Problemen met het gebruik van PNP met FDN op nieuwere Cisco IOS®-releases

Inhoud

Inleiding

Dit document beschrijft hoe u het juiste certificaat kunt genereren en exporteren vanuit de Windows Private Key Infrastructure (PKI) voor gebruik in combinatie met Plug and Play (PNP) op Field Network Director (FND).

Probleem

Wanneer u probeert PNP te gebruiken om Zero Touch Implementation (ZTD) uit te voeren op nieuwere releases van Cisco IOS® en Cisco IOS®-XE, faalt het proces met een van deze PNP-fouten:

```
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
```

Sinds enige tijd moet in het veld PNP-code in Cisco IOS®/Cisco IOS®-XE het veld Onderwerp Alternatieve naam (SAN) worden ingevuld in het certificaat dat door de PNP-server/controller (in dit geval FND) wordt aangeboden.

De PNP Cisco IOS® Agent controleert alleen het veld voor het certificaat-SAN op de identiteit van de server. Het controleert niet meer het gebied van de gemeenschappelijke naam (CN).

Dit is geldig voor deze releases:

- Cisco IOS®-softwarerelease 15.2(6)E2 en hoger
- Cisco IOS®-softwarerelease 15.6(3)M4 en hoger
- Cisco IOS®softwarerelease 15.7(3)M2 en hoger
- Cisco IOS® XE Denali 16.3.6 en hoger
- Cisco IOS® XE Everest 16.5.3 en hoger
- Cisco IOS® Everest 16.6.3 en hoger

- Alle Cisco IOS®-releases van 16.7.1 en hoger

Meer informatie vindt u hier: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html#id_70663

Oplossing

De meeste gidsen en documentatie voor FND vermelden nog niet dat het SAN-veld moet worden ingevuld.

Om het juiste certificaat voor gebruik met PNP te maken en te exporteren en het toe te voegen aan de sleutel store, volg deze stappen.

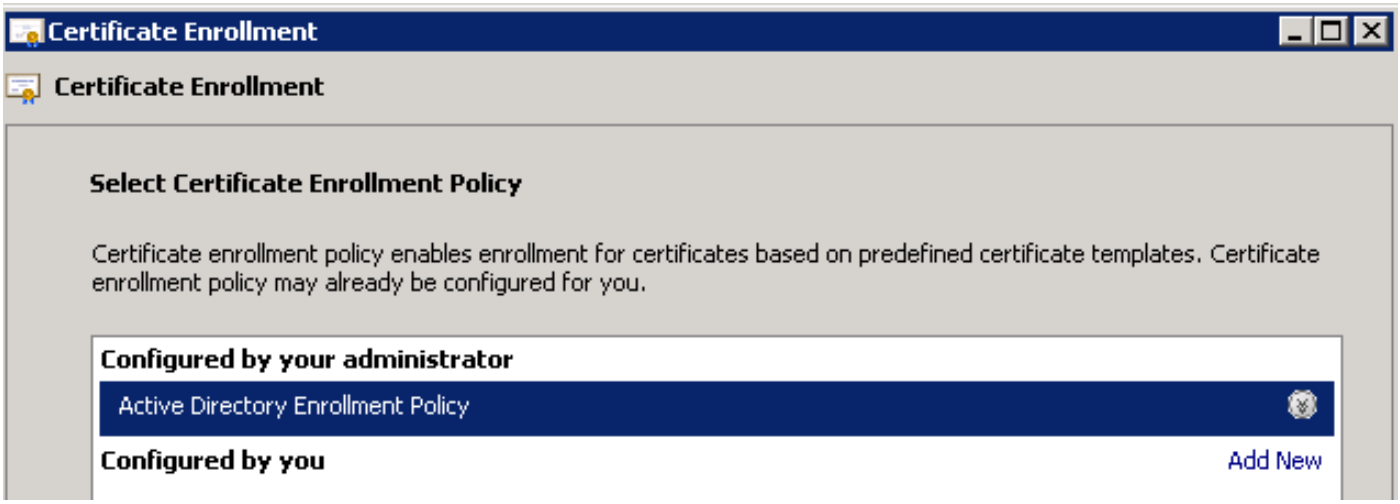
Een nieuw certificaat genereren met behulp van de FND/NMS-sjabloon op de Windows CA-server

Navigeer naar **Start > Uitvoeren > mmc > Bestand > Magnetisch toevoegen/verwijderen... > Certificaten > Toevoegen > Computeraccount > Lokale computer > OK** en open de certificaten MMC-invoegtoepassing.

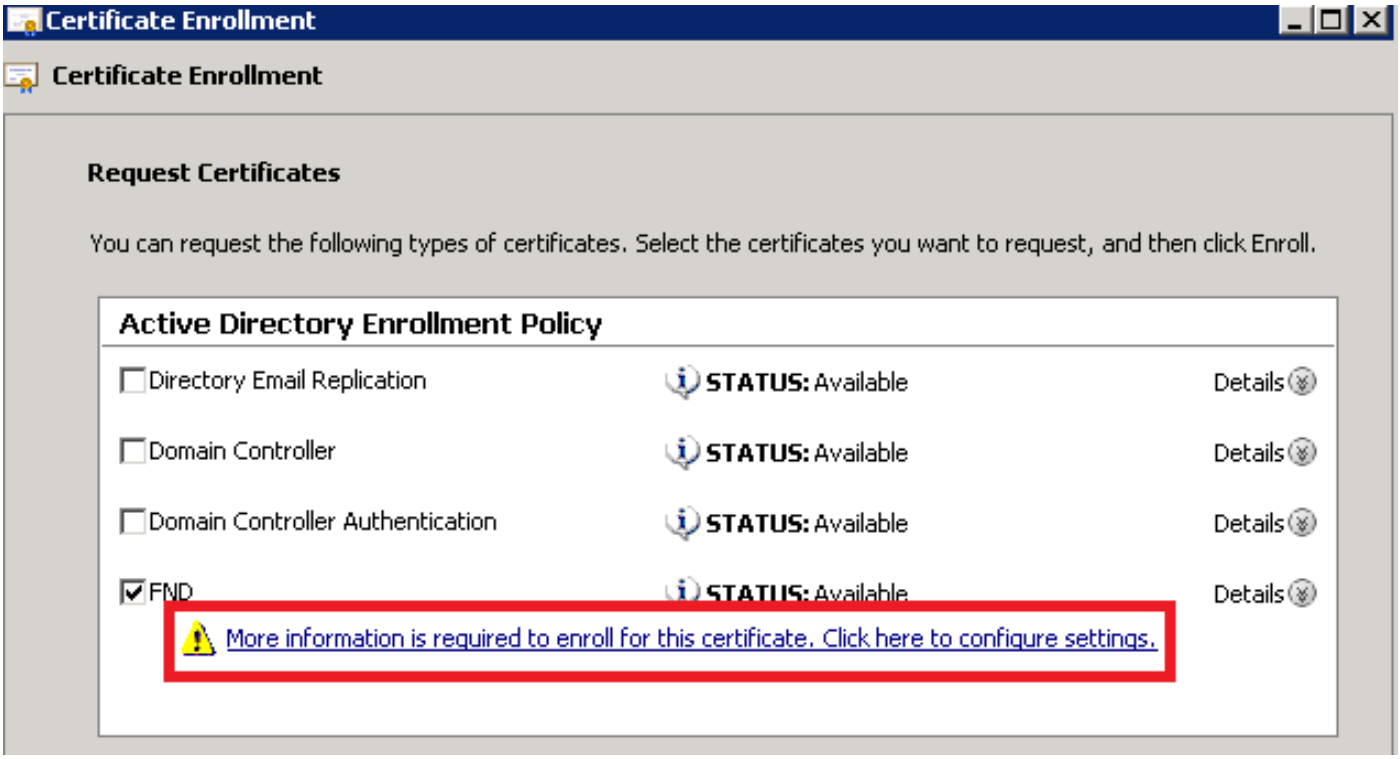
Certificaten uitvouwen (lokale computer) > Persoonlijk > Certificaten

Klik met de rechtermuisknop op Certificaten en selecteer **Alle taken > Nieuw certificaat aanvragen...** zoals in de afbeelding.

Klik op **Volgende** en selecteer **Active Directory-inschrijvingsbeleid** zoals in de afbeelding.



Klik op **Volgende** en selecteer de sjabloon die is gemaakt voor NMS/FND-server (herhaal dit later voor TelePresence Server (TPS)) en klik op de koppeling **Meer informatie** zoals in de afbeelding.



Geef in de eigenschappen van het certificaat deze informatie op:

Onderwerpnaam:

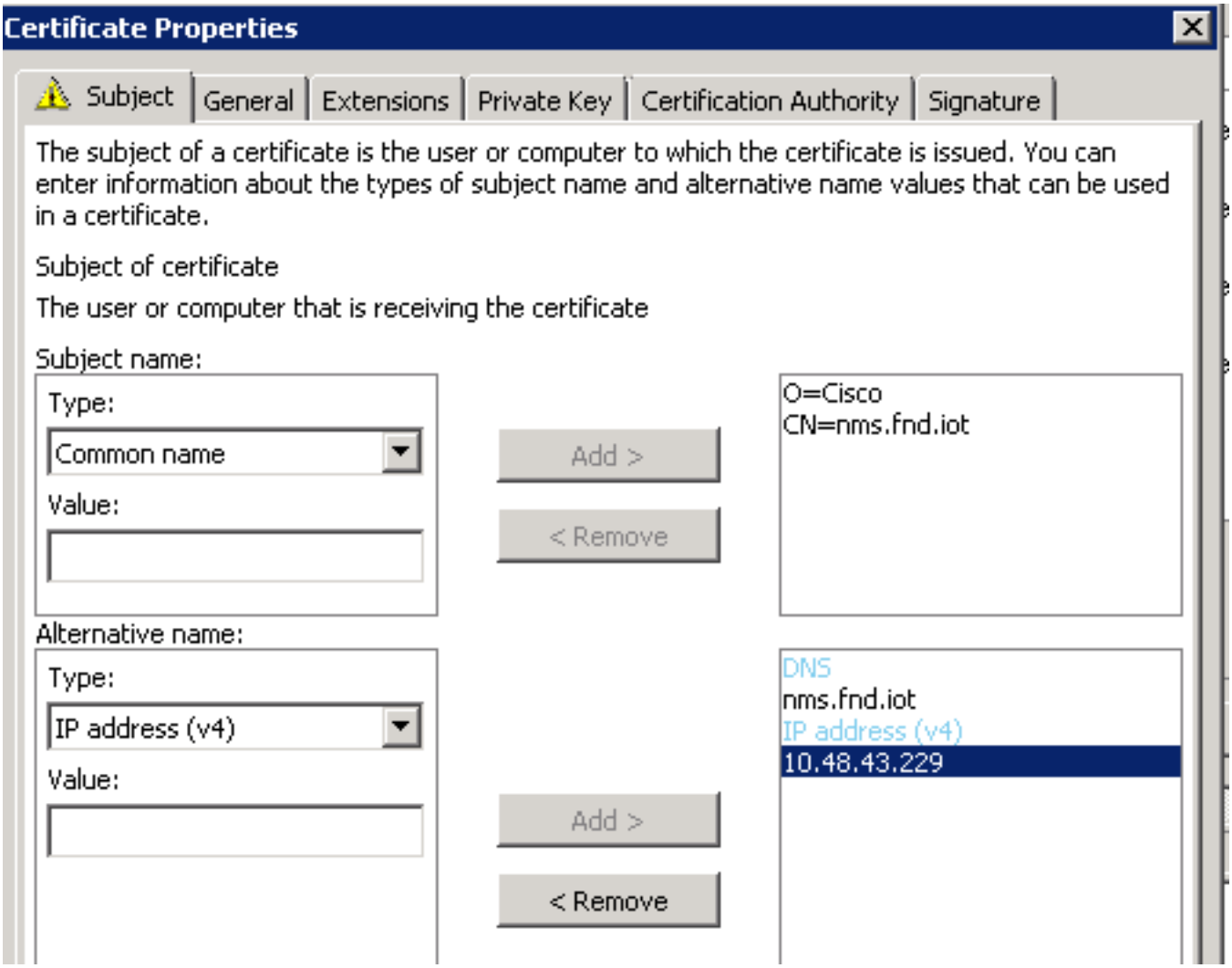
- Organisatie: de naam van uw organisatie
- Gebruikelijke naam: de volledig gekwalificeerde domeinnaam (FQDN) van de FND-server (of TPS indien van toepassing)

Alternatieve naam (het SAN-veld):

- Als u Domain Name System (DNS) gebruikt om contact op te nemen met het PNP-deel van de FND-server, voegt u een DNS-ingang toe voor de FQDN
- Als u IP gebruikt om contact op te nemen met het PNP-onderdeel van de FND-server, voeg dan een IPv4-vermelding toe voor het IP

Het wordt aanbevolen om meerdere SAN-waarden in het certificaat op te nemen, mochten er verschillende detectiemethoden zijn. U kunt bijvoorbeeld zowel het controller-FQDN als het IP-adres (of NAT IP-adres) in het SAN-veld opnemen. Als u beide wel meeneemt, stelt u de FQDN in als de eerste SAN-waarde, gevolgd door het IP-adres.

Voorbeeldconfiguratie:



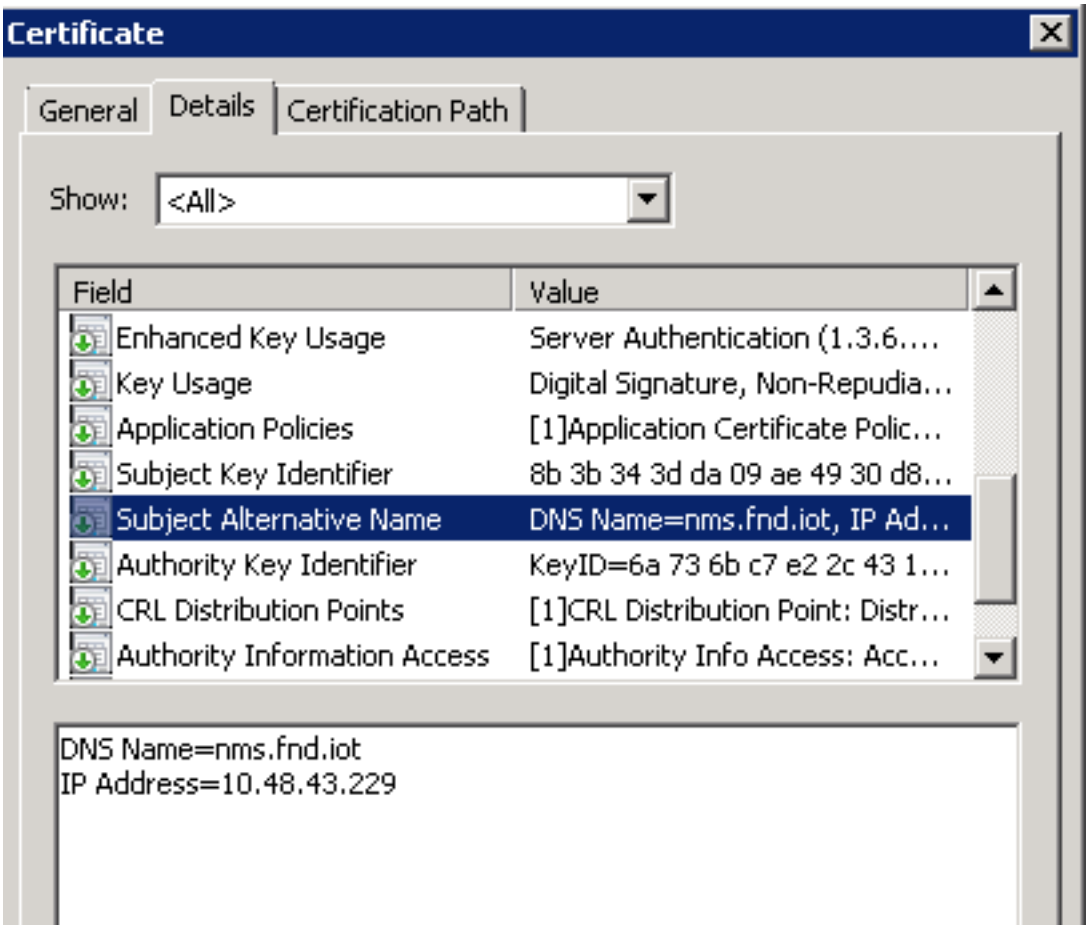
Als u klaar bent, klikt u op **OK** in het venster Certificaateigenschappen, **schrijft u** in om het certificaat te genereren en **eindigt u** wanneer de generatie is voltooid.

Controleer het SAN-veld in het gegenereerde certificaat

Alleen om te controleren of het gegenereerde certificaat de juiste informatie bevat, kunt u het als volgt controleren:

Open de certificaten Snap-In in Microsoft Management Console (MMC) en breid **Certificaten (Lokale Computer) > Persoonlijk > Certificaten uit**.

Dubbelklik op het gegenereerde certificaat en open het tabblad **Details**. Blader naar beneden om het SAN-veld te vinden, zoals in de afbeelding wordt weergegeven.

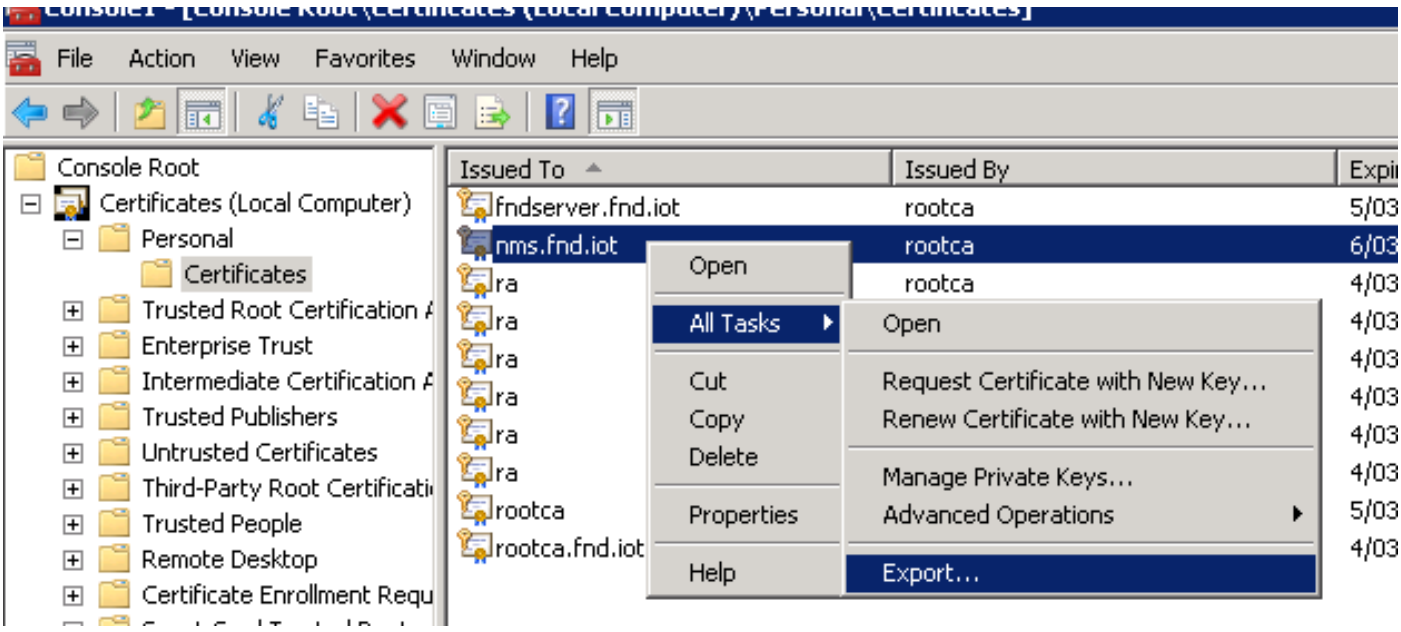


Certificaat exporteren naar Importeren in het FND Keystore

Alvorens u het certificaat kunt invoeren of vervangen dat in FND keystore bestaat, moet u het naar een **.pfd-**bestand exporteren.

In de certificaten Snap-In in MMC, breid **Certificaten (Lokale Computer) > Persoonlijk > Certificaten uit**

Klik met de rechtermuisknop op het gegenereerde certificaat en selecteer **Alle taken > Exporteren...** zoals in de afbeelding.



Klik op **Volgende**, selecteer deze om de privé-sleutel te exporteren zoals in de afbeelding.

Selecteer deze optie om alle certificaten op te nemen in het certificatiepad zoals in de afbeelding.

Klik op **Volgende**, selecteer een wachtwoord voor het exporteren en sla **.pfx** op een bekende locatie op.

Maak de FND Keystore voor gebruik met PNP

Nu u het certificaat geëxporteerd hebt, kunt u de keystore bouwen die nodig is voor FND.

Breng het gegenereerde **.pfx** van de vorige stap veilig over naar de FND-server (Network Management Systems (NMS) machine of OVA host), bijvoorbeeld met het gebruik van SCP.

Maak een lijst van de inhoud van de **.pfx** om het automatisch gegenereerde alias te leren kennen in de export:

```
[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
```

Maak een nieuwe keystore met het gebruik van deze opdracht:

```
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".
```

Zorg er in de opdracht voor dat u **nms.pfx** vervangt met het juiste bestand (geëxporteerd vanuit Windows CA) en dat de srcaliawaarde overeenkomt met de uitvoer van de vorige opdracht (**keytool -list**).

Nadat u deze hebt gegenereerd, converteert u deze naar het nieuwe formaat zoals wordt voorgesteld:

```
[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".
```

Voeg het CA-certificaat, dat eerder is geëxporteerd, toe aan de keystore:

```
[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
```

En tot slot, voeg het SUDI-certificaat toe, dat wordt gebruikt om de identiteit per serie van de FAR te verifiëren wanneer u PNP gebruikt, aan de keystore.

Voor een RPM-installatie is het SUDI-certificaat gebundeld met de pakketten en kan worden gevonden in: **/opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem**

Voor een OVA installatie, eerste kopie van het SUDI certificaat aan de host:

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

Voeg het dan toe aan de keystore zoals vertrouwd met 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
```

Op dit punt is de keystore klaar om te worden gebruikt met FND.

Activeer de Nieuwe/Aangepaste Keystore voor Gebruik met FND

Alvorens u keystore gebruikt, vervang de vorige versie en update naar keuze het wachtwoord in het **cgms.Properties** bestand.

Neem eerst een back-up van de reeds bestaande keystore:

Voor een RPM-installatie:

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

Voor een OVA-installatie:

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

Vervang de bestaande door de nieuwe:

Voor een RPM-installatie:

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

Voor een OVA-installatie:

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

U kunt het wachtwoord voor het toetsenbord optioneel bijwerken in het bestand cgms.Properties:

Genereert eerst een nieuwe versleutelde wachtwoordstring.

Voor een RPM-installatie:

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

Voor een OVA-installatie:

```
[root@iot-fnd ~]# docker exec -it fnd-container /opt/cgms/bin/encryption_util.sh encrypt
```

```
keystore
7jlXPniVpMvat+TrDWqh1w==
```

Zorg ervoor dat u keystore vervangt met het juiste wachtwoord voor uw keystore.

Wijzig cgms.Properties in **/opt/cgms/server/cgms/conf/cgms.properties** voor de op RPM gebaseerde installatie of **/opt/fnd/data/cgms.properties** voor de op OVA gebaseerde installatie om het nieuwe gecodeerde wachtwoord op te nemen.

Start FND opnieuw om te beginnen met het gebruik van de nieuwe keystore en het wachtwoord.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.