Configurar o Field Network Diretor para usar Plug and Play em IR800

Contents

Introduction

Este documento descreve como começar com o Field Network Diretor (FND) e Plug and Play (PNP) com o uso de um conjunto mínimo de componentes.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Experiência com o Linux e conhecimento para editar arquivos de configuração de execução em uma máquina Linux
- Pelo menos um dos roteadores suportados a ser gerenciado pelo FND. Por exemplo, IR809 ou IR829. Acesso ao consoleVersão mínima do IOS® 15.7(3)M1
- Arquivo OVA implantado em um hipervisor (por exemplo: VMWare ESXi). O arquivo OVA, se qualificado, pode ser baixado de: https://software.cisco.com/download/home/286287993/type/286320249

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Arquivo OVA para FND versão 4.5.0-122 (CISCO-IOTFND-V-K9-4.5.0-122.zip)
- VMWare ESX
- IR809 com IOS® versão 15.8(3)M2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

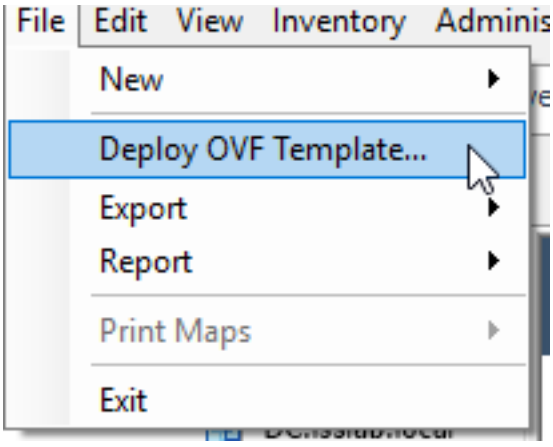
Como o FND tem muitas opções de implantação diferentes, o objetivo é poder configurar uma instalação mínima, mas funcional, para o FND. Essa configuração pode servir como ponto de partida para mais personalização e para adicionar mais recursos. A configuração explicada aqui é com o uso da instalação de FND do Open Virtual Appliance (OVA) empacotada como ponto de partida e usa o modo fácil para evitar a necessidade de PKI (Public Key Infrastructure, Infraestrutura de Chave Pública) e provisionamento de túnel. Use o PNP para simplificar e adicionar dispositivos à instalação.

O resultado deste guia não deve ser usado na produção, pois pode haver alguns riscos de segurança devido à senha do texto do plano e à ausência de túneis e PKI.

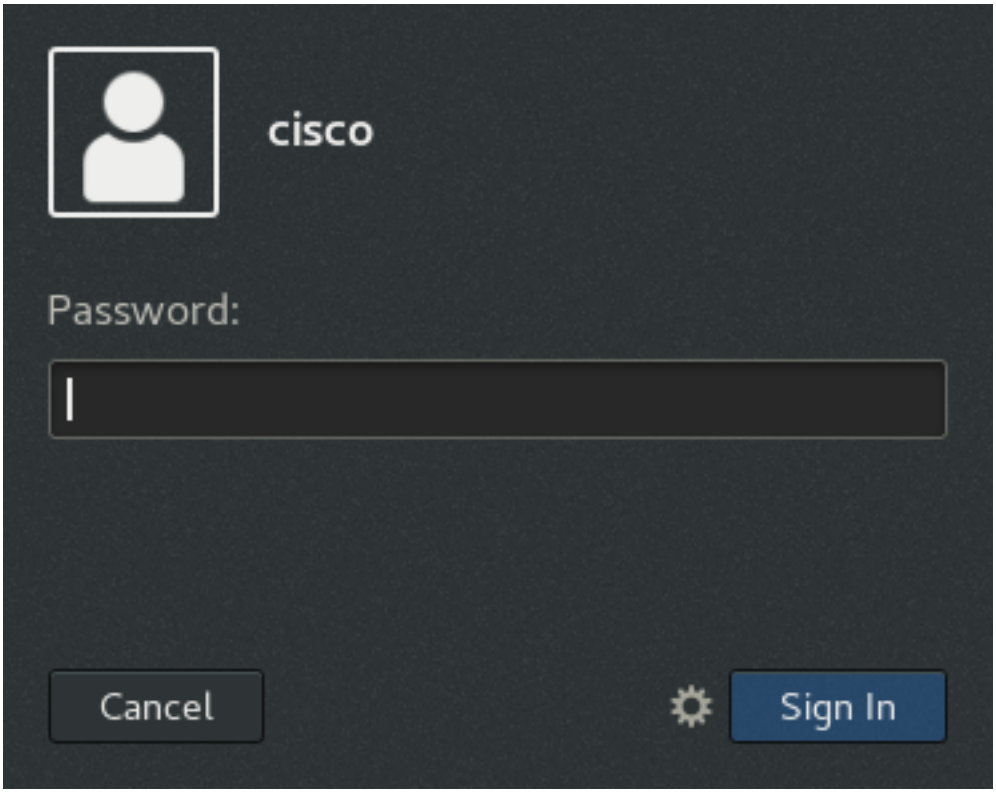
Configurar

Implante e configure o FND OVA

Etapa 1. faça download e implante o arquivo OVA do FND no hipervisor. Por exemplo, para o VMWare, isso será através de **Arquivo > Implantar modelo OVF** como mostrado na imagem.



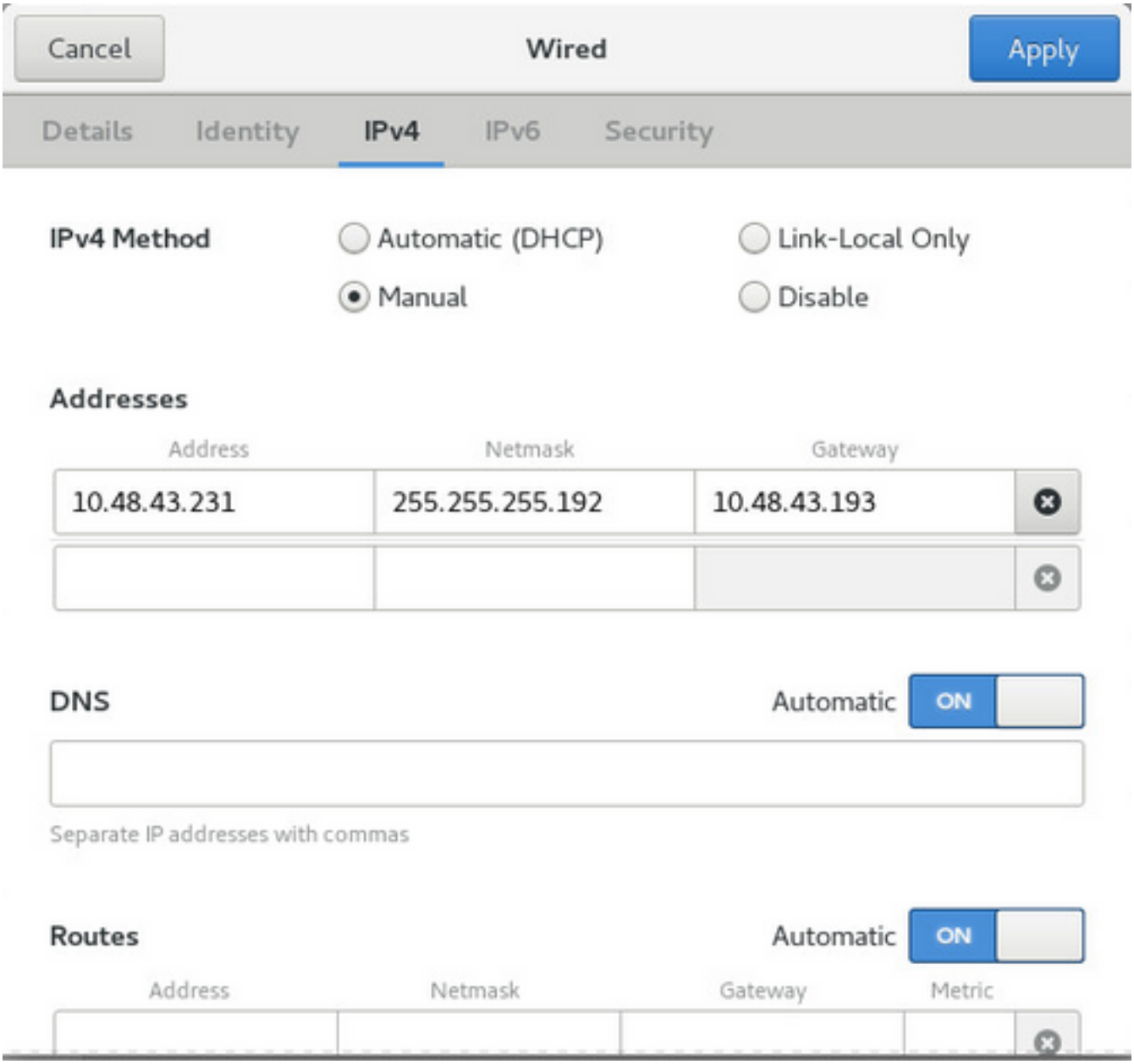
Etapa 2. Depois de implantar, você pode iniciar a VM e é apresentado uma tela de login, mostrada na imagem.



As senhas padrão para o arquivo OVA são:

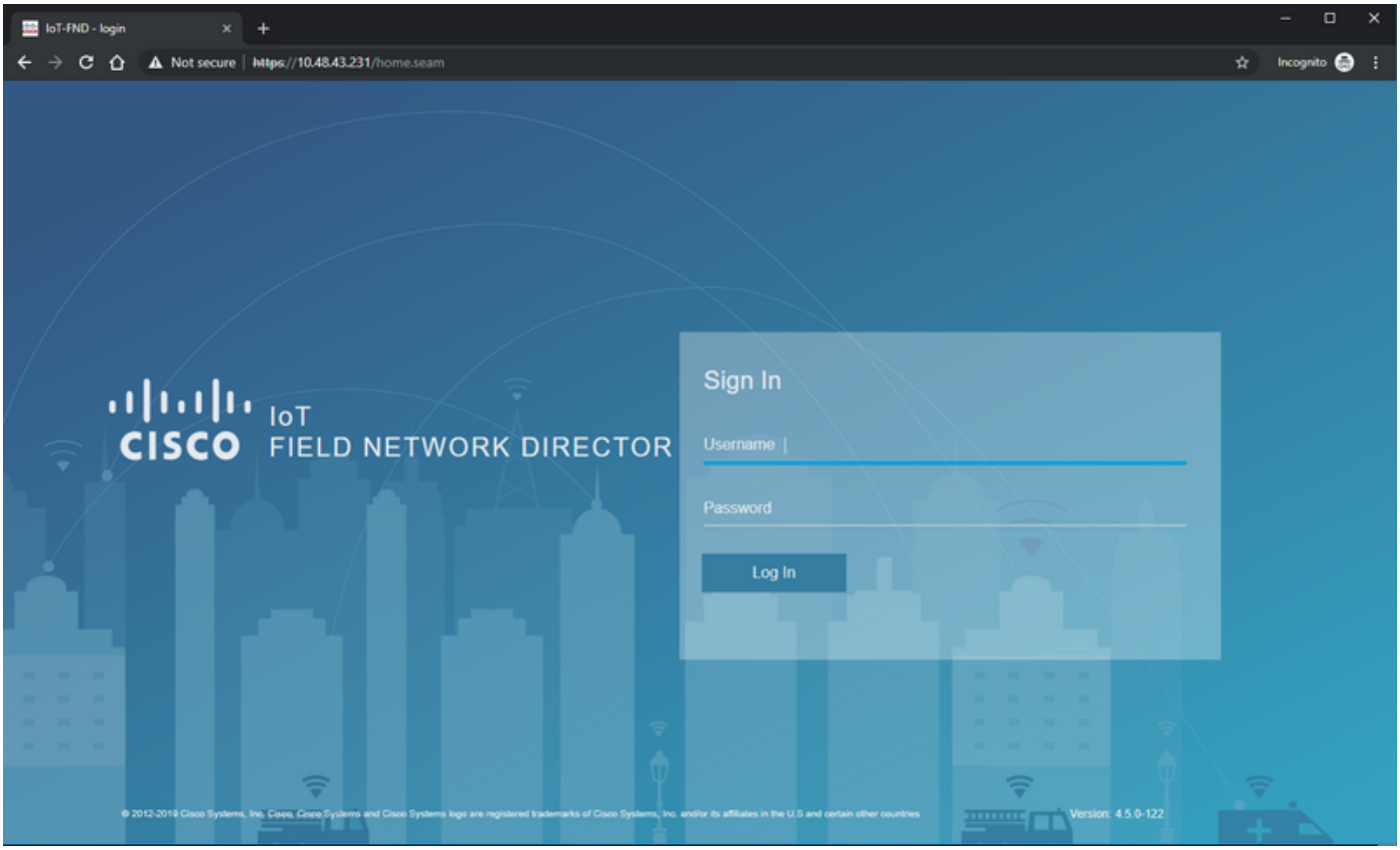
- nome de usuário: senha raiz: **cisco123**
- nome de usuário: senha da cisco: **C_sco123**

Etapa 3. Faça login com o usuário e a senha da cisco e navegue para **Applications > System Tools > Settings > Network.** Adicione um perfil com fio e, na guia IPv4, defina o endereço IP ou DHCP desejado como mostrado na imagem.



Etapa 4. Clique em **Apply** e ative/desligue a conexão para garantir que as novas configurações sejam aplicadas.

Nesse ponto, você deve conseguir navegar até a **GUI do FND** com seu navegador e o endereço IP configurado como mostrado na imagem.



Etapa 5. Faça login na GUI com o uso do nome de usuário e senha padrão: **raiz/raiz123**

Você será solicitado a alterar sua senha imediatamente e, em seguida, será redirecionado para o login novamente.

Se tudo correr bem, você poderá fazer login com sua nova senha e navegar pela GUI do FND.

Além disso, o modo PNP e de demonstração são descritos, seguido da configuração do FND.

Sobre o PNP

O PNP é o método mais atual da Cisco para implantação automatizada (ZTD). Com o uso do PNP, um dispositivo pode ser totalmente configurado e a necessidade de tocar a configuração manualmente não ocorrerá.

Para o FND, com o uso do PNP, a necessidade de primeiro inicializar o roteador é evitada. Na verdade, tudo o que o PNP faz, redireciona-o para o FND, de forma segura, e busca a configuração do bootstrap.

Quando a configuração de bootstrap estiver presente no dispositivo, o resto do processo será continuado como com um dispositivo de bootstrapped clássico.

Há maneiras diferentes de usar o PNP:

- Através do serviço Cisco PNP (devicehelper.cisco.com), com o uso de uma Smart Account. Ativado por padrão fora da fábrica em determinados dispositivos
- Com o uso da opção de DHCP 43 para fornecer o IP ou o nome do host ao qual se conectar para bootstrapping
- Definindo manualmente o servidor PNP na configuração

Para essa configuração, o IP do servidor PNP é definido manualmente, que é o IP do servidor FND, e a porta no dispositivo. Caso deseje fazer isso com o DHCP, você deve fornecer as seguintes informações:

Para o Cisco IOS®, o servidor DHCP deve ser configurado da seguinte maneira:

```
ip dhcp pool pnp_pool
network 192.168.10.0 255.255.255.248
default-router 192.168.10.1
dns-server 8.8.8.8
option 43 ascii "5A;K4;B2;I10.48.43.231;J9125"
!
```

Para DHCPd no Linux:

```
[jedepuyd@KJK-SRVIOT-10 ~]$ cat /etc/dhcp/dhcpd.conf
subnet 192.168.100.0 netmask 255.255.255.0 {

option routers 192.168.100.1;
range 192.168.100.100 192.168.100.199;
option domain-name-servers 192.168.100.1;
option domain-name "test.dom";
option vendor-encapsulated-options "5A;K4;B2;I10.48.43.231;J9125";
}
```

Nesta configuração para a opção 43 ou opções encapsuladas pelo fornecedor, você precisa especificar estas strings ASCII:

```
"5A;K4;B2;I10.50.215.252;J9125"
```

Pode ser adaptado da seguinte forma:

- 5 - Código de tipo de DHCP 5
- A - Código de operação do recurso ativo
- K4 - Protocolo de transporte HTTP
- B2 - O tipo de endereço IP do servidor PnP/TPS/FND é IPv4
- I10.48.43.231 - FND server IP address
- J9125 - Número da porta 9125 (porta para PNP no servidor FND)

Mais informações sobre o PNP com DHCP podem ser encontradas aqui: https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/guide/4_3/iot_fnd_ug4_3/sys_mgmt.html#31568 na seção: **Configurar a opção 43 de DHCP no servidor DHCP do Cisco IOS®**

Sobre o EasyMode

O modo fácil foi introduzido desde o FND 4.1, embora fosse chamado de modo de demonstração no momento, e permite executar o FND de forma menos segura. Embora isso não seja recomendado para a produção, é uma boa maneira de começar.

Com o uso do modo fácil, você pode se concentrar no processo de PNP, no bootstrapping e na configuração do roteador. Caso algo não funcione, você não precisa suspeitar do acúmulo de túnel ou dos certificados.

Alterações que ocorrem quando você configura o FND para execução no modo fácil:

- Não há necessidade de um HER (Head End Router) ou um túnel para o servidor FND.
- Não há necessidade de configuração de PKI (Public Key Infrastructure, Infraestrutura de Chave Pública) e SCEP (Simple Certificate Enrollment Protocol, Protocolo de Inscrição de Certificado Simples).
- Não há necessidade de certificados de roteador, ponto de confiança e certificados SSL.
- Toda comunicação está ocorrendo através de HTTP em vez de HTTPS.

Mais informações sobre o modo fácil podem ser encontradas aqui:

https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/guide/4_1_B/iot_fnd_ug4_1_b/device_mgmt.html#85516

Configurar FND para PNP e modo fácil

Agora, você sabe o que é modo de demonstração/PNP e por que ele é usado nesse contexto. Vamos alterar a configuração do FND para habilitá-la:

Na VM FND, originada do arquivo OVA, conecte-se ao SSH e edite o **cgms.properties** da seguinte maneira:

```
[root@iot-fnd ~]# cat /opt/fnd/data/cgms.properties
cgms-keystore-password-hidden=dD5KmzJHa64Oyvpqdu8SCg==
use-router-ip-from-db=true
rabbit-broker-ip=
rabbit-broker-port=
rabbit-broker-username=
rabbit-broker-password=
fogd-ip=192.68.5.3
enable-reverse-dns-lookup=false
enableApiAuth=false
fnd-router-mgmt-mode=1
enable-bootstrap-service=true
proxy-bootstrap-ip=10.48.43.231
```

As três últimas linhas foram alteradas no arquivo de configuração.

- Linha 10: permite o modo fácil
- Linha 11: ativa o PNP
- Linha 12: define o IP do servidor FND a ser contatado

Depois de alterar o arquivo, reinicie o contêiner FND para adaptar as alterações feitas:

```
[root@iot-fnd ~]# /opt/fnd/scripts/fnd-container.sh restart
Stopping FND container...
fnd-container
[root@iot-fnd ~]# Starting FND container...
fnd-container
```

Depois de reiniciado, o resto da configuração pode ser feito com o uso da GUI.

Prepare o CSV e adicione o roteador ao FND

Pode parecer um pouco ilógico adicionar o dispositivo neste ponto do processo de configuração, mas, infelizmente, partes da configuração não estão disponíveis até que determinados tipos de dispositivo tenham sido adicionados.

Isso é feito para evitar que a GUI seja muito esmagadora à medida que dispositivos diferentes introduzem opções diferentes.

Aqui, vamos tentar adicionar um IR809 ao FND.

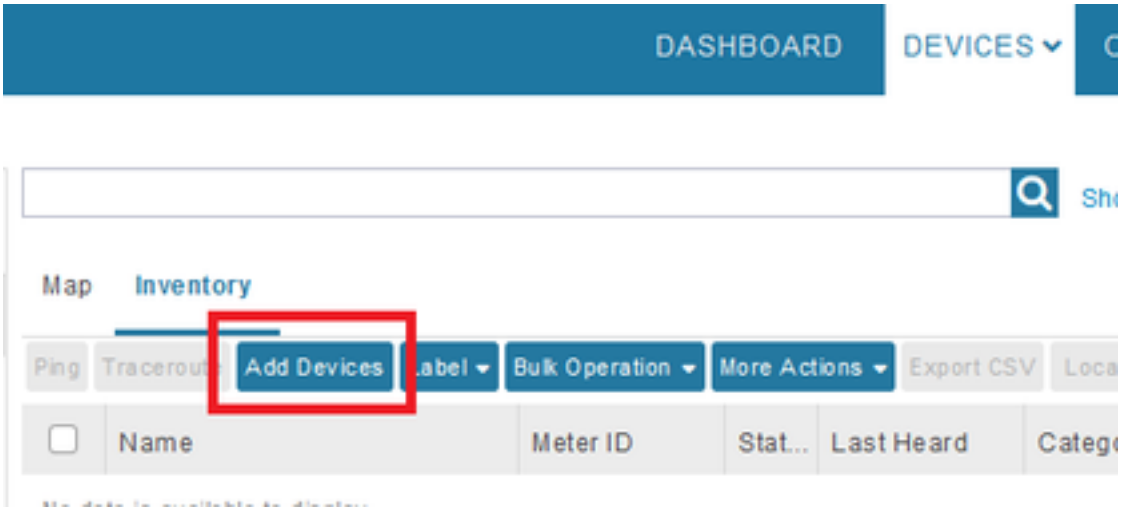
O CSV tem a seguinte aparência:

```
deviceType,eid,adminUsername,adminPassword,ip
ir800,IR809G-LTE-GA-K9+JMX2022X04S,fndadmin,C1sc0123!,10.48.43.250
```

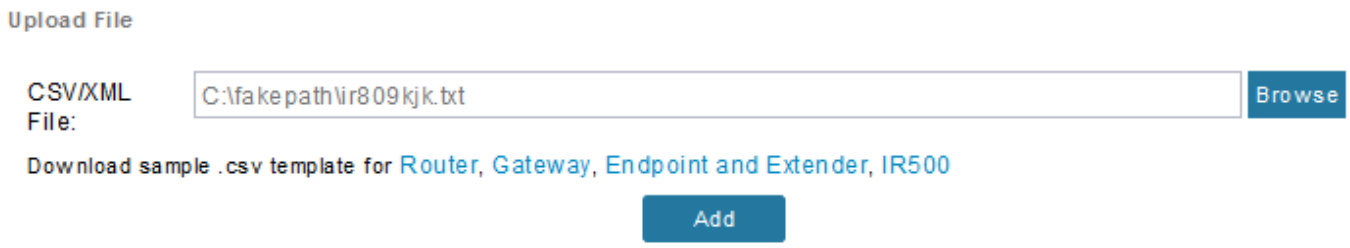
Os campos no CSV são:

- **tipo de dispositivo**: ir800
- **eid**: PID e serial juntamente com +
- **adminUsername**: esse nome de usuário será adicionado à configuração do roteador e, posteriormente, será usado para concluir o processo de registro
- **adminPassword**: senha para adminUsername
- **ip:** o endereço IP a ser substituído na configuração do dispositivo após a implantação

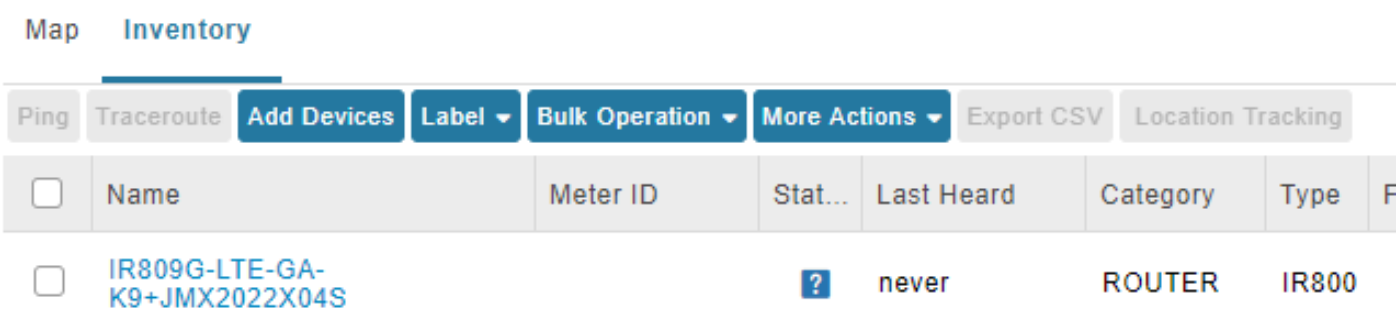
Para adicionar esse dispositivo, conecte-se à GUI e navegue até **Dispositivos > Dispositivos de campo > Inventário > Adicionar dispositivos** como mostrado na imagem.



Na caixa de diálogo, especifique o local do arquivo CSV e clique em **Adicionar** para adicioná-lo ao FND, como mostrado na imagem.



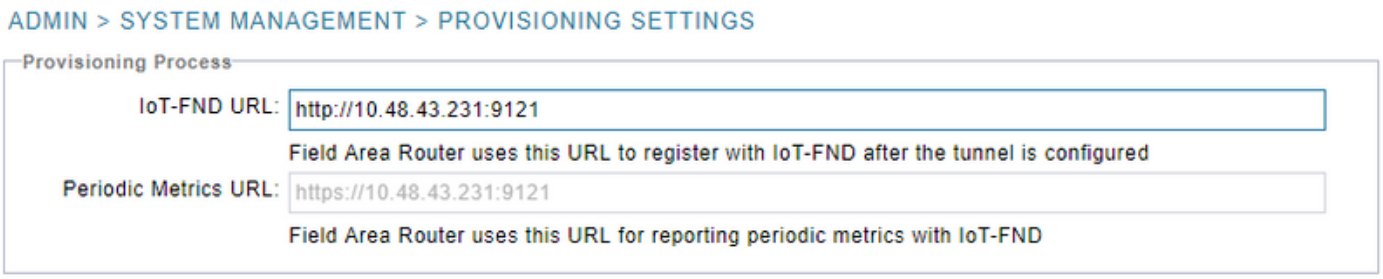
Se tudo correr bem, você verá o item de histórico para listar "CONCLUÍDO". Depois de fechar a caixa de diálogo, o dispositivo deve aparecer no inventário como mostrado na imagem.



Como o dispositivo de deviceType ir800 foi adicionado, os modelos e grupos aplicáveis estarão disponíveis na GUI neste ponto.

Prepare as configurações de provisionamento, o modelo de bootstrap e o modelo de configuração

Como o FND está configurado para o modo de demonstração, é necessário alterar o URL de provisionamento para usar o HTTP. Navegue até **Admin > Provisioning Settings** para fazer isso:



Altere o URL da IoT-FND para **http://<FND IP>:9121**

Em seguida, configure dois modelos mínimos para bootstrapping e configuração.

A primeira, chamada de modelo de **configuração de bootstrap do roteador**, é a configuração enviada ao roteador quando ele puder entrar em contato com o FND com o uso de PNP.

Se o PNP não estiver em uso, será a configuração colocada no roteador manualmente ou na fábrica no momento do processo de bootstrap. Essa configuração contém apenas informações suficientes para que o roteador inicie o processo de registro no FND.

A segunda, chamada de modelo de configuração, será a configuração adicionada à configuração em execução no momento do dispositivo. Na verdade, ele pode ser visto como um incremento na configuração existente.

Na maioria dos casos, isso leva a uma situação estranha, portanto, é recomendável primeiro apagar todas as configurações no roteador antes de adicioná-lo ao FND.

Para definir o modelo Router Fatory Reprovision, navegue até **Configure > Tunnel Provisioning > Router Bootstrap Configuration** e substitua-o pelo seguinte modelo:

```
<#if isBootstrapping = true>
<#assign mgmtintf = "GigabitEthernet0">
<#assign fndserver = "10.48.43.231">
```

```
<#assign sublist=far.eid?split("+")[0..1]>
<#assign pid=sublist[0]>
<#assign sn=sublist[1]>

<#-- General parameters  -->
hostname ${sn}BS
ip domain-name ${sn}
ip host fndserver.fnd.iot ${fndserver}
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
<#-- Users  -->
username backup privilege 15 password C1sc0123!
username ${far.adminUsername} privilege 15 password ${far.adminPassword}
!
<#-- Interfaces  -->
interface ${mgmtintf}
  ip address ${far.ip} 255.255.255.192
exit
!
<#-- Clock  -->
clock timezone UTC +2
!
<#-- Archive  -->
file prompt quiet
do mkdir flash:archive
archive
  path flash:/archive
  maximum 8
exit
!
<#-- HTTP -->
ip http server
ip http client connection retry 5
ip http client connection timeout 5
ip http client source-interface ${mgmtintf}
ip http authentication local
ip http timeout-policy idle 600 life 86400 requests 3
ip http max-connections 2
!
<#-- WSMA -->
wsma profile listener exec
  transport http path /wsma/exec
exit
!
wsma profile listener config
  transport http path /wsma/config
exit
!
wsma agent exec
  profile exec
exit
!
wsma agent config
  profile config
exit
!
<#-- CGNA -->
cgna gzip
!
cgna profile cg-nms-register
  add-command show hosts | format flash:/managed/odm/cg-nms.odm
  add-command show interfaces | format flash:/managed/odm/cg-nms.odm
  add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
```

```
  add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
  add-command show platform hypervisor | format flash:/managed/odm/cg-nms.odm
  add-command show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
  add-command show iox host list detail | format flash:/managed/odm/cg-nms.odm
  add-command show version | format flash:/managed/odm/cg-nms.odm
  interval 10
  url http://fndserver.fnd.iot:9121/cgna/ios/registration
  gzip
  active
exit
!
<#-- Script to generate RSA for SSH -->
event manager applet genkeys
  event timer watchdog name genkeys time 30 maxrun 60
    action 10 cli command "enable"
    action 20 cli command "configure terminal"
    action 30 cli command "crypto key generate rsa modulus 2048"
    action 80 cli command "no event manager applet genkeys"
    action 90 cli command "exit"
    action 99 cli command "end"
exit

end
</#if>
```

Para definir o modelo de configuração. Navegue até **Config > Device Configuration > Edit Configuration Template** e adicione este modelo:

```
<#-- Enable periodic inventory notification every 1 hour to report metrics. -->
    cgna profile cg-nms-periodic
      interval 60
    exit
<#-- Enable periodic configuration (heartbeat) notification every 15 min. -->
   cgna heart-beat interval 15

<#-- Enable SSH access -->
line vty 0 4
  transport input ssh
  login local
exit
```

Esse modelo será a configuração atual do roteador resultante. Portanto, qualquer configuração específica para esse grupo de configuração deve ser adicionada aqui.

O mais fácil é começar com esse modelo mínimo. Após o sucesso, atualize e personalize o modelo de acordo com suas necessidades.

Neste ponto, a configuração/preparação do FND é feita e você pode começar com a preparação do roteador.

Preparar o IR800 para provisionamento/PNP

Se o dispositivo que você deseja provisionar já contiver uma configuração ou tiver sido usado antes, é melhor apagar completamente a configuração do roteador antes de adicioná-lo ao FND com PNP.

Obviamente, se este for um novo dispositivo, esta etapa pode ser ignorada.

A maneira mais fácil de fazer isso é com o uso do comando **write erase** e recarregar o roteador

com o uso do console.

```
ir809kjk#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
*Oct 18 11:42:54.367 UTC: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
ir809kjk#reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]

Starting File System integrity check
NOTE: File System will be deinited and later rebuilt
```

Depois de algum tempo, o IR800 deve voltar com o prompt para executar o diálogo de configuração inicial:

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!
```

Certifique-se de que não há mais restos de uma tentativa anterior de PNP/ZTD, é melhor recriar o arquivo e diretório e remover a **configuração anterior ao registro** no roteador também:

```
IR800#delete /f before-*
IR800#delete /f /r archive*
IR800#mkdir archive
Create directory filename [archive]?
Created dir flash:/archive
IR800#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IR800(config)#archive
IR800(config-archive)#path flash:/archive
IR800(config-archive)#maximum 8
IR800(config-archive)#end
```

Neste momento, você tem um novo dispositivo ou um dispositivo com uma configuração vazia, portanto, se necessário, esse é o momento em que uma configuração mínima para que o roteador acesse o FND pode ser aplicada.

Caso você tenha um servidor DHCP, a maior parte deve ser feita automaticamente.

A seguinte configuração manual está selecionada no dispositivo:

```
IR800>enable
IR800#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IR800(config)#int gi0
IR800(config-if)#ip addr dhcp
IR800(config-if)#no shut
IR800(config-if)#end
*Aug 1 12:02:02.887: %SYS-5-CONFIG_I: Configured from console by console

IR800#ping 10.48.43.231
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.48.43.231, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
IR800#
```

Como você vê, um ping rápido foi executado para testar se o roteador conseguiu acessar o FND com a configuração de IP aplicada.

Provisione o Roteador IR800

Neste ponto, todos os pré-requisitos estão completos e você pode iniciar o processo de PNP. É feito manualmente nesta instância.

Em um ambiente de produção, provavelmente, o PNP será usado com a opção de DHCP 43. Isso significa que, quando o roteador é iniciado, ele recebe um IP e a configuração do PNP e você pode pular essa etapa e a próxima.

Para configurar manualmente o PNP no IR800 sem DHCP, você precisa especificar o destino para as solicitações, que será o servidor FND.

Isso pode ser feito da seguinte forma:

```
IR800(config)#pnp profile pnp-zero-touch
IR800(config-pnp-init)#transport http ipv4 10.48.43.231 port 9125
IR800(config-pnp-init)#end
```

Assim que você inserir a linha começando com "transporte", o roteador iniciará o processo PNP e tentará entrar em contato com o FND no IP e na porta específicos.

Se tudo correr bem, o dispositivo passa por estes:

- [ATUALIZAÇÃO_ODM]: atualizar os arquivos ODM (Operational Data Model) no dispositivo para corresponder aos válidos para a versão atual do FND
- [ATUALIZAÇÃO_ODM_VERIFY_HASH]: verifique se os arquivos atualizados estão corretos
- [UPDATED_ODM]
- [COLLECTING_INVENTORY]: coletar a configuração atual e as informações do dispositivo
- [COLLECTED_INVENTORY]
- [VALIDATING_CONFIGURATION]: tente aplicar a configuração do bootstrap config (modelo substituído de reprovisionamento de fábrica do roteador)
- [VALIDATED_CONFIGURATION]
- [PUSHING_BOOTSTRAP_CONFIG_FILE]: aplicar a configuração validada
- [PUSHING_BOOTSTRAP_CONFIG_VERIFY_HASH]: verifique se a configuração aplicada está correta
- [PUSHED_BOOTSTRAP_CONFIG_FILE]
- [CONFIGURING_STARTUP_CONFIG]:escreva a configuração como configuração de inicialização
- [CONFIGURED_STARTUP_CONFIG]
- [APPLYING_CONFIG]: aplicar a configuração de inicialização
- [APPLIED_CONFIG]
- [TERMINATING_BS_PROFILE]: pare de bootstrapping.

Você pode acompanhar o processo no FND server.log.

Na GUI, você verá a movimentação do dispositivo quando navegar para **Unheard > Boostrapping > Bootstrapped**

Após a conclusão do bootstrapping, o roteador tem o modelo substituído de reprovisionamento de fábrica do roteador e se comporta como um dispositivo de bootstrapped normal sem PNP.

Em outras palavras, um perfil CGNA no IR800 tenta se registrar no servidor FND.

Verifique o status do perfil CGNA:

```
JMX2022X04SBS#sh cgna profile-state all
Profile 1:
Profile Name: cg-nms-register
Activated at: Thu Aug  1 15:31:14 2019
URL: http://fndserver.fnd.iot:9121/cgna/ios/registration
Payload content type: xml
Interval: 10 minutes
gzip: activated
Profile command:
    show hosts | format flash:/managed/odm/cg-nms.odm
    show interfaces | format flash:/managed/odm/cg-nms.odm
    show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
    show ipv6 interface | format flash:/managed/odm/cg-nms.odm
    show platform hypervisor | format flash:/managed/odm/cg-nms.odm
    show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
    show iox host list detail | format flash:/managed/odm/cg-nms.odm
    show version | format flash:/managed/odm/cg-nms.odm
State: Wait for timer for next action
Timer started at Thu Aug  1 15:31:14 2019
Next update will be sent in 9 minutes 30 seconds
Last successful response not found
Last failed response not found
```

Com a configuração fornecida, o dispositivo tentará se registrar no FND após dez minutos. Você pode ver que, nessa saída, restam nove minutos e trinta segundos antes do roteador iniciar o processo de registro.

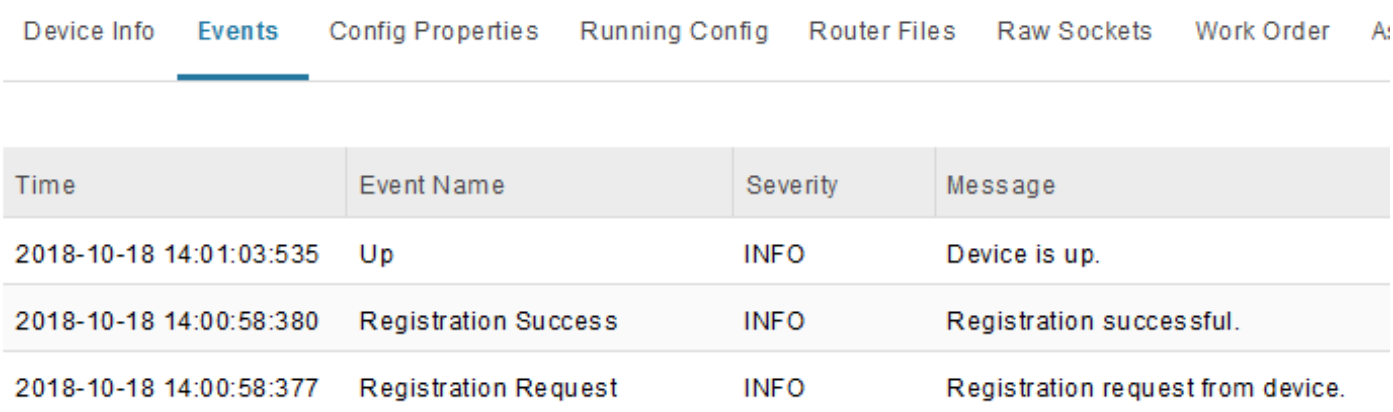
Você pode esperar que o temporizador termine ou executar manualmente o perfil **cg-nms-register** imediatamente:

```
IR800-Bootstrap#cgna exec profile cg-nms-register
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

O dispositivo deve mover para o status UP (UP) no FND, conforme mostrado na imagem.



Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Para solucionar problemas do processo de bootstrapping, verifique os seguintes itens:

- Login do servidor FND: **/opt/fnd/logs/server.log**
- Aumente a verbosidade do login: **Admin > Log > Log Level Settings > Router Bootstrapping > Debug**
- A partir do console IR800: **show pnp ? ou debug pnp ?**
- Na GUI do FND: **Dispositivos > Inventário > Selecionar Dispositivo > Eventos**
- A maioria dos problemas nesta etapa estão relacionados a erros (sintaxe) no modelo Router Fatory Reprovision

Para solucionar problemas do processo de registro, verifique os seguintes itens:

- Login do servidor FND: **/opt/fnd/logs/server.log**
- A partir do console IR800:

  show cgna profile-state alldebug cgna logging ?debug wsma agent
- Na GUI do FND: **Dispositivos > Inventário > Selecionar Dispositivo > Eventos**
- Verifique a conectividade WSMA sobre HTTP para IR800 da VM FND
  URI usado pelo FND: http://10.48.43.231:80/wsma/execMétodo: POSTSegurança: **autenticação básica**