Creación de certificados SAN para la integración de IND e ISE pxGrid mediante OpenSSL

Contenido

Introducción

Este documento describe cómo crear certificados SAN para la integración de pxGrid entre Industrial Network Director (IND) e Identity Services Engine.

Antecedentes

Al crear certificados en Cisco ISE para el uso de pxGrid, los nombres de host cortos del servidor no se pueden introducir en la GUI de ISE, ya que ISE solo permite el FQDN o la dirección IP.

Para crear certificados que incluyan el nombre de host y el FQDN, se debe crear un archivo de solicitud de certificado fuera de ISE. Esto se puede hacer mediante OpenSSL para crear una solicitud de firma de certificado (CSR) con entradas de campo de nombre alternativo del sujeto (SAN).

Este documento no incluye los pasos integrales para habilitar la comunicación pxGrid entre el servidor IND y el servidor ISE. Estos pasos se pueden utilizar después de que pxGrid se haya configurado y se haya confirmado que el nombre de host del servidor es obligatorio. Si se encuentra este error en los archivos de registro de ISE Profiler, la comunicación requiere el certificado de nombre de host.

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

Los pasos para la implementación inicial de IND con la comunicación pxGrid se pueden encontrar en https://www.cisco.com/c/dam/en/us/td/docs/switches/ind/install/IND_PxGrid_Registration_Guide_Final.pdf

Aplicaciones necesarias

- Cisco Industrial Network Director (IND)
- Cisco Identity Services Engine (ISE)
- OpenSSL
    - En la mayoría de las versiones modernas de Linux, así como en MacOS, el paquete OpenSSL se instala de forma predeterminada. Si descubre que los comandos no

están disponibles, instale OpenSSL utilizando la aplicación de gestión de paquetes de su sistema operativo.
    - Puede encontrar información sobre OpenSSL para Windows en https://wiki.openssl.org/index.php/Binaries

Additional Information

A los efectos de este documento, se utilizan estos datos:

- Nombre de host del servidor IND: rch-mas-ind
- FQDN: rch-mas-ind.cisco.com
- Configuración de OpenSSL: rch-mas-ind.req
- Nombre del archivo de solicitud de certificado: rch-mas-ind.csr
- Nombre del archivo de clave privada: rch-mas-ind.pem
- Nombre del archivo del certificado: rch-mas-ind.cer

Pasos del proceso

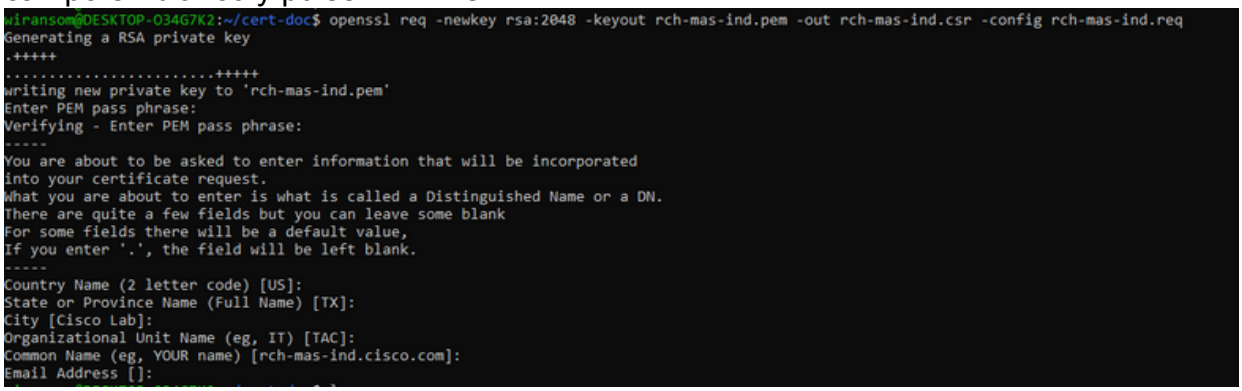
Crear el certificado CSR

1. En un sistema con OpenSSL instalado, cree un archivo de texto de solicitud para las opciones de OpenSSL, incluida la información de SAN.
    - La mayoría de los campos "_default" son opcionales, ya que las respuestas se pueden ingresar mientras se ejecuta el comando OpenSSL en el paso #2.
    - Los detalles de SAN (DNS.1, DNS.2) son obligatorios y deben incluir tanto el nombre de host corto DNS como el FQDN del servidor. Si es necesario, se pueden agregar nombres DNS adicionales mediante DNS.3, DNS.4, etc.
    - Archivo de texto de solicitud de ejemplo:

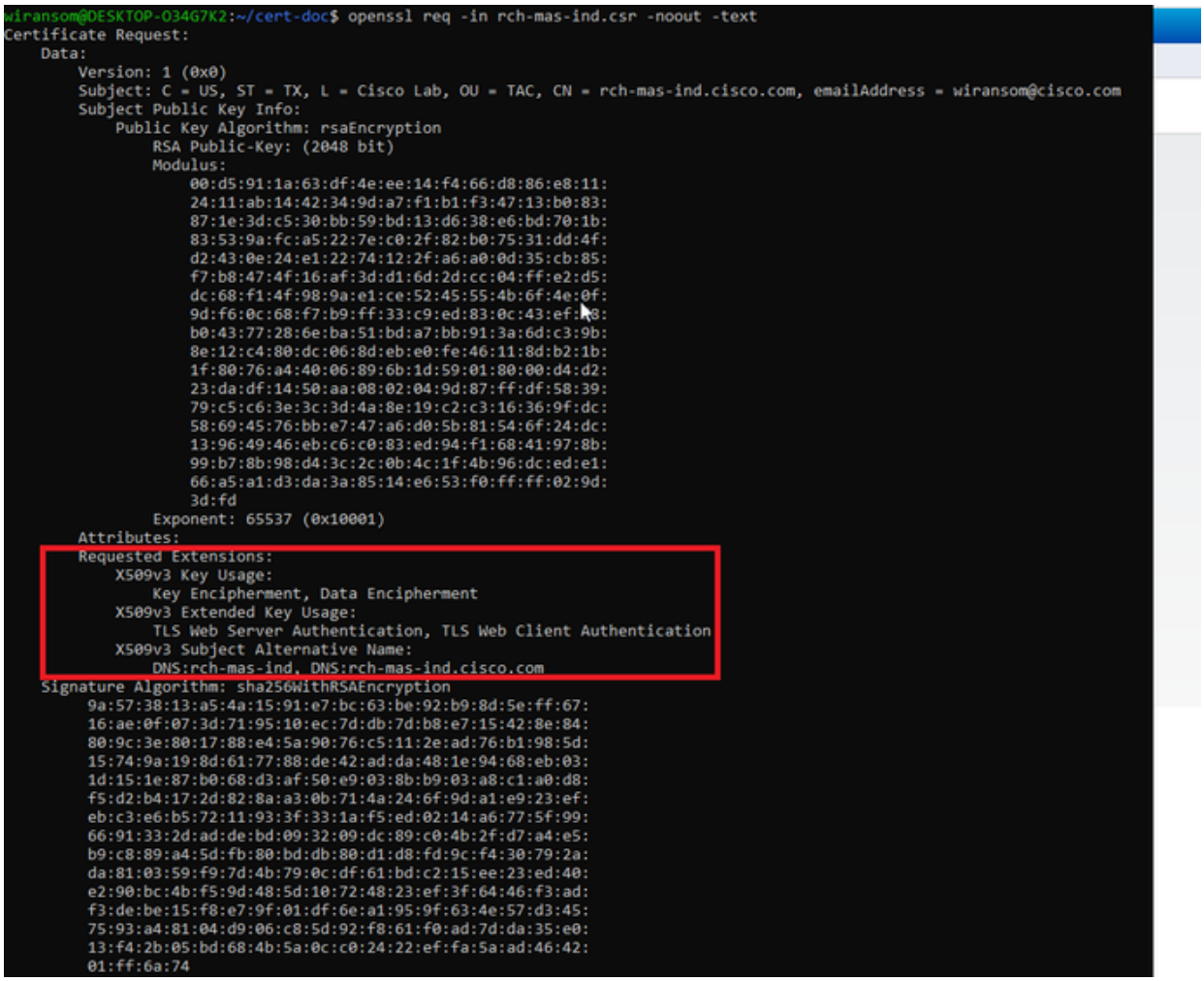
```
[req]
nombre_distinguido = nombre
req_extensions = v3_req

[nombre]
countryName = Nombre del país (código de 2 letras)
countryName_default = EE. UU.
stateOrProvinceName = Estado o nombre de provincia (nombre completo)
stateOrProvinceName_default = TX
localityName = Ciudad
localityName_default = Cisco Lab
organizationUnitName = Nombre de la unidad organizativa (por ejemplo, IT)
organizationUnitName_default = TAC
commonName = Nombre común (por ejemplo, SU nombre)
commonName_max = 64
commonName_default = rch-mas-ind.cisco.com
```

```
emailAddress = Dirección de correo electrónico
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. Utilice OpenSSL para crear CSR con nombre de host corto DNS en el campo SAN. Cree un archivo de clave privada además del archivo CSR.
   - Comando:
     openssl req -newkey rsa:2048 -keyout <server>.pem -out <server>.csr -config <server>.req
   - Cuando se le solicite, introduzca la contraseña que desee. Recuerde esta contraseña, ya que se utilizará en los pasos posteriores.
   - Introduzca una dirección de correo electrónico válida cuando se le solicite o deje el campo en blanco y pulse <INTRO>.



3. Si lo desea, verifique la información del archivo CSR. Para obtener un certificado de SAN, compruebe el "nombre alternativo del sujeto x509v3", como se resalta en esta captura de pantalla.
   - Línea de comandos:
     openssl req -in <server>.csr -noout -text



4. Abra el archivo CSR en un editor de texto. Por motivos de seguridad, la captura de pantalla de ejemplo está incompleta y editada. El archivo CSR generado real contiene más líneas.

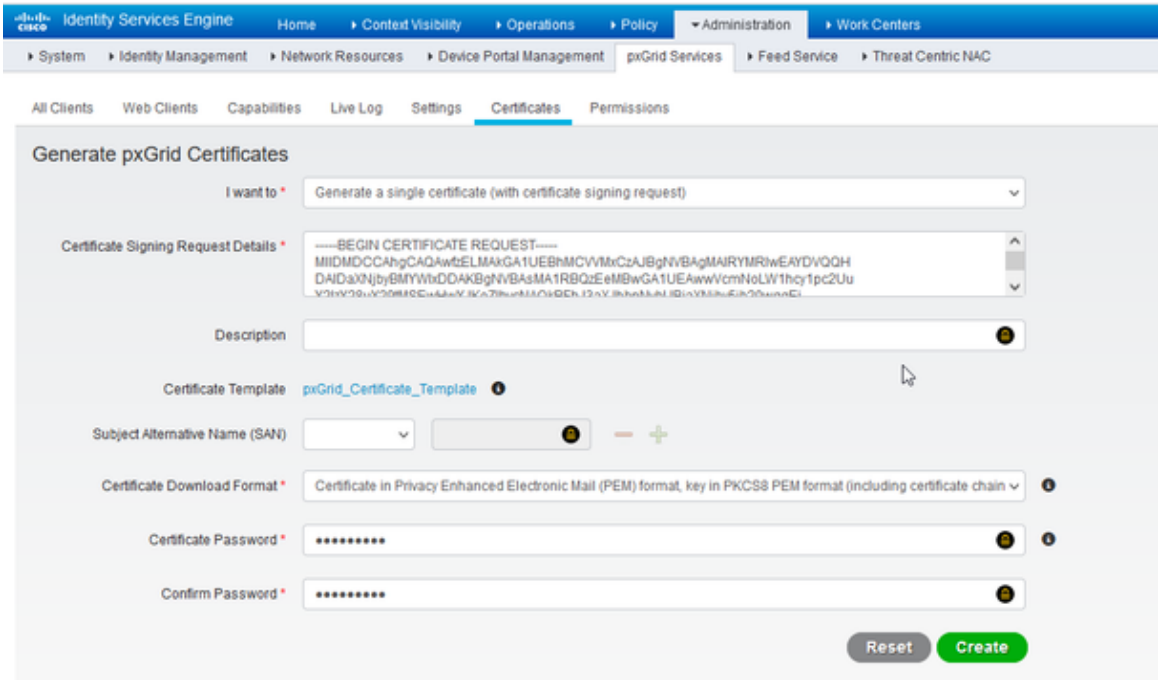
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDMDCCAhgCAQAwfzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAlRYMRIwEAYDVQQH
DAlDaXNjbyBMYWIxDDAKBgNVBAsMA1RBQzEeMBwGA1UEAwwVcmNoLW1hcy1pbmQu
Y2lzY28uY29tMSEwHwYJKoZIhvcNAQkBFhJ3aXJhbnNvbUBjaXNjby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVkRpj307uFPRm2IboESQRqxRC
NJ2n8bHzRxOwg4cePcUwu1m9E9Y45r1wG4NTmvylIn7AL4KwdTHdT9JDDiThInQS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

5. Copie el archivo de clave privada (<server>.pem) en el PC tal y como se utilizará en un paso posterior.

Utilice Cisco ISE para generar un certificado mediante la información del archivo CSR creado

En la GUI de ISE:

1. Elimine el cliente pxGrid existente.
    - Vaya a Administration > pxGrid Services > All Clients.
    - Busque y seleccione el nombre de host del cliente existente, si aparece,
    - Si se encuentra y selecciona, haga clic en el botón Eliminar y seleccione "Eliminar seleccionados". Confirme lo que sea necesario.
2. Cree el nuevo certificado.
    - Haga clic en la ficha Certificados en la página de servicios pxGrid.
    - Seleccione las opciones:
        - "Quiero":
            - "Generar un solo certificado (con solicitud de firma de certificado)"
        - "Detalles de la solicitud de firma de certificado:
            - Copie y pegue los detalles de CSR desde el editor de texto. Asegúrese de incluir las líneas BEGIN y END.
        - "Formato de descarga de certificados"
            - "Certificado en formato PEM (Privacy Enhanced Electronic Mail), clave en formato PEM PKCS8."
        - Introduzca una contraseña de certificado y confírmela.
        - Haga clic en el botón Crear.

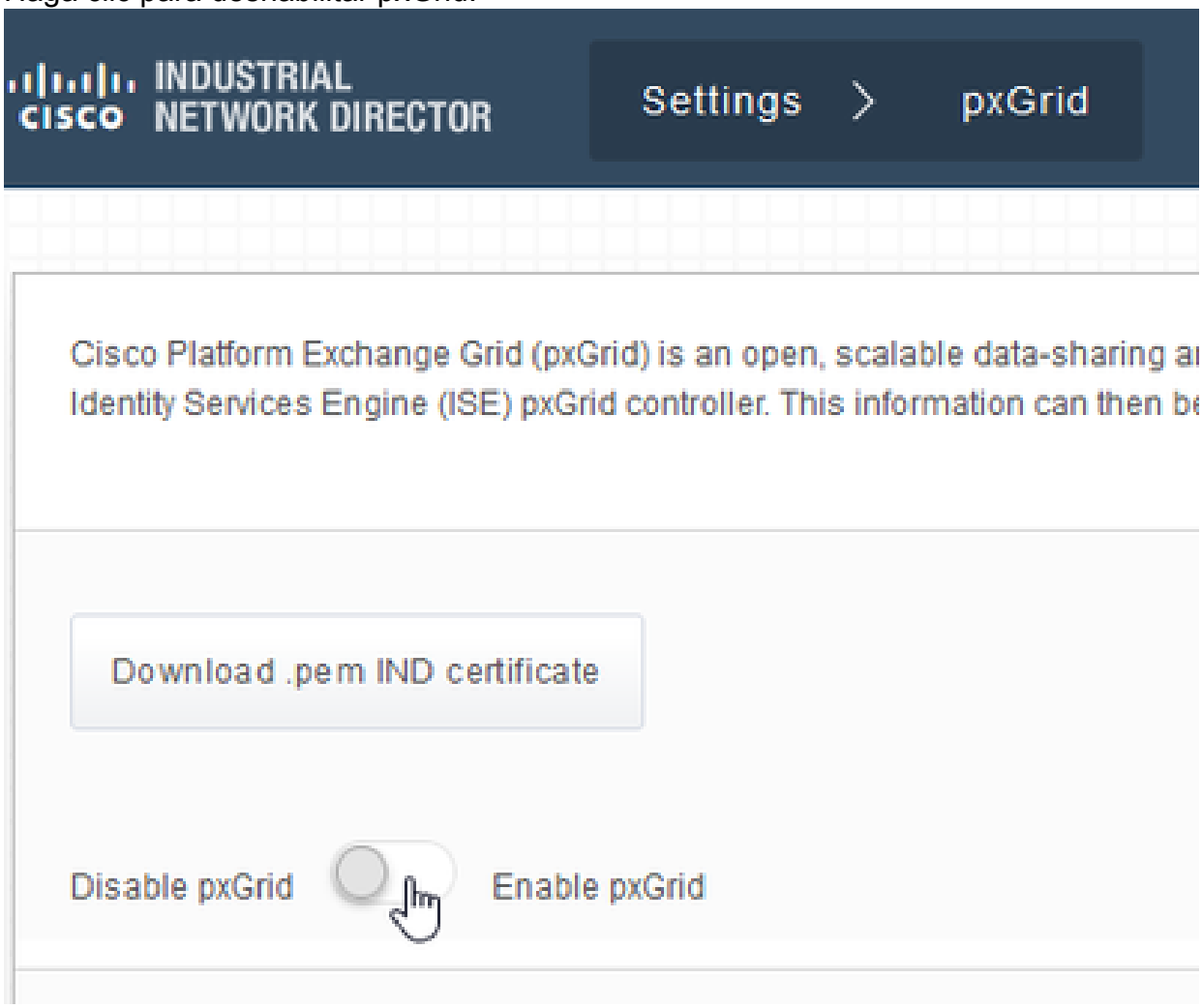


        - Esto crea y descarga un archivo ZIP que contiene el archivo de certificado, así como archivos adicionales para la cadena de certificados. Abra el ZIP y extraiga el certificado.
            - El nombre de archivo suele ser <IND server fqdn>.cer
            - En algunas versiones de ISE, el nombre de archivo es <IND fqdn>_<IND short name>.cer

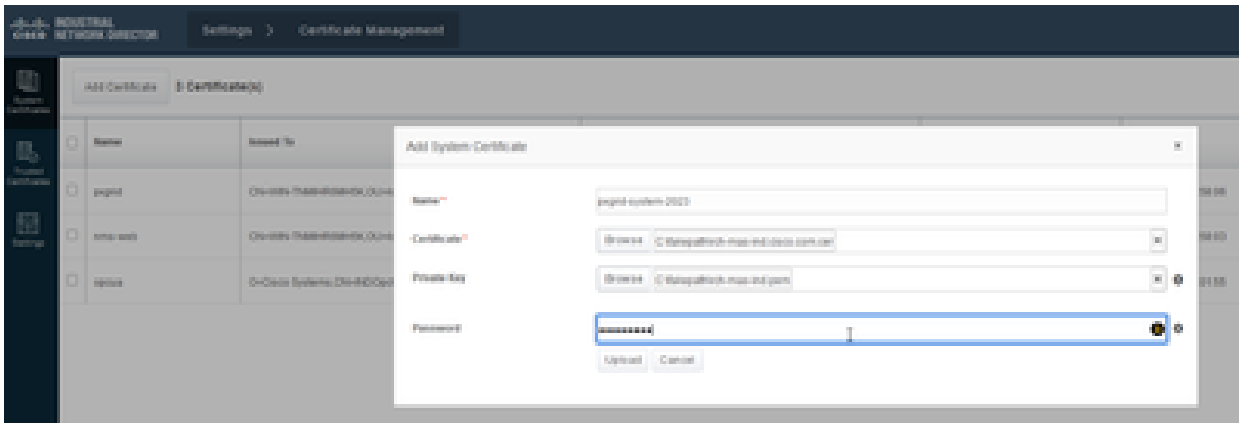
Importe el nuevo certificado en el servidor IND y habilítelo para que lo utilice pxGrid

En la GUI de IND:

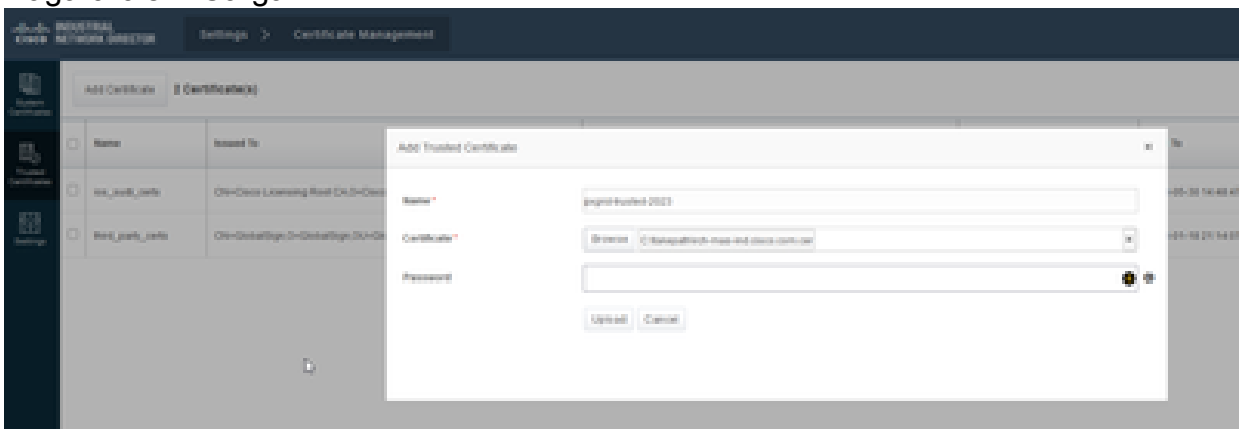
1. Deshabilite el servicio pxGrid para que el nuevo certificado se pueda importar y establecer como el certificado activo.
    - Vaya a Configuración > pxGrid.
    - Haga clic para deshabilitar pxGrid.



2. Importe el nuevo certificado en Certificados del sistema.
    - Vaya a Configuración > Administración de certificados.
    - Haga clic en "Certificados del sistema".
    - Haga clic en "Agregar certificado".
    - Introduzca un nombre de certificado.
    - Haga clic en "Examinar", a la izquierda de "Certificado", y localice el nuevo archivo de certificado.
    - Haga clic en "Examinar", a la izquierda de "Certificado", y localice la clave privada guardada al crear el CSR.
    - Introduzca la contraseña utilizada anteriormente al crear la clave privada y CSR con OpenSSL.
    - Haga clic en "Cargar".



3. Importe el nuevo certificado como certificado de confianza.
    - Vaya a Configuración > Administración de certificados y haga clic en "Certificados de confianza".
    - Haga clic en "Agregar certificado".
    - Introduzca un nombre de certificado; debe ser un nombre distinto del que se utiliza en Certificados del sistema.
    - Haga clic en "Examinar" a la izquierda de "Certificado" y localice el nuevo archivo de certificado.
    - El campo de contraseña puede dejarse vacío.
    - Haga clic en "Cargar".



4. Configure pxGrid para utilizar el nuevo certificado.
    - Navegue hasta Configuraciones > Administración de certificados, haga clic en "Configuraciones".
    - Si aún no lo ha hecho, seleccione "Certificado de CA" en "pxGrid".
    - Seleccione el nombre del certificado del sistema creado durante la importación del certificado.
    - Click Save.

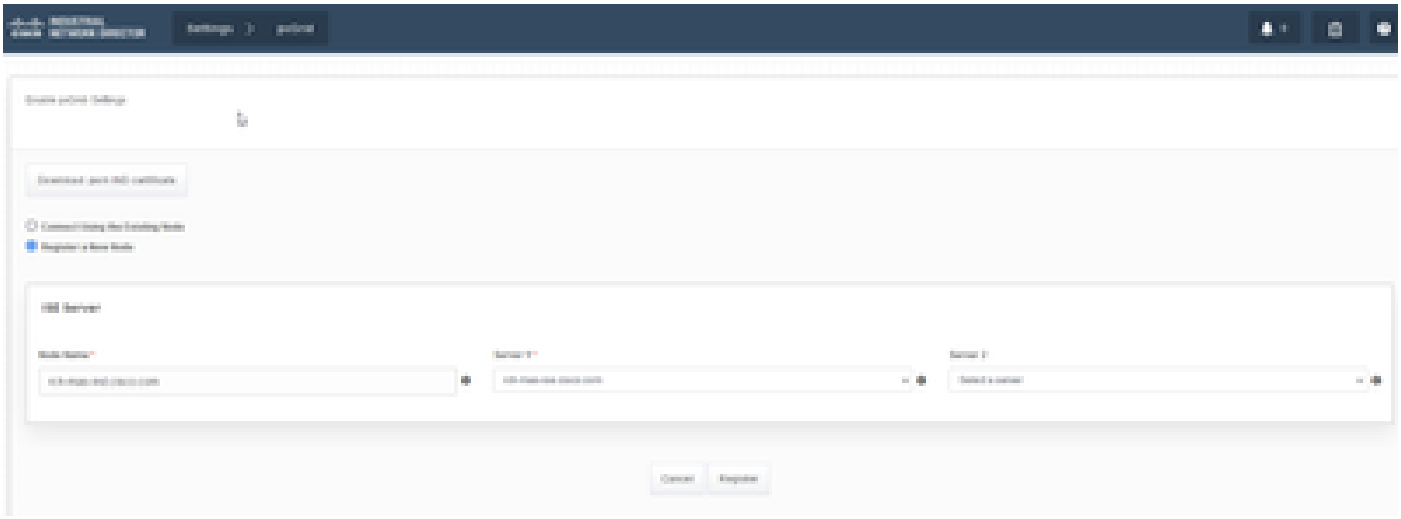
Habilitar y registrar pxGrid con el servidor ISE

En la GUI de IND:

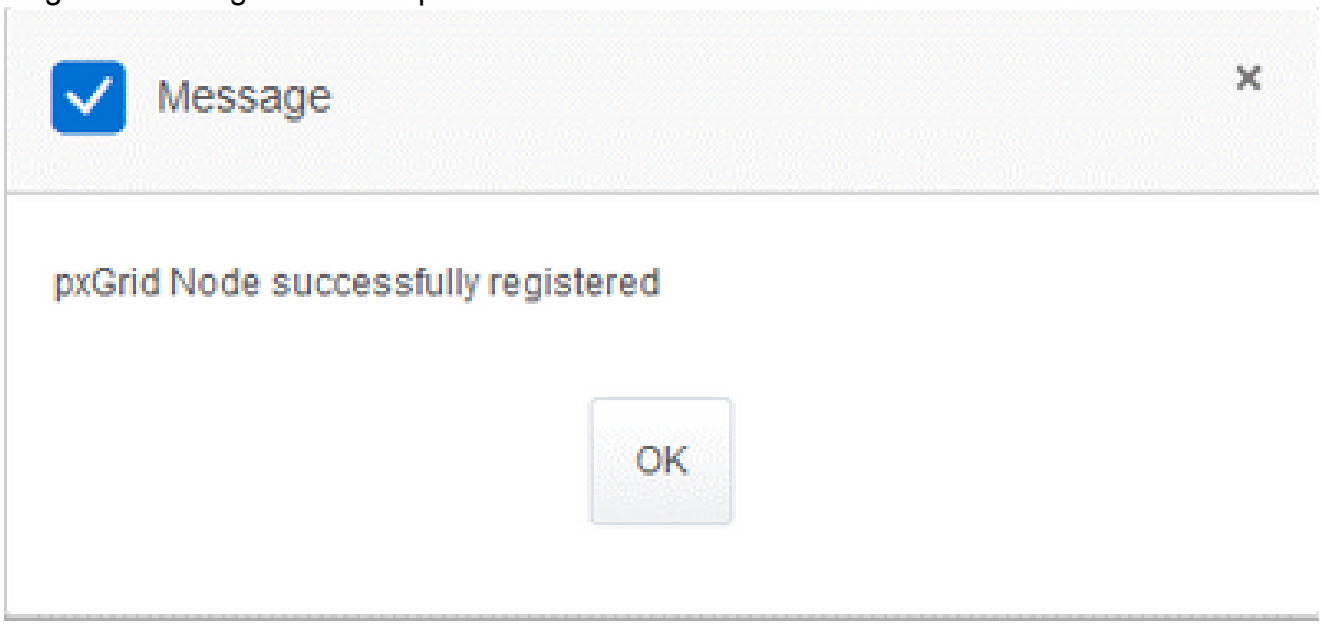
1. Vaya a Configuración > pxGrid.
2. Haga clic en el control deslizante para habilitar pxGrid.
3. Si no es la primera vez que se registra pxGrid con ISE en este servidor IND,

seleccione "Conectar usando el nodo existente". La información del nodo IND y del servidor ISE se rellena automáticamente.

4. Para registrar un nuevo servidor IND para utilizar pxGrid, si es necesario, elija "Registrar un nuevo nodo". Introduzca el nombre del nodo IND y seleccione los servidores ISE que necesite.
    - Si el servidor ISE no aparece en las opciones desplegables de Servidor 1 o Servidor 2, se puede agregar como un nuevo servidor pxGrid mediante Configuración > Servidor de políticas



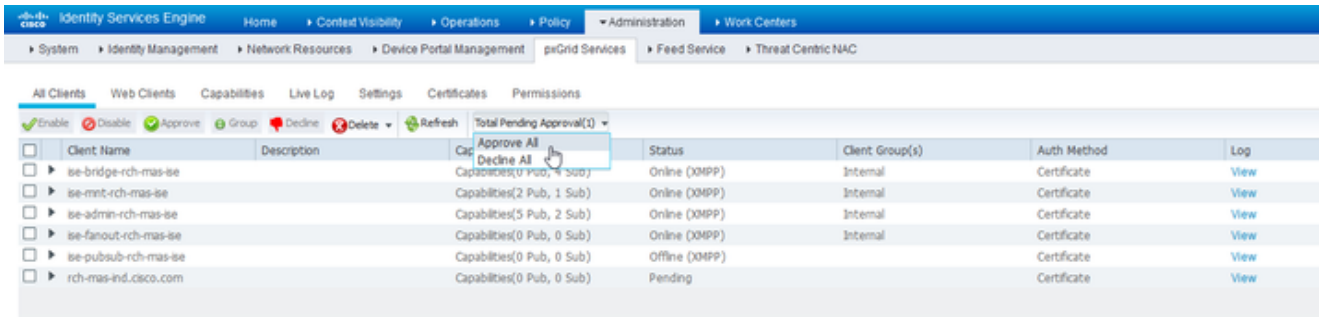
5. Haga clic en Registrar. En la pantalla se muestra una confirmación.



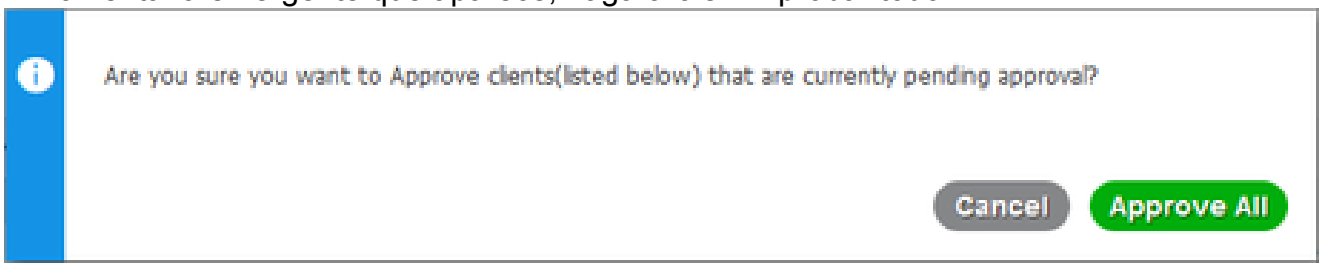
Aprobar solicitud de registro en servidor ISE

En la GUI de ISE:

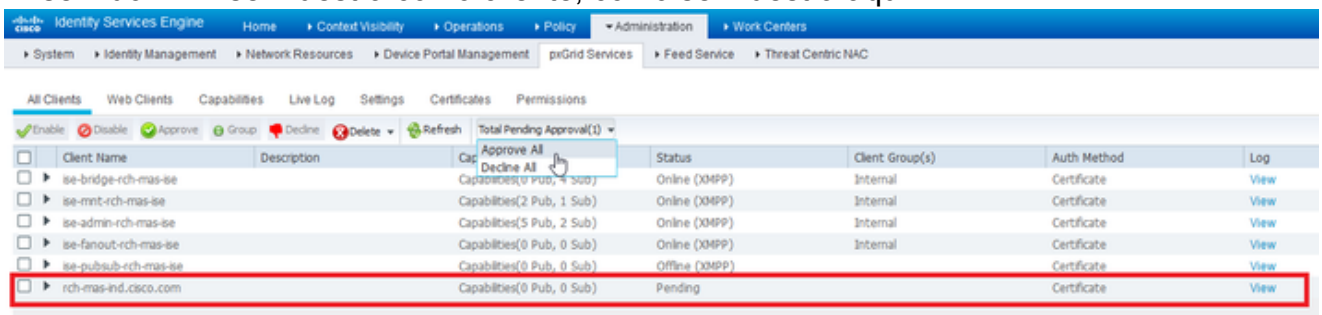
1. Vaya a Administration > pxGrid Services > All Clients. Una solicitud pendiente de aprobación se muestra como "Total pendiente de aprobación(1)".
2. Haga clic en "Total pendiente de aprobación(1)" y seleccione "Aprobar todo".



3. En la ventana emergente que aparece, haga clic en "Aprobar todo".



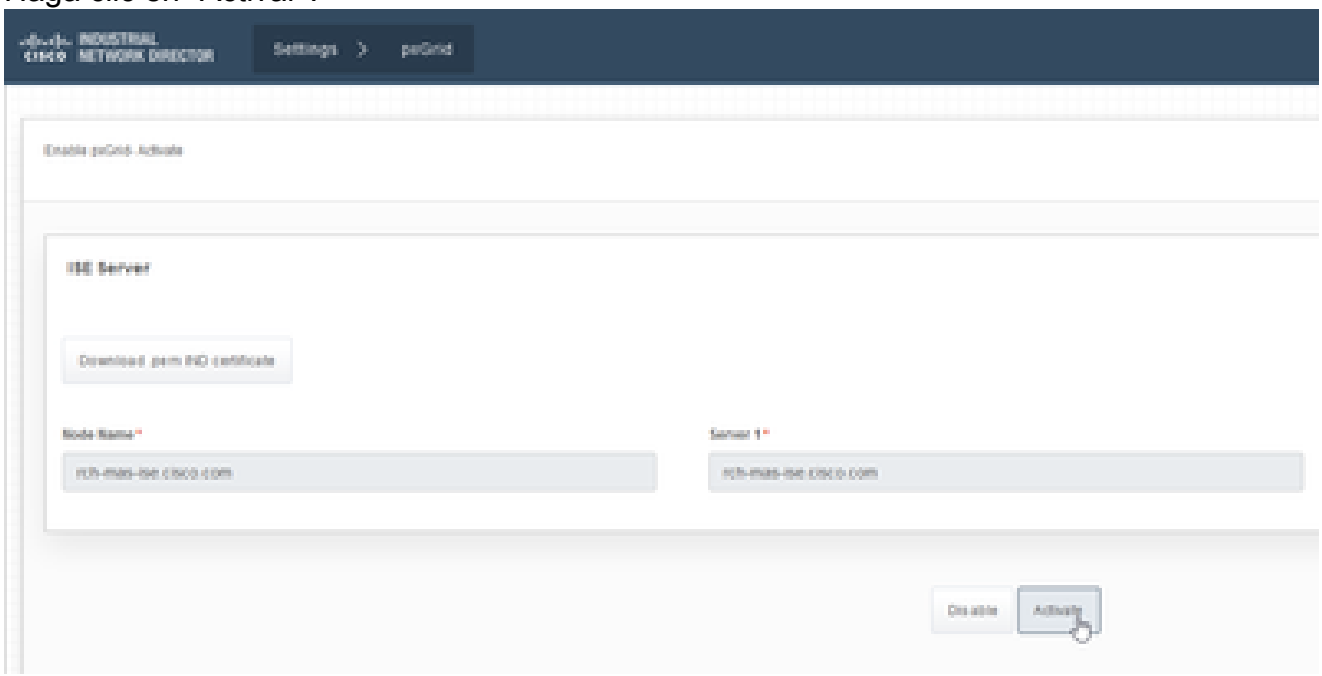
4. El servidor IND se muestra como cliente, como se muestra aquí.



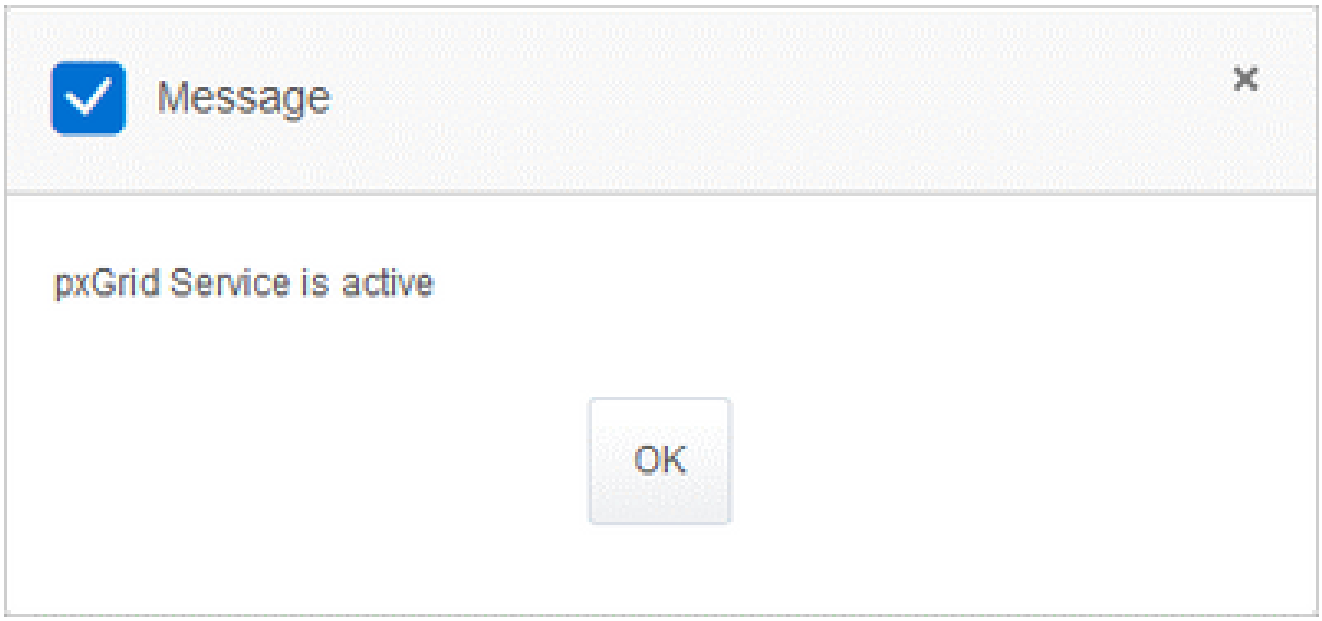
Activar el servicio pxGrid en el servidor IND

En la GUI de IND:

1. Vaya a Configuración > pxGrid.
2. Haga clic en "Activar".



3. En la pantalla se muestra una confirmación.


Message
pxGrid Service is active
OK

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).