Problemas com o uso de PNP com FND em versões mais recentes do Cisco IOS®

Contents

Introduction

Este documento descreve como gerar e exportar o certificado correto do Windows Private Key Infrastructure (PKI) para uso em combinação com Plug and Play (PNP) no Field Network Diretor (FND).

Problema

Quando você tenta usar o PNP para fazer Zero Touch Deployment (ZTD) nas versões mais recentes do Cisco IOS® e do Cisco IOS®-XE, o processo falha com um destes erros do 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
```

Desde algum tempo, o código PNP no Cisco IOS®/Cisco IOS®-XE exige que o campo Nome Alternativo do Assunto (SAN) seja preenchido no certificado oferecido pelo servidor/controlador PNP (FND, neste caso).

O Agente PNP Cisco IOS® verifica somente o campo SAN do certificado quanto à identidade do servidor. Ele não verifica mais o campo de nome comum (CN).

Isso é válido para estas versões:

- Cisco IOS® versão 15.2(6)E2 e posterior
- Cisco IOS® versão 15.6(3)M4 e posterior
- Cisco IOS® versão 15.7(3)M2 e posterior
- Cisco IOS® XE Denali 16.3.6 e posterior
- Cisco IOS® XE Everest 16.5.3 e posterior
- Cisco IOS® Everest 16.6.3 e posterior
- Todas as versões do Cisco IOS® de 16.7.1 e posterior

Mais informações podem ser encontradas aqui:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html#id_70663

Solução

A maioria dos guias e da documentação do FND ainda não mencionam que o campo SAN precisa ser preenchido.

Para criar e exportar o certificado correto para uso com PNP e adicioná-lo ao armazenamento de chaves, siga estas etapas.

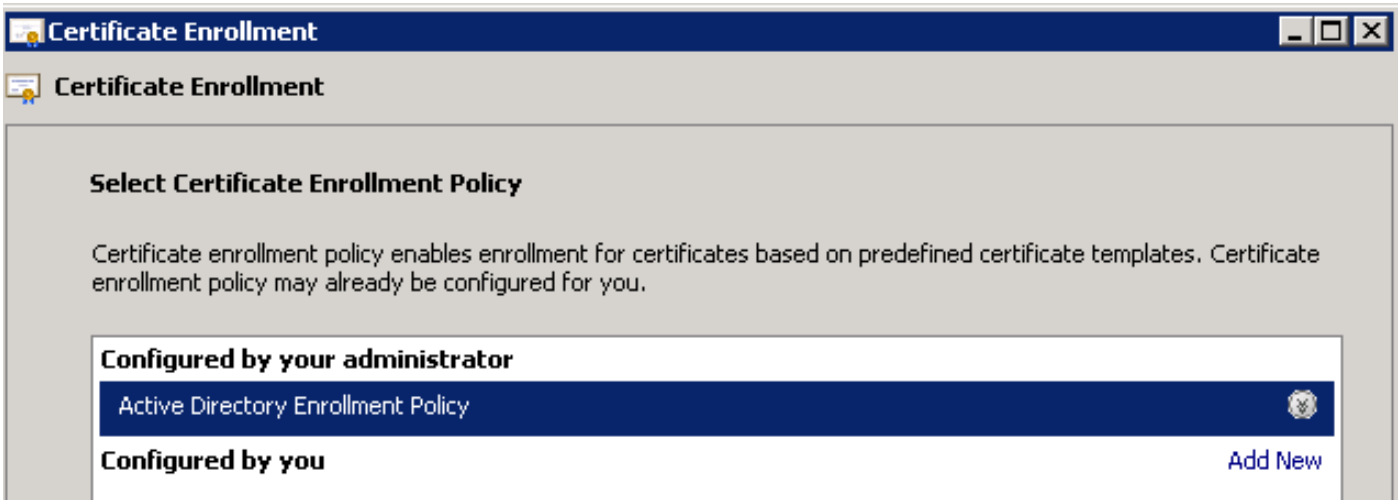
Gerar um novo certificado com o uso do modelo FND/NMS no servidor CA do Windows

Navegue até **Start > Run > mmc > File > Add/Remove Snap-in... > Certificates > Add > Computer Account > Local Computer > OK** e abra o snap-in MMC de certificados.

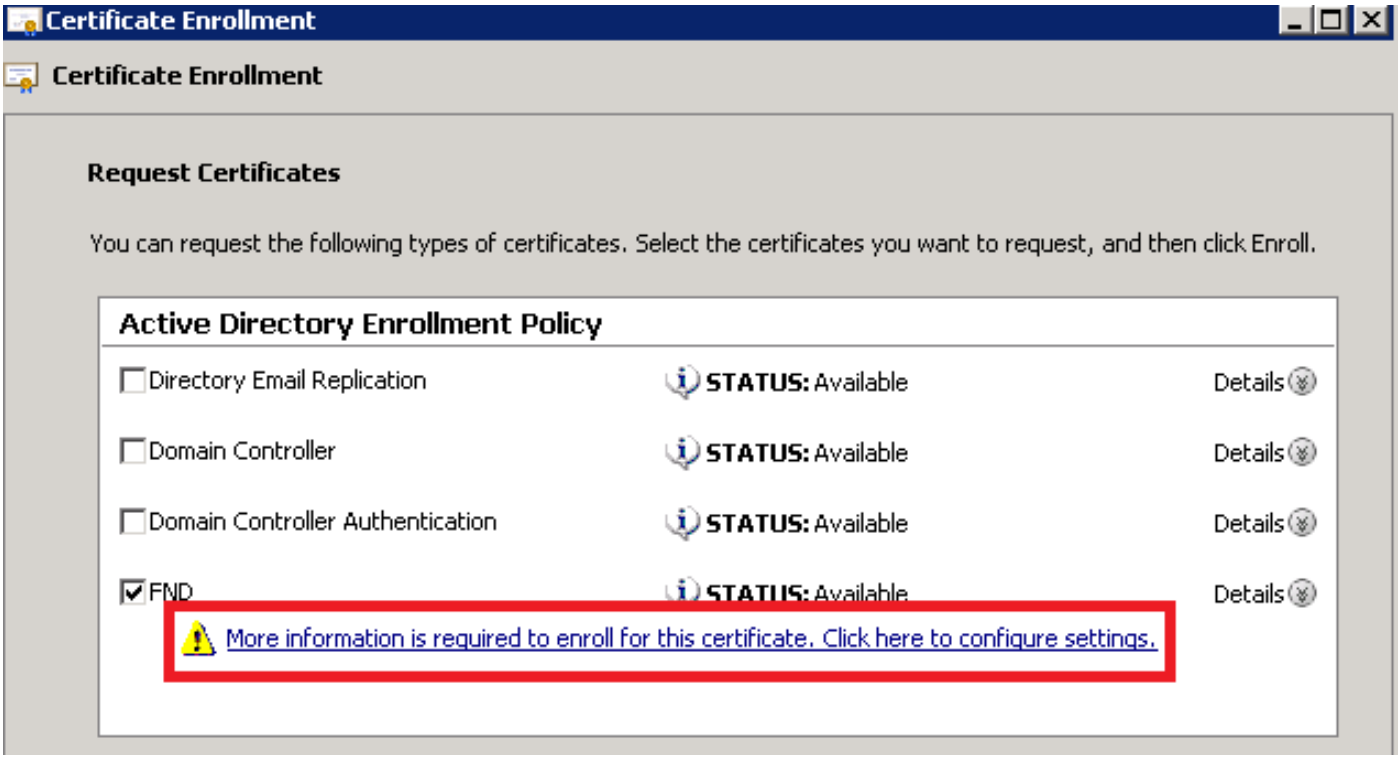
Expanda Certificados (Computador Local) > Pessoal > Certificados

Clique com o botão direito do mouse em Certificates e selecione **All Tasks > Request New Certificate...** como mostrado na imagem.

Clique em **Avançar** e selecione **Diretiva de Registro do Ative Diretory** conforme mostrado na imagem.



Clique em **Next** e selecione o modelo criado para o servidor NMS/FND (repita mais tarde para o TelePresence Server (TPS)) e clique no link **More Information**, conforme mostrado na imagem.



Nas propriedades do certificado, forneça estas informações:

Nome da entidade:

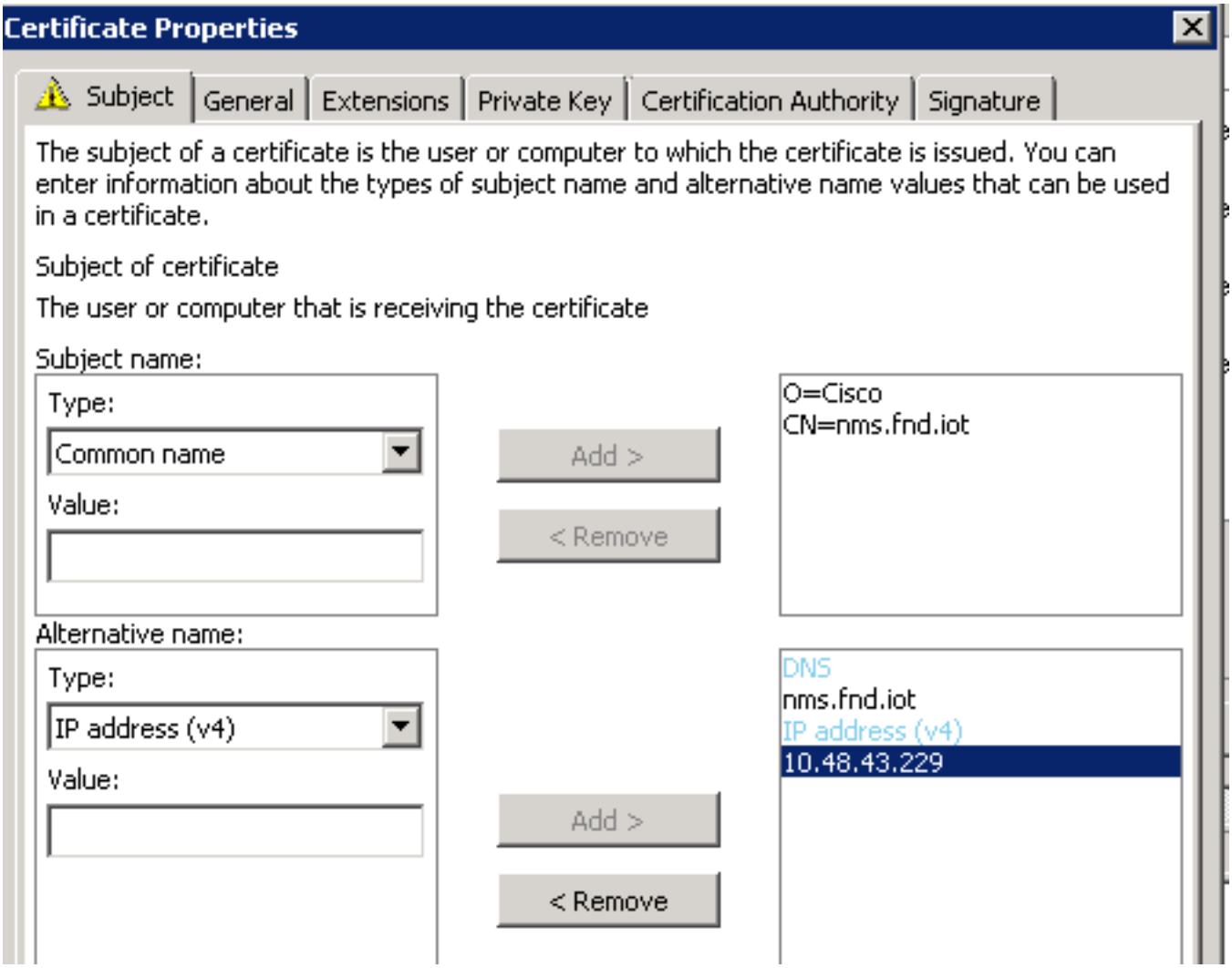
- Organização: nome da sua organização
- Nome comum: o nome de domínio totalmente qualificado (FQDN) do servidor FND (ou TPS, se aplicável)

Nome alternativo (campo SAN):

- Se você usar o DNS (Domain Name System) para contatar a parte PNP do servidor FND, adicione uma entrada DNS para o FQDN
- Se você usar IP para contatar a parte PNP do servidor FND, adicione uma entrada IPv4 para o IP

É recomendável incluir vários valores de SAN no certificado, caso os métodos de detecção variem. Por exemplo, você pode incluir o FQDN do controlador e o endereço IP (ou o endereço IP NAT) no campo SAN. Se você incluir ambos, defina o FQDN como o primeiro valor de SAN, seguido pelo endereço IP.

Exemplo de configuração:



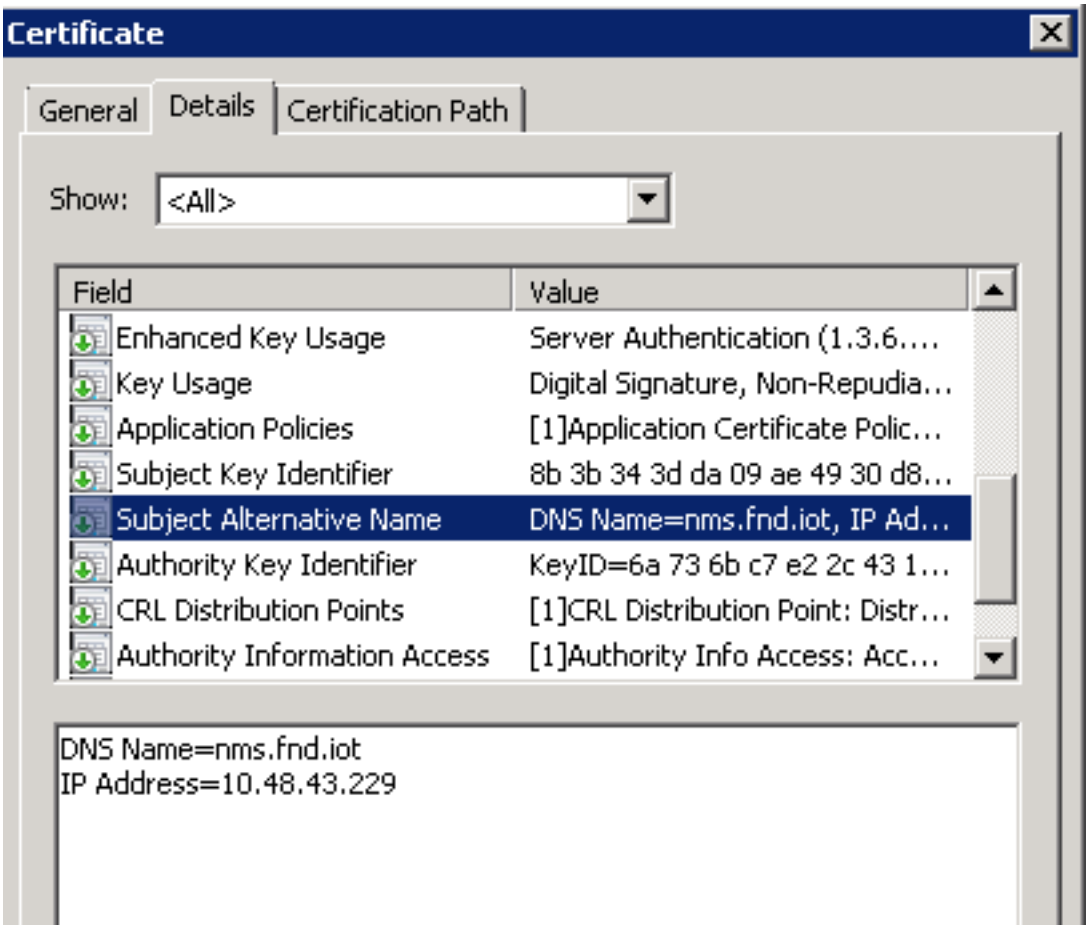
Depois de concluir, clique em **OK** na janela de propriedades do certificado e em **Enroll** para gerar o certificado e **Finish** quando a geração estiver concluída.

Verifique o campo SAN no certificado gerado

Apenas para verificar se o certificado gerado contém as informações corretas, você pode verificá-las da seguinte maneira:

Abra o Snap-In de certificados no Console de Gerenciamento Microsoft (MMC) e expanda **Certificados (Computador Local) > Pessoal > Certificados**.

Clique duas vezes no certificado gerado e abra a guia **Detalhes**. Role para baixo para encontrar o campo SAN, conforme mostrado na imagem.

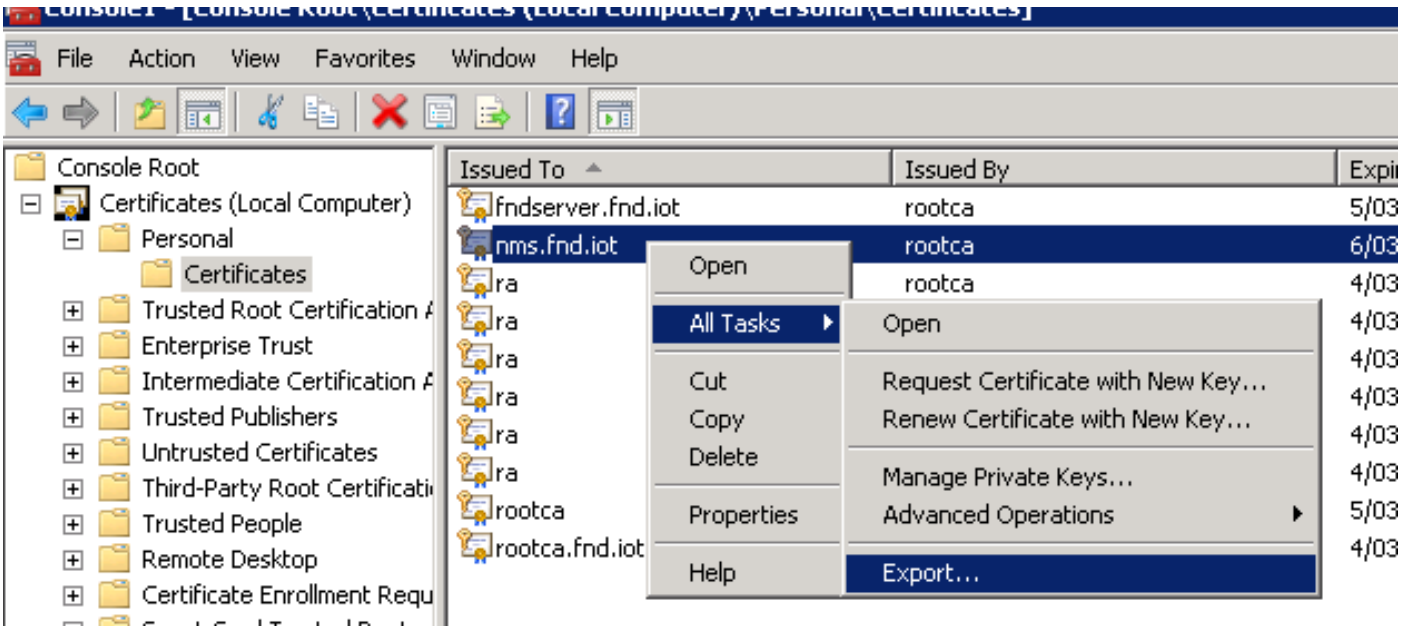


Exportar o certificado a importar para o armazenamento de chaves FND

Antes de importar ou substituir o certificado que existe no armazenamento de chaves FND, você precisa exportá-lo para um arquivo **.pfd**.

No Snap-In de certificados no MMC, expanda **Certificados (Computador Local) > Pessoal > Certificados**

Clique com o botão direito do mouse no certificado gerado e selecione **All Tasks > Export...** como mostrado na imagem.



Clique em **Next**, selecione para exportar a chave privada como mostrado na imagem.

Selecione para incluir todos os certificados no caminho de certificação conforme mostrado na imagem.

Clique em **Next**, selecione uma senha para a exportação e salve o **.pfx** em um local conhecido.

Criar o armazenamento de chaves FND para uso com PNP

Agora que o certificado foi exportado, você pode criar o armazenamento de chaves necessário para o FND.

Transfira o **.pfx** gerado da etapa anterior com segurança para a máquina FND-server (Network Management Systems (NMS) ou host OVA), por exemplo, com o uso de SCP.

Liste o conteúdo de **.pfx** para saber o alias gerado automaticamente na exportação:

```
[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
```

Crie um novo armazenamento de chaves com o uso deste 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".
```

No comando, certifique-se de substituir **nms.pfx** pelo arquivo correto (exportado da CA do Windows) e de que o valor srcalias corresponda à saída do comando anterior (**keytool -list**).

Depois de gerá-lo, converta-o para o novo formato como sugerido:

```
[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".
```

Adicione o certificado CA, exportado anteriormente, ao armazenamento de chaves:

```
[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
```

Por fim, adicione o certificado SUDI, que é usado para verificar a identidade por série do FAR quando você usa PNP, ao armazenamento de chaves.

Para uma instalação RPM, o certificado SUDI é fornecido com os pacotes e pode ser encontrado em: **/opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem**

Para uma instalação OVA, primeiro copie o certificado SUDI para o host:

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

Em seguida, adicione-o ao armazenamento de chaves como confiável com o 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
```

Nesse ponto, o armazenamento de chaves está pronto para ser usado com o FND.

Ativar o armazenamento de chaves novo/modificado para uso com o FND

Antes de usar o armazenamento de chaves, substitua a versão anterior e, opcionalmente, atualize a senha no arquivo **cgms.properties**.

Primeiro, faça um backup do armazenamento de chaves que já existe:

Para uma instalação RPM:

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

Para uma instalação OVA:

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

Substitua o que existe pelo novo:

Para uma instalação RPM:

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

Para uma instalação OVA:

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

Opcionalmente, atualize a senha para o armazenamento de chaves no arquivo cgms.properties:

Primeiro, gere uma nova sequência de senha criptografada.

Para uma instalação RPM:

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

Para uma instalação OVA:

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

Certifique-se de substituir o armazenamento de chaves pela senha correta para o

armazenamento de chaves.

Altere cgms.properties em **/opt/cgms/server/cgms/conf/cgms.properties** para a instalação baseada em RPM ou **/opt/fnd/data/cgms.properties** para a instalação baseada em OVA para incluir a nova senha criptografada.

Por fim, reinicie o FND para começar a usar o novo armazenamento de chaves e a senha.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.