新しいCisco IOS®リリースでのFNDでのPNPの使用に関する問題

内容

概要

このドキュメントでは、Field Network Director(FND)のプラグアンドプレイ(PNP)と組み合わせて使用するために、Windows Private Key Infrastructure(PKI)から正しい証明書を生成してエクスポートする方法について説明します。

問題

新しいCisco IOS®およびCisco IOS®-XEリリースでPNPを使用してZero Touch Deployment(ZTD)を実行しようとすると、次のいずれかのPNPエラーでプロセスが失敗します。

```
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
```

Cisco IOS®/Cisco IOS®-XEのPNPコードでは、PNPサーバ/コントローラ（この場合はFND）が提供する証明書にサブジェクト代替名(SAN)フィールドを入力する必要があります。

PNP Cisco IOS®エージェントは、サーバIDの証明書SANフィールドのみをチェックします。共通名(CN)フィールドはチェックされなくなりました。

これは次のリリースで有効です。

- Cisco IOS®リリース15.2(6)E2以降
- Cisco IOS®リリース15.6(3)M4以降
- Cisco IOS®リリース15.7(3)M2以降
- Cisco IOS® XE Denali 16.3.6以降
- Cisco IOS® XE Everest 16.5.3以降
- Cisco IOS® Everest 16.6.3以降
- 16.7.1以降のすべてのCisco IOS®リリース

詳細については、次のサイトを参照してください。
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html#id_70663

解決方法

FNDに関するガイドやドキュメントのほとんどは、SANフィールドにデータを入力する必要があることを言及していません。

PNPで使用する正しい証明書を作成してエクスポートし、キーストアに追加するには、次の手順を実行します。

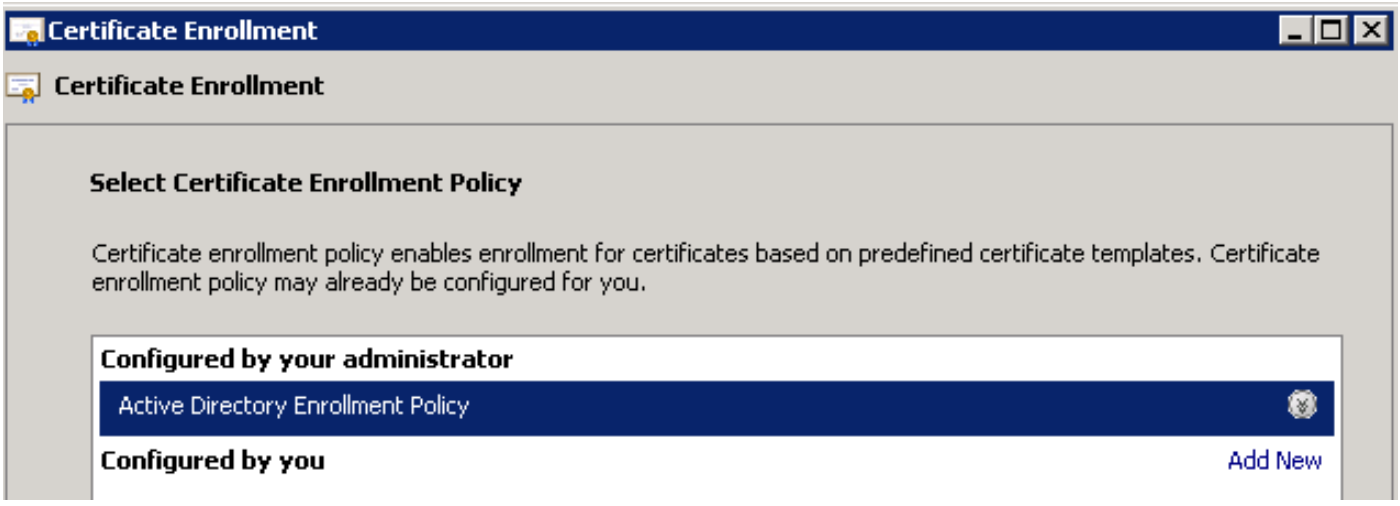
Windows CAサーバ上のFND/NMSテンプレートを使用した新しい証明書の生成

[Start] > [Run] > [mmc] > [File] > [Add/Remove Snap-in...] > [Certificates] > [Add] > [Computer Account] > [Local Computer] > [OK] に移動し、証明書MMCスナップインを開きます。

[Certificates (Local Computer)] > [Personal] > [Certificates]を展開します

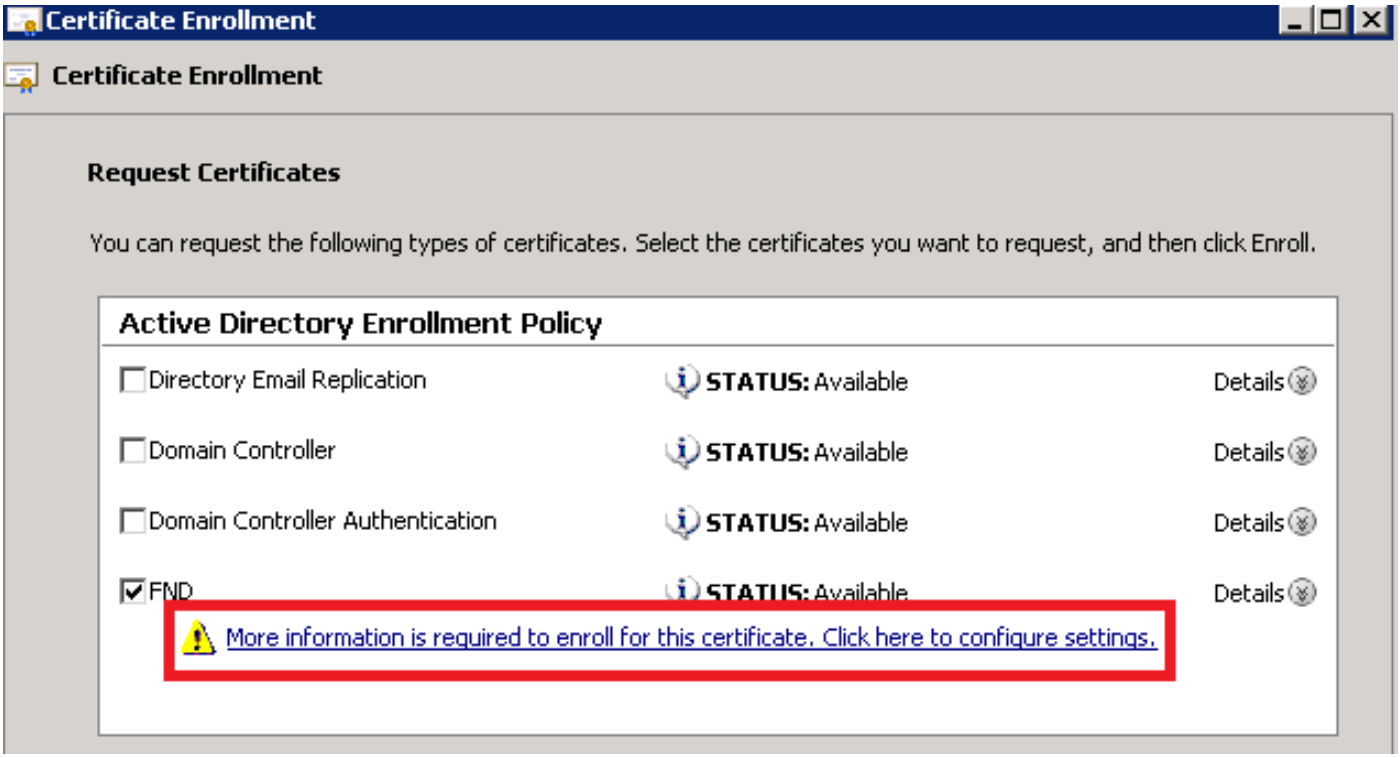
図に示すように、[Certificates]を右クリックし、[All Tasks] > [Request New Certificate...] を選択します。

図に示すように、[Next] をクリックし、[Active Directory Enrollment Policy] を選択します。



[Next] をクリックし、NMS/FND-server用に作成したテンプレートを選択し(後でTelePresence Server(TPS)に対して繰り返します)、図に示すように[More Information] リンクをクリックします

。



証明書のプロパティで、次の情報を入力します。

Subject Name:

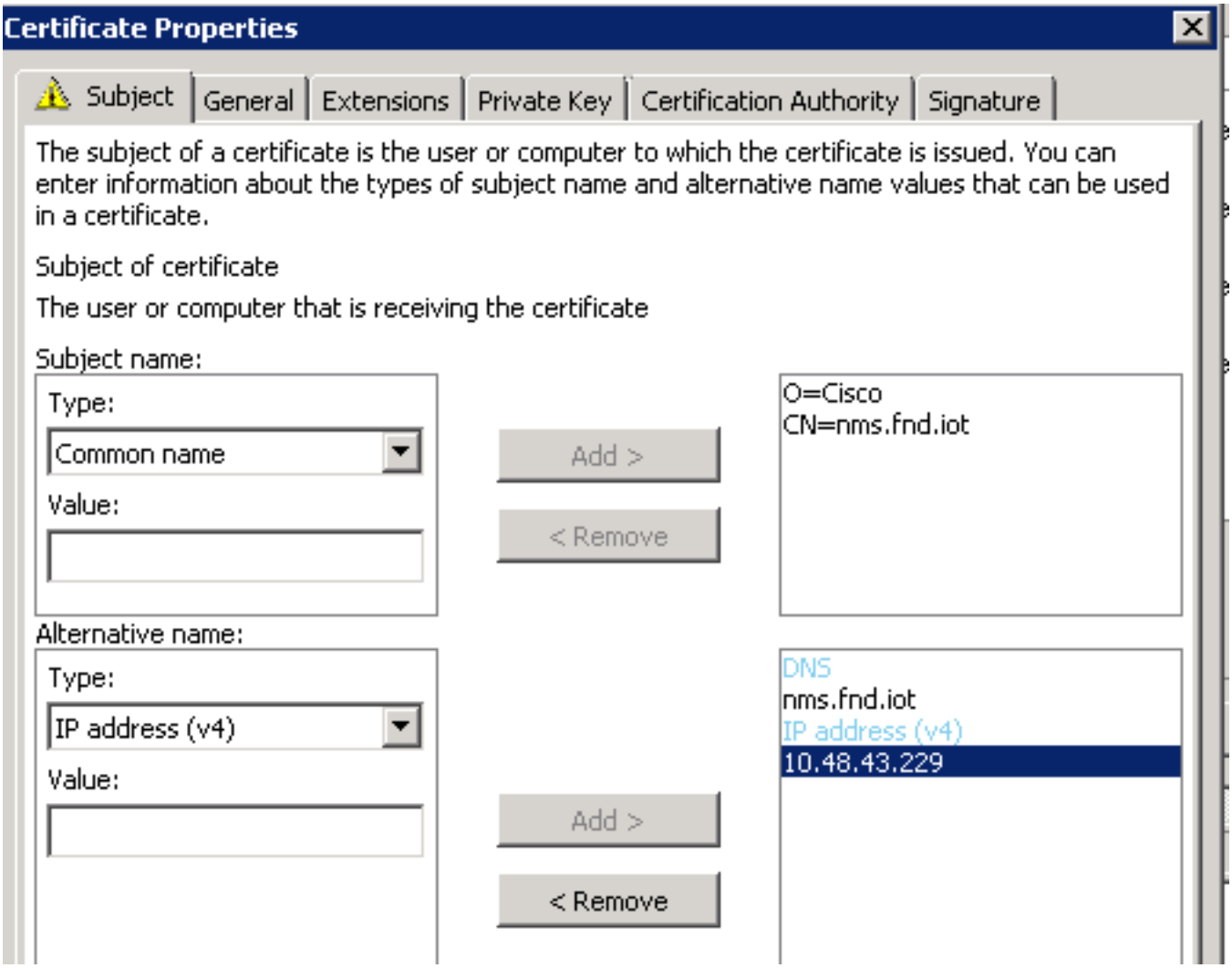
- 組織：組織名
- 一般名：FNDサーバの完全修飾ドメイン名(FQDN)（該当する場合はTPS）

別名（SANフィールド）：

- ドメインネームシステム(DNS)を使用してFNDサーバのPNP部分に接続する場合は、FQDNのDNSエントリを追加します
- IPを使用してFNDサーバのPNP部分に接続する場合は、IPのIPv4エントリを追加します

検出方法が異なる場合に備えて、証明書に複数のSAN値を含めることを推奨します。たとえば、SANフィールドにコントローラのFQDNとIPアドレス（またはNAT IPアドレス）の両方を含めることができます。両方を含める場合は、最初のSAN値としてFQDNを設定し、その後にIPアドレスを設定します。

設定例：



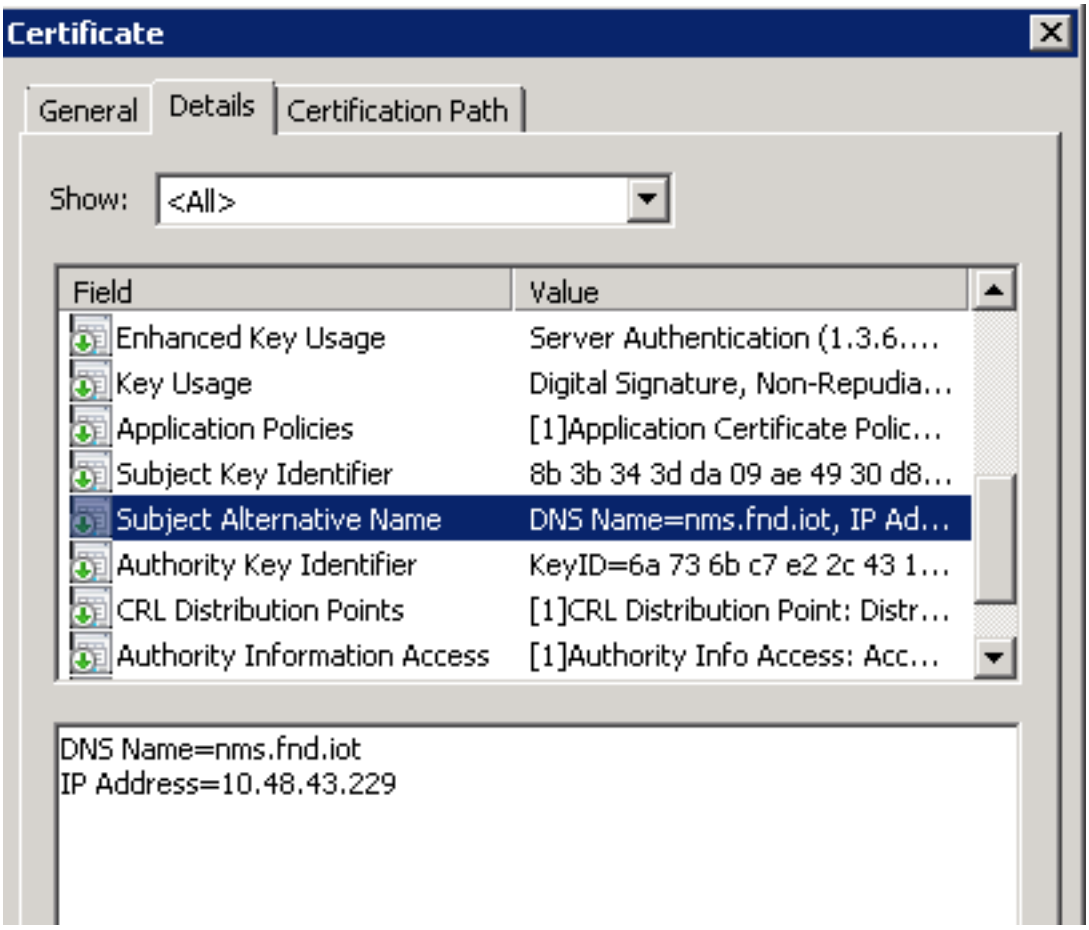
完了したら、[Certificate Properties]ウィンドウで[OK] をクリックし、[Enroll] をクリックして証明書を生成し、生成が完了したら[Finish] をクリックします。

生成された証明書のSANフィールドを確認します。

生成された証明書に正しい情報が含まれているかどうかを確認するには、次のように確認します。

Microsoft管理コンソール(MMC)で証明書スナップインを開き、[Certificates (Local Computer)] > [Personal] > [Certificates] を展開します。

生成された証明書をダブルクリックし、[Details] タブを開きます。下にスクロールして、図のように[SAN]フィールドを探します。

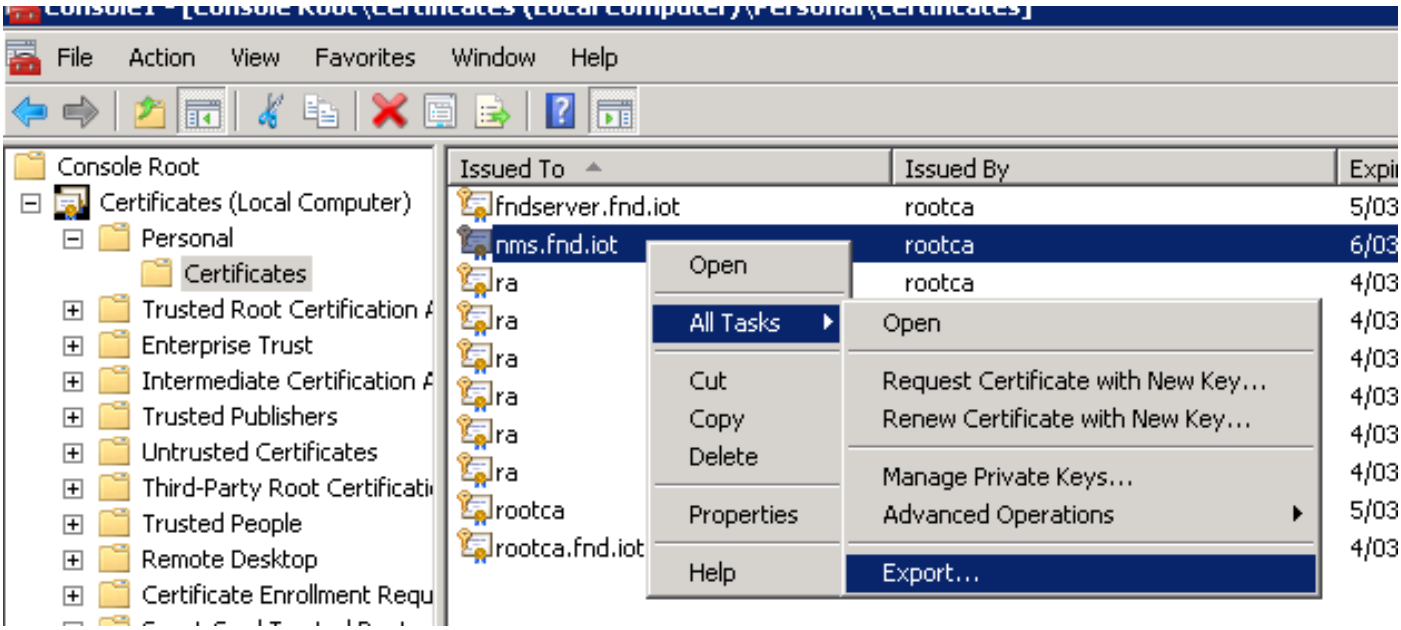


FNDキーストアにインポートする証明書のエクスポート

FNDキーストアに存在する証明書をインポートまたは置き換える前に、**.pfd**ファイルにエクスポートする必要があります。

MMCの証明書スナップインで、[証明書（ローカルコンピューター）] > [個人] > [証明書] の順に展開します

生成された証明書を右クリックし、図に示すように[All Tasks] > [Export...] を選択します。



Nextをクリックし、図に示すように秘密キーをエクスポートするために選択します。

図に示すように、すべての証明書を認証パスに含めるために選択します。

Nextをクリックし、エクスポート用のパスワードを選択して、.pfxを既知の場所に保存します。

PNPで使用するFNDキーストアの作成

証明書をエクスポートしたので、FNDに必要なキーストアを構築できます。

前の手順で生成した.pfxを、SCPなどを使用して、FNDサーバ(Network Management Systems(NMS)マシンまたはOVAホスト)に安全に転送します。

.pfxの内容をリストして、エクスポートで自動生成されたエイリアスを確認します。

```
[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
```

次のコマンドを使用して、新しいキーストアを作成します。

```
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".
```

コマンドで、**nms.pfx**を正しいファイル（Windows CAからエクスポートされたファイル）に置き換え、srcalias値が前のコマンド(**keytool -list**)の出力と一致することを確認します。

生成した後で、次に示すように新しい形式に変換します。

```
[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".
```

先ほどエクスポートしたCA証明書をキーストアに追加します。

```
[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
```

最後に、キーストアにSUDI証明書を追加します。この証明書は、PNPを使用するときにFARのシリアルによるIDを確認するために使用されます。

RPMインストールの場合、SUDI証明書はパッケージにバンドルされており、**/opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem**にあります。

OVAをインストールする場合は、最初にSUDI証明書をホストにコピーします。

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

次に、これをエイリアスSUDIで信頼できるキーストアに追加します。

```
[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
```

この時点で、キーストアはFNDで使用できる状態になります。

FNDで使用する新規/変更されたキーストアのアクティブ化

キーストアを使用する前に、以前のバージョンを置き換え、オプションでcgms.propertiesファイルのパスワードを更新します。

まず、既存のキーストアのバックアップを取ります。

RPMインストールの場合：

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

OVAインストールの場合：

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

既存のものを新しいものと置き換えます。

RPMインストールの場合：

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

OVAインストールの場合：

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

必要に応じて、cgms.propertiesファイルのキーストアのパスワードを更新します。

まず、新しい暗号化されたパスワード文字列を生成します。

RPMインストールの場合：

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

OVAインストールの場合：

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

キーストアをキーストアの正しいパスワードに置き換えてください。

新しい暗号化パスワードを含めるには、RPMベースのインストールの場合は

/opt/cgms/server/cgms/conf/cgms.propertiesでcgms.propertiesを変更し、OVAベースのインストールの場合は/opt/fnd/data/cgms.propertiesで変更します。

最後に、FNDを再起動して、新しいキーストアとパスワードの使用を開始します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。