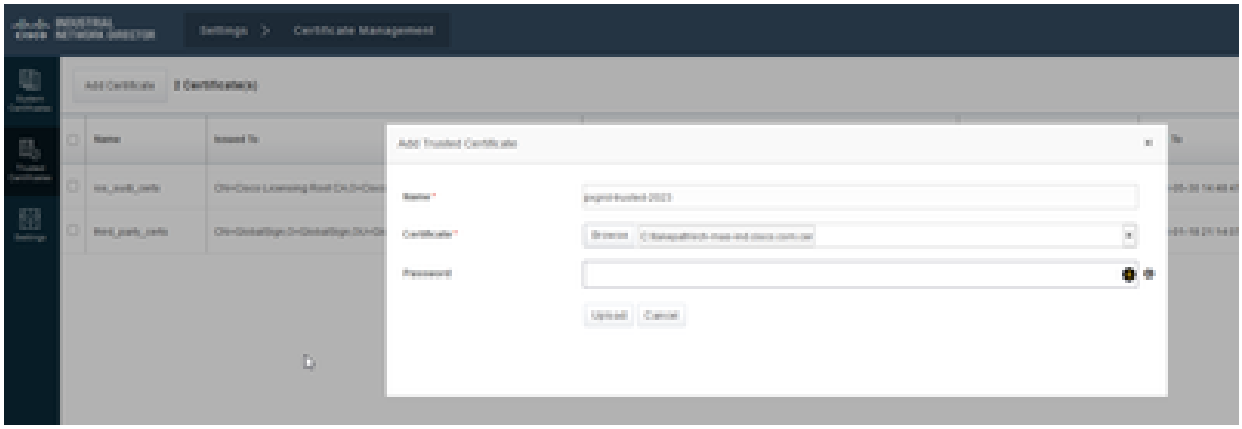


2. 將新證書匯入系統證書。
   - 導覽至Settings > Certificate Management。
   - 按一下「System Certificates（系統證書）」
   - 按一下「Add Certificate」。
   - 輸入證書名稱。
   - 按一下「Certificate」左邊的「Browse」，然後找到新的證書檔案。
   - 按一下「Certificate」左邊的「Browse」，然後找到建立CSR時儲存的私鑰。
   - 輸入之前使用OpenSSL建立私鑰和CSR時使用的密碼。
   - 按一下「上傳」。



3. 將新證書匯入為受信任的證書。
   - 導航到Settings > Certificate Management，點選Trusted Certificates。

- 按一下「Add Certificate」。
- 輸入證書名稱；該名稱必須不同於系統證書上使用的名稱。
- 按一下「Certificate」左側的「Browse」，然後找到新的證書檔案。
- 密碼欄位可以留空。
- 按一下「上傳」。

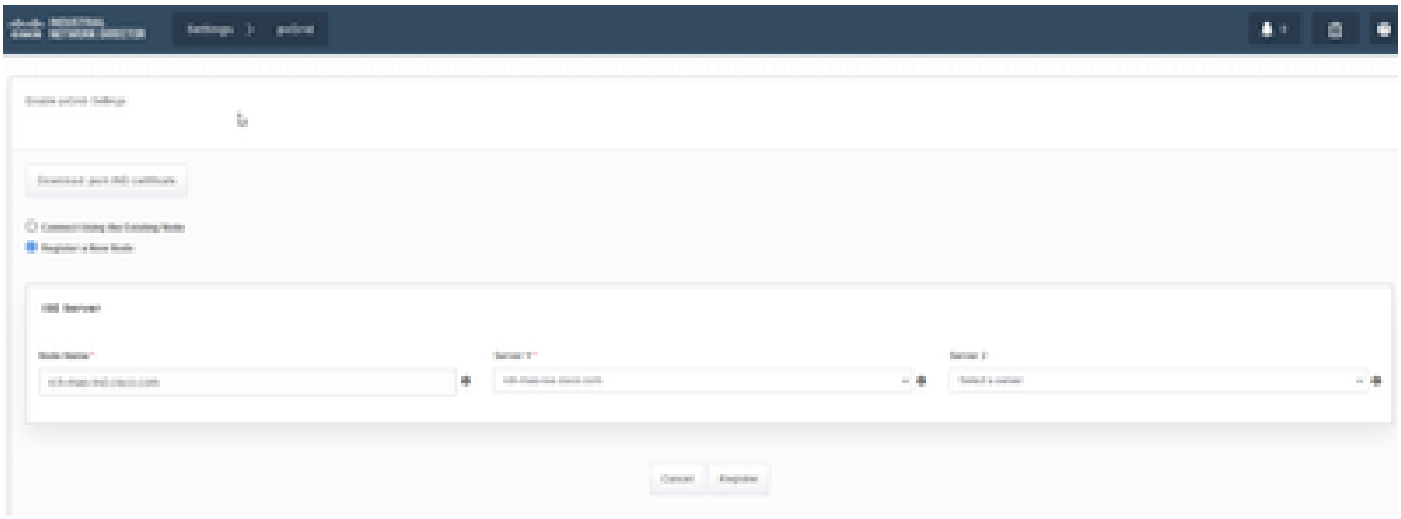


4. 設定pxGrid以使用新證書。
    - 導航到Settings（設定）> Certificate Management（證書管理），按一下Settings（設定）。
    - 如果尚未完成，請選擇「pxGrid」下的「CA證書」。
    - 選擇在證書匯入期間建立的系統證書名稱。
    - 按一下「儲存」。

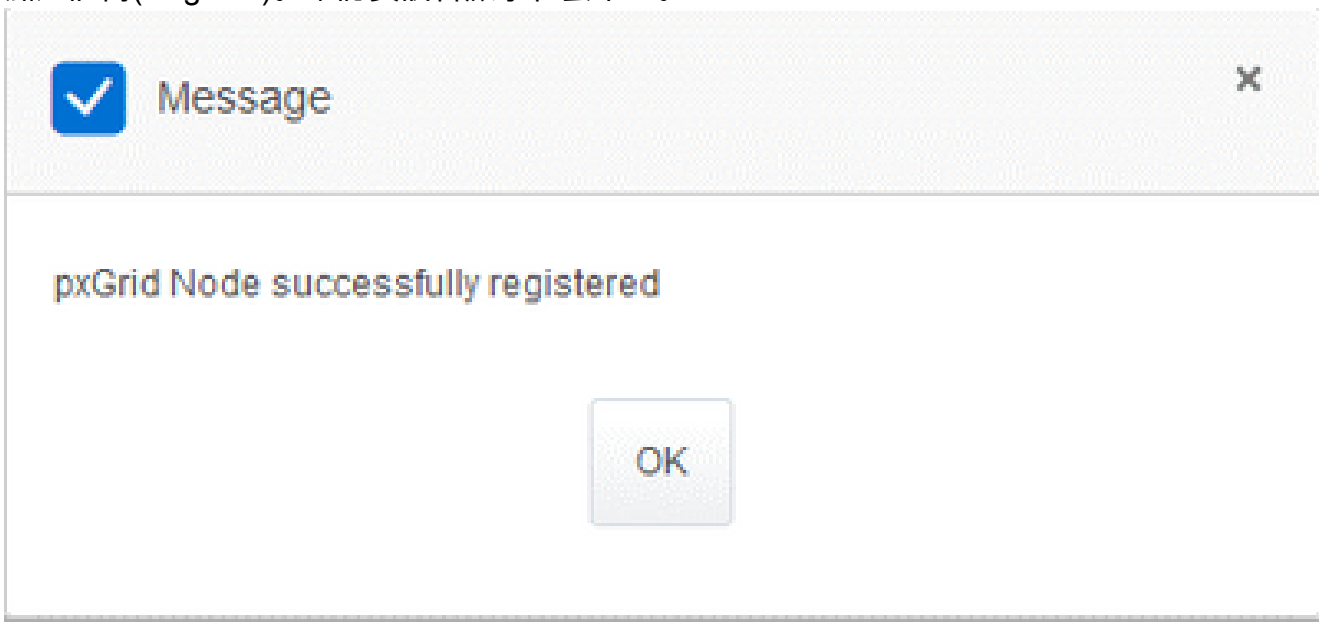
在ISE伺服器中啟用並註冊pxGrid

在IND GUI中：

1. 導航到Settings > pxGrid。
2. 按一下滑塊以啟用pxGrid。
3. 如果這不是第一次在該IND伺服器上向ISE註冊pxGrid，請選擇「使用現有節點連線」。自動填充IND節點和ISE伺服器資訊。
4. 要註冊新的IND伺服器以使用pxGrid，如果需要，請選擇「註冊新節點」。 輸入IND節點名稱，並根據需要選擇ISE伺服器。
    - 如果ISE伺服器未列在伺服器1或伺服器2的下拉選項中，則可以使用Settings > Policy Server將其新增為新的pxGrid伺服器



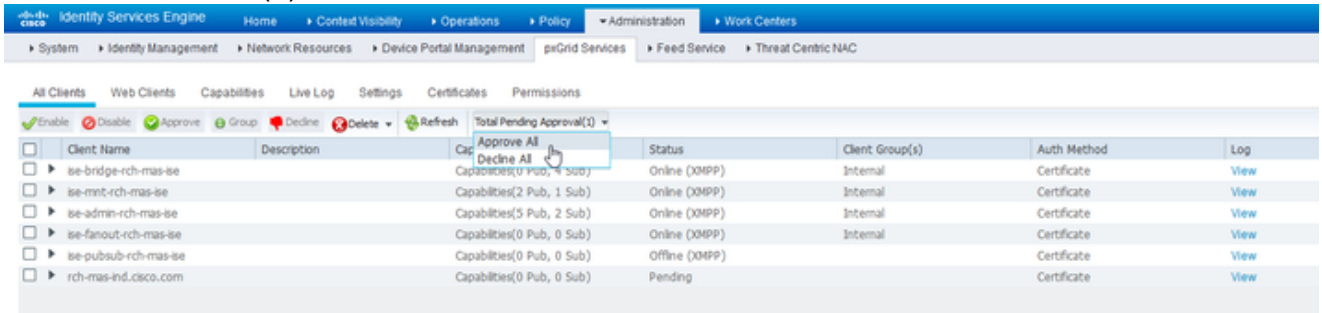
5. 點選註冊(Register)。確認資訊會顯示在螢幕上。



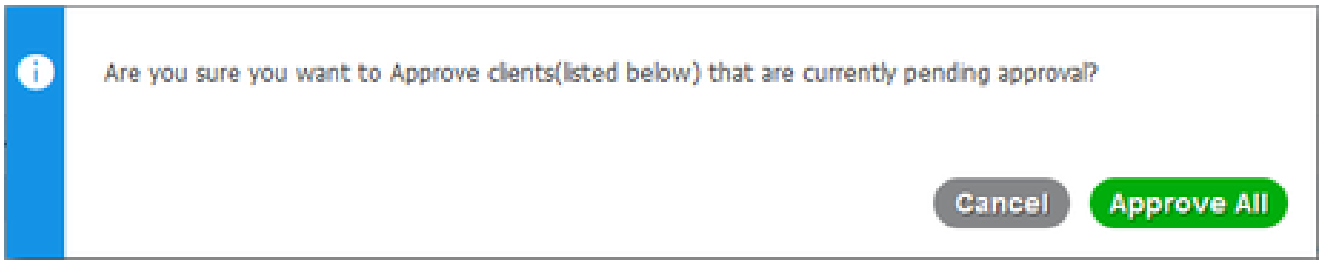
在ISE伺服器中批准註冊請求

在ISE GUI中：

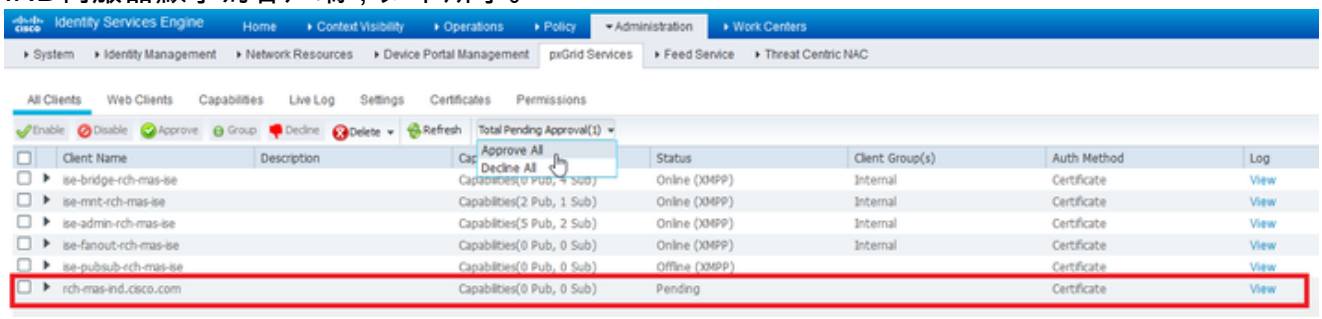
1. 導航到Administration > pxGrid Services > All Clients。 待批准請求顯示為「待批准總數(1)」。
2. 點選「待批准總數(1)」，然後選擇「全部批准」。



3. 在顯示的彈出視窗中，按一下「全部批准」。



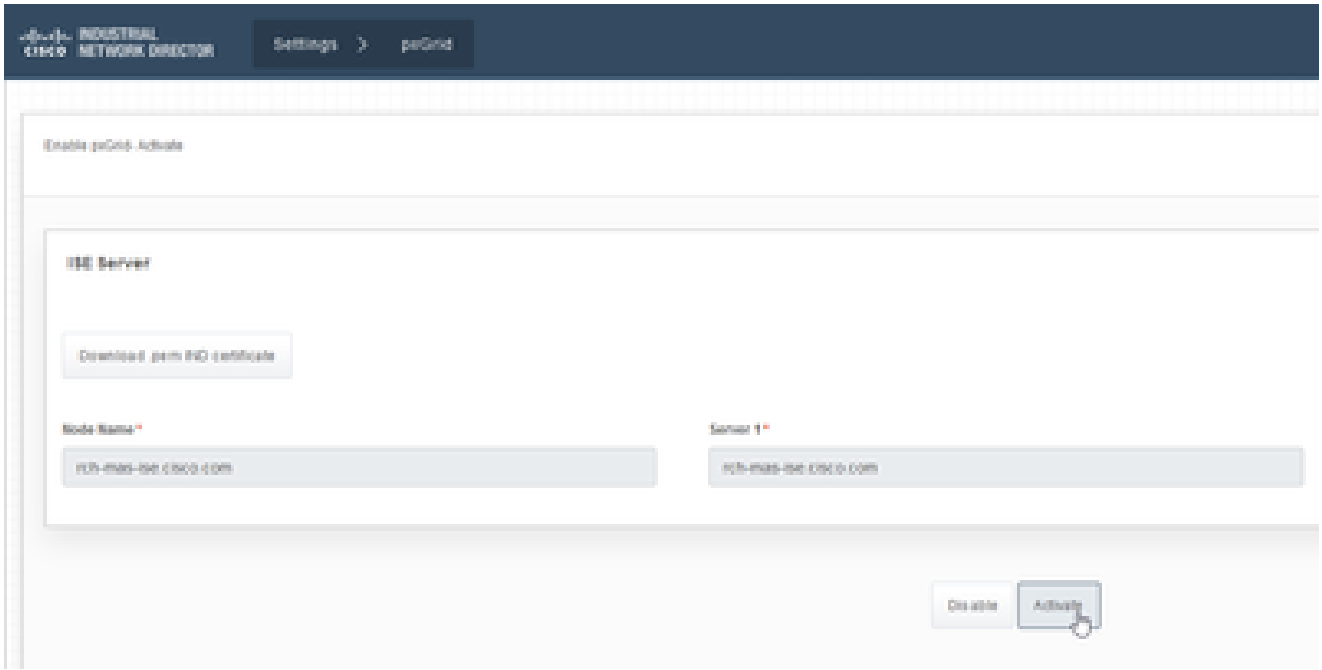
4. IND伺服器顯示為客戶端，如下所示。



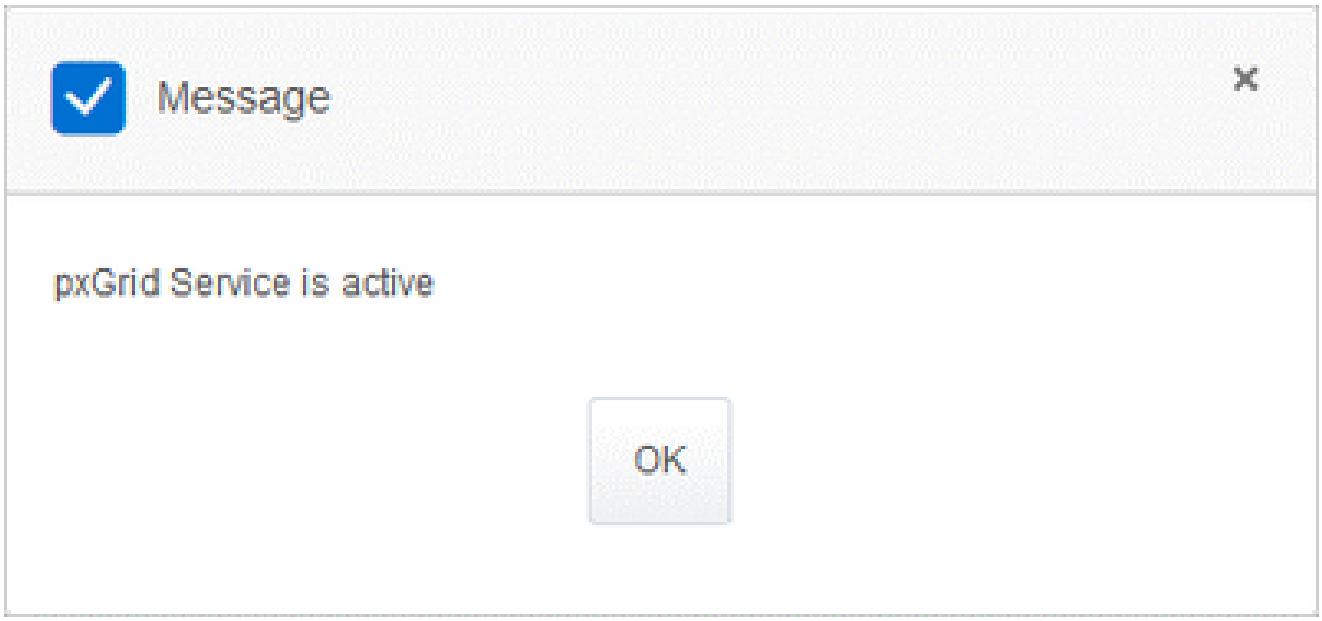
在IND伺服器中啟用pxGrid服務

在IND GUI中：

1. 導航到Settings > pxGrid。
2. 按一下「啟用」。



3. 確認資訊會顯示在螢幕上。


Message
pxGrid Service is active
OK

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。