Problemas con el uso de PNP con FND en las versiones más recientes de Cisco IOS®

Contenido

Introducción

En este documento se describe cómo generar y exportar el certificado correcto desde la infraestructura de clave privada (PKI) de Windows para su uso en combinación con Plug and Play (PNP) en Field Network Director (FND).

Problema

Cuando intenta utilizar PNP para realizar la implementación sin intervención del usuario (ZTD) en las versiones más recientes de Cisco IOS® y Cisco IOS®-XE, el proceso falla con uno de estos errores PNP:

```
Error while creating FND trustpoint on the device. errorCode: PnP Service Error 3341,
errorMessage: SSL Server ID check failed after cert-install
Error while creating FND trustpoint on the device. errorCode: PnP Service Error 3337,
errorMessage: Cant get PnP Hello Response after cert-install
```

Desde hace algún tiempo, el código PNP en Cisco IOS®/Cisco IOS®-XE requiere que el campo Nombre alternativo del sujeto (SAN) se rellene en el certificado ofrecido por el servidor/controlador PNP (FND en este caso).

El agente PNP de Cisco IOS® comprueba solamente el campo SAN de certificado para la identidad del servidor. Ya no comprueba el campo de nombre común (CN).

Esto es válido para estas versiones:

- Cisco IOS® Release 15.2(6)E2 y versiones posteriores
- Cisco IOS® versión 15.6(3)M4 y posteriores
- Cisco IOS® Release 15.7(3)M2 y posterior
- Denali Cisco IOS® XE 16.3.6 y versiones posteriores
- Cisco IOS® XE Everest 16.5.3 y versiones posteriores
- Cisco IOS® Everest 16.6.3 y versiones posteriores

- Todas las versiones de Cisco IOS® de 16.7.1 y posteriores

Puede encontrar más información aquí:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html#id_70663

Solución

La mayoría de las guías y la documentación de FND aún no mencionan que es necesario rellenar el campo SAN.

Para crear y exportar el certificado correcto para utilizarlo con PNP y agregarlo al almacén de claves, siga estos pasos.

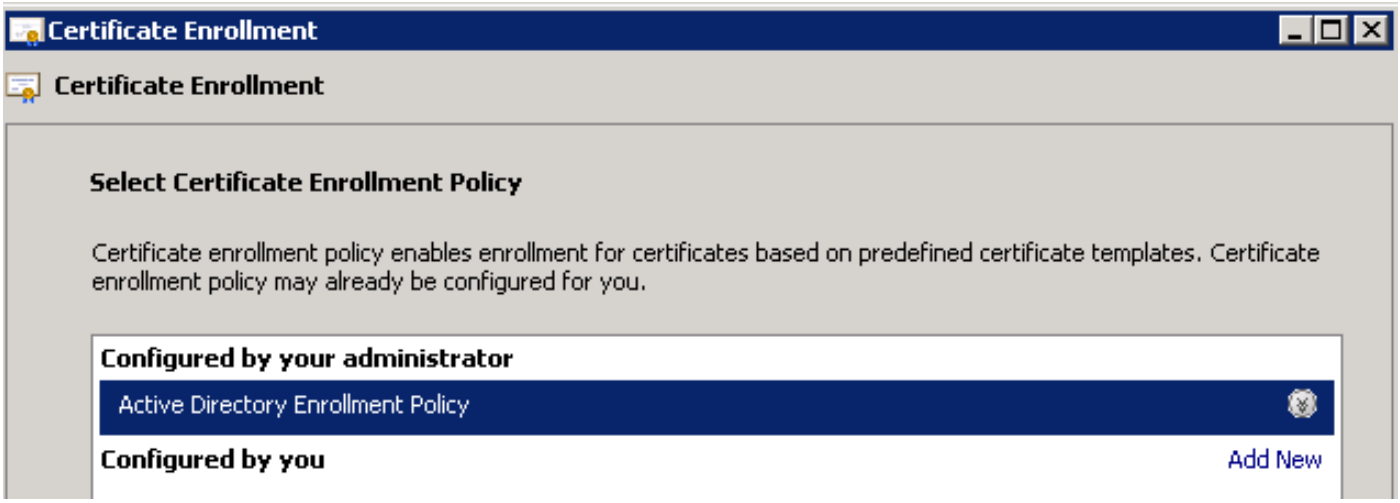
Generar un certificado nuevo con el uso de la plantilla FND/NMS en el servidor CA de Windows

Vaya a **Inicio > Ejecutar > mmc > Archivo > Agregar o quitar complemento... > Certificados > Agregar > Cuenta de equipo > Equipo local > Aceptar** y abra el complemento MMC de certificados.

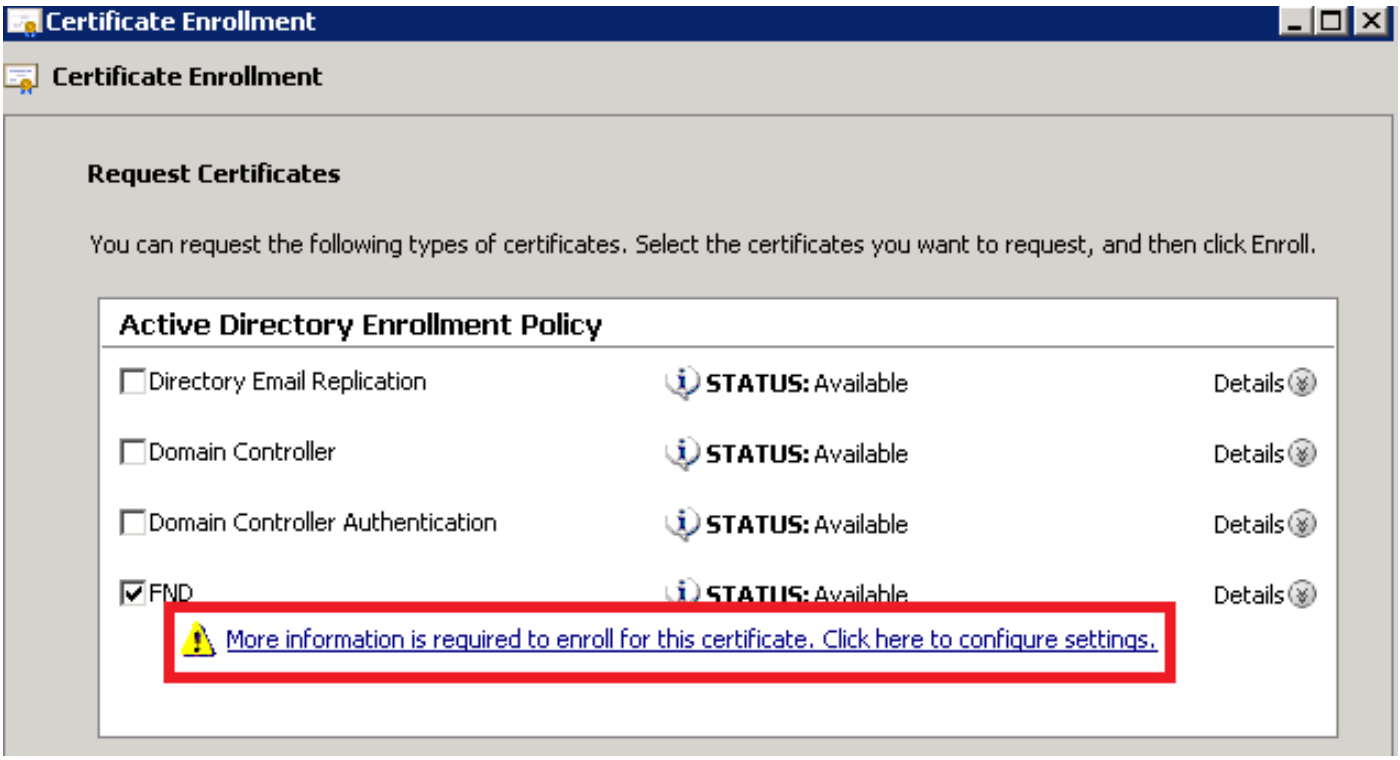
Expanda Certificados (Equipo local) > Personal > Certificados

Haga clic con el botón derecho del ratón en Certificados y seleccione **Todas las tareas > Solicitar nuevo certificado...** como se muestra en la imagen.

Haga clic en **Next** y seleccione **Active Directory Enrollment Policy** como se muestra en la imagen.



Haga clic en **Next** y seleccione la plantilla creada para el servidor NMS/FND (repita más tarde para TelePresence Server (TPS)) y haga clic en el enlace **More Information** (**Más información**), como se muestra en la imagen.



En las propiedades del certificado, proporcione esta información:

Nombre del asunto:

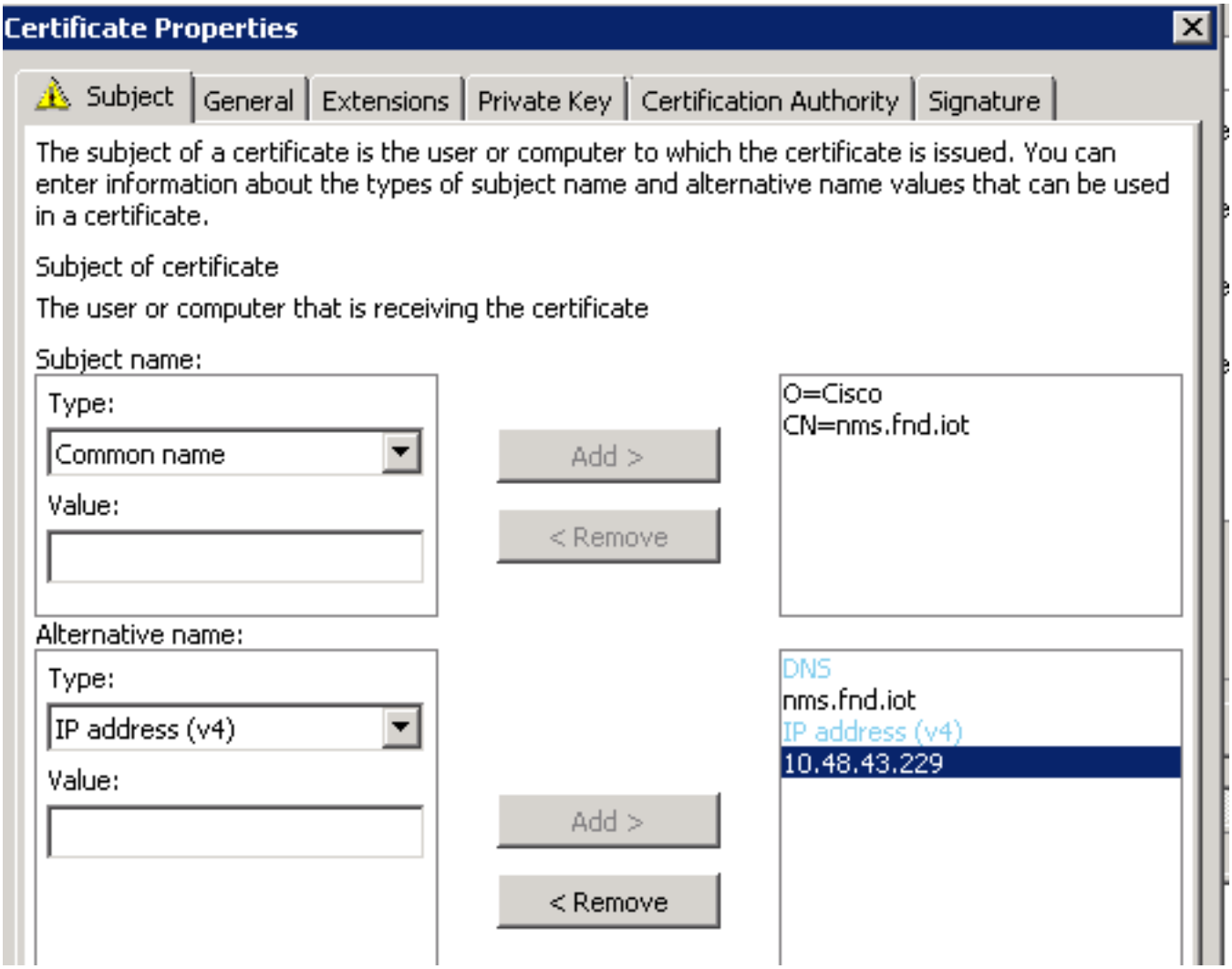
- Organización: el nombre de su organización
- Nombre común: el nombre de dominio completo (FQDN) del servidor FND (o TPS, si procede)

Nombre alternativo (el campo SAN):

- Si utiliza el Sistema de nombres de dominio (DNS) para ponerse en contacto con la parte PNP del servidor FND, agregue una entrada DNS para el FQDN
- Si utiliza IP para comunicarse con la parte PNP del servidor FND, agregue una entrada IPv4 para la IP

Se recomienda incluir varios valores SAN en el certificado, en caso de que los métodos de detección varíen. Por ejemplo, puede incluir el FQDN del controlador y la dirección IP (o la dirección IP de NAT) en el campo SAN. Si incluye ambos, establezca el FQDN como el primer valor de SAN, seguido de la dirección IP.

Ejemplo de configuración:



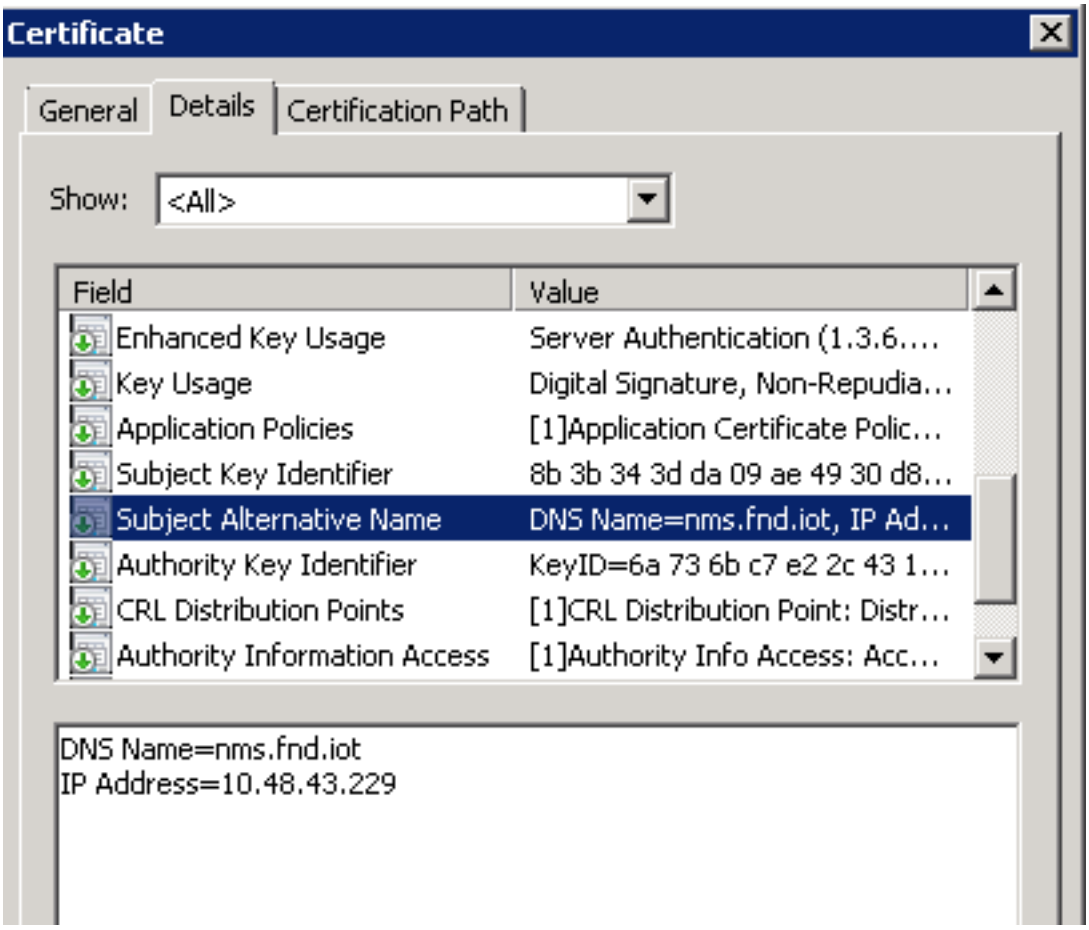
Una vez completada, haga clic en **Aceptar** en la Ventana Propiedades del Certificado, luego en **Inscribirse** para generar el certificado y en **Finalizar** cuando la generación haya terminado.

Compruebe el campo SAN del certificado generado

Sólo para comprobar si el certificado generado contiene la información correcta, puede comprobarlo de la siguiente manera:

Abra el complemento certificados en Microsoft Management Console (MMC) y expanda **Certificados (equipo local) > Personal > Certificados**.

Haga doble clic en el certificado generado y abra la ficha **Detalles**. Desplácese hacia abajo para buscar el campo SAN, como se muestra en la imagen.

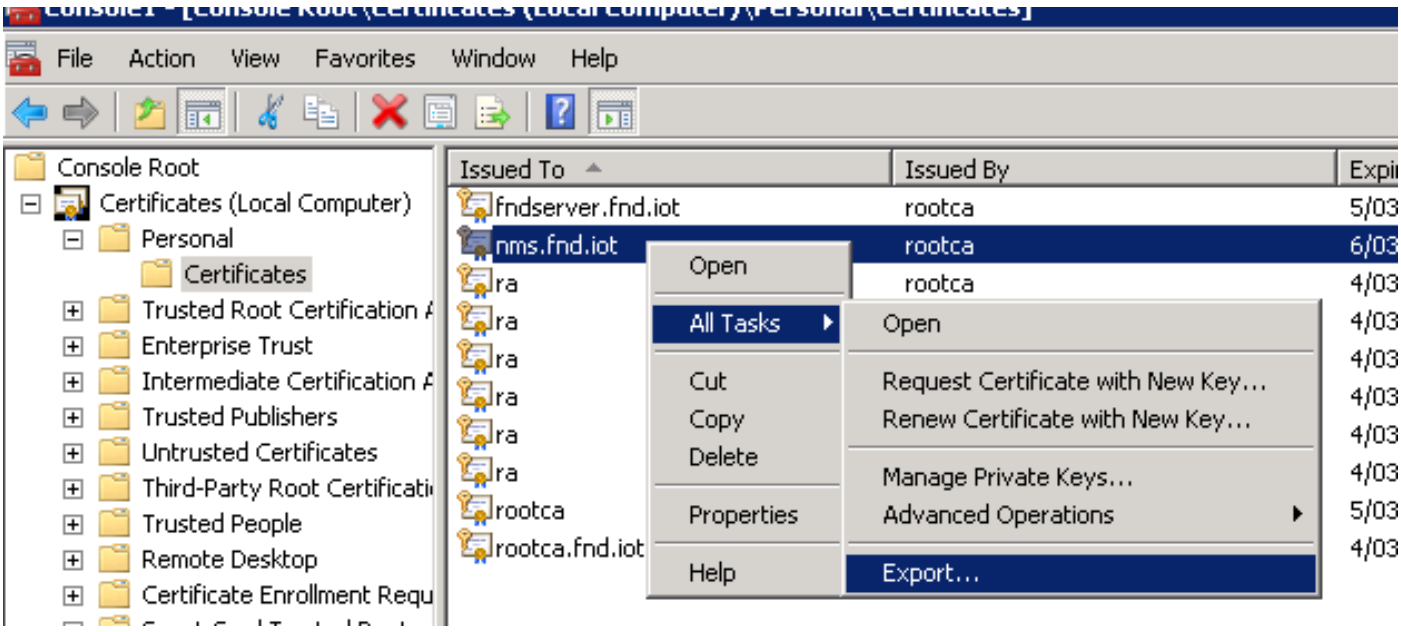


Exportar el certificado para importar al almacén de claves FND

Para poder importar o reemplazar el certificado que existe en el almacén de claves FND, debe exportarlo a un archivo **.pfd**.

En el complemento certificados de MMC, expanda **Certificados (equipo local) > Personal > Certificados**

Haga clic con el botón derecho en el certificado generado y seleccione **Todas las tareas > Exportar...** como se muestra en la imagen.



Haga clic en **Siguiente**, seleccione para exportar la clave privada como se muestra en la imagen.

Seleccione esta opción para incluir todos los certificados en la ruta de certificación como se muestra en la imagen.

Haga clic en **Next**, seleccione una contraseña para la exportación y guarde el archivo **.pfx** en una ubicación conocida.

Creación del almacén de claves FND para su uso con PNP

Ahora que ha exportado el certificado, puede crear el almacén de claves necesario para FND.

Transfiera el **.pfx** generado desde el paso anterior de forma segura al servidor FND (máquina de Network Management Systems (NMS) o host OVA), por ejemplo con el uso de SCP.

Enumere el contenido de **.pfx** para conocer el alias generado automáticamente en la exportación:

```
[root@iot-fnd ~]# keytool -list -v -keystore nms.pfx -srcstoretype pkcs12 | grep Alias
Enter keystore password:  keystore
Alias name: le-fnd-8f0908aa-dc8d-4101-a526-93b4eaad9481
```

Cree un nuevo almacén de claves con el uso de este comando:

```
root@iot-fnd ~]# keytool -importkeystore -v -srckeystore nms.pfx -srcstoretype pkcs12 -
destkeystore cgms_keystore_new -deststoretype jks -srcalias le-fnd-8f0908aa-dc8d-4101-a526-
93b4eaad9481 -destalias cgms -destkeypass keystore
Importing keystore nms.pfx to cgms_keystore_new...
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
[Storing cgms_keystore_new]

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an
industry standard format using "keytool -importkeystore -srckeystore cgms_keystore_new -
destkeystore cgms_keystore_new -deststoretype pkcs12".
```

En el comando, asegúrese de reemplazar **nms.pfx** con el archivo correcto (exportado desde Windows CA) y de que el valor srcalias coincida con la salida del comando anterior (**keytool -list**).

Después de generarlo, conviértalo al nuevo formato como se sugiere:

```
[root@iot-fnd ~]# keytool -importkeystore -srckeystore cgms_keystore_new -destkeystore
cgms_keystore_new -deststoretype pkcs12 Enter source keystore password: Entry for alias cgms
successfully imported. Import command completed: 1 entries successfully imported, 0 entries
failed or cancelled Warning: Migrated "cgms_keystore_new" to Non JKS/JCEKS. The JKS keystore is
backed up as
"cgms_keystore_new.old".
```

Agregue el certificado de CA, exportado anteriormente, al almacén de claves:

```
[root@iot-fnd ~]# keytool -import -trustcacerts -alias root -keystore cgms_keystore_
new -file rootca.cer Enter keystore password: Owner: CN=rootca, DC=fnd, DC=iot Issuer:
CN=rootca, DC=fnd, DC=iot ... Trust this certificate? [no]: yes Certificate was added to
keystore
```

Y finalmente, agregue el certificado SUDI, que se utiliza para verificar la identidad por serie del FAR cuando utiliza PNP, al almacén de claves.

Para una instalación RPM, el certificado SUDI se incluye con los paquetes y se puede encontrar en: **/opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem**

Para una instalación OVA, copie primero el certificado SUDI en el host:

```
[root@iot-fnd ~]# docker cp fnd-container:/opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem
.
```

Luego agréguelo al almacén de claves como confiable con el alias SUDI:

```
[root@iot-fnd ~]# keytool -import -trustcacerts -alias sudi -keystore cgms_keystore_new -file
cisco-sudi-ca.pem
Enter keystore password:
Owner: CN=ACT2 SUDI CA, O=Cisco
Issuer: CN=Cisco Root CA 2048, O=Cisco Systems
...
```

```
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

En este momento, el almacén de claves está listo para utilizarse con FND.

Activar el almacén de claves nuevo/modificado para su uso con FND

Antes de utilizar el almacén de claves, reemplace la versión anterior y, opcionalmente, actualice la contraseña en el archivo **cgms.properties**.

Primero, haga una copia de seguridad del almacén de claves que ya existe:

Para una instalación RPM:

```
[root@fndnms ~]# cp /opt/cgms/server/cgms/conf/cgms_keystore cgms_keystore_backup
```

Para una instalación de OVA:

```
[root@iot-fnd ~]# cp /opt/fnd/data/cgms_keystore cgms_keystore_backup
```

Reemplace el que existe por el nuevo:

Para una instalación RPM:

```
[root@fndnms ~]# cp cgms_keystore_new /opt/cgms/server/cgms/conf/cgms_keystore
```

Para una instalación de OVA:

```
[root@iot-fnd ~]# cp cgms_keystore_new /opt/fnd/data/cgms_keystore
```

Opcionalmente, actualice la contraseña para el almacén de claves en el archivo cgms.properties:

En primer lugar, genere una nueva cadena de contraseña cifrada.

Para una instalación RPM:

```
[root@fndnms ~]# /opt/cgms/bin/encryption_util.sh encrypt keystore
7jlXPniVpMvat+TrDWqh1w==
```

Para una instalación de OVA:

```
[root@iot-fnd ~]# docker exec -it fnd-container /opt/cgms/bin/encryption_util.sh encrypt
keystore
7jlXPniVpMvat+TrDWqh1w==
```

Asegúrese de reemplazar el almacén de claves por la contraseña correcta para el almacén de

claves.

Cambie cgms.properties en **/opt/cgms/server/cgms/conf/cgms.properties** para la instalación basada en RPM o **/opt/fnd/data/cgms.properties** para la instalación basada en OVA para incluir la nueva contraseña cifrada.

Por último, reinicie FND para empezar a utilizar el nuevo almacén de claves y la nueva contraseña.

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).