إنشاء شهادات شبكة منطقة التخزين (SAN) لتكامل IND و ISE PxGrid باستخدام OpenSSL

المحتويات

المقدمة

يوضح هذا المستند كيفية إنشاء شهادات SAN لتكامل PXgrid بين مدير الشبكة الصناعية (IND) ومحرك خدمات الهوية.

معلومات أساسية

عند إنشاء شهادات في Cisco ISE لاستخدام pxGrid، الا يمكن إدخال أسماء المضيف القصيرة للخادم في واجهة المستخدم الرسومية (GUI) ل ISE حيث إن ISE يسمح فقط ب FQDN أو عنوان IP.

لإنشاء شهادات تتضمن اسم المضيف وكذلك FQDN، يجب إنشاء ملف طلب شهادة خارج ISE. يمكن القيام بذلك باستخدام OpenSSL لإنشاء طلب توقيع شهادة (CSR) بإدخالات حقل اسم موضوع بديل (SAN).

ال يتضمن هذا المستند خطوات شاملة لتمكين اتصال PxGrid بين خادم IND وخادم ISE. يمكن إستخدام هذه الخطوات بعد تكوين pxGrid، وقد تم التأكد من أن اسم مضيف الخادم مطلوب. إذا تم العثور على هذا الخطأ في ملفات سجل ISE Profiler، يتطلب الاتصال شهادة اسم المضيف.

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

يمكن الاطلاع على خطوات النشر الأولي للدائرة الوطنية للمعلومات (IND) مع اتصال PxGrid على الموقع
https://www.cisco.com/c/dam/en/us/td/docs/switches/ind/install/IND_PxGrid_Registration_Guide_Final.pdf

التطبيقات المطلوبة

- مدير شبكة Cisco الصناعية (IND)
- محرك خدمات الهوية من Cisco (ISE)
- OpenSSL
  - في معظم إصدارات نظام التشغيل Linux الحديثة، بالإضافة إلى نظام التشغيل MacOS، يتم تثبيت حزمة OpenSSL بشكل افتراضي. إذا اكتشفت أن الأوامر غير متوفرة، فيرجى تثبيت OpenSSL باستخدام تطبيق إدارة حزمة نظام التشغيل

الخاص بك.
    - يمكن العثور على معلومات حول OpenSSL ل Windows على https://wiki.openssl.org/index.php/Binaries

معلومات إضافية

لأغراض هذا المستند، يتم إستخدام هذه التفاصيل:

- اسم مضيف خادم IND: RCH-MAS-IND
- شبكة FQDN: rch-mas-ind.cisco.com
- تكوين OpenSSL: rch-mas-ind.req
- اسم ملف طلب الشهادة: rch-mas-ind.csr
- اسم ملف المفتاح الخاص: rch-mas-ind.pem
- اسم ملف الشهادة: rch-mas-ind.cer

خطوات العملية

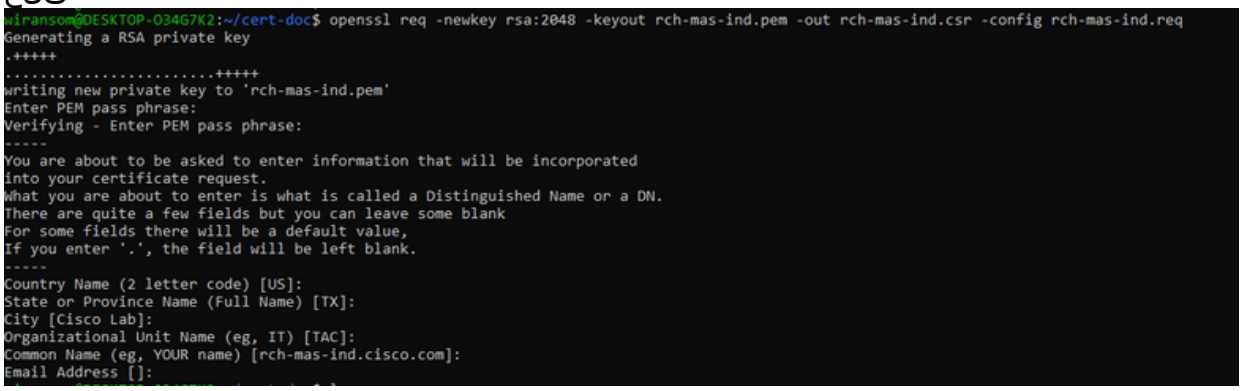
إنشاء CSR للشهادة

1. على نظام مثبت عليه OpenSSL، قم بإنشاء ملف نص طلب لخيارات OpenSSL بما في ذلك معلومات SAN.
    - تكون معظم الحقول "_default" إختيارية، حيث يمكن إدخال الإجابات أثناء تشغيل الأمر OpenSSL في الخطوة #2.
    - تفاصيل شبكة التخزين (SAN) (DNS.1 و DNS.2) مطلوبة ويجب أن تتضمن كل من اسم المضيف المختصر ل DNS و FQDN للخادم. يمكن إضافة أسماء DNS إضافية إذا لزم الأمر، باستخدام DNS.3 و DNS.4 وما إلى ذلك.
    - مثال على ملف نص الطلب:

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

[الاسم]
اسم البلد = اسم البلد (رمز حرف)
countryName_default = الولايات المتحدة
StateOrProvinceName = اسم الولاية أو المقاطعة (الاسم الكامل)
stateOrProvinceName_default = Tx
LocalityName = City
localityName_default = Cisco Lab
OrganizationUnitName = اسم الوحدة التنظيمية (على سبيل المثال، IT)
organizationUnitName_default = TAC
CommonName = اسم عام (على سبيل المثال، اسمك)
commonName_max = 64
commonName_default = rch-mas-ind.cisco.com
عنوان البريد الإلكتروني = عنوان البريد الإلكتروني
```

```
emailAddress_max = 40

[v3_req]
KeyUsage = مفاتاح التشفير، تشفير البياانات
ExtendedKeyUsage = serverAuth، clientAuth
subjectAltName = @alt_names

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

2. أستخدم OpenSSL لإنشاء CSR باستخدام اسم المضيف القصير ل DNS في حقل SAN. قم بإنشاء ملف مفاتاح خاص باإلضافة إلى ملف CSR.
   - :
     openssl req -newKey rsa:2048 -keyout <server>.pem -out <server>.csr -config <server>.req
   - عند مطالبتك بذلك، أدخل كلمة مرور من إختياراك. تأكد من تذكر كلمة المرور هذه، كما يتم إستخدامها في الخطواات اللاحقة.
   - أدخل عنوان بريد إلكتروني صالح عند المطالبة به أو أترك الحقل فارغا واضغط على <ENTER>.



3. تحقق من معلومات ملف CSR، إذا كنت ترغب في ذلك. للحصول على شهادة شبكة التخزين (SAN)، تحقق من "االسم البديل للموضوع x509v3" كما هو موضح في لقطة الشاشة هذه.
   - سطر الأوامر:
     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. افتح ملف CSR في محرر نصي. لأسباب تتعلق بالأمان، لم تكتمل لقطة الشاشة العينة وتم تحريرها. يحتوي ملف CSR الفعلي الذي تم إنشاؤه على المزيد من البيانات.

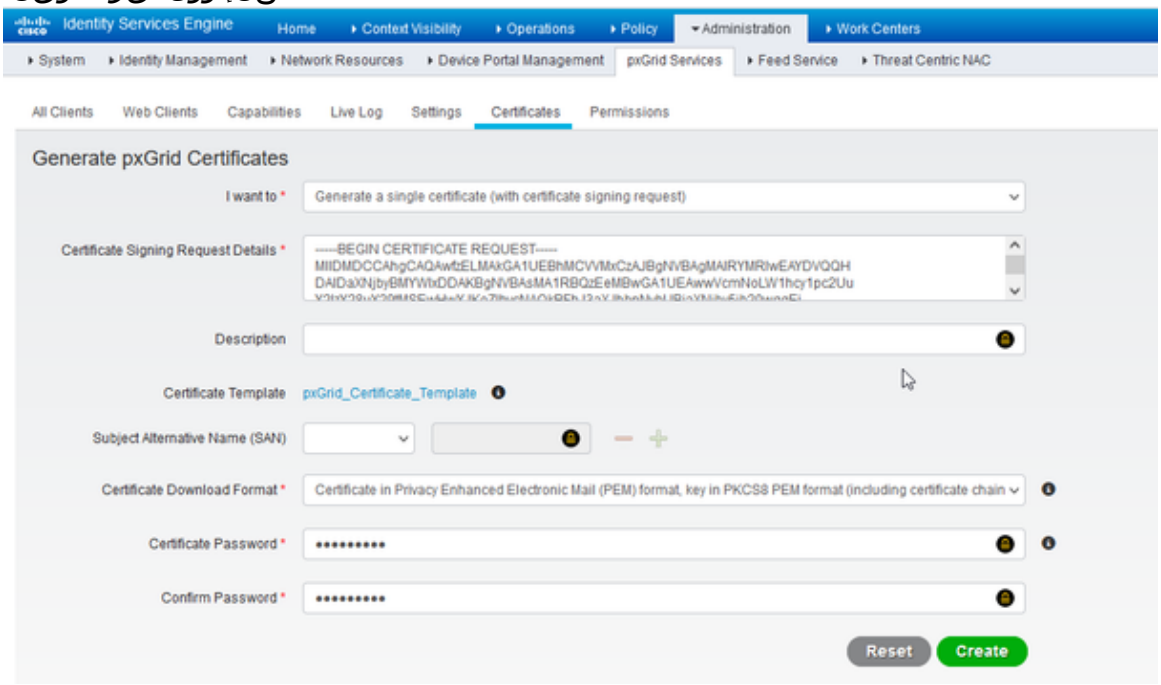
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDMDCCAhgCAQAwfzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAlRYMRIwEAYDVQQH
DAlDaXNjbyBMYWIxDDAKBgNVBAsMA1RBQzEeMBwGA1UEAwwVcmNoLW1hcy1pbmQu
Y2lzY28uY29tMSEwHwYJKoZIhvcNAQkBFhJ3aXJhbnNvbUBjaXNjby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVkRpj307uFPRm2IboESQRqxRC
NJ2n8bHzRxOwg4cePcUwu1m9E9Y45r1wG4NTmvylIn7AL4KwdTHdT9JDDiThInQS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

5. انسخ ملف المفتاح الخاص (<server>.pem) إلى الكمبيوتر الخاص بك كما هو مستخدم في خطوة لاحقة.

أستخدم Cisco ISE لإنشاء شهادة، باستخدام معلومات ملف CSR الذي تم إنشاؤه

داخل واجهة المستخدم الرسومية ISE:

1. إزالة عميل pxGrid الموجود.
   - انتقل إلى إدارة > خدمات PxGrid > جميع العملاء.
   - ابحث عن اسم المضيف للعميل الموجود وقم بتحديده، إذا كان مدرجا،
   - إذا تم العثور عليه وتحديده، انقر زر الحذف ، واختر "حذف المحدد." تأكد حسب الحاجة.
2. إنشاء الشهادة الجديدة.
   - انقر فوق علامة التبويب شهادات في صفحة خدمات pxGrid.
   - أختر الخيارات:
     - "أريد ذلك":
       - "إنشاء شهادة مفردة (مع طلب توقيع الشهادة)"
     - "تفاصيل طلب توقيع الشهادة:
       - انسخ/الصق تفاصيل CSR من محرر النصوص. تأكد من تضمين أسطر BEGIN و END.
     - "تنسيق تنزيل الشهادة"
       - "شهادة بتنسيق البريد الإلكتروني المحسن للخصوصية (PEM)، مفتاح بتنسيق PKCS8 PEM."
     - أدخل كلمة مرور الشهادة وأكدها.
     - انقر فوق الزر إنشاء.



     - يقوم ذلك بإنشاء وتنزيل ملف ZIP يحتوي على ملف الترخيص بالإضافة إلى ملفات إضافية لسلسلة الترخيص. افتح الرمز البريدي واستخرج الشهادة.
       - اسم الملف هو عادة <IND server fqdn>.cer
       - في بعض الإصدارات من ISE، يكون اسم الملف <IND fqdn>_<IND Short Name>.cer

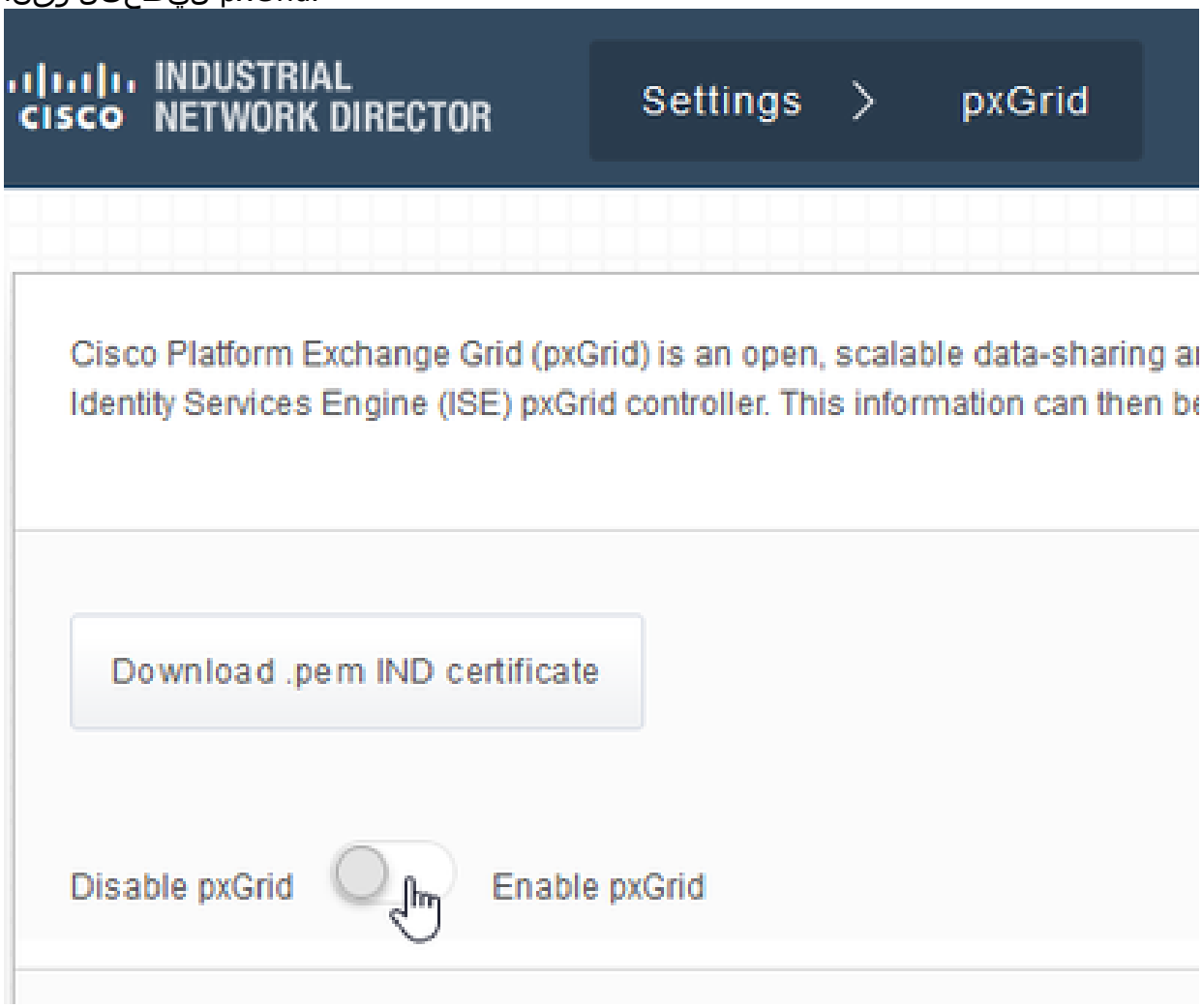
إستيراد الشهادة الجديدة إلى خادم IND، وتمكينها لاستخدام pxGrid

داخل واجهة المستخدم الرسومية IND:

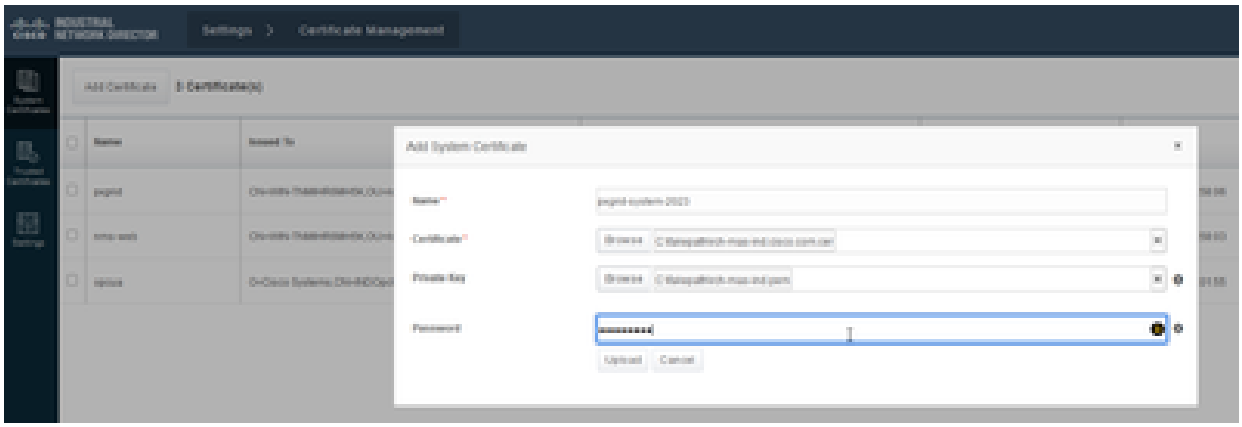
1. قم بتعطيل خدمة pxGrid، حتى يمكن إستيراد الشهادة الجديدة وتعيينها كشهادة

نشطة.

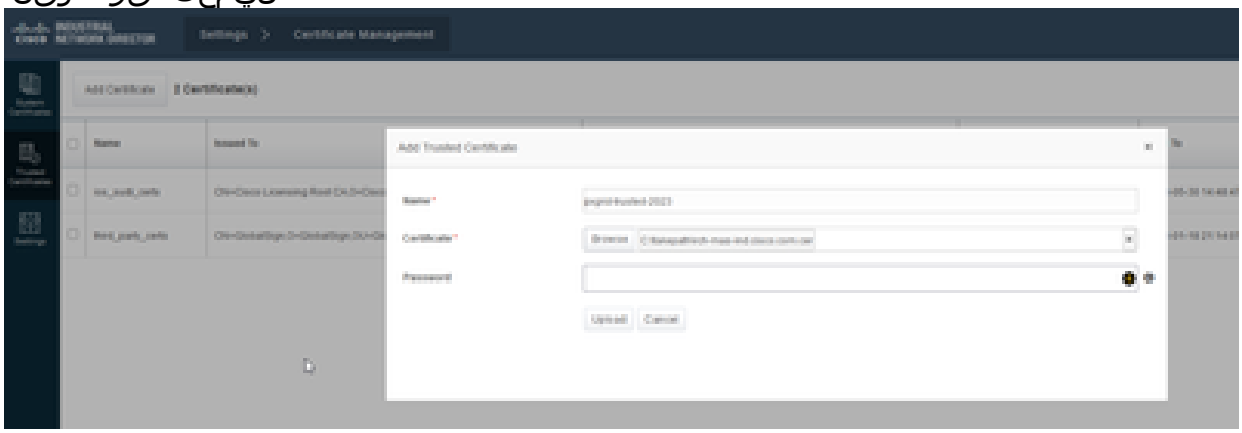
- انتقل إلى الإعدادات > pxGrid.
- انقر لتعطيل pxGrid.



2. إستيراد الشهادة الجديدة إلى شهادات النظام.
   - انتقل إلى الإعدادات > إدارة الشهادات.
   - انقر على "شهادات النظام"
   - انقر فوق "إضافة ترخيص".
   - أدخل اسم شهادة.
   - انقر "تصفح" على يسار "الترخيص"، وحدد مكان ملف الشهادة الجديد.
   - انقر فوق "إستعراض" إلى يسار "الترخيص"، وحدد مكان المفتاح الخاص المحفوظ عند إنشاء CSR.
   - أدخل كلمة المرور المستخدمة مسبقا عند إنشاء المفتاح الخاص و CSR باستخدام OpenSSL.
   - انقر فوق "تحميل".



3. إستيراد الشهادة الجديدة كشهادة موثوق بها.
   - انتقل إلى الإعدادات > إدارة الشهادات، وانقر على "الشهادات الموثوق بها".
   - انقر فوق "إضافة ترخيص".
   - أدخل اسم شهادة، يجب أن يكون هذا الاسم مختلفا عن الاسم المستخدم في "شهادات النظام".
   - انقر "تصفح" على يسار "الترخيص" وحدد مكان ملف الشهادة الجديد.
   - يمكن ترك حقل كلمة المرور فارغا.
   - انقر فوق "تحميل".



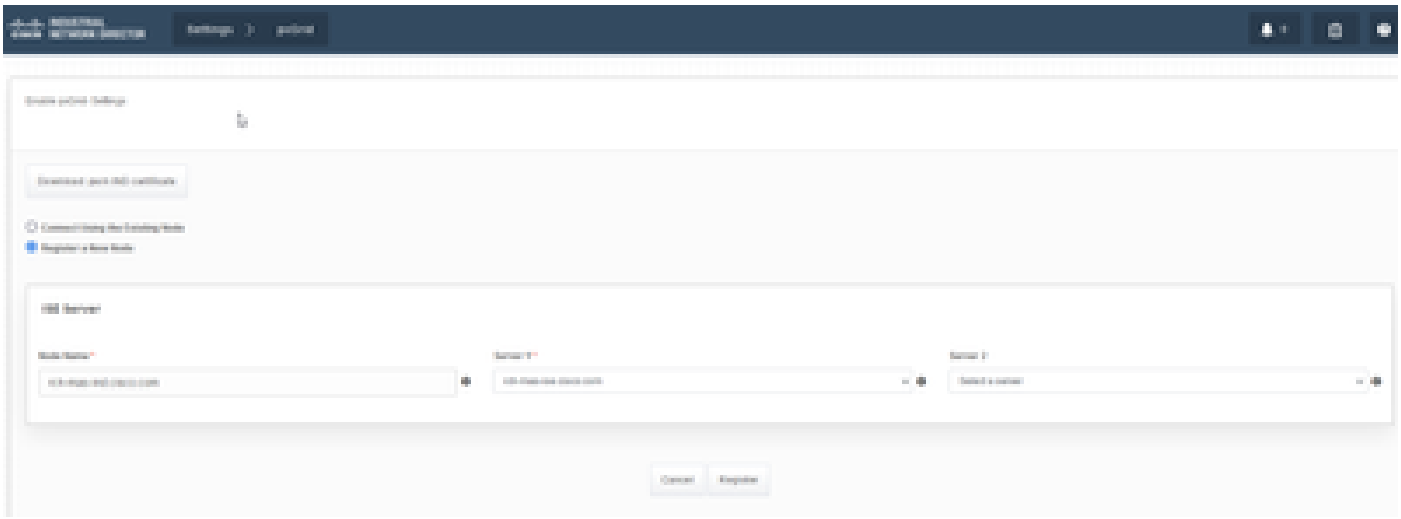
4. تعيين pxGrid لاستخدام الشهادة الجديدة.
   - انتقل إلى الإعدادات > إدارة الترخيص، انقر على "إعدادات".
   - إذا لم يكن قد تم بالفعل، حدد "شهادة CA" تحت "pxGrid."
   - حدد اسم شهادة النظام الذي تم إنشاؤه أثناء إستيراد الشهادة.
   - انقر حفظ.

تمكين PxGrid وتسجيله باستخدام خادم ISE

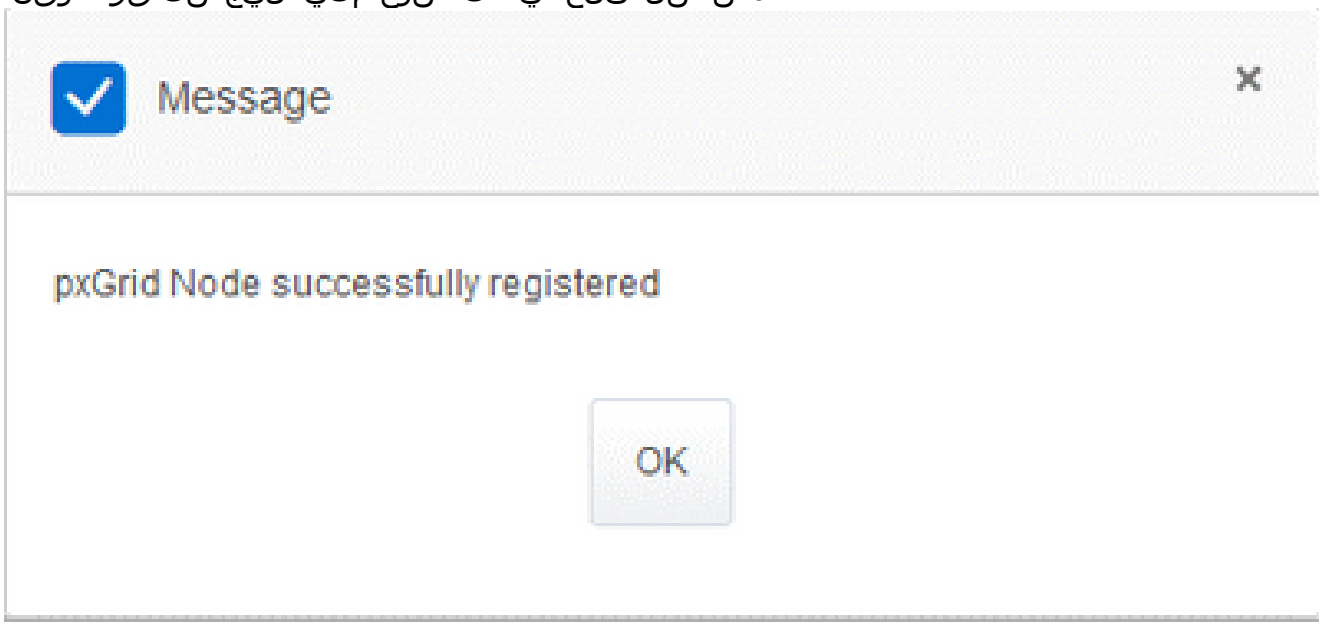
داخل واجهة المستخدم الرسومية IND:

1. انتقل إلى الإعدادات > pxGrid.
2. انقر المنزلق لتمكين pxGrid.
3. إذا لم تكن هذه هي المرة الأولى التي يتم فيها تسجيل PxGrid مع ISE على خادم IND هذا، أختر "الاتصال باستخدام العقدة الموجودة". يتم تلقائيا تعبئة عقدة IND ومعلومات خادم ISE.
4. لتسجيل خادم IND جديد لاستخدام pxGrid، إذا لزم الأمر، أختر "تسجيل عقدة جديدة". أدخل اسم عقدة IND واختر خوادم ISE حسب الحاجة.

- إذا لم يكن خادم ISE مدرج ضمن الخيارات المنسدلة للخادم 1 أو الخادم 2، فيمكن إضافته كخادم pxGrid جديد باستخدام الإعدادات > خادم النهج



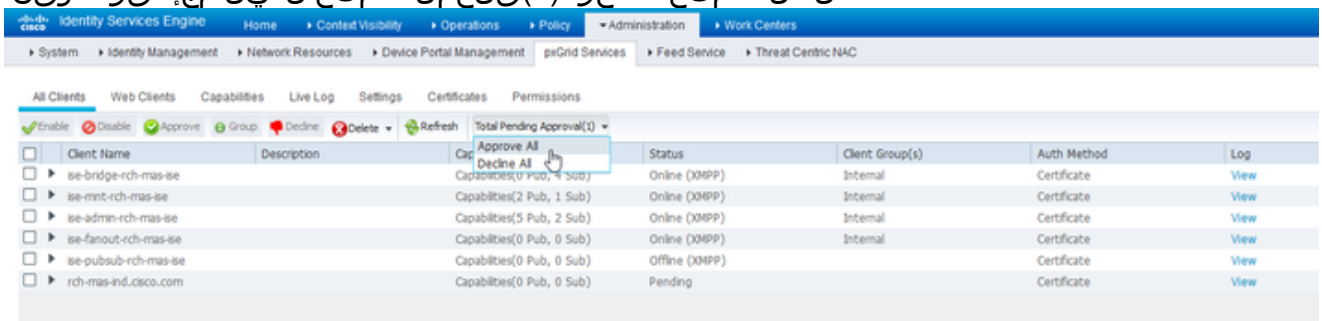
5. انقر فوق تسجيل. يتم عرض تأكيد على الشاشة.



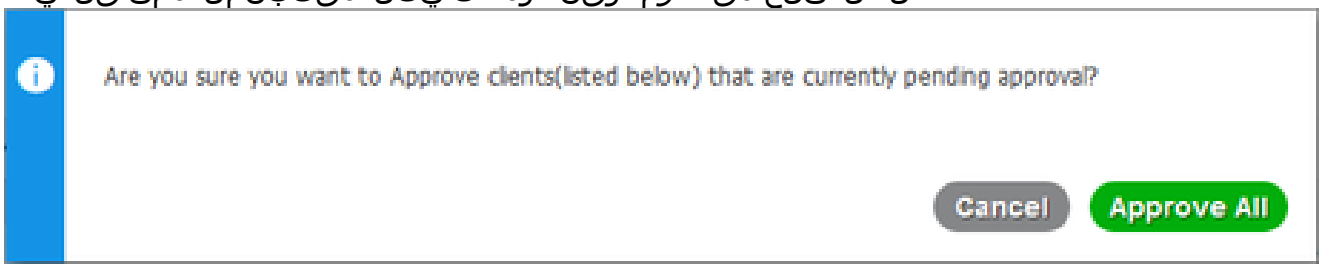
الموافقة على طلب التسجيل في خادم ISE

داخل واجهة المستخدم الرسومية ISE:

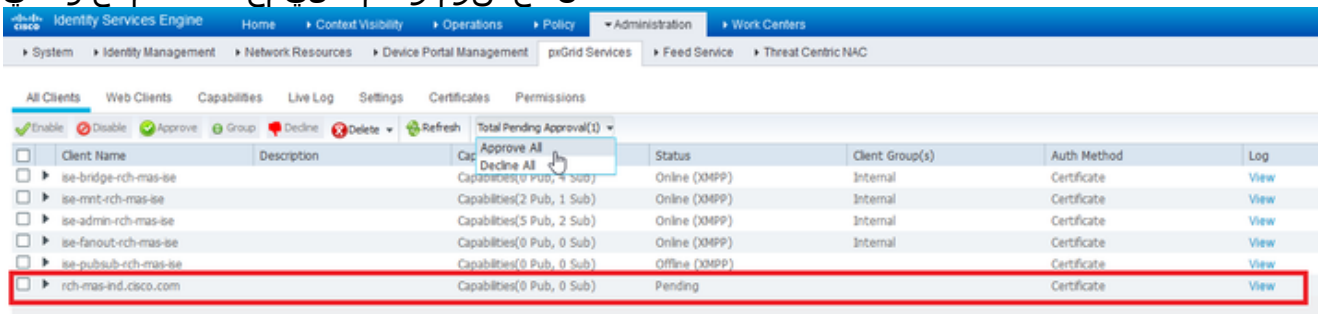
1. انتقل إلى إدارة > خدمات PxGrid > جميع العملاء. يظهر طلب الموافقة المعلقة على أنه "مجموع الموافقة المعلقة (1)."
2. انقر فوق "إجمالي الاعتماد المعلق(1)" وحدد "اعتماد الكل."



3. في القائمة المنبثقة التي تظهر، انقر "موافقة على الكل".



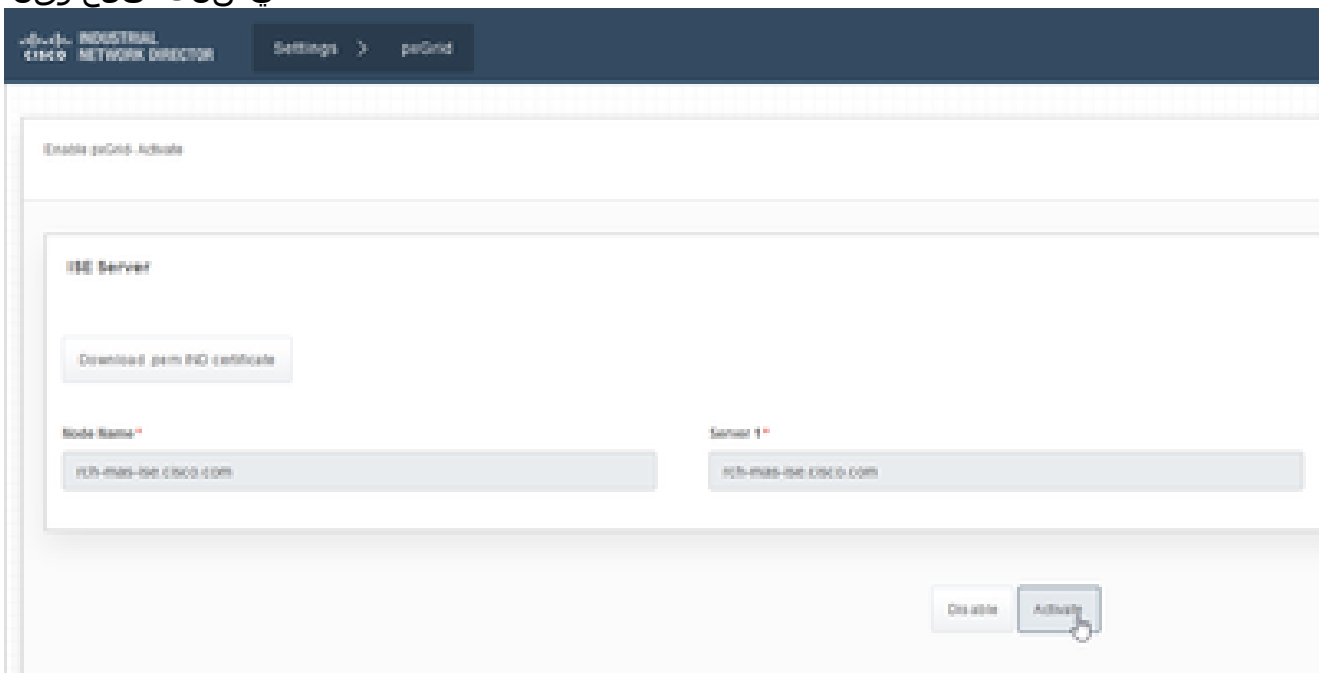
4. يظهر خادم IND كعميل كما هو موضح هنا.



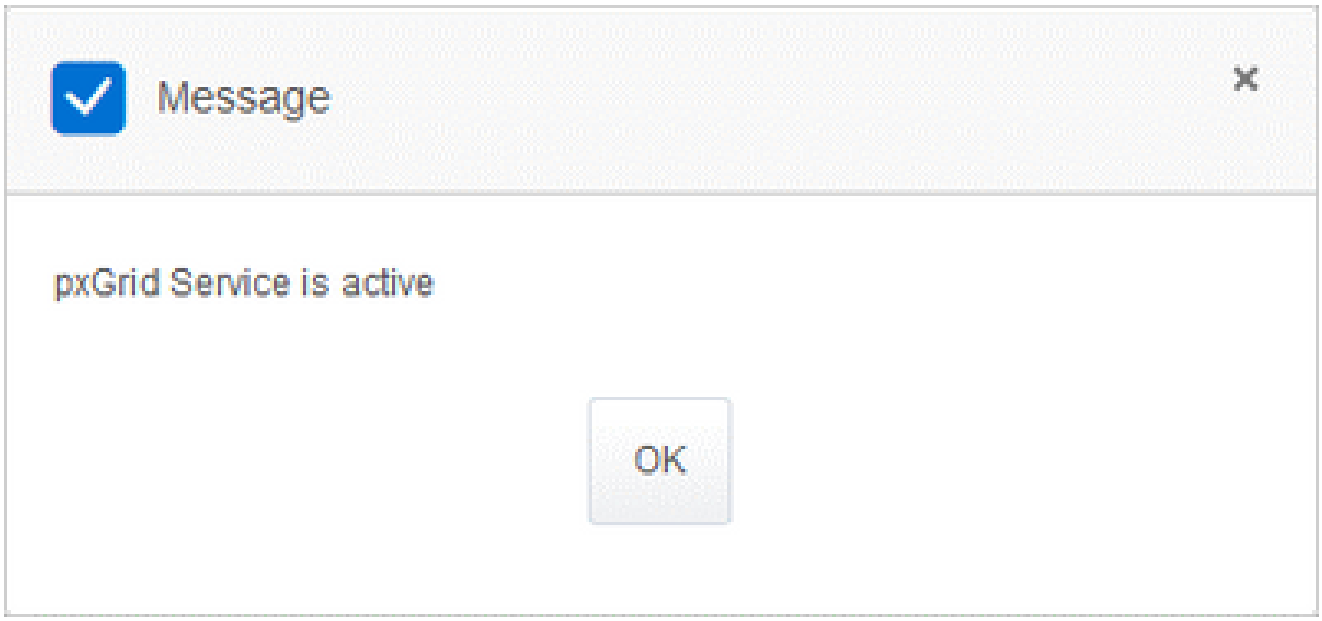
تنشيط خدمة pxGrid في خادم IND

داخل واجهة المستخدم الرسومية IND:

1. انتقل إلى الإعدادات > pxGrid.
2. انقر على "تنشيط".



3. يتم عرض تأكيد على الشاشة.


Message
pxGrid Service is active
OK

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).