Configure Field Network Director para utilizar Plug and Play en IR800

Contenido

Introducción

Este documento describe cómo empezar con Field Network Director (FND) y Plug and Play (PNP) con el uso de un conjunto mínimo de componentes.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Experiencia con Linux y conocimiento para editar archivos de configuración en una máquina Linux
- Al menos uno de los routers soportados que será administrado por FND. Por ejemplo, IR809 o IR829. Acceso a la consolaVersión mínima de IOS® 15.7(3)M1
- Archivo OVA implementado en un hipervisor (por ejemplo: VMWare ESXi). El archivo OVA, si lo autoriza, puede descargarse de: https://software.cisco.com/download/home/286287993/type/286320249

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Archivo OVA para FND versión 4.5.0-122 (CISCO-IOTFND-V-K9-4.5.0-122.zip)
- VMWare ESX
- IR809 con IOS® versión 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

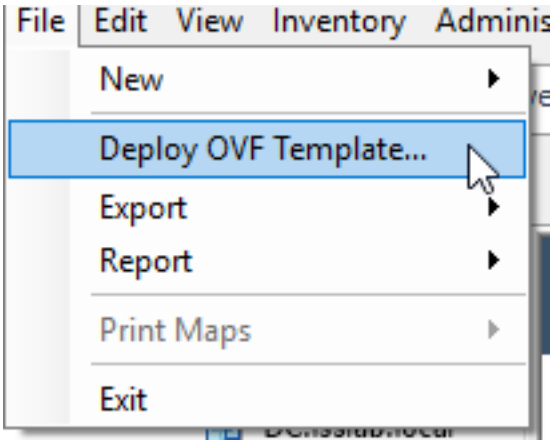
Dado que FND tiene muchas opciones de implementación diferentes, el objetivo es poder configurar una instalación mínima pero funcional para FND. Esta configuración puede servir como punto de partida para una mayor personalización y para agregar más funciones. La configuración que se explica aquí se basa en el uso de la instalación FND empaquetada para Open Virtual Appliance (OVA) como punto de partida y utiliza el modo sencillo para evitar la necesidad de infraestructura de clave pública (PKI) y aprovisionamiento de túneles. Utilice PNP para simplificar y agregar dispositivos a la instalación.

El resultado de esta guía no está destinado a ser utilizado en producción, ya que podría haber algunos riesgos de seguridad debido a la contraseña del texto del plan y a la ausencia de túneles y PKI.

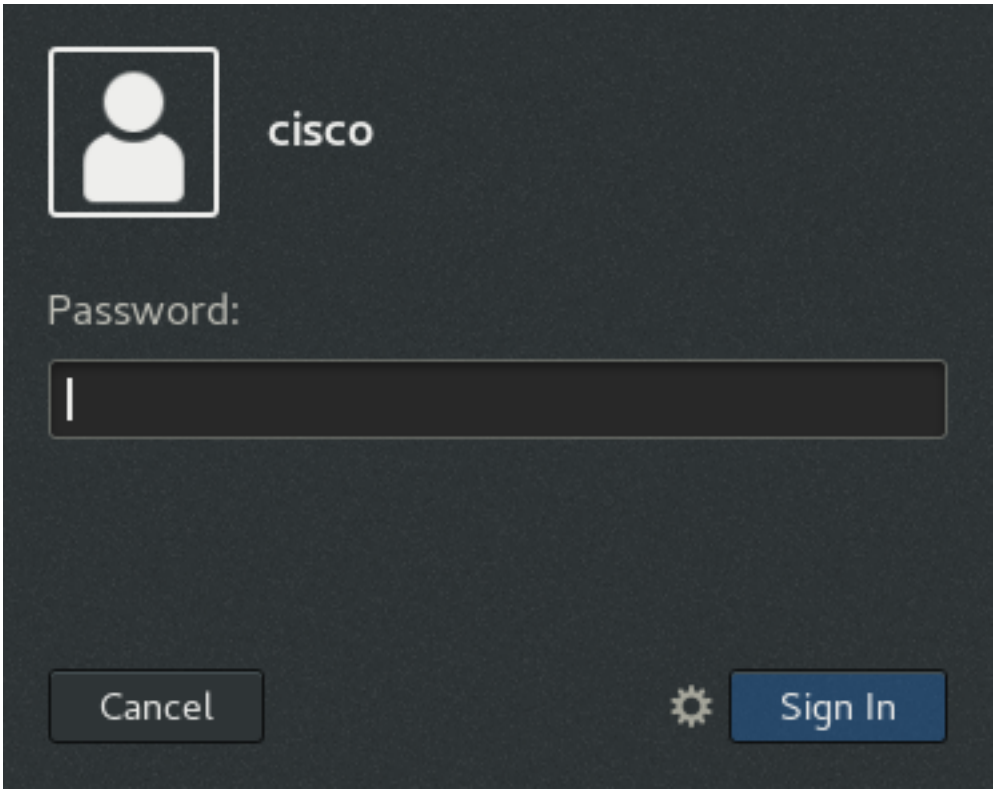
Configurar

Implementación y configuración del OVA FND

Paso 1. descargue e implemente el archivo OVA FND en su hipervisor. Por ejemplo para VMWare, esto se realizará a través de **File > Deploy OVF Template** como se muestra en la imagen.



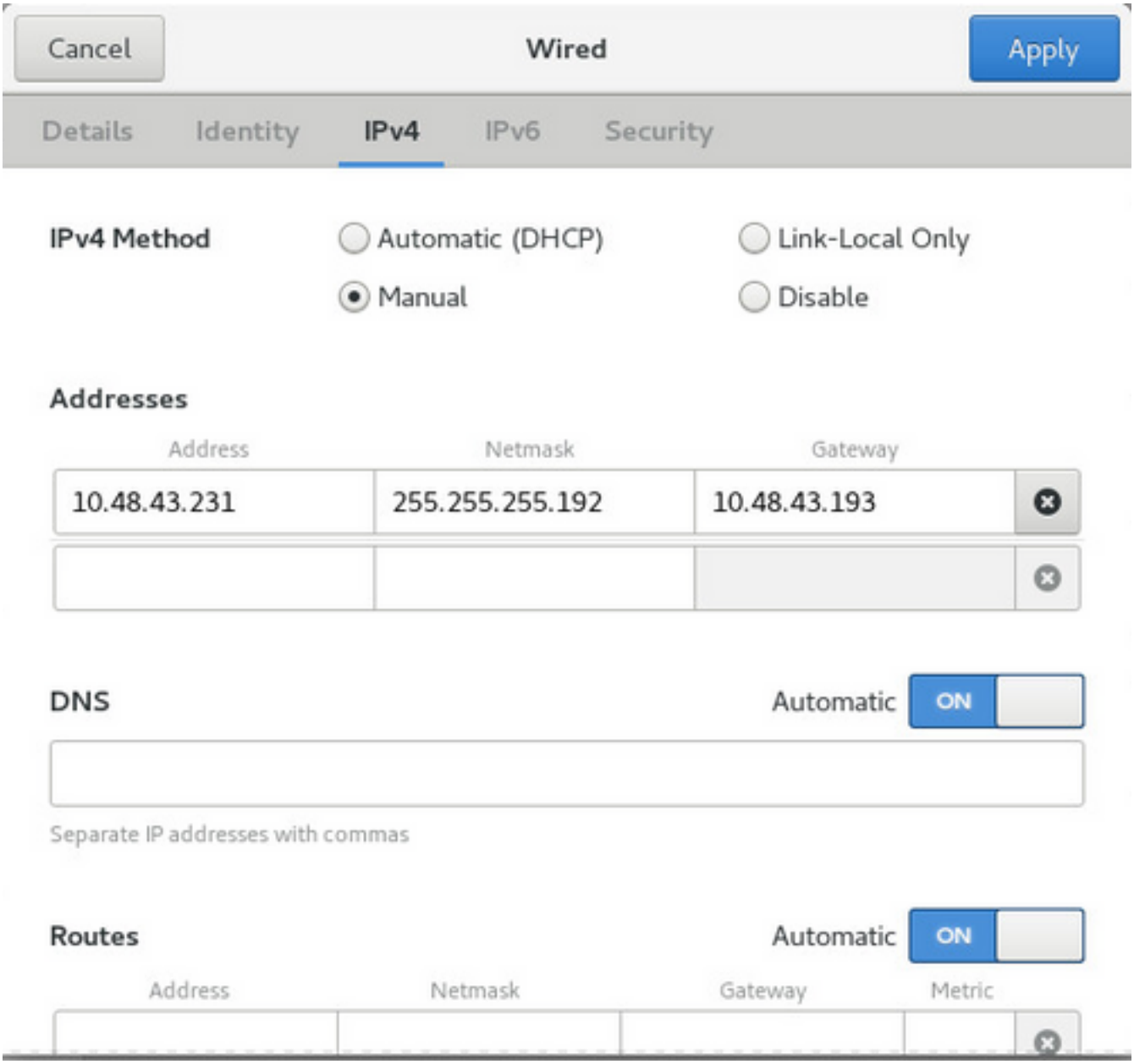
Paso 2. Una vez implementada, puede iniciar la máquina virtual y se le mostrará una pantalla de inicio de sesión, que se muestra en la imagen.



Las contraseñas predeterminadas para el archivo OVA son:

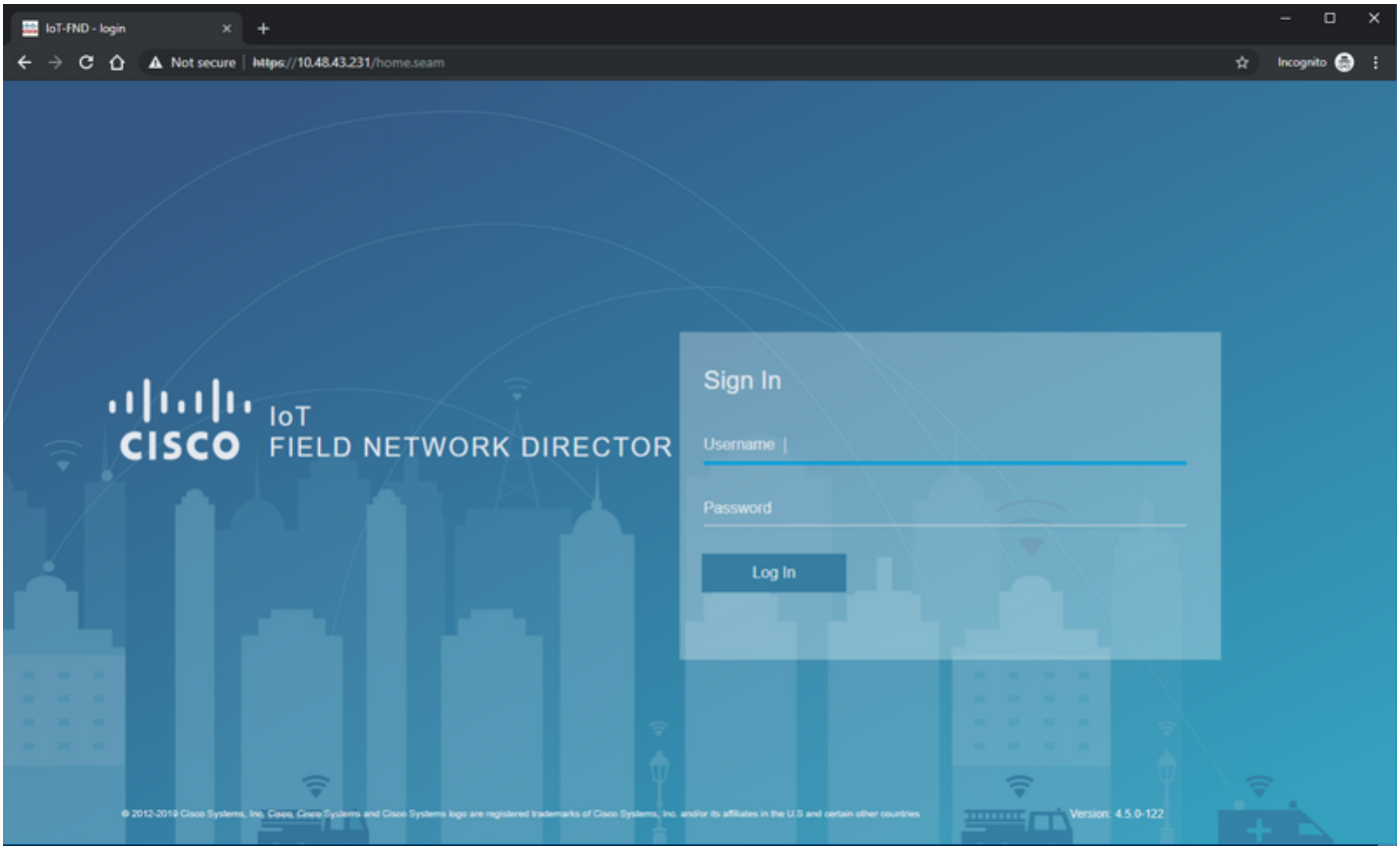
- nombre de usuario: contraseña raíz: **cisco123**
- nombre de usuario: contraseña de Cisco: **C_sco123**

Paso 3. Inicie sesión con el usuario y la contraseña de cisco y navegue hasta **Aplicaciones > Herramientas del sistema > Configuración > Red.** Agregue un perfil con cables y, en la ficha IPv4, establezca la dirección IP o DHCP que desee, como se muestra en la imagen.



Paso 4. Haga clic en **Aplicar** y active la conexión para asegurarse de que se apliquen los nuevos parámetros.

En este punto, debería poder navegar a la **GUI de FND** con su navegador y la dirección IP configurada como se muestra en la imagen.



Paso 5. Inicie sesión en la GUI con el uso del nombre de usuario y la contraseña predeterminados: **root / root123**

Se le solicitará que cambie la contraseña inmediatamente y luego se le redirigirá una vez más al inicio de sesión.

Si todo va bien, debería poder iniciar sesión con su nueva contraseña y navegar por la GUI de FND.

Además, se describen los modos PNP y de demostración seguidos de la configuración de FND.

Acerca de PNP

PNP es el método más actual de Cisco para realizar la implementación sin intervención (ZTD). Con el uso de PNP, un dispositivo puede configurarse completamente y no surgirá la necesidad de tocar la configuración manualmente.

Para FND, con el uso de PNP, se evita la necesidad de iniciar primero el router. De hecho, todo lo que PNP hace, lo redirige al FND de una manera segura, y obtiene la configuración de bootstrap.

Una vez que la configuración de bootstrap está presente en el dispositivo, el resto del proceso continúa como con un dispositivo bootstrap clásico.

Hay diferentes maneras de usar PNP:

- A través del servicio PNP de Cisco (devicehelper.cisco.com), con el uso de una cuenta inteligente. Habilitado de forma predeterminada fuera de la fábrica en determinados dispositivos
- Con el uso de la opción DHCP 43 para suministrar la IP o el nombre de host al cual

conectarse para bootstrapping
- Configurando manualmente el servidor PNP en la configuración

Para esta configuración, la IP del servidor PNP se establece manualmente, que es la IP del servidor FND, y el puerto en el dispositivo. En caso de que desee hacer esto con DHCP, debe proporcionar la siguiente información:

Para Cisco IOS®, el servidor DHCP debe configurarse de la siguiente manera:

```
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 en 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";
}
```

En esta configuración para la opción 43 o las opciones encapsuladas por el proveedor, debe especificar estas cadenas ASCII:

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

Se puede adaptar de la siguiente manera:

- 5 - Código de tipo DHCP 5
- A - Código de operación de función activa
- K4: protocolo de transporte HTTP
- B2 - El tipo de dirección IP del servidor PnP/TPS/FND es IPv4
- I10.48.43.231 - Dirección IP del servidor FND
- J9125 - Número de puerto 9125 (puerto para PNP en el servidor FND)

Puede encontrar más información con respecto a PNP con DHCP aquí: https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/guide/4_3/iot_fnd_ug4_3/sys_mgmt.html#31568 en la sección: **Configuración de la opción DHCP 43 en el servidor DHCP de Cisco IOS®**

Acerca de EasyMode

El modo sencillo se ha introducido desde el FND 4.1, aunque se llamaba modo de demostración en ese momento, y le permite ejecutar FND de una manera menos segura. Aunque no se recomienda para la producción, es una buena manera de empezar.

Con el uso del modo fácil, puede centrarse en el proceso PNP, bootstrapping y la configuración del router. En caso de que algo no funcione, no es necesario sospechar la acumulación o los certificados del túnel.

Cambios que se producen cuando se configura FND para que se ejecute en modo fácil:

- No es necesario un router de cabecera (HER) o un túnel para el servidor FND.
- No es necesario establecer una infraestructura de clave pública (PKI) ni un protocolo simple de inscripción de certificados (SCEP).
- No se necesitan certificados de router, punto de confianza y certificados SSL.
- Toda la comunicación se está produciendo a través de HTTP en lugar de HTTPS.

Puede encontrar más información sobre el modo sencillo aquí:

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

Configuración de FND para PNP y modo sencillo

Ahora, ya sabe qué es el modo de demostración/PNP y por qué se utiliza en este contexto. Cambiemos la configuración FND para habilitarla:

En la VM FND, que se originó en el archivo OVA, conéctese con SSH y edite **cgms.properties** de la siguiente manera:

```
[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
```

Las últimas tres líneas han cambiado en el archivo de configuración.

- Línea 10: habilita el modo sencillo
- Línea 11: habilita PNP
- Línea 12: establece la IP del servidor FND con el que se debe contactar

Después de cambiar el archivo, reinicie el contenedor FND para adaptar los cambios realizados:

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

Una vez reiniciada, el resto de la configuración se puede realizar con el uso de la GUI.

Prepare el CSV y agregue el router al FND

Puede parecer un poco ilógico agregar el dispositivo en este punto del proceso de configuración, pero lamentablemente, partes de la configuración no están disponibles hasta que se hayan

agregado ciertos tipos de dispositivos.

Esto se hace para evitar que la GUI sea demasiado abrumadora, ya que los diferentes dispositivos presentan diferentes opciones.

Aquí, intentemos agregar un IR809 al FND.

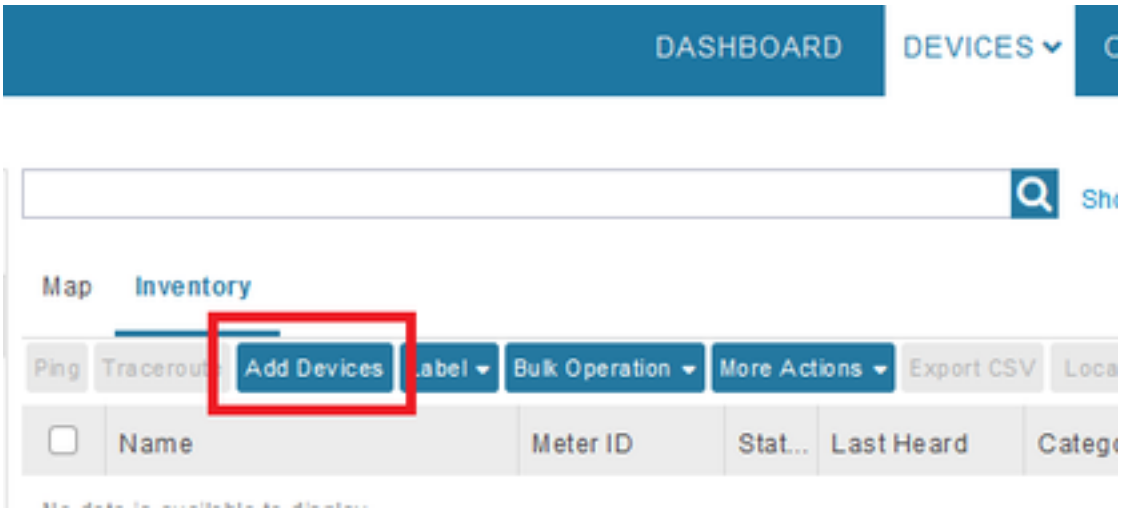
El CSV es el siguiente:

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

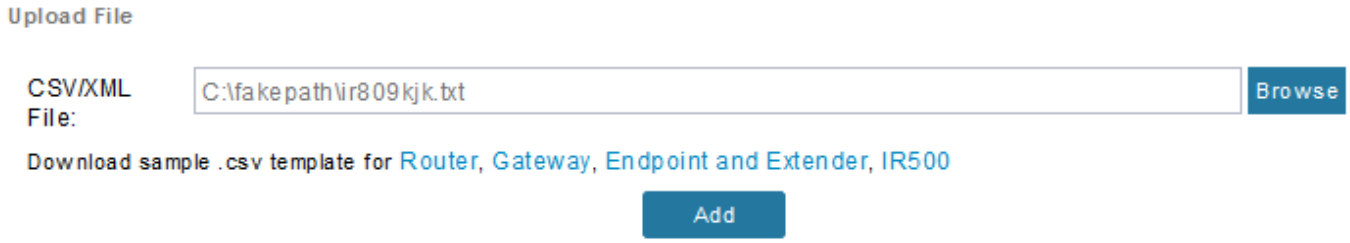
Los campos en el CSV son:

- **deviceType**: ir800
- **eid**: PID y serie junto con +
- **adminUsername**: este nombre de usuario se agregará a la configuración del router y posteriormente se utilizará para completar el proceso de registro
- **adminPassword**: contraseña para adminUsername
- **ip:** la dirección IP a sustituir en la configuración del dispositivo después de la implementación

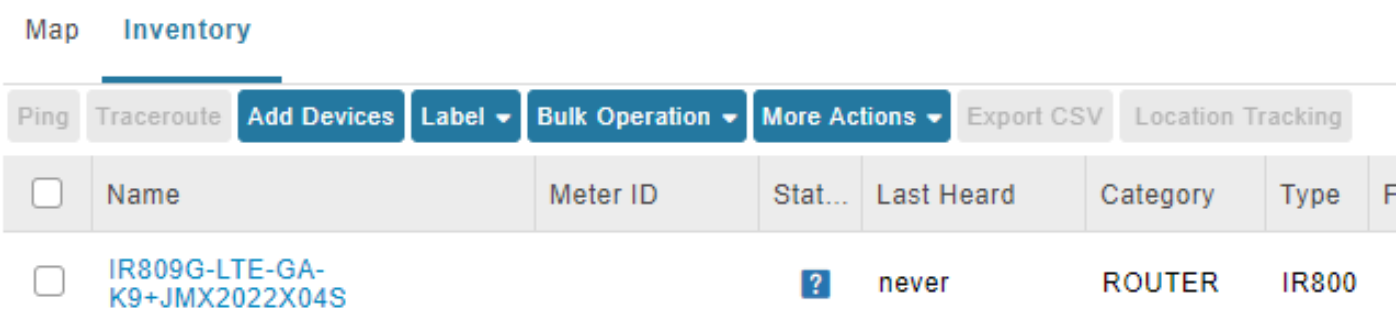
Para agregar este dispositivo, conéctese a la GUI y navegue hasta **Dispositivos > Dispositivos de campo > Inventario > Agregar dispositivos** como se muestra en la imagen.



En el diálogo, especifique la ubicación del archivo CSV y haga clic en **Agregar** para agregarlo a FND como se muestra en la imagen.



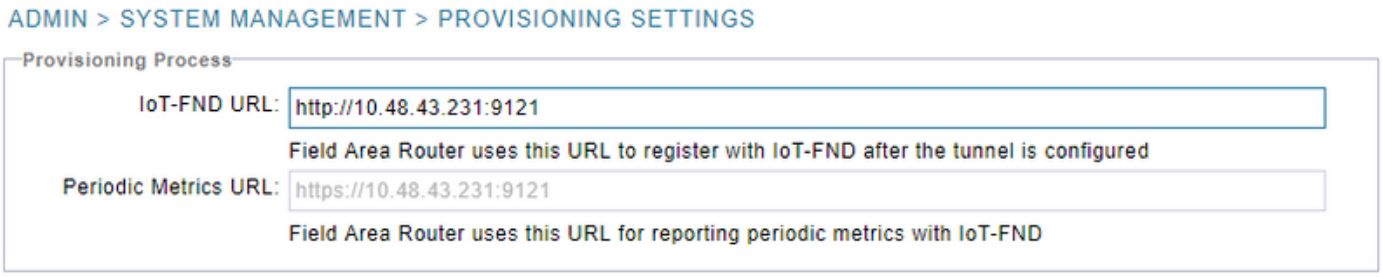
Si todo va bien, debería ver el elemento de historial como "COMPLETADO". Después de cerrar el diálogo, el dispositivo debe aparecer en el inventario como se muestra en la imagen.



Desde que se agregó el dispositivo deviceType ir800, las plantillas y grupos aplicables estarán disponibles en la GUI en este momento.

Prepare los parámetros de aprovisionamiento, la plantilla de arranque y la plantilla de configuración

Dado que FND está configurado para el modo de demostración, es necesario cambiar la URL de aprovisionamiento para utilizar HTTP en su lugar. Navegue hasta **Admin > Provisioning Settings** para hacerlo:



Cambie la URL de IoT-FND a **http://<FND IP>:9121**

A continuación, configure dos plantillas mínimas para bootstrapping y configuration.

La primera, llamada **plantilla Router Bootstrap Configuration**, es la configuración que se envía al router una vez que puede contactar con FND con éxito con el uso de PNP.

Si PNP no está en uso, sería la configuración que se coloca en el router manualmente o en la fábrica en el momento del proceso de bootstrap. Esta configuración contiene suficiente información para que el router inicie el proceso de registro en FND.

La segunda, denominada plantilla de configuración, será la configuración que se agrega a la configuración que se ejecuta actualmente en el dispositivo. De hecho, se puede ver como un incremento en la configuración existente.

En la mayoría de los casos, esto provoca una situación extraña, por lo que se recomienda borrar primero todas las configuraciones del router antes de agregarlo al FND.

Para configurar la plantilla de reaprovisionamiento de fábrica del router, navegue hasta **Configurar > Aprovisionamiento de túnel > Configuración de arranque del router** y reemplácelo por la siguiente plantilla:

```
<#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 establecer la plantilla de configuración. Navegue hasta **Config > Device Configuration > Edit Configuration Template y agregue esta plantilla:**

```
<#-- 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
```

Esta plantilla será la configuración en ejecución del router resultante. Por lo tanto, cualquier configuración específica para este grupo de configuración debe agregarse aquí.

Lo más fácil es comenzar con esta plantilla mínima. Una vez que tenga éxito, actualice y adapte la plantilla según sus necesidades.

En este punto, se realiza la configuración/preparación de FND y puede comenzar con la preparación del router.

Prepare el IR800 para el aprovisionamiento/PNP

Si el dispositivo que desea aprovisionar ya contiene una configuración o se ha utilizado anteriormente, es mejor borrar completamente la configuración del router antes de agregarlo al FND con PNP.

Obviamente, si se trata de un dispositivo nuevo, este paso se puede saltar.

La manera más fácil de hacerlo es con el uso del comando **write erase** y recargar el router con el uso de la consola.

```
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
```

Después de algún tiempo, el IR800 debe volver con el mensaje para ejecutar el diálogo de configuración inicial:

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

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


Press RETURN to get started!
```

Asegúrese de que no haya más restos de un intento anterior de PNP/ZTD, es mejor recrear el archivo y el directorio y quitar el **pre-registration-config** en el router también:

```
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
```

En este momento, ya sea que tenga un dispositivo nuevo o un dispositivo con una configuración vacía, por lo tanto, si es necesario, este es el momento en el que se puede aplicar una configuración mínima para que el router alcance FND.

En el caso de que tenga un servidor DHCP, la mayor parte de esto debe ir automáticamente.

Se selecciona la siguiente configuración manual en el 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 puede ver, se realizó un ping rápido para probar si el router pudo alcanzar FND con la configuración IP aplicada.

Aprovisionamiento del router IR800

En este momento, todos los requisitos previos están completos y usted puede iniciar el proceso PNP. Se realiza manualmente en este caso.

En un entorno de producción, lo más probable es que la PNP se utilice con la opción DHCP 43. Significa que una vez que se inicia el router, recibe una IP y la configuración PNP y puede saltarse este paso y el siguiente.

Para configurar manualmente el PNP en el IR800 sin DHCP, debe especificar el destino para las solicitudes, que serán el servidor FND.

Esto puede hacerse de la siguiente manera:

```
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
```

Tan pronto como ingrese la línea que comienza con "transport", el router inicia el proceso PNP e intentará contactar con FND en la IP y puerto dados.

Si todo va bien, el dispositivo pasa por lo siguiente:

- [UPDATING_ODM]: actualizar los archivos ODM (modelo de datos operativos) del dispositivo para que coincidan con los válidos para la versión actual de FND
- [UPDATING_ODM_VERIFY_HASH]: verifique si los archivos actualizados son correctos
- [UPDATED_ODM]
- [COLLECTING_INVENTORY]: recopile la configuración actual y la información del dispositivo
- [COLLECTED_INVENTORY]
- [VALIDATING_CONFIGURATION]: intente aplicar la configuración desde la configuración de bootstrap (plantilla sustituida de reaprovisionamiento de fábrica del router)
- [VALIDATED_CONFIGURATION]
- [PUSHING_BOOTSTRAP_CONFIG_FILE]: aplicar la configuración validada
- [PUSHING_BOOTSTRAP_CONFIG_VERIFY_HASH]: verifique si la configuración aplicada es correcta
- [PUSHED_BOOTSTRAP_CONFIG_FILE]
- [CONFIGURING_STARTUP_CONFIG]:escriba la configuración como configuración de inicio
- [CONFIGURED_STARTUP_CONFIG]
- [APPLYING_CONFIG]: apply the startup config
- [APPLIED_CONFIG]
- [TERMINATING_BS_PROFILE]: detener el bootstrapping.

Puede realizar un seguimiento del proceso en el archivo server.log de FND.

En la GUI, verá el dispositivo moverse cuando navegue a **Unheard > Boostrapping > Bootstrapped**.

Después de que se complete el bootstrapping, el router tiene la plantilla de reaprovisionamiento de fábrica del router sustituida y se comporta como un dispositivo normal de arranque sin PNP.

En otras palabras, un perfil CGNA en el IR800 intenta registrarse con el servidor FND.

Verifique el estado del 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
```

Con la configuración proporcionada, el dispositivo intentará registrarse en FND después de diez minutos. Puede ver que en esta salida quedan nueve minutos y treinta segundos antes de que el router inicie el proceso de registro.

Puede esperar a que el temporizador termine o ejecutar manualmente el perfil **cg-nms-register** inmediatamente:

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

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

El dispositivo debe pasar al estado UP en FND como se muestra en la imagen.

Device Info | Events | Config Properties | Running Config | Router Files | Raw Sockets | Work Order | A

Time	Event Name	Severity	Message
2018-10-18 14:01:03:535	Up	INFO	Device is up.
2018-10-18 14:00:58:380	Registration Success	INFO	Registration successful.
2018-10-18 14:00:58:377	Registration Request	INFO	Registration request from device.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Para resolver el problema del proceso de bootstrapping, verifique lo siguiente:

- Inicio de sesión del servidor FND: **/opt/fnd/logs/server.log**
- Aumente la verbosidad del inicio de sesión: **Admin > Logging > Log Level Settings > Router Bootstrapping > Debug**
- Desde la consola IR800: **show pnp ? o debug pnp ?**
- En la GUI de FND: **Dispositivos > Inventario > Seleccionar dispositivo > Eventos**
- La mayoría de los problemas en esta etapa están relacionados con errores (sintaxis) en la plantilla de reaprovisionamiento de fábrica del router

Para resolver los problemas del proceso de registro, verifique lo siguiente:

- Inicio de sesión del servidor FND: **/opt/fnd/logs/server.log**
- Desde la consola IR800:

  show cgna profile-state alldebug cgna logging ?debug wsma agent
- En la GUI de FND: **Dispositivos > Inventario > Seleccionar dispositivo > Eventos**
- Verifique la conectividad WSMA a través de HTTP al IR800 desde la VM FND
  URI utilizado por FND: http://10.48.43.231:80/wsma/execMétodo: POSTSeguridad: **autenticación básica**