Configurar o diretor da rede do campo para usar o Plug and Play em IR800

Índice

Introdução

Este documento descreve como obter começado com o diretor da rede do campo (FND) e o Plug and Play (PNP) com o uso do ajuste mínimo dos componentes.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Experiência com Linux e conhecimento a fim editar arquivos de configuração da corrida em uma máquina de Linux
- Pelo menos um do Roteadores apoiado a ser controlado por FND. Por exemplo IR809 ou IR829. Acesso de consoleVersão 15.7(3)M1 mínima IOS®
- Arquivo dos ÓVULOS distribuído a um hypervisor (por exemplo: VMware ESXi). O arquivo dos ÓVULOS, se autorizado, pode ser transferido de: https://software.cisco.com/download/home/286287993/type/286320249

Componentes Utilizados

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

- Os ÓVULOS arquivam para a versão 4.5.0-122 FND (CISCO-IOTFND-V-K9-4.5.0-122.zip)
- VMware ESX
- IR809 com versão 15.8(3)M2 IOS®

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

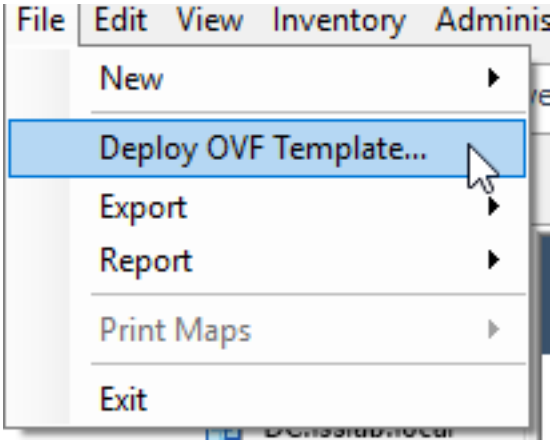
Desde que FND tem muitas opções de distribuição diferentes, o objetivo é poder estabelecer um mínimo mas o trabalho, a instalação para FND. Esta instalação pode então servir como o ponto do começo para uma personalização mais adicional e a fim adicionar mais características. A instalação explicada aqui é com o uso do dispositivo virtual aberto (ÓVULOS) - a instalação empacotada FND enquanto o ponto e do começo usam o modo fácil a fim evitar a necessidade para o Public Key Infrastructure (PKI) e escavar um túnel o abastecimento. Use PNP, a fim simplificar e adicionar dispositivos à instalação.

O resultado deste guia não é pretendido ser usado na produção enquanto pôde haver uma senha devida do plano-texto de alguns riscos de segurança e a ausência de túneis e de PKI.

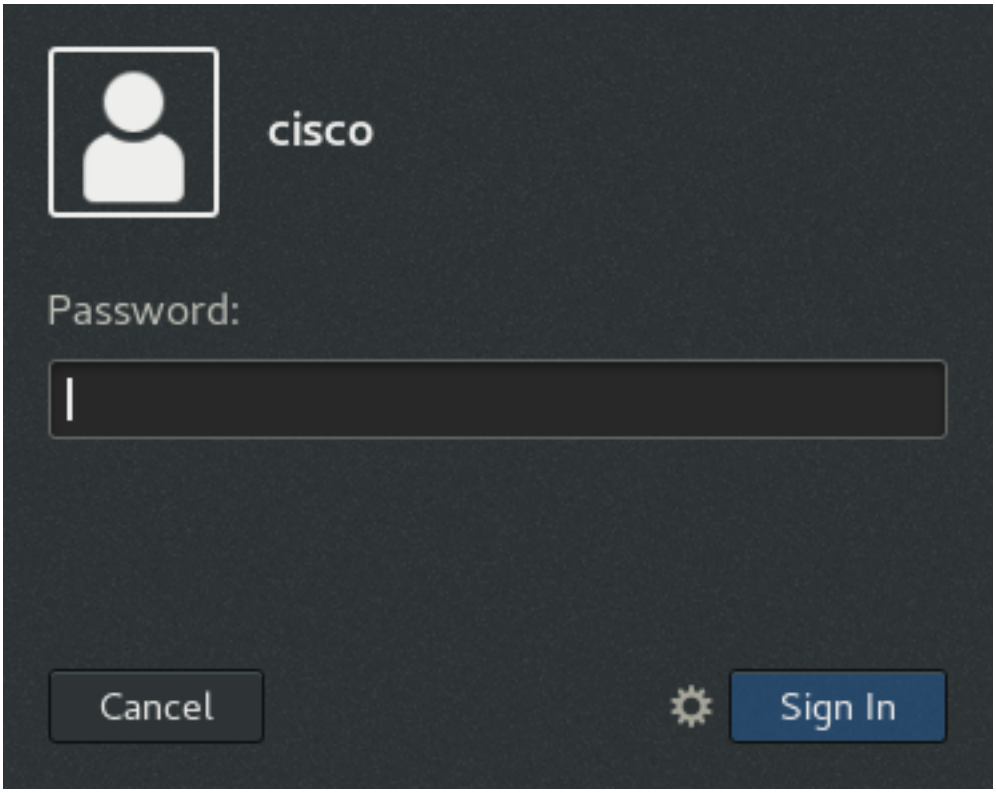
Configurar

Distribua e configurar os ÓVULOS FND

A transferência de etapa 1. e distribui os ÓVULOS FND arquiva a seu hypervisor. Por exemplo para VMware, isto será através do **arquivo > distribui o molde OVF** segundo as indicações da imagem.



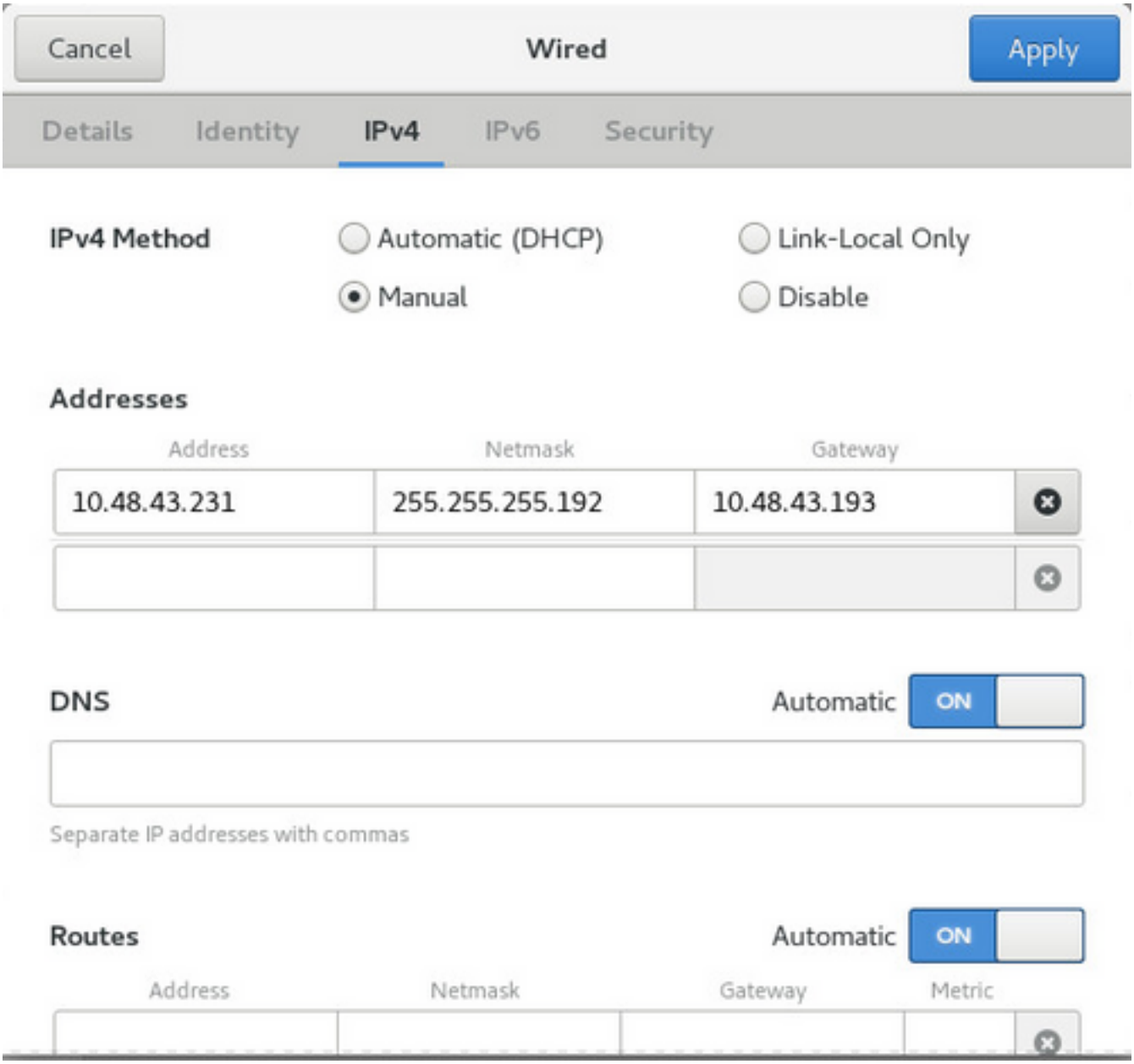
Etapa 2. Uma vez que obtém distribuída, você pode começar o VM e é presentado com uma tela de login, mostrada na imagem.



As senhas padrão para o arquivo dos ÓVULOS são:

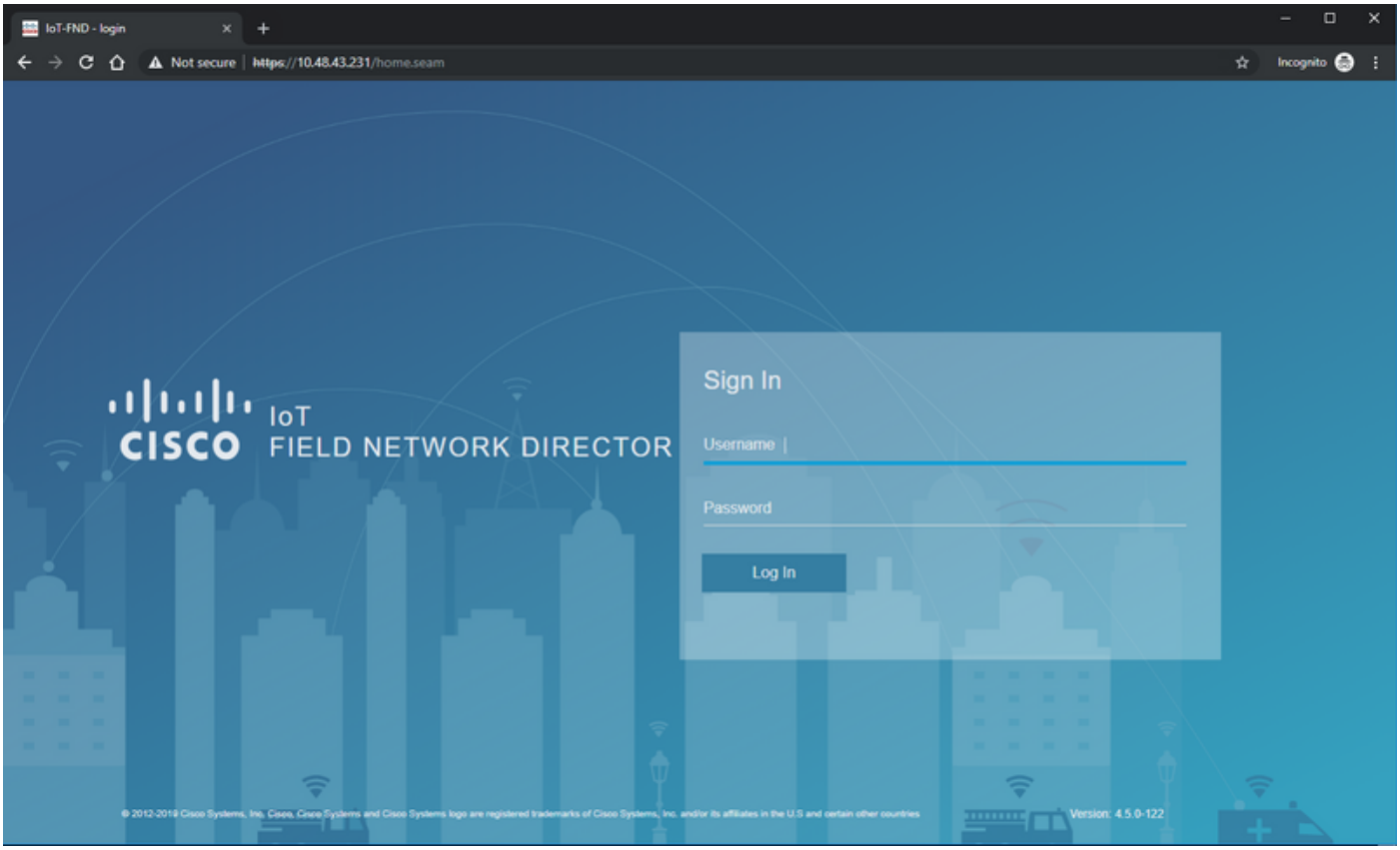
- nome de usuário: senha root: **cisco123**
- nome de usuário: senha Cisco: **C_sco123**

Etapa 3. O início de uma sessão com o usuário de Cisco e a senha e navegam aos **aplicativos > às ferramentas de sistema > aos ajustes > à rede.** Adicionar um perfil prendido e na aba do IPv4, ajustam o endereço IP desejado ou o DHCP segundo as indicações da imagem.



Etapa 4. Clique **aplicam** e firmam o ligar/desligar da conexão a fim assegurar-se de que os ajustes novos obtenham aplicados.

Neste momento, você deve poder navegar ao **FND GUI** com seu navegador e o IP address configurado segundo as indicações da imagem.



Etapa 5. Entre ao GUI com o uso do nome de usuário padrão e da senha: **raiz/root123**

Você é alertado mudar imediatamente a sua senha e reorientado então ao início de uma sessão uma vez mais.

Se tudo vai bem, você deve poder entrar com sua senha nova e poder navegar com o FND GUI.

Mais, PNP e o modo de programa demostrativo são descritos seguiram pela configuração de FND.

Sobre PNP

PNP é o método o mais atual de Cisco para fazer o desenvolvimento zero do toque (ZTD). Com o uso de PNP, um dispositivo pode inteiramente ser configurado e a necessidade de tocar na configuração manualmente não elevarará.

Para FND, com o uso de PNP, a necessidade de amarrar primeiramente o roteador é evitada. De fato, tudo que PNP faz, para reorientá-lo ao FND, em uma maneira segura, e busca a configuração da tira de bota.

Uma vez que a configuração da tira de bota esta presente no dispositivo, o resto do processo está continuado como com um dispositivo amarrado clássico.

Há umas maneiras diferentes de usar PNP:

- Com o serviço de Cisco PNP (devicehelper.cisco.com), com o uso de uma conta esperta. Permitido à revelia fora da fábrica em determinados dispositivos
- Com o uso da opção de DHCP 43 a fim fornecer o IP ou o hostname para conectar para a amarrar

- Manualmente ajustando o PNP-server na configuração

Para esta configuração, o IP do PNP-server é ajustado manualmente, que é o IP dos FND-server, e porta no dispositivo. Caso que você gostaria de fazer este com DHCP, você deve fornecer a informação como segue:

Para o ® do Cisco IOS, o DHCP-server deve ser configurado como segue:

```
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 em 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 as vendedor-encapsular-opções, você precisa de especificar estes string ascii:

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

Pode ser costurada como segue:

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

Mais informação a propósito de PNP com DHCP pode ser encontrada 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 de DHCP 43 no servidor DHCP de Cisco IOS®**

Sobre EasyMode

O modo fácil foi introduzido desde que FND 4.1, embora fosse chamado modo de programa demostrativo naquele tempo, e permite que você execute FND em uma maneira menos segura. Embora isto não seja recomendado para a produção, é uma boa maneira de obter começado.

Com o uso do modo fácil, você pode centrar-se sobre o PNP-processo, amarrando e configurando do roteador. Caso que algo não trabalha, você não precisa de suspeitar o acúmulo ou os Certificados do túnel.

Muda que ocorre quando você configurar FND para ser executado no modo fácil:

- Nenhuma necessidade para um roteador da extremidade principal (ELA) ou um túnel ao server FND.
- Nenhuma necessidade para uma instalação do Public Key Infrastructure (PKI) e um protocolo simple certificate enrollment (SCEP).
- Nenhuma necessidade para certificados de roteador, ponto confiável, e Certificados SSL.
- Toda a comunicação está ocorrendo sobre o HTTP em vez do HTTPS.

Mais informação em relação ao modo fácil pode ser encontrada 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 o modo fácil

Agora, você sabe o que o programa demonstrativo mode/PNP é e porque é usado neste contexto. Deixe-nos mudar a configuração FND a fim permiti-la:

No FND VM, que originou dos ÓVULOS arquive, conecte com o SSH e edite o **cgms.properties como segue**:

```
[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 últimas três linhas mudadas no arquivo de configuração.

- Linha 10: permite o modo fácil
- Linha 11: permite PNP
- Linha 12: ajusta o IP do FND-server para contactar

Depois que você muda o arquivo, reinicie o recipiente FND a fim adaptar as mudanças feitas:

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

Uma vez que reiniciado, o resto da configuração pode ser feito com o uso do GUI.

Prepare o CSV e adicionar o roteador a FND

Pôde soar um bit ilógico para adicionar neste momento o dispositivo do processo de configuração

mas infelizmente, as partes da configuração não estão disponíveis até que determinados tipos de dispositivo estejam adicionados.

Isto está feito a fim evitar o GUI para ser demasiado opressivamente enquanto os dispositivos diferentes introduzem opções diferentes.

Aqui, deixe-nos tentar adicionar um IR809 a FND.

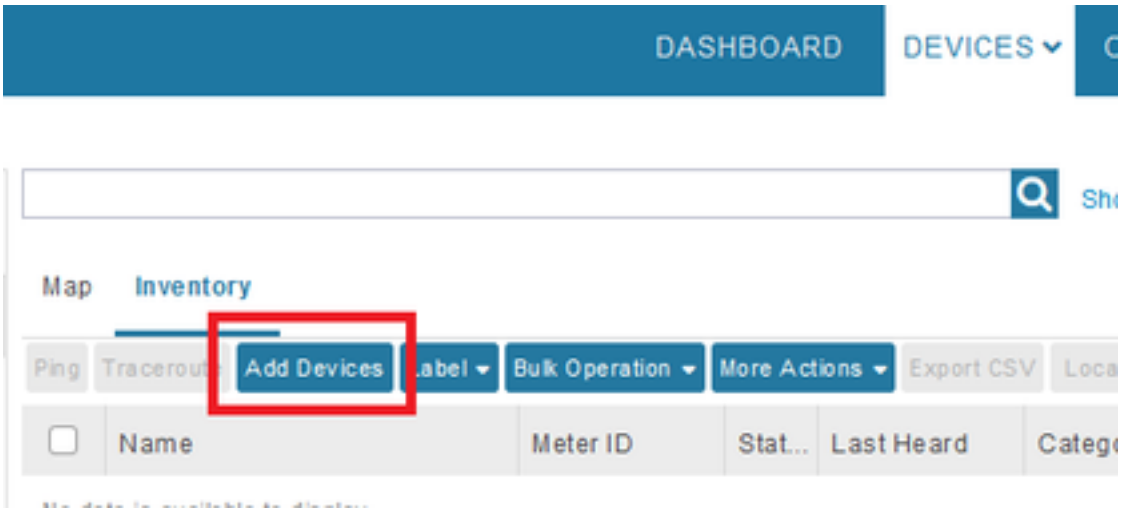
O CSV olha como segue:

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

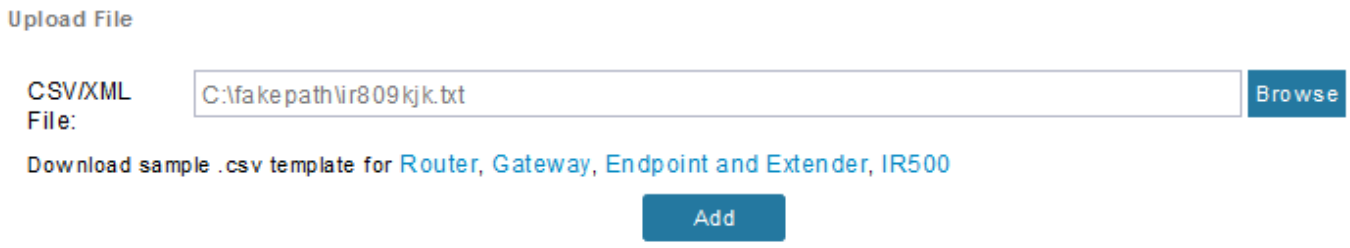
Os campos no CSV são:

- **deviceType**: ir800
- **eid**: PID e série junto com +
- **adminUsername**: este username será adicionado à configuração do roteador e mais tarde usado para terminar o processo de registro
- **adminPassword**: senha para o adminUsername
- **IP**: o endereço IP de Um ou Mais Servidores Cisco ICM NT ao substitue na configuração do dispositivo após o desenvolvimento

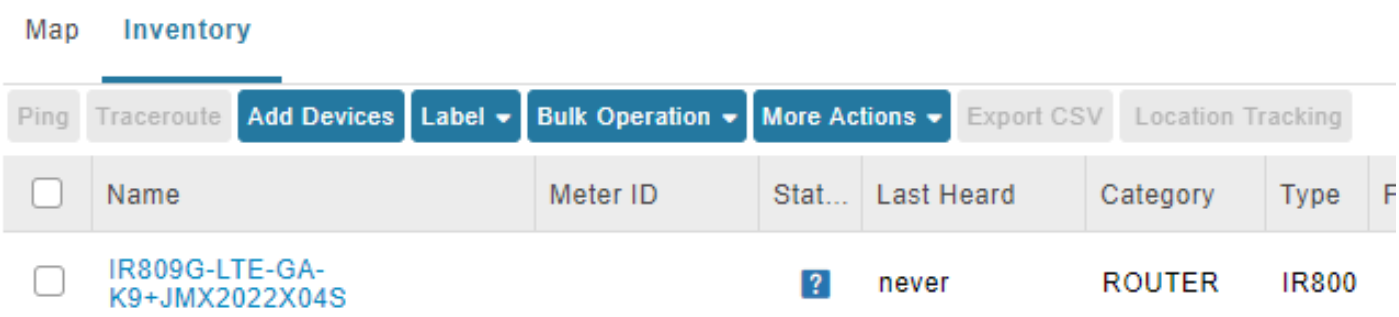
A fim adicionar este dispositivo, conecte ao GUI e navegue aos **dispositivos do > Add dos dispositivos > dos dispositivos > do inventário do campo** segundo as indicações da imagem.



No diálogo, especifique o lugar de seu arquivo CSV e o clique **adiciona** para adicionar-lo a FND segundo as indicações da imagem.



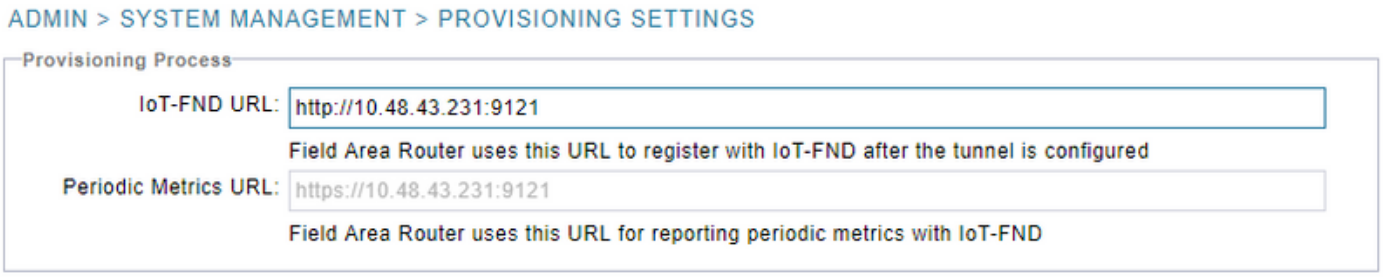
Se tudo vai bem, você deve ver o artigo da história para alistar “TERMINADO”. Depois que você fecha o diálogo, o dispositivo deve aparecer no inventário segundo as indicações da imagem.



Desde que o dispositivo do deviceType ir800 foi adicionado, os moldes e os grupos aplicáveis tornar-se-ão disponíveis no GUI neste momento.

Prepare os ajustes do abastecimento, o molde da tira de bota e o gabarito de configuração

Desde que FND é configurado para o modo de programa demostrativo, é precisado de mudar o abastecimento URL para usar pelo contrário o HTTP. Navegue a **Admin > ajustes do abastecimento** a fim fazer assim:



Mude o IoT-FND URL a **http:// <FND IP>:9121**

Em seguida, configurar dois moldes mínimos para amarrar e configuração.

Primeiro, chamado **gabarito de configuração de Roteador Tira de bota**, é a configuração que é empurrada para o roteador uma vez que pode contactar com sucesso FND com o uso de PNP.

Se PNP não é dentro uso, seria a configuração que é posta sobre o roteador manualmente ou na fábrica na altura do processo de auto desenvolvimento. Esta configuração contém apenas bastante informação para que o roteador comece o processo de registro em FND.

Segundo, chamado o gabarito de configuração, será a configuração que é adicionada à configuração atualmente sendo executado do dispositivo. De fato, pode-se ver como um incremento na configuração existente.

Na maioria dos casos, isto conduz a uma situação impar, assim que recomenda-se a primeiramente apaga todas as configurações no roteador antes que você o adicione a FND.

A fim ajustar o molde de Reprovision da fábrica do roteador, navegue **para configurar > abastecimento do túnel > configuração da tira de bota do roteador** e para substitui-la com o seguinte molde:

```
<#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>
```

A fim ajustar o gabarito de configuração. Navegue à **configuração > à configuração de dispositivo > editam o gabarito de configuração e adicionam este molde:**

```
<#-- 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
```

Este molde será a configuração running do roteador resultante. Tão toda a configuração específica para este grupo de configuração deve ser adicionada aqui.

O mais fácil é começar com este molde mínimo. Uma vez que bem sucedido, atualize e costure o molde de acordo com suas necessidades.

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

Prepare o IR800 para Provisioning/PNP

Se o dispositivo que você quer provision já contém uma configuração ou foi usado antes, é melhor apagar completamente a configuração do roteador antes que você a adicione a FND com PNP.

Obviamente, se este é um dispositivo novo, esta etapa pode ser saltada.

A maneira a mais fácil de fazer isto é com o uso do comando write erase e de 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
```

Após alguma hora, o IR800 deve voltar com a alerta 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!
```

Assegure-se de que não haja não mais sobras de uma tentativa precedente PNP/ZTD, é o melhor recrear o arquivo e o diretório e remover também a antes-registro-**configuração no** roteador:

```
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
```

Agora, você ou tem um dispositivo novo ou um dispositivo com uma configuração vazia, assim, se necessário, isto é o momento onde uma configuração mínima para que o roteador alcance FND pode ser aplicada.

Caso que você tem um DHCP-server, a maioria desta deve ir automaticamente.

A configuração manual do seguimento é 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 sibilo rápido foi executado a fim testar se o roteador podia alcançar FND com a configuração IP aplicada.

Provision o roteador IR800

Neste momento, todas as condições prévias estão completas e você pode iniciar o processo PNP. É feito manualmente nesta instância.

Em um ambiente de produção, mais provável, PNP será usado com opção de DHCP 43. Significa que uma vez que o roteador é ligado, ele recebe um IP e a configuração PNP e você pode saltar esta etapa e o seguinte.

A fim configurar manualmente PNP no IR800 sem DHCP, você precisa de especificar o destino para os pedidos, que serão o FND-server.

Isto pode ser feito como segue:

```
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 incorporar a linha que começa com “transporte”, o roteador começa o processo PNP e tentá-lo-á contactar FND no IP e na porta dados.

Se tudo vai bem, as passagens de dispositivo com estes:

- [UPDATING_ODM]: atualize os arquivos ODM (modelo de dados operacionais) no dispositivo para combinar com esses válidos para a versão atual FND
- [UPDATING_ODM_VERIFY_HASH]: verifique se os arquivos actualizados estão corretos
- [UPDATED_ODM]
- [COLLECTING_INVENTORY]: recolha a configuração atual e a informação do dispositivo
- [COLLECTED_INVENTORY]
- [VALIDATING_CONFIGURATION]: tente aplicar a configuração da configuração da tira de bota (o molde substituído de Reprovision da fábrica do roteador)
- [VALIDATED_CONFIGURATION]
- [PUSHING_BOOTSTRAP_CONFIG_FILE]: aplique 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 a configuração de inicialização
- [CONFIGURED_STARTUP_CONFIG]
- [APPLYING_CONFIG]: aplique a configuração de inicialização
- [APPLIED_CONFIG]
- [TERMINATING_BS_PROFILE]: pare de amarrar.

Você pode seguir o processo no FND server.log.

No GUI, você verá o dispositivo mover-se quando você navega a **inaudito > Boostrapping > amarrado**

Depois que amarrar é terminado, o roteador tem o molde substituído de Reprovision da fábrica do roteador e comporta-se como um dispositivo amarrado regular sem PNP.

Ou seja um perfil CGNA no IR800 tenta registrar-se com o server FND.

Verifique o estado 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 registrar-se com o FND após dez minutos. Você pode ver aquele nesta saída, nove minutos e trinta segundos permanecem antes que o roteador comece o processo de registro.

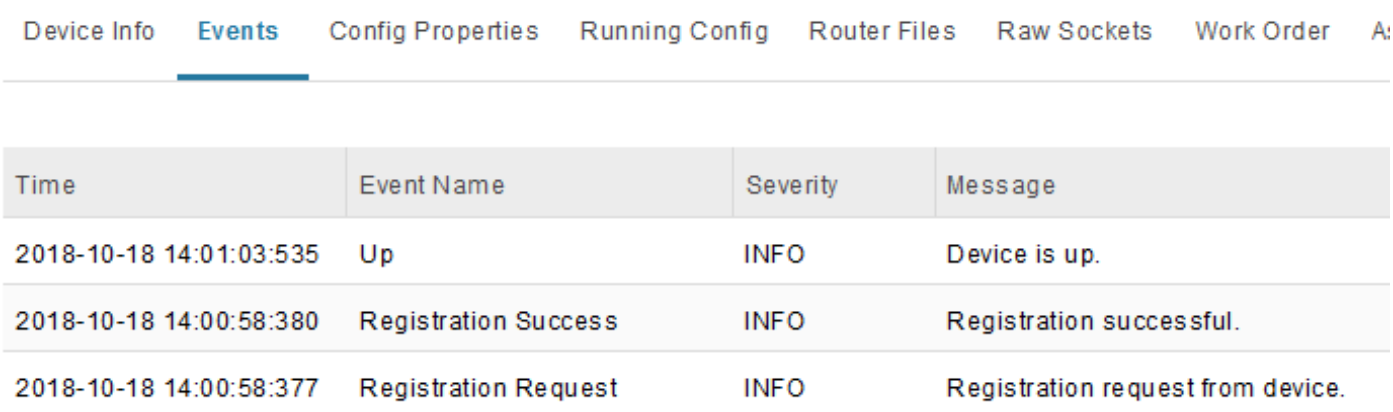
Você pode esperar o temporizador para terminar imediatamente ou executar manualmente o perfil do cg-nanômetro-**registro**:

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

Verificar

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

O dispositivo deve mover-se para o estado ASCENDENTE em FND segundo as indicações da imagem.



Troubleshooting

Esta seção fornece informações que você pode usar na solução de problemas de sua configuração.

A fim pesquisar defeitos o processo amarrando, verifique estes:

- Início de uma sessão do server FND: **/opt/fnd/logs/server.log**
- Aumente a verbosidade do início de uma sessão: **Os Admin > registrando > ajustes nivelados > roteador do log que amarra > debugam**
- Do console IR800: **mostre o pnp? ou debugar o pnp?**
- No FND GUI: **Dispositivos > inventário > dispositivo seleto > eventos**
- A maioria das edições nesta fase são relacionadas aos erros (da sintaxe) no molde de Reprovision da fábrica do roteador

A fim pesquisar defeitos o processo de registro, verifique estes:

- Início de uma sessão do server FND: **/opt/fnd/logs/server.log**
- Do console IR800:

  mostre o perfil-estado todo do cgnadebugar o registro do cgna?debugar o agente do wsma
- No FND GUI: **Dispositivos > inventário > dispositivo seleto > eventos**
- Verifique a Conectividade WSMA sobre o HTTP ao IR800 do FND VM
  URI usado por FND: http://10.48.43.231:80/wsma/execMétodo: POSTSegurança: **AUTH básico**