Probleme bei der Verwendung von PNP mit FND für neuere Cisco IOS®-Versionen

Inhalt

[Einleitung](#)
[Problem](#)
[Lösung](#)
[Erstellen eines neuen Zertifikats mit der FND/NMS-Vorlage auf dem Windows-Zertifizierungsstellenserver](#)
[Überprüfen Sie das SAN-Feld im generierten Zertifikat.](#)
[Zertifikat in FND-Schlüsselspeicher exportieren](#)
[Erstellen eines FND-Schlüsselspeichers zur Verwendung mit PNP](#)
[Aktivieren des neuen/geänderten Schlüsselspeichers für die Verwendung mit FND](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie das richtige Zertifikat aus der Windows Private Key Infrastructure (PKI) generieren und exportieren, um es in Kombination mit Plug and Play (PNP) auf Field Network Director (FND) verwenden zu können.

Problem

Wenn Sie versuchen, PNP für die Zero Touch Deployment (ZTD) auf neueren Cisco IOS®- und Cisco IOS®-XE-Versionen einzusetzen, schlägt der Prozess mit einem der folgenden PNP-Fehler fehl:

```
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
```

Seit einiger Zeit muss der PNP-Code in Cisco IOS®/Cisco IOS®-XE das Feld "Subject Alternative Name (SAN)" (Alternativer Name des Antragstellers) in das vom PNP-Server/Controller (in diesem Fall FND) bereitgestellte Zertifikat einfügen.

Der PNP Cisco IOS® Agent überprüft nur das SAN-Feld des Zertifikats auf die Serveridentität. Das Feld für den allgemeinen Namen (CN) wird nicht mehr überprüft.

Dies gilt für folgende Versionen:

- Cisco IOS® Version 15.2(6)E2 und höher
- Cisco IOS® Version 15.6(3)M4 und höher
- Cisco IOS® Version 15.7(3)M2 und höher
- Cisco IOS® XE Denali 16.3.6 und höher
- Cisco IOS® XE Everest 16.5.3 und höher

- Cisco IOS® Everest 16.6.3 und höher
- Alle Cisco IOS® Versionen ab 16.7.1

Weitere Informationen finden Sie hier:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html#id_70663

Lösung

In den meisten Leitfäden und Dokumentationen für FND wird noch nicht erwähnt, dass das SAN-Feld ausgefüllt werden muss.

Führen Sie die folgenden Schritte aus, um das richtige Zertifikat für die Verwendung mit PNP zu erstellen und zu exportieren und es dem Schlüsselspeicher hinzuzufügen.

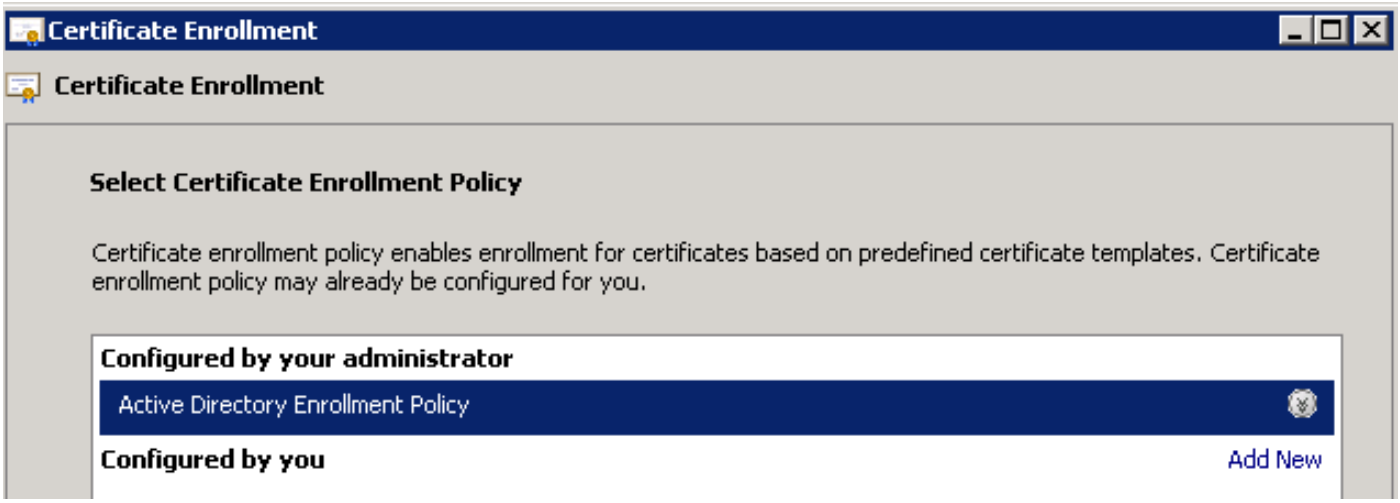
Erstellen eines neuen Zertifikats mit der FND/NMS-Vorlage auf dem Windows-Zertifizierungsstellenserver

Navigieren Sie zu **Start > Ausführen > mmc > Datei > Snap-In hinzufügen/entfernen... > Zertifikate > Hinzufügen > Computerkonto > Lokaler Computer > OK,** und öffnen Sie das MMC-Snap-In Zertifikate.

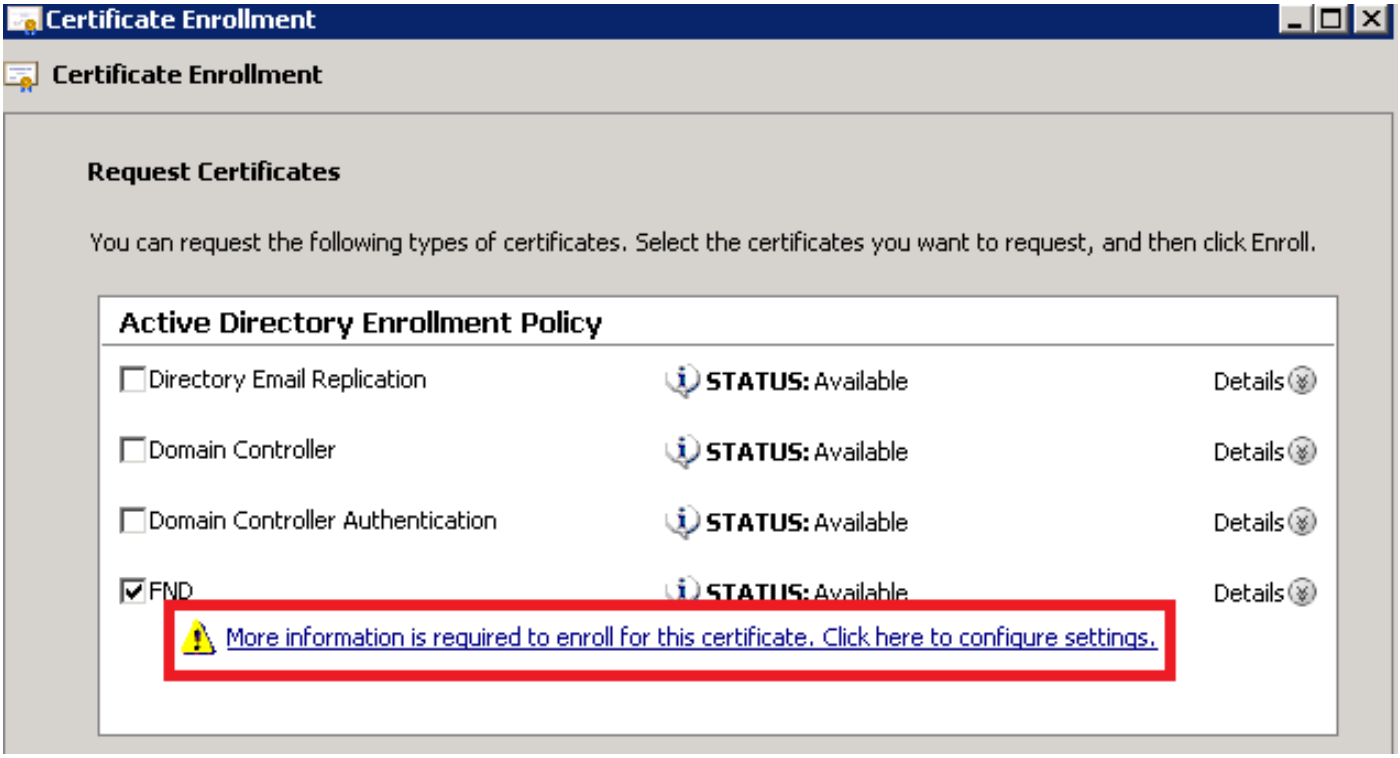
Erweitern Sie Zertifikate (Lokaler Computer) > Persönlich > Zertifikate

Klicken Sie mit der rechten Maustaste auf Zertifikate, und wählen Sie **Alle Aufgaben > Neues Zertifikat anfordern...** aus, wie im Bild gezeigt.

Klicken Sie auf **Weiter**, und wählen Sie **Active Directory-Registrierungsrichtlinie** aus, wie im Bild dargestellt.



Klicken Sie auf **Weiter**, wählen Sie die Vorlage aus, die für den NMS/FND-Server erstellt wurde (wiederholen Sie den Vorgang später für TelePresence Server (TPS)), und klicken Sie auf den Link **Weitere Informationen,** wie im Bild dargestellt.



Geben Sie in den Zertifikateigenschaften folgende Informationen an:

Betreffname:

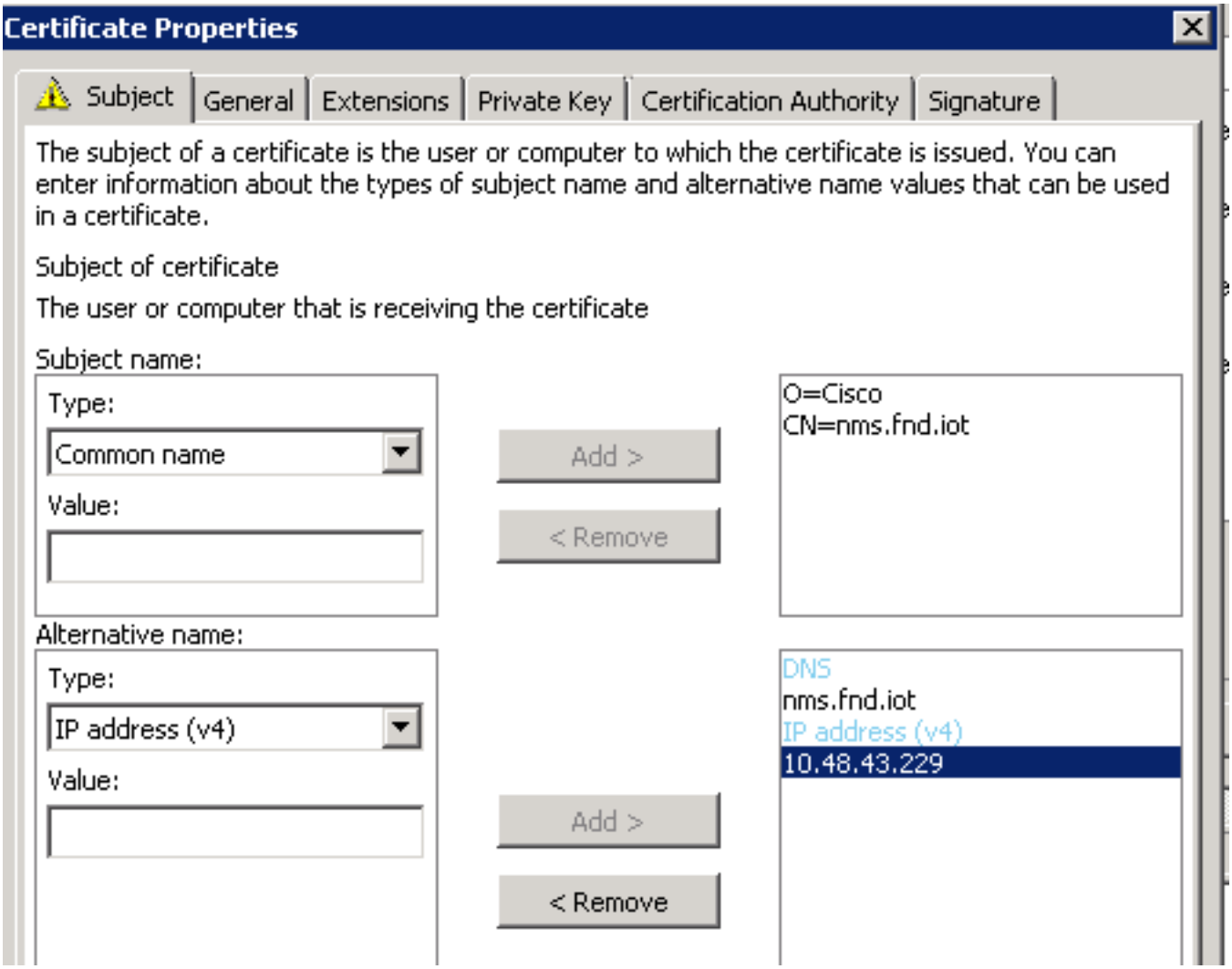
- Organisation: Ihres Unternehmens
- Gebräuchliche Bezeichnung: den vollqualifizierten Domänennamen (FQDN) des FND-Servers (oder TPS, falls zutreffend)

Alternativer Name (SAN-Feld):

- Wenn Sie Domain Name System (DNS) verwenden, um den PNP-Teil des FND-Servers zu kontaktieren, fügen Sie einen DNS-Eintrag für den FQDN hinzu.
- Wenn Sie IP verwenden, um den PNP-Teil des FND-Servers zu kontaktieren, fügen Sie einen IPv4-Eintrag für die IP hinzu

Es wird empfohlen, mehrere SAN-Werte in das Zertifikat aufzunehmen, falls die Erkennungsmethoden variieren. Sie können beispielsweise sowohl den FQDN als auch die IP-Adresse (oder die NAT-IP-Adresse) des Controllers in das SAN-Feld einschließen. Wenn Sie beide angeben, legen Sie den FQDN als ersten SAN-Wert fest, gefolgt von der IP-Adresse.

Beispielkonfiguration:



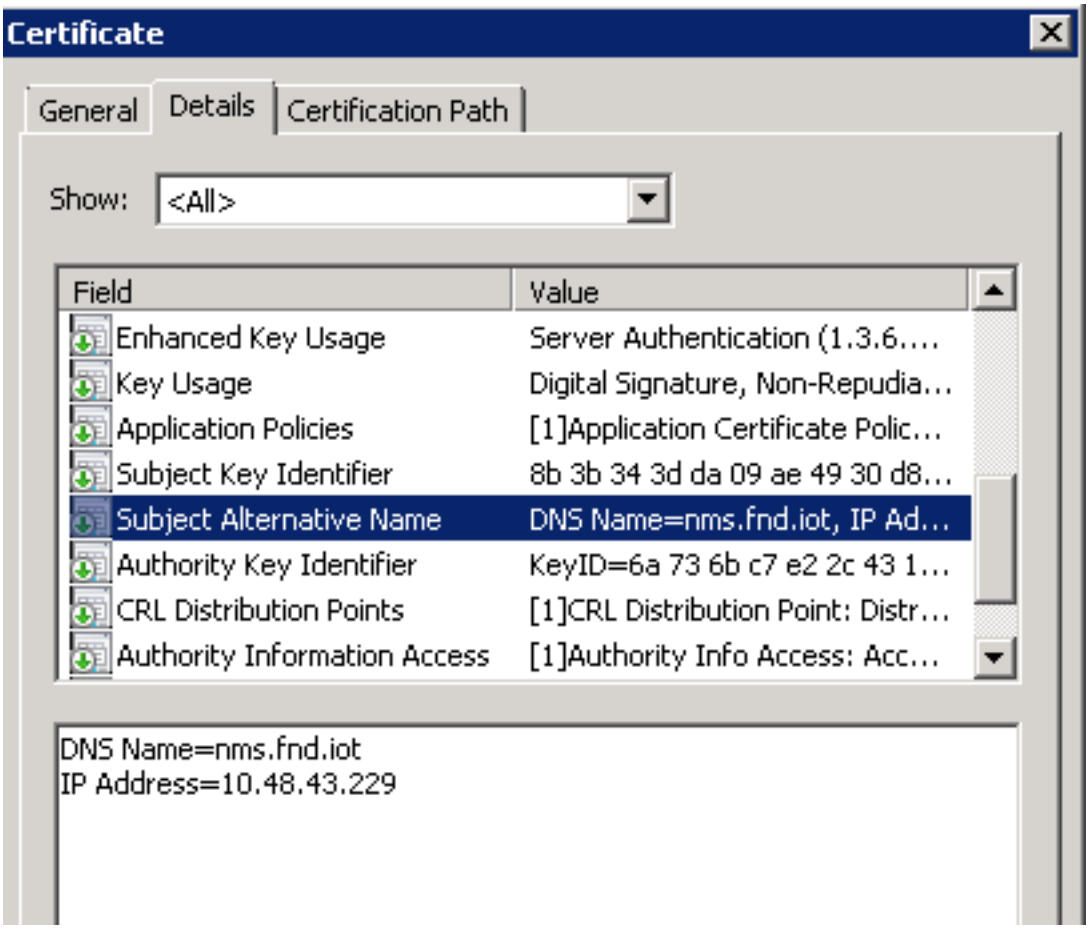
Klicken Sie abschließend im Fenster Zertifikateigenschaften auf **OK** und anschließend auf **Registrieren,** um das Zertifikat zu generieren und nach Abschluss der Generierung **abzuschließen**.

Überprüfen Sie das SAN-Feld im generierten Zertifikat.

Um zu überprüfen, ob das generierte Zertifikat die richtigen Informationen enthält, können Sie es wie folgt überprüfen:

Öffnen Sie das Zertifikat-Snap-In in der Microsoft Management Console (MMC), und erweitern Sie **Zertifikate (Lokaler Computer) > Personal > Zertifikate**.

Doppelklicken Sie auf das generierte Zertifikat, und öffnen Sie die Registerkarte **Details**. Blättern Sie nach unten, um das SAN-Feld zu finden, wie im Bild dargestellt.

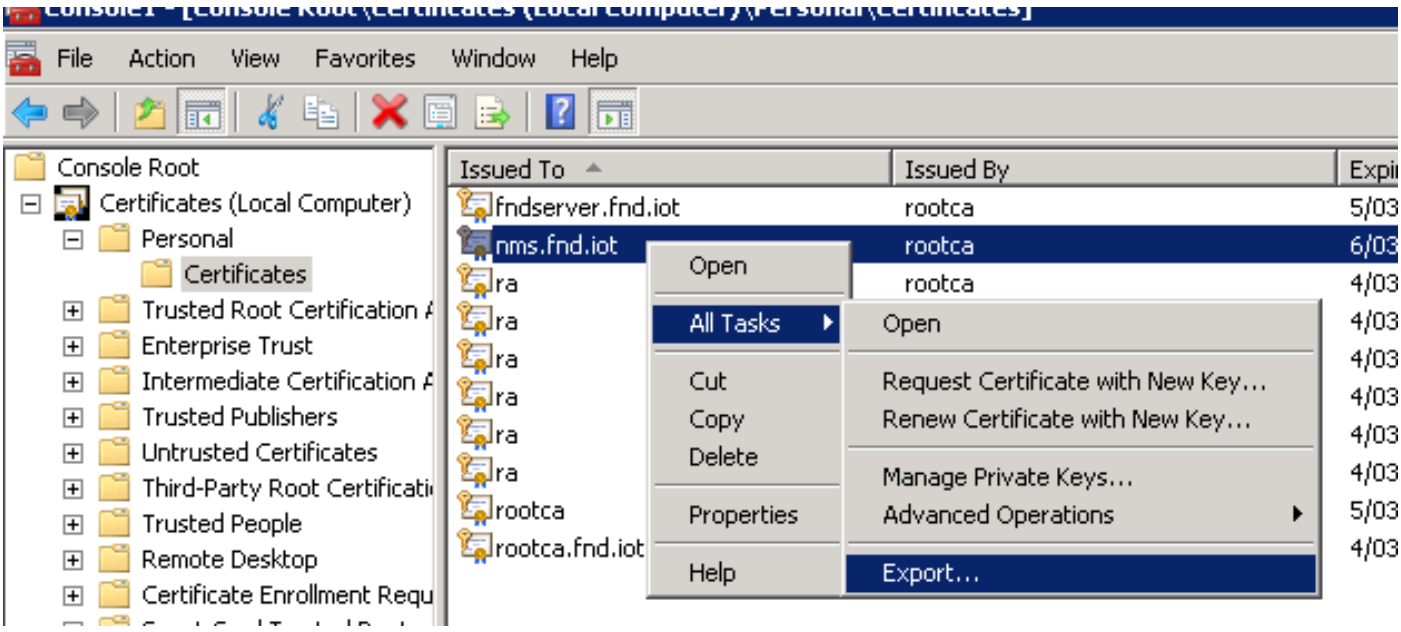


Zertifikat in FND-Schlüsselspeicher exportieren

Bevor Sie das im FND-Schlüsselspeicher vorhandene Zertifikat importieren oder ersetzen können, müssen Sie es in eine **.pfd-**Datei exportieren.

Erweitern Sie im Snap-In Zertifikate in MMC die Option **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate**

Klicken Sie mit der rechten Maustaste auf das erstellte Zertifikat, und wählen Sie **Alle Aufgaben > Exportieren...** aus, wie im Bild gezeigt.



Klicken Sie auf **Weiter**, um den privaten Schlüssel wie im Bild dargestellt zu exportieren.

Wählen Sie diese Option aus, um alle Zertifikate in den Zertifizierungspfad aufzunehmen, wie im Bild dargestellt.

Klicken Sie auf **Weiter**, wählen Sie ein Kennwort für den Export aus, und speichern Sie die **.pfx-Datei** an einem bekannten Ort.

Erstellen eines FND-Schlüsselspeichers zur Verwendung mit PNP

Nachdem Sie das Zertifikat exportiert haben, können Sie den für FND erforderlichen Schlüsselspeicher erstellen.

Übertragen Sie die generierte **.pfx** aus dem vorherigen Schritt sicher auf den FND-Server (Network Management Systems (NMS) Maschine oder OVA Host), z.B. unter Verwendung von SCP.

Listen Sie den Inhalt der **.pfx** auf, um den automatisch generierten Alias im Export zu erfahren:

```
[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
```

Erstellen Sie mit dem folgenden Befehl einen neuen Schlüsselspeicher:

```
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".
```

Stellen Sie im Befehl sicher, dass Sie **nms.pfx** durch die richtige Datei ersetzen (aus der Windows-CA exportiert) und dass der srcalias-Wert mit der Ausgabe des vorherigen Befehls (**keytool -list)** übereinstimmt.

Konvertieren Sie die Datei nach der Generierung in das neue Format wie vorgeschlagen:

```
[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".
```

Fügen Sie das zuvor exportierte Zertifizierungsstellenzertifikat dem Schlüsselspeicher hinzu:

```
[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
```

Und schließlich, fügen Sie das SUDI-Zertifikat, das verwendet wird, um die Identität durch serielle der FAR zu überprüfen, wenn Sie PNP verwenden, an den Keystore.

Bei einer RPM-Installation ist das SUDI-Zertifikat im Paket enthalten und kann unter folgender Adresse abgerufen werden: **/opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem**

Für eine OVA-Installation kopieren Sie zuerst das SUDI-Zertifikat an den Host:

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

Fügen Sie sie dann dem Schlüsselspeicher als vertrauenswürdig mit dem Alias SUDI hinzu:

```
[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
```

An diesem Punkt kann der Schlüsselspeicher mit FND verwendet werden.

Aktivieren des neuen/geänderten Schlüsselspeichers für die Verwendung mit FND

Bevor Sie den Schlüsselspeicher verwenden, ersetzen Sie die vorherige Version, und aktualisieren Sie optional das Kennwort in der Datei **cgms.properties**.

Erstellen Sie zunächst eine Sicherung des bereits vorhandenen Schlüsselspeichers:

Für eine RPM-Installation:

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

Für eine OVA-Installation:

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

Ersetzen Sie das vorhandene durch das neue:

Für eine RPM-Installation:

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

Für eine OVA-Installation:

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

Aktualisieren Sie optional das Kennwort für den Schlüsselspeicher in der Datei "cgms.properties":

Generieren Sie zunächst eine neue verschlüsselte Kennwortzeichenfolge.

Für eine RPM-Installation:

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

Für eine OVA-Installation:

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

Stellen Sie sicher, dass Sie den Schlüsselspeicher durch das richtige Kennwort für den Schlüsselspeicher ersetzen.

Ändern Sie cgms.properties in **/opt/cgms/server/cgms/conf/cgms.properties** für die RPM-basierte Installation oder **/opt/fnd/data/cgms.properties** für die OVA-basierte Installation, um das neue verschlüsselte Kennwort einzuschließen.

Starten Sie FND neu, um den neuen Schlüsselspeicher und das neue Kennwort zu verwenden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.