Problèmes d'utilisation de PNP avec FND sur les versions récentes de Cisco IOS®

Contenu

Introduction

Ce document décrit comment générer et exporter le certificat correct à partir de l'infrastructure de clé privée Windows (PKI) pour une utilisation combinée avec Plug and Play (PNP) sur Field Network Director (FND).

Problème

Lorsque vous essayez d'utiliser PNP pour effectuer un déploiement automatique (ZTD) sur les versions récentes de Cisco IOS® et Cisco IOS®-XE, le processus échoue avec l'une des erreurs PNP suivantes :

```
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
```

Depuis un certain temps, le code PNP dans Cisco IOS®/Cisco IOS®-XE nécessite que le champ Subject Alternative Name (SAN) soit renseigné dans le certificat offert par le serveur/contrôleur PNP (FND dans ce cas).

L'agent Cisco IOS® PNP vérifie uniquement le champ SAN du certificat pour l'identité du serveur. Il ne vérifie plus le champ du nom commun (CN).

Ceci est valable pour ces versions :

- Cisco IOS® version 15.2(6)E2 et ultérieure
- Cisco IOS® version 15.6(3)M4 et ultérieure
- Cisco IOS® version 15.7(3)M2 et ultérieure
- Cisco IOS® XE Denali 16.3.6 et versions ultérieures
- Cisco IOS® XE Everest 16.5.3 et versions ultérieures
- Cisco IOS® Everest 16.6.3 et versions ultérieures

- Toutes les versions de Cisco IOS® 16.7.1 et ultérieures

Pour plus d'informations, consultez le site : https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html#id_70663

Solution

La plupart des guides et de la documentation de FND ne mentionnent pas encore que le champ SAN doit être renseigné.

Afin de créer et d'exporter le certificat correct pour une utilisation avec PNP et de l'ajouter au magasin de clés, suivez ces étapes.

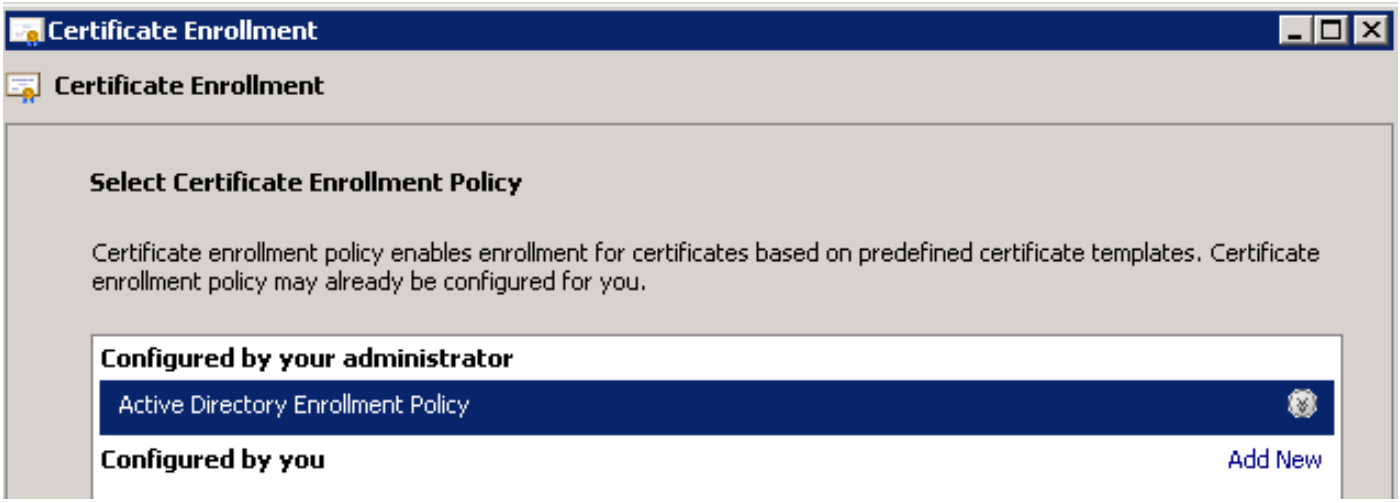
Générer un nouveau certificat avec l'utilisation du modèle FND/NMS sur le serveur AC Windows

Accédez à **Démarrer > Exécuter > mmc > Fichier > Ajouter/Supprimer un composant logiciel enfichable... > Certificats > Ajouter > Compte d'ordinateur > Ordinateur local > OK** et ouvrez le composant logiciel enfichable MMC de certificats.

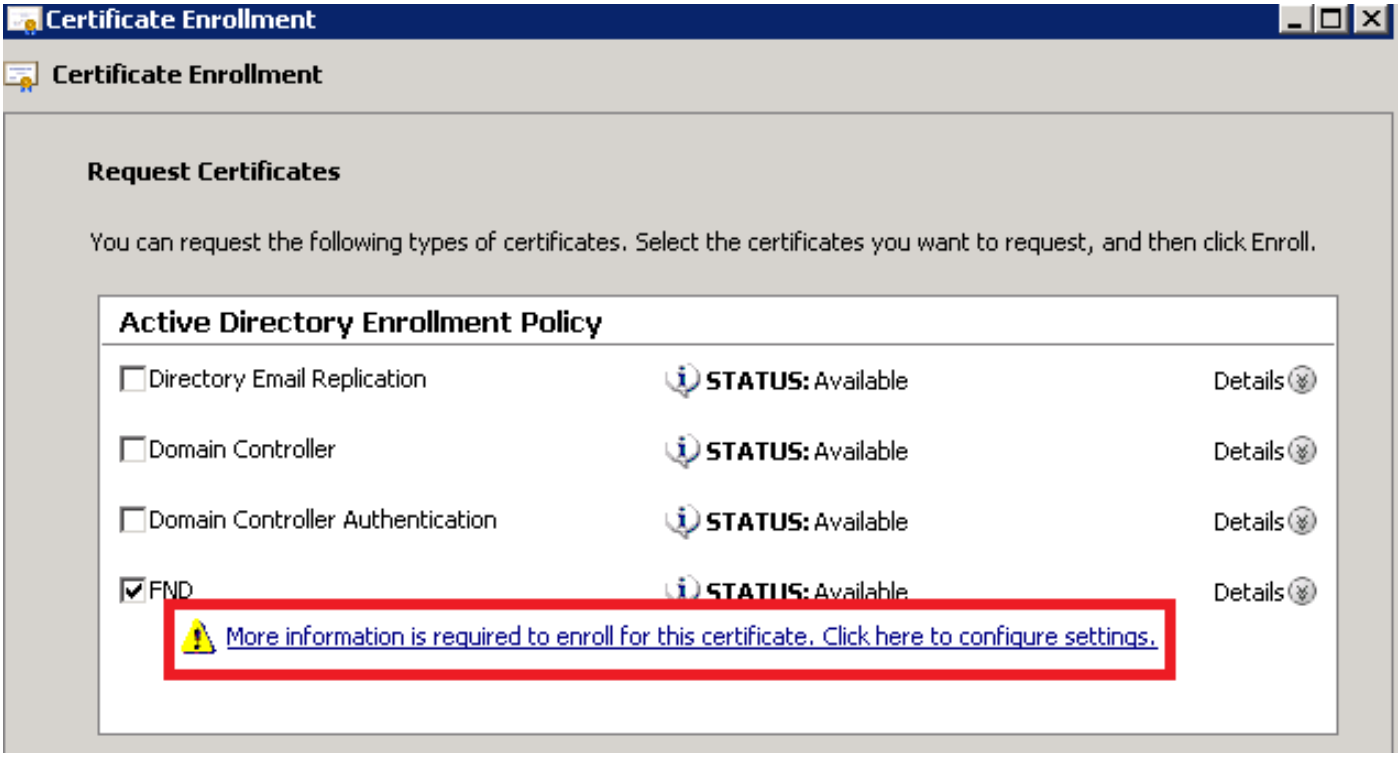
Développez Certificats (Ordinateur local) > Personnel > Certificats

Cliquez avec le bouton droit sur Certificats et sélectionnez **Toutes les tâches > Demander un nouveau certificat...** comme illustré dans l'image.

Cliquez sur **Next** et sélectionnez **Active Directory Enrollment Policy** comme indiqué dans l'image.



Cliquez sur **Next** et sélectionnez le modèle créé pour NMS/FND-server (répétez plus tard pour TelePresence Server (TPS)) et cliquez sur le lien **More Information** comme indiqué dans l'image.



Dans les propriétés du certificat, fournissez les informations suivantes :

Nom du sujet :

- Organisation : nom de votre entreprise
- Nom commun : le nom de domaine complet (FQDN) du serveur FND (ou TPS le cas échéant)

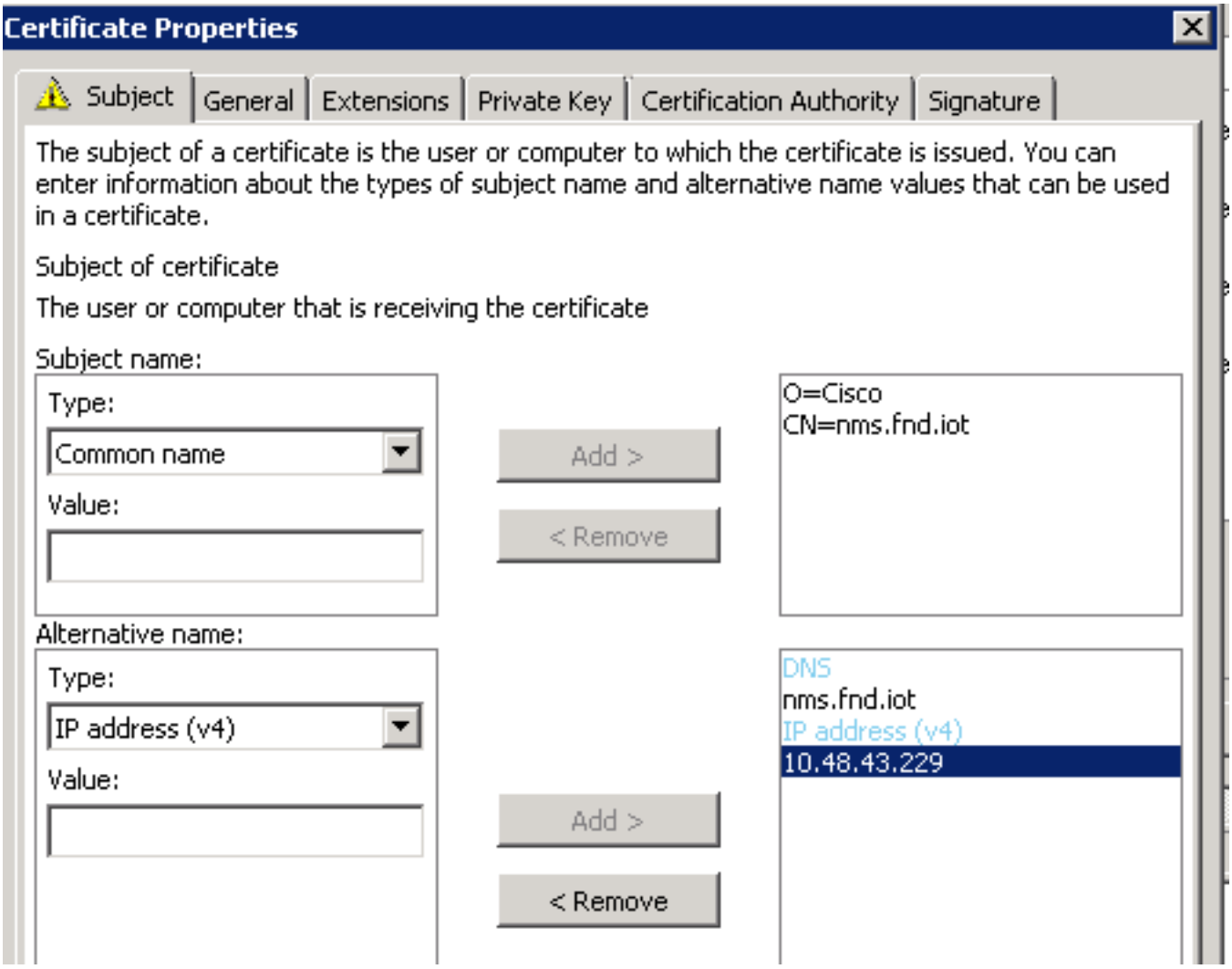
Autre nom (champ SAN) :

- Si vous utilisez le système de noms de domaine (DNS) afin de contacter la partie PNP du serveur FND, ajoutez une entrée DNS pour le FQDN
- Si vous utilisez IP afin de contacter la partie PNP du serveur FND, ajoutez une entrée IPv4 pour l'IP

Il est recommandé d'inclure plusieurs valeurs SAN dans le certificat, au cas où les méthodes de détection varient. Par exemple, vous pouvez inclure le nom de domaine complet du contrôleur et

l'adresse IP (ou l'adresse IP NAT) dans le champ SAN. Si vous incluez les deux, définissez le FQDN comme première valeur SAN, suivi de l'adresse IP.

Exemple de configuration :



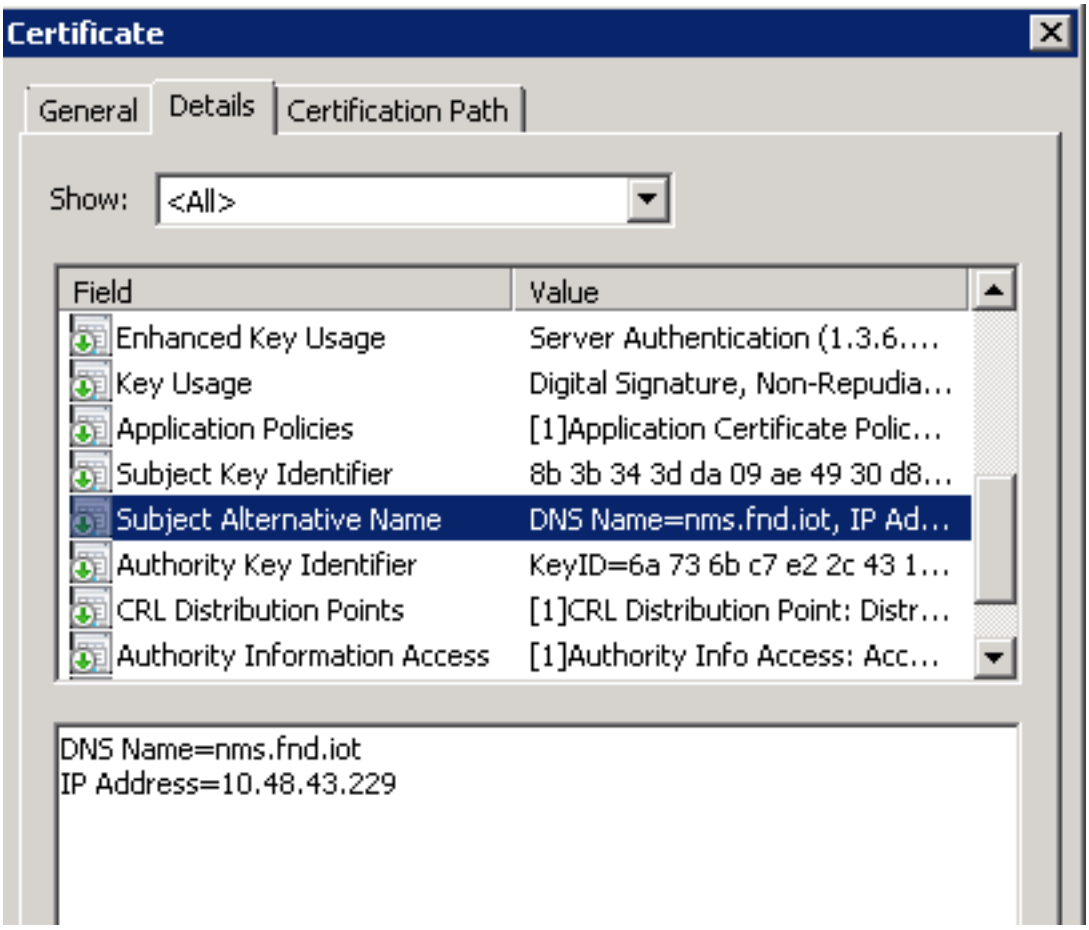
Une fois terminé, cliquez sur **OK** dans la fenêtre Propriétés du certificat, puis **Enroll** afin de générer le certificat et **Finish** lorsque la génération est terminée.

Vérifiez le champ SAN dans le certificat généré

Juste pour vérifier si le certificat généré contient les informations correctes, vous pouvez le vérifier comme suit :

Ouvrez le composant logiciel enfichable Certificats dans Microsoft Management Console (MMC) et développez **Certificats (Ordinateur local) > Personnel > Certificats**.

Double-cliquez sur le certificat généré et ouvrez l'onglet **Détails**. Faites défiler la page vers le bas pour rechercher le champ SAN comme indiqué dans l'image.

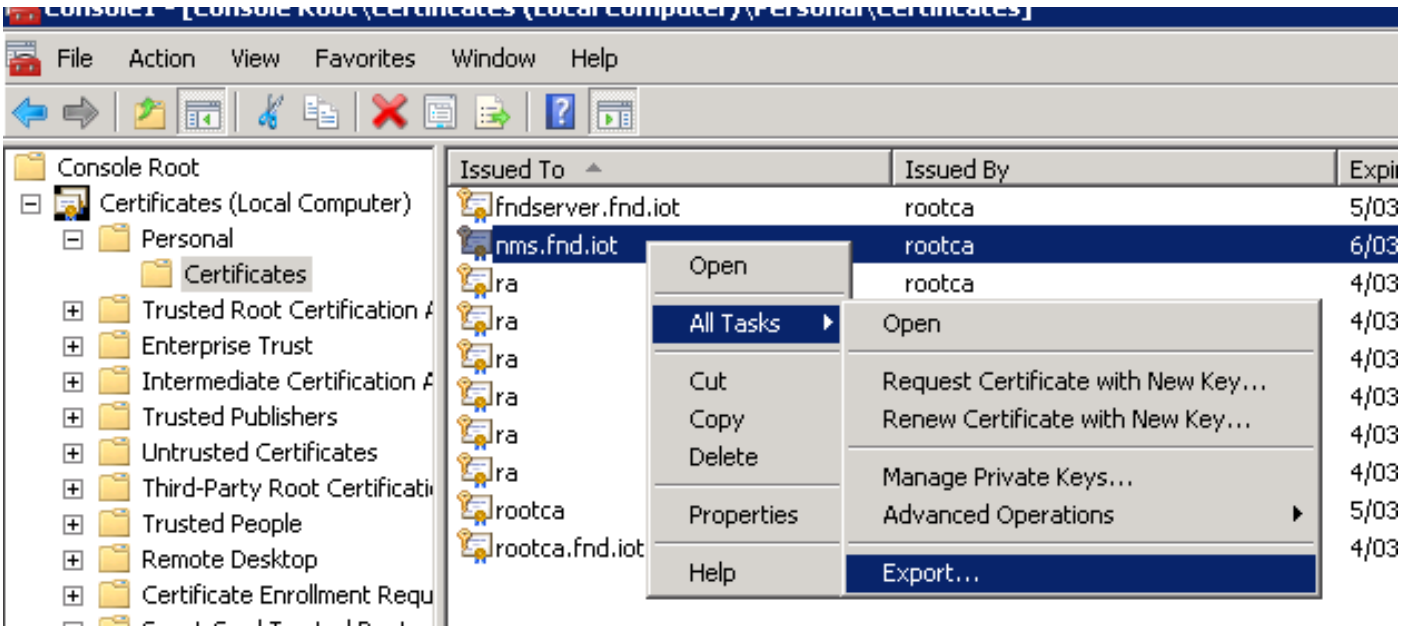


Exporter le certificat à importer vers le magasin de clés FND

Avant de pouvoir importer ou remplacer le certificat qui existe dans le magasin de clés FND, vous devez l'exporter dans un fichier **.pfd**.

Dans le composant logiciel enfichable Certificats de MMC, développez **Certificates (Local Computer) > Personal > Certificates**

Cliquez avec le bouton droit sur le certificat généré et sélectionnez **Toutes les tâches > Exporter...** comme illustré dans l'image.



Cliquez sur **Next**, sélectionnez afin d'exporter la clé privée comme montré dans l'image.

Sélectionnez afin d'inclure tous les certificats dans le chemin de certification comme indiqué dans l'image.

Cliquez sur **Next**, sélectionnez un mot de passe pour l'exportation et enregistrez le fichier **.pfx** dans un emplacement connu.

Créer le magasin de clés FND à utiliser avec PNP

Maintenant que le certificat a été exporté, vous pouvez créer le magasin de clés nécessaire pour FND.

Transférez le **.pfx** généré de l'étape précédente en toute sécurité vers le serveur FND (machine Network Management Systems (NMS) ou hôte OVA), par exemple avec l'utilisation de SCP.

Répertoriez le contenu du fichier **.pfx** pour connaître l'alias généré automatiquement lors de l'exportation :

```
[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
```

Créez une nouvelle banque de clés à l'aide de cette commande :

```
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".
```

Dans la commande, assurez-vous que vous remplacez **nms.pfx** avec le fichier correct (exporté depuis Windows CA) et que la valeur srcalias correspond au résultat de la commande précédente (**keytool -list**).

Après l'avoir généré, convertissez-le au nouveau format comme suggéré :

```
[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".
```

Ajoutez le certificat CA, exporté précédemment, au 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
```

Et enfin, ajoutez le certificat SUDI, qui est utilisé afin de vérifier l'identité par série du FAR lorsque vous utilisez PNP, au keystore.

Pour une installation RPM, le certificat SUDI est fourni avec les paquets et peut être trouvé dans : **/opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem**

Pour une installation OVA, copiez d'abord le certificat SUDI sur l'hôte :

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

Ensuite, ajoutez-le au keystore comme approuvé avec l'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
```

Àce stade, le keystore est prêt à être utilisé avec FND.

Activer le magasin de clés nouveau/modifié pour une utilisation avec FND

Avant d'utiliser le keystore, remplacez la version précédente et mettez éventuellement à jour le mot de passe dans le fichier **cgms.properties**.

Commencez par effectuer une sauvegarde du keystore qui existe déjà :

Pour une installation RPM :

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

Pour une installation OVA :

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

Remplacez celui qui existe par le nouveau :

Pour une installation RPM :

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

Pour une installation OVA :

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

Le cas échéant, mettez à jour le mot de passe du keystore dans le fichier cgms.properties :

Commencez par générer une nouvelle chaîne de mot de passe chiffrée.

Pour une installation RPM :

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

Pour une installation OVA :

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

Veillez à remplacer keystore par le mot de passe correct pour votre keystore.

Modifiez cgms.properties dans **/opt/cgms/server/cgms/conf/cgms.properties** pour l'installation basée sur RPM ou **/opt/fnd/data/cgms.properties** pour l'installation basée sur OVA afin d'inclure le nouveau mot de passe chiffré.

Enfin, redémarrez FND pour commencer à utiliser le nouveau keystore et le nouveau mot de passe.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.