Problemi con l'uso di PNP con FND sulle nuove versioni di Cisco IOS®

Sommario

Introduzione

In questo documento viene descritto come generare ed esportare il certificato corretto dall'infrastruttura a chiave privata Windows (PKI) per l'utilizzo in combinazione con Plug and Play (PNP) in Field Network Director (FND).

Problema

Quando si tenta di utilizzare PNP per eseguire la distribuzione Zero Touch (ZTD) sulle nuove versioni di Cisco IOS® e Cisco IOS®-XE, il processo ha esito negativo e si verifica uno dei seguenti errori 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
```

Da qualche tempo, il codice PNP in Cisco IOS®/Cisco IOS®-XE richiede che il campo relativo al nome alternativo del soggetto (SAN) sia compilato nel certificato offerto dal server/controller PNP (in questo caso FND).

L'agente PNP Cisco IOS® controlla solo il campo SAN del certificato per l'identità del server. Non viene più controllato il campo Nome comune (CN).

Questa procedura è valida per le seguenti release:

- Cisco IOS® versione 15.2(6)E2 e successive
- Cisco IOS® versione 15.6(3)M4 e successive
- Cisco IOS® versione 15.7(3)M2 e successive
- Cisco IOS® XE Denali 16.3.6 e versioni successive
- Cisco IOS® XE Everest 16.5.3 e versioni successive
- Cisco IOS® Everest 16.6.3 e versioni successive

- Tutte le versioni Cisco IOS® da 16.7.1 e successive

Per ulteriori informazioni, visitare il sito Web all'indirizzo https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html#id_70663

Soluzione

La maggior parte delle guide e della documentazione di FND non menziona ancora la necessità di compilare il campo SAN.

Per creare ed esportare il certificato corretto da utilizzare con PNP e aggiungerlo all'archivio chiavi, eseguire la procedura seguente.

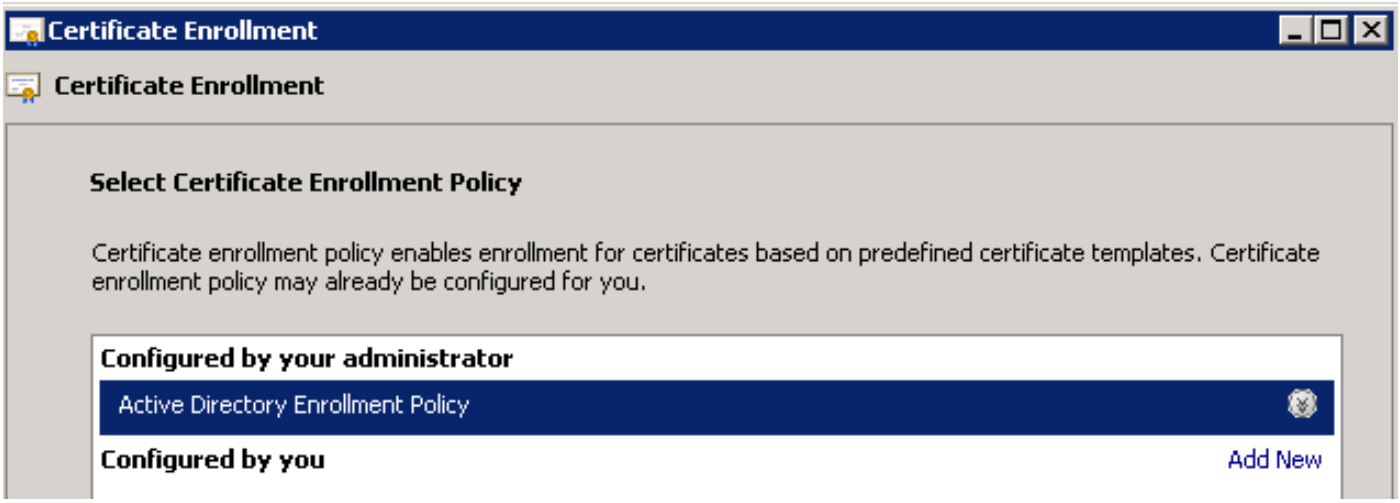
Genera un nuovo certificato con l'utilizzo del modello FND/NMS sul server CA di Windows

Selezionare **Start > Esegui > mmc > File > Aggiungi/Rimuovi snap-in... > Certificati > Aggiungi > Account computer > Computer locale > OK** e aprire lo snap-in MMC certificati.

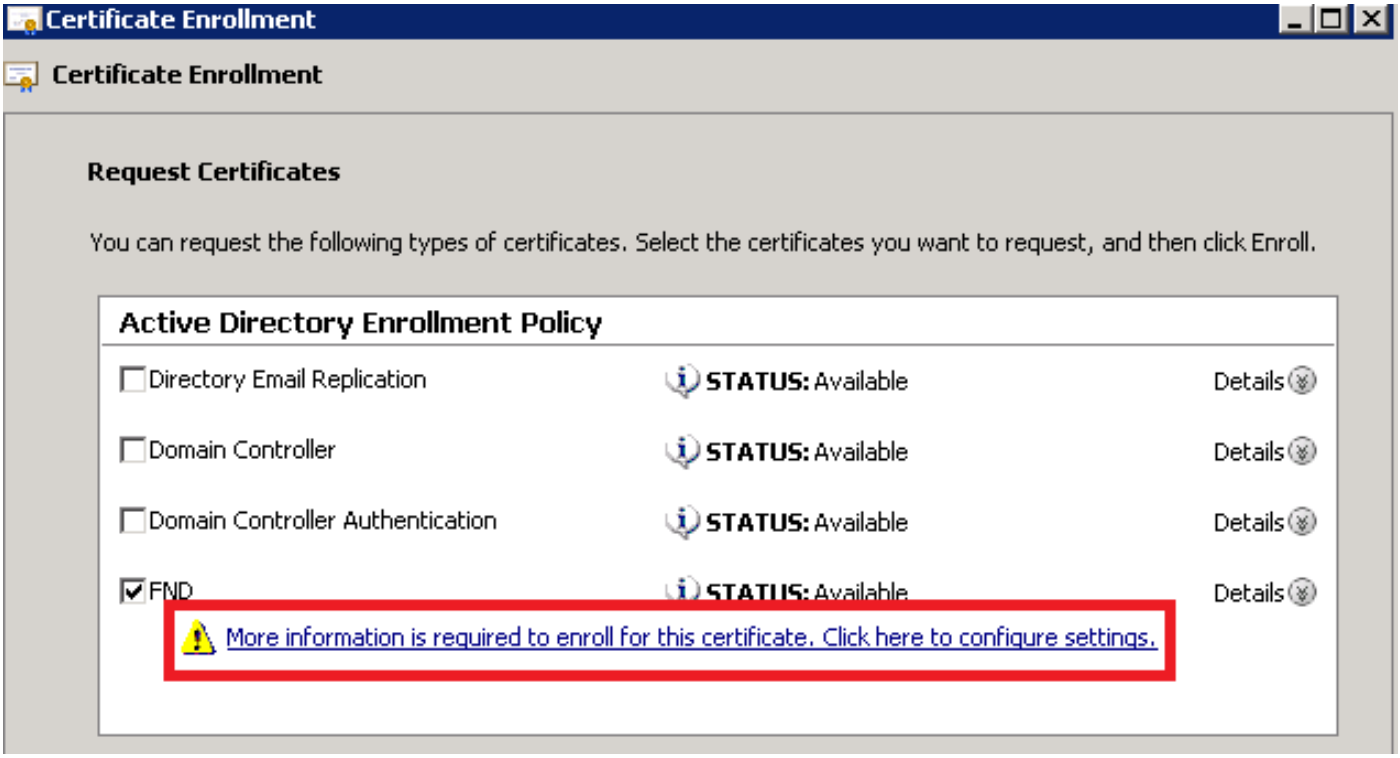
Espandi Certificati (Computer locale) > Personale > Certificati

Fare clic con il pulsante destro del mouse su Certificati e selezionare **All Tasks > Request New Certificate...** come mostrato nell'immagine.

Fare clic su **Avanti** e selezionare **Criteri di registrazione Active Directory** come illustrato nell'immagine.



Fare clic su **Avanti** e selezionare il modello creato per NMS/FND-server (ripetere in seguito per TelePresence Server (TPS)) e fare clic sul collegamento **Ulteriori informazioni** come mostrato nell'immagine.



Nelle proprietà del certificato, fornire le seguenti informazioni:

Nome soggetto:

- Organizzazione: nome dell'organizzazione
- Nome comune: il nome di dominio completo (FQDN) del server FND (o TPS se applicabile)

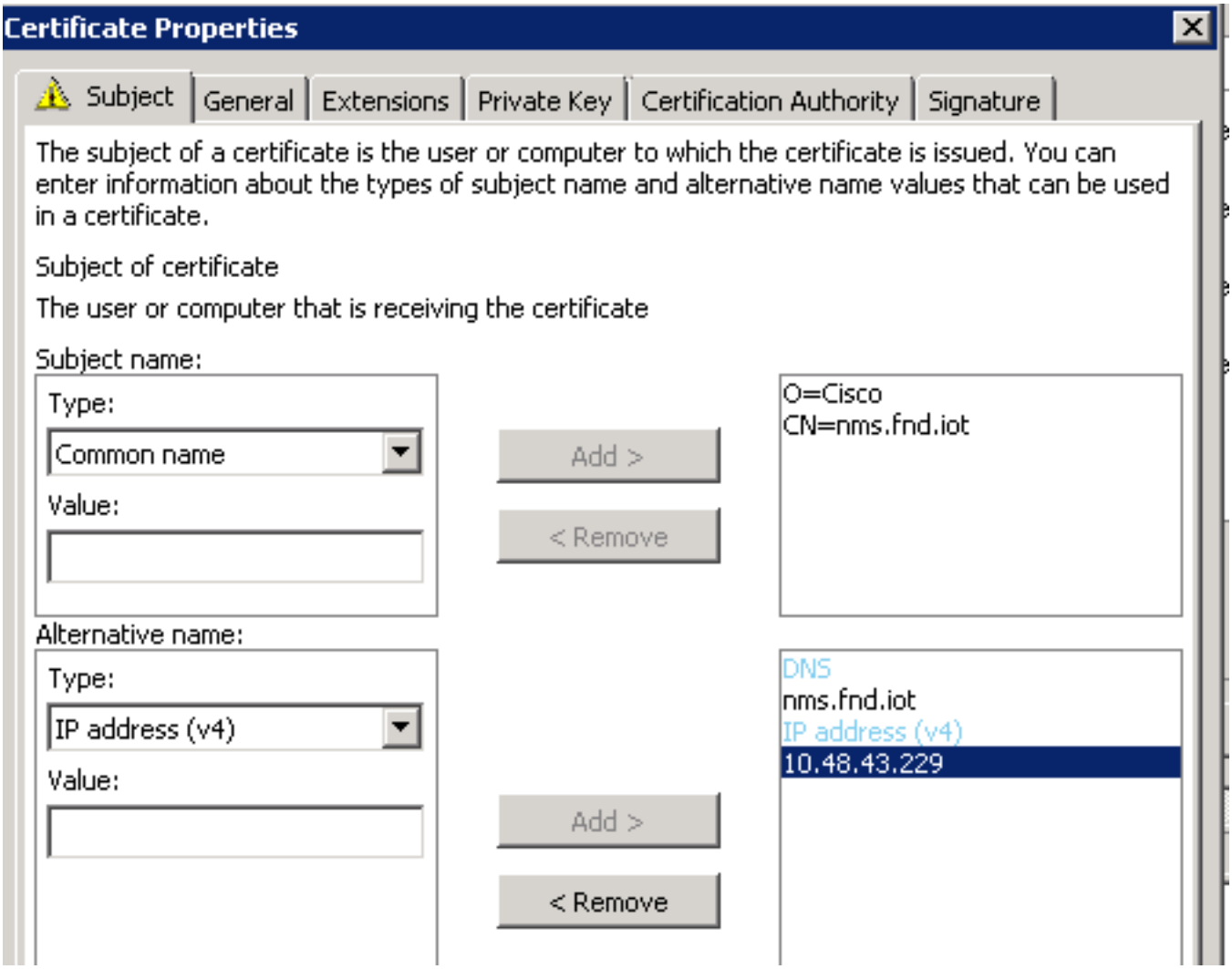
Nome alternativo (campo SAN):

- Se si utilizza il DNS (Domain Name System) per contattare la parte PNP del server FND, aggiungere una voce DNS per il nome FQDN
- Se si utilizza IP per contattare la parte PNP del server FND, aggiungere una voce IPv4 per l'indirizzo IP

È consigliabile includere più valori SAN nel certificato, nel caso in cui i metodi di individuazione

possano variare. Ad esempio, è possibile includere sia l'FQDN del controller che l'indirizzo IP (o indirizzo IP NAT) nel campo SAN. Se si includono entrambi, impostare l'FQDN come primo valore SAN, seguito dall'indirizzo IP.

Esempio di configurazione:



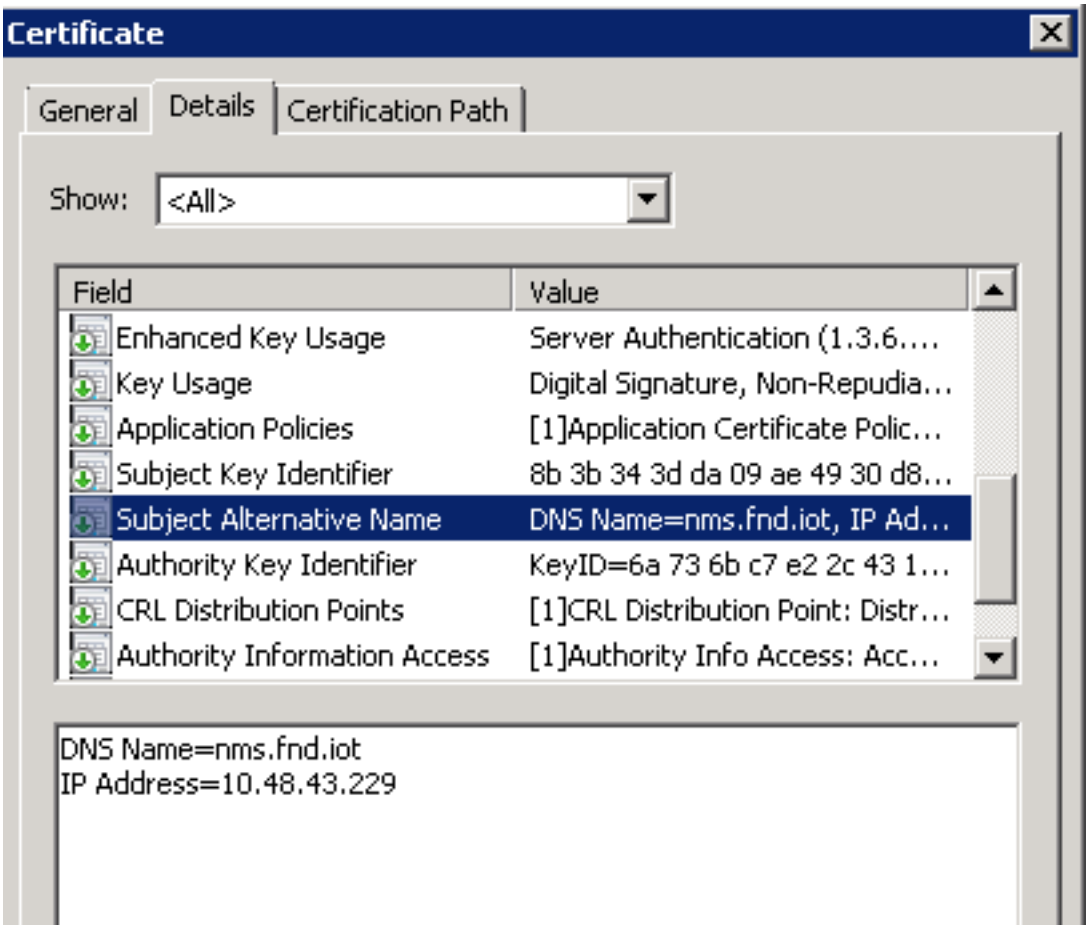
Al termine, fare clic su **OK** nella finestra Proprietà certificato, quindi su **Registra** per generare il certificato e su **Fine** al termine della generazione.

Controllare il campo SAN nel certificato generato

Per verificare se il certificato generato contiene le informazioni corrette, è possibile eseguire il controllo nel modo seguente:

Aprire lo snap-in certificati in Microsoft Management Console (MMC) ed espandere **Certificati (Computer locale) > Personale > Certificati**.

Fare doppio clic sul certificato generato e aprire la scheda **Dettagli**. Scorrere verso il basso per trovare il campo SAN come mostrato nell'immagine.

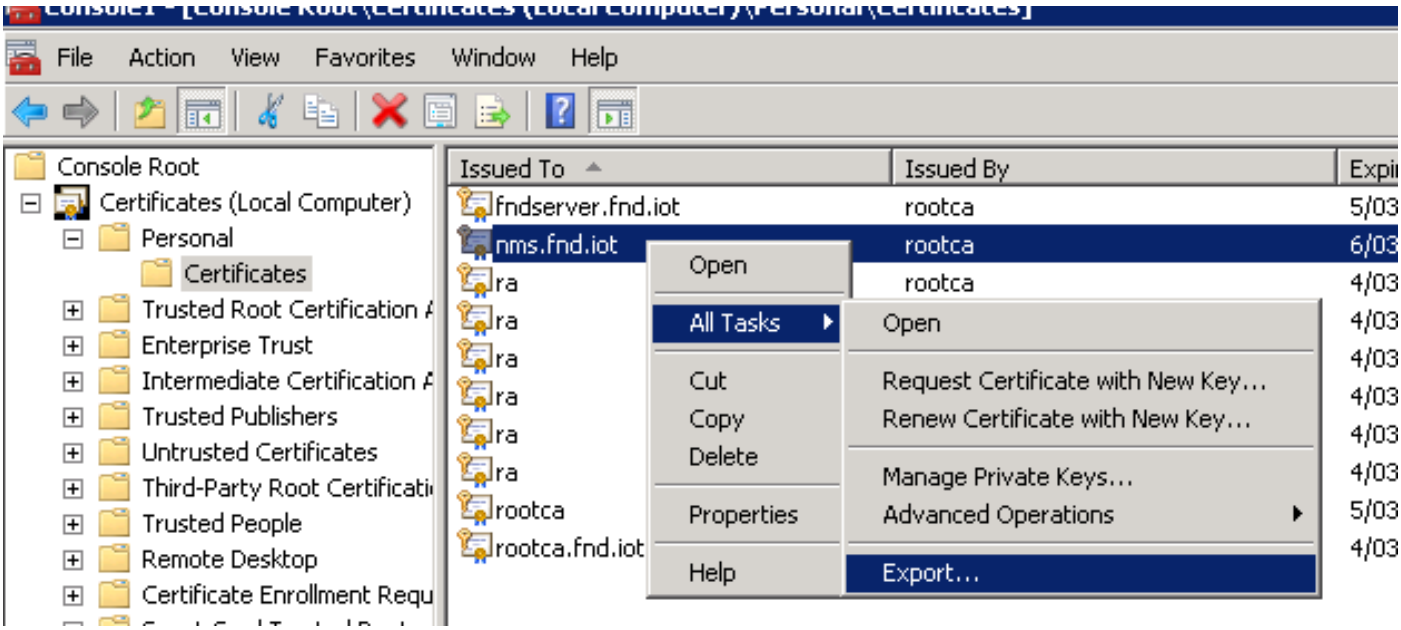


Esporta il certificato da importare nell'archivio chiavi FND

Prima di poter importare o sostituire il certificato esistente nel keystore FND, è necessario esportarlo in un file **.pfd**.

Nello snap-in certificati di MMC espandere **Certificati (computer locale) > Personale > Certificati**

Fare clic con il pulsante destro del mouse sul certificato generato e selezionare **All Tasks > Export...** come mostrato nell'immagine.



Fare clic su **Next** (Avanti), quindi selezionare per esportare la chiave privata come mostrato nell'immagine.

Selezionare questa opzione per includere tutti i certificati nel percorso di certificazione, come illustrato nell'immagine.

Fare clic su **Avanti**, selezionare una password per l'esportazione e salvare il file **.pfx** in una posizione nota.

Crea il keystore FND da utilizzare con PNP

Dopo aver esportato il certificato, è possibile creare il keystore necessario per FND.

Trasferire il file **.pfx** generato dalla fase precedente in modo sicuro al server FND (computer NMS (Network Management Systems) o all'host OAV), ad esempio utilizzando SCP.

Elencare il contenuto del file **.pfx** per conoscere l'alias generato automaticamente nell'esportazione:

```
[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
```

Creare un nuovo keystore con questo 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".
```

Nel comando, accertarsi di sostituire **nms.pfx** con il file corretto (esportato dalla CA di Windows) e che il valore srcalias corrisponda all'output del comando precedente (**keytool -list**).

Dopo averlo generato, convertirlo nel nuovo formato come suggerito:

```
[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".
```

Aggiungere il certificato CA esportato in precedenza al 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
```

Infine, aggiungere al keystore il certificato SUDI utilizzato per verificare l'identità tramite il numero di serie del dispositivo FAR quando si utilizza PNP.

Per un'installazione RPM, il certificato SUDI è fornito con i pacchetti ed è disponibile in: **/opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem**

Per l'installazione degli OVA, copiare prima il certificato SUDI sull'host:

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

Quindi aggiungerlo al keystore come trusted con 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
```

A questo punto, il keystore è pronto per essere utilizzato con FND.

Attiva il keystore nuovo/modificato da utilizzare con FND

Prima di utilizzare il keystore, sostituire la versione precedente e facoltativamente aggiornare la password nel file **cgms.properties**.

Eseguire innanzitutto un backup del keystore già esistente:

Per un'installazione RPM:

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

Per un impianto OAV:

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

Sostituire quello esistente con quello nuovo:

Per un'installazione RPM:

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

Per un impianto OAV:

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

Facoltativamente, aggiornare la password per il keystore nel file cgms.properties:

Generare innanzitutto una nuova stringa di password crittografata.

Per un'installazione RPM:

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

Per un impianto OAV:

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

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

Assicurarsi di sostituire keystore con la password corretta per il keystore.

Modificare cgms.properties in **/opt/cgms/server/cgms/conf/cgms.properties** per l'installazione basata su RPM o **/opt/fnd/data/cgms.properties** per l'installazione basata su OVA in modo da includere la nuova password crittografata.

Riavviare infine FND per iniziare a utilizzare il nuovo keystore e la nuova password.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).