Configure al director de la red del campo para utilizar el plug and play en IR800

Contenido

Introducción

Este documento describe cómo conseguir comenzado con el director de la red del campo (FND) y el plug and play (PNP) con el uso del conjunto mínimo de componentes.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Experiencia con Linux y el conocimiento para editar los archivos de configuración de ejecución en una máquina de Linux
- Por lo menos uno del Routers soportado que se manejará por FND. Por ejemplo IR809 o IR829. Acceso a la consolaVersión 15.7(3)M1 mínima IOS®
- Archivo de los HUEVOS desplegado a un hipervisor (por ejemplo: VMware ESXi). El archivo de los HUEVOS, si está dado derecho, puede ser descargado 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.

- Los HUEVOS clasifían para la versión 4.5.0-122 (CISCO-IOTFND-V-K9-4.5.0-122.zip) FND
- VMware ESX
- IR809 con la versión 15.8(3)M2 IOS®

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

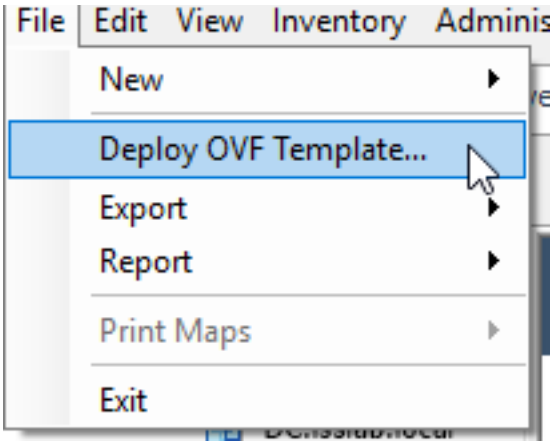
Puesto que FND tiene muchas diversas Opciones de instrumentación, la meta es poder configurar un mínimo pero el trabajo, instalación para FND. Esta configuración puede entonces servir como la punta del comienzo para el arreglo para requisitos particulares adicional y para agregar más características. La configuración explicada aquí está con el uso del dispositivo virtual abierto (HUEVOS) - instalación embalada FND mientras que la punta y ella del comienzo utiliza el modo fácil para evitar la necesidad del Public Key Infrastructure (PKI) y del aprovisionamiento del túnel. Utilice PNP, para simplificar y agregar los dispositivos a la instalación.

El resultado de esta guía no se piensa para ser utilizado en la producción mientras que pudo haber contraseña debida del plan-texto de algunos riesgos de seguridad y la ausencia de túneles y de PKI.

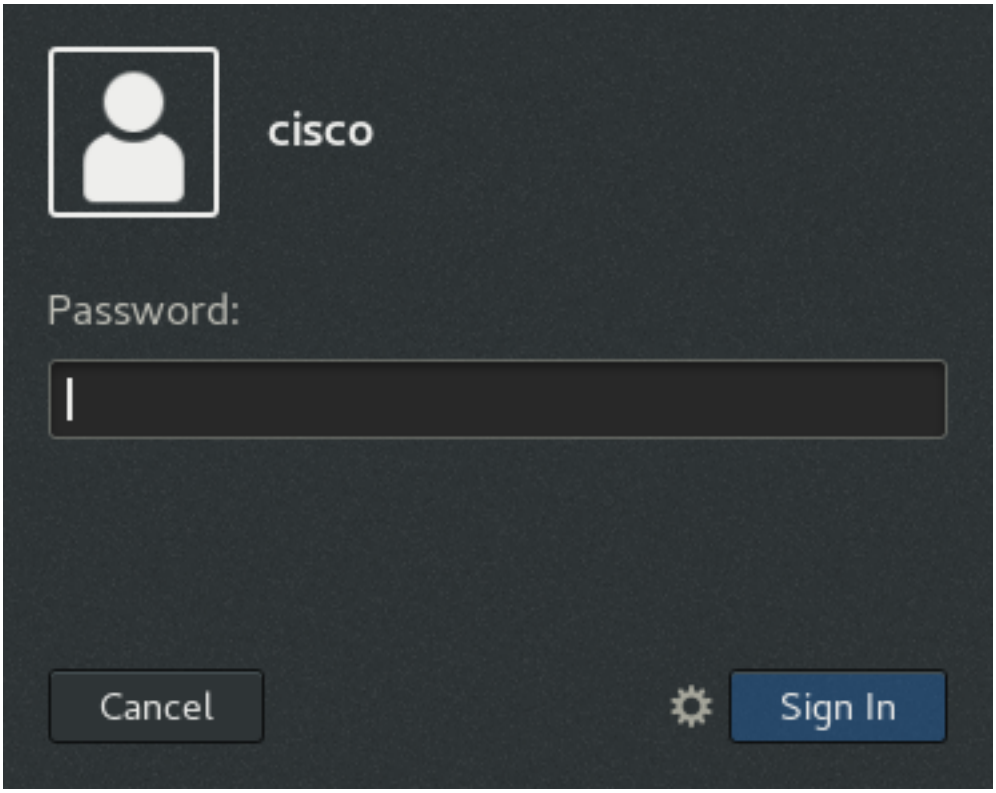
Configurar

Despliegue y configure los HUEVOS FND

La descarga del paso 1. y despliega los HUEVOS FND clasifía a su hipervisor. Por ejemplo para VMware, esto estará a través de **archivo > despliega la plantilla OVF** tal y como se muestra en de la imagen.



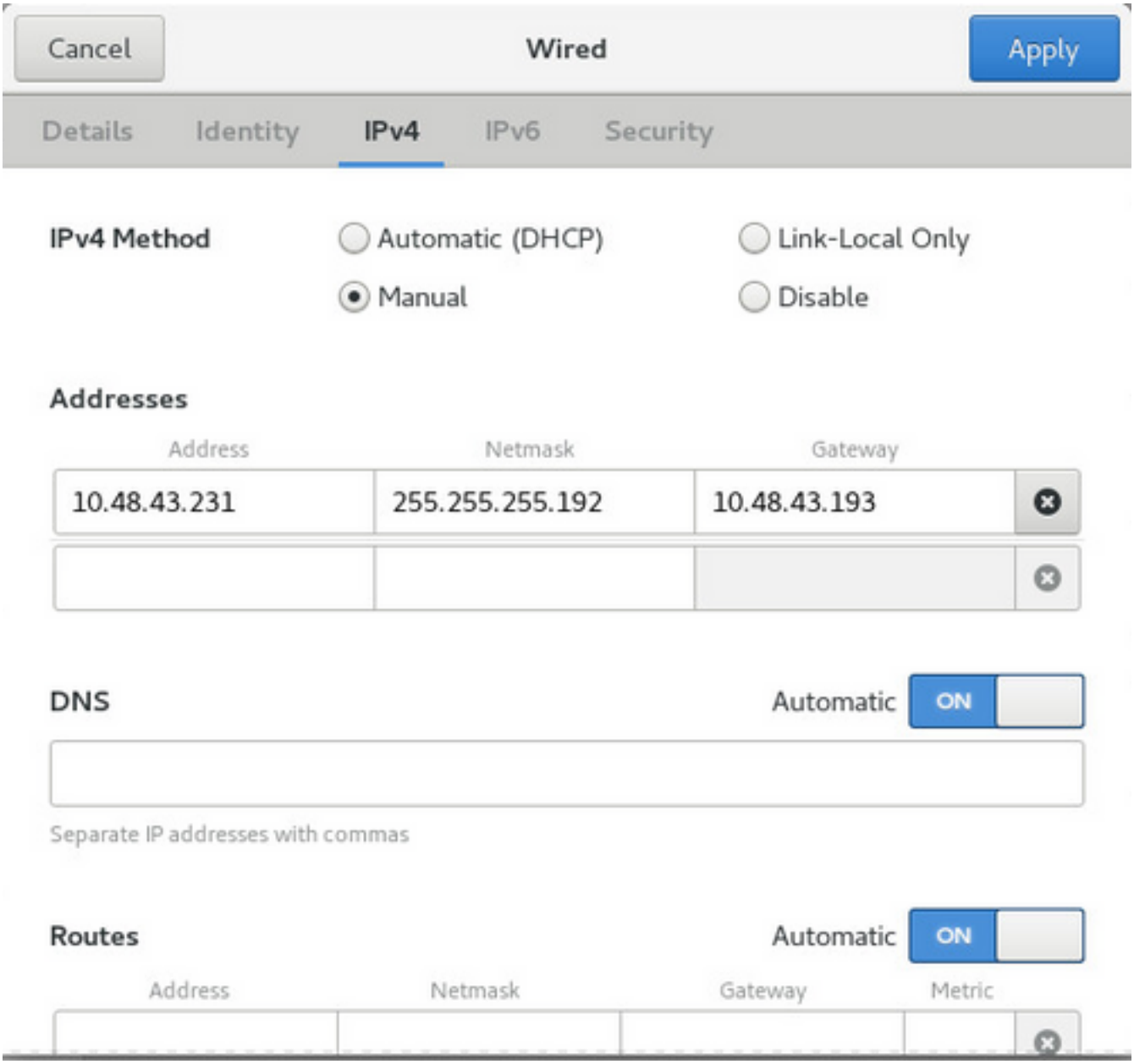
Paso 2. Una vez que consigue desplegado, usted puede comenzar el VM y se presenta con una pantalla de inicio de sesión, mostrada en la imagen.



Las contraseñas predeterminadas para el archivo de los HUEVOS son:

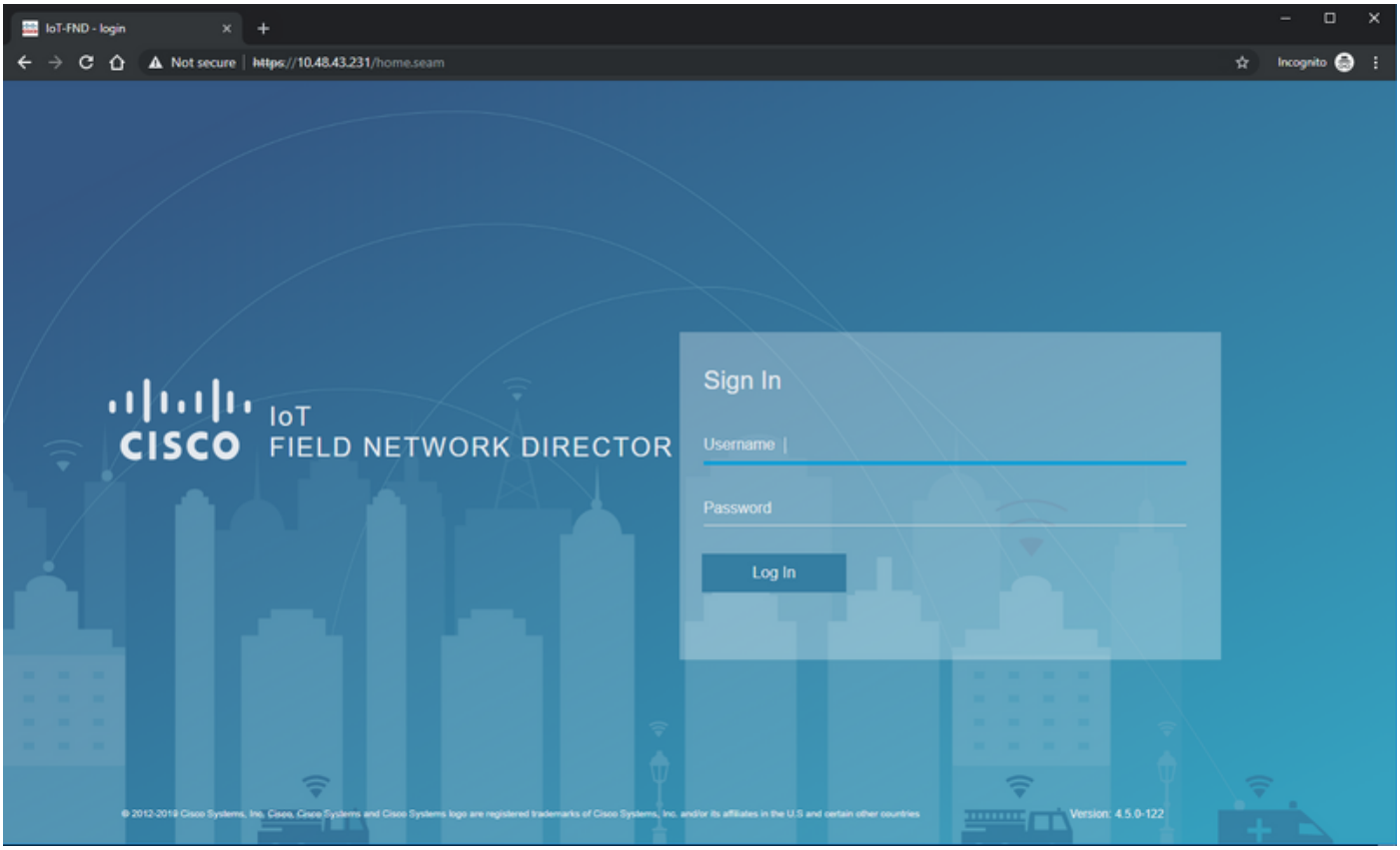
- nombre de usuario: contraseña de raíz: **cisco123**
- nombre de usuario: clave de Cisco: **C_sco123**

Paso 3. El login con el usuario de Cisco y la contraseña y navegan a las **aplicaciones > a las herramientas > a las configuraciones > a la red de sistema.** Agregue un perfil atado con alambre y en la lengueta del IPv4, fijan el IP Address deseado o el DHCP tal y como se muestra en de la imagen.



Paso 4. El tecleo **aplica** y conecta la conexión off/on para asegurarse de que las nuevas configuraciones consiguen aplicadas.

En este momento, usted debe poder navegar al **FND GUI** con su navegador y el IP address configurado tal y como se muestra en de la imagen.



Paso 5. Inicie sesión al GUI con el uso del nombre de usuario predeterminado y de la contraseña: **raíz/root123**

A le indican que cambie su contraseña inmediatamente y entonces reorientado al login una vez más.

Si va todo bien, usted debe poder iniciar sesión con su nueva contraseña y poder navegar con el FND GUI.

Además, describen PNP y al modo de demostración siguieron por la configuración de FND.

Sobre PNP

PNP es el método más actual de Cisco para hacer el despliegue cero del tacto (ZTD). Con el uso de PNP, un dispositivo puede ser de configuración completa y la necesidad de tocar la configuración no se presentará manualmente.

Para FND, con el uso de PNP, se evita la necesidad primero de atar al router con correa. De hecho, todo que lo hace PNP, reorientarlo al FND, de una manera segura, y trae la configuración de la carga inicial.

Una vez que la configuración de la carga inicial está presente en el dispositivo, el resto del proceso se continúa como con un dispositivo atado con correa clásico.

Hay maneras diferentes de utilizar PNP:

- Con el servicio de Cisco PNP (devicehelper.cisco.com), con el uso de una cuenta elegante. Por abandono fábrica habilitada de los en ciertos dispositivos
- Con el uso de la opción DHCP 43 para suministrar el IP o el nombre de host para conectar

con para atar con correa
- Manualmente fijando el PNP-servidor en la configuración

Para esta configuración, el IP del PNP-servidor se fija manualmente, que es el IP de los FND-servidores, y puerto en el dispositivo. En caso de que usted quisiera hacer esto con el DHCP, usted debe suministrar la información como sigue:

Para el ® del Cisco IOS, el DHCP-servidor debe ser configurado como sigue:

```
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 vendedor-encapsular-opciones, usted necesita especificar estas cadenas de ASCII:

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

Puede ser adaptada como sigue:

- 5 – Código 5 del tipo del DHCP
- A – Código de funcionamiento de las características activo
- K4 – Transport Protocol HTTP
- B2 – El tipo del dirección IP del servidor de PnP server/TPS/FND es IPv4
- I10.48.43.231 – Dirección IP del servidor FND
- J9125 – Número del puerto 9125 (puerto para PNP en el servidor FND)

Más información en lo que respecta a PNP con el DHCP se puede encontrar 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: **Opción DHCP 43 de la configuración en el servidor DHCP de Cisco IOS®**

Sobre EasyMode

El modo fácil se ha introducido puesto que FND 4.1, aunque fuera llamado modo de demostración en ese entonces, y permite que usted ejecute FND de una manera menos segura. Aunque esto no se recomiende para la producción, es una buena manera conseguir comenzado.

Con el uso del modo fácil, usted puede centrarse en el PNP-proceso, atando con correa y configurando del router. En caso de que algo no trabaje, usted no necesita sospechar la acumulación o los Certificados del túnel.

Cambia que ocurre cuando usted configura FND para ejecutarse en el modo fácil:

- Ninguna necesidad de un router del centro distribuidor (ELLA) o de un túnel al servidor FND.
- Ninguna necesidad de una configuración y de un protocolo simple certificate enrollment (SCEP) del Public Key Infrastructure (PKI).
- Ninguna necesidad de los certificados del router, del trustpoint, y de los Certificados SSL.
- Toda la comunicación está ocurriendo sobre el HTTP en vez del HTTPS.

Más información con respecto al modo fácil se puede encontrar 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 FND para PNP y el modo fácil

Ahora, usted sabe cuáles es la versión parcial de programa mode/PNP y porqué se utiliza en este contexto. Cambiemos la configuración FND para habilitarla:

En el FND VM, que originó de los HUEVOS clasifíe, conecte con SSH y edite el **cgms.properties como sigue**:

```
[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 tres líneas más recientes cambiadas en el archivo de configuración.

- Línea 10: habilita el modo fácil
- Línea 11: permisos PNP
- Línea 12: fija el IP del FND-servidor para entrar en contacto

Después de que usted cambie el archivo, recomience el envase 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 que está recomenzado, el resto de la configuración se puede hacer con el uso del GUI.

Prepare el CSV y agregue al router a FND

Puede ser que suene un bit ilógico agregar el dispositivo en este momento del proceso de

configuración pero desafortunadamente, las partes de la configuración no están disponibles hasta que hayan agregado a ciertos tipos de dispositivo.

Esto se hace para evitar el GUI para ser demasiado de forma aplastante mientras que diversos dispositivos introducen diversas opciones.

Aquí, intentemos agregar un IR809 a FND.

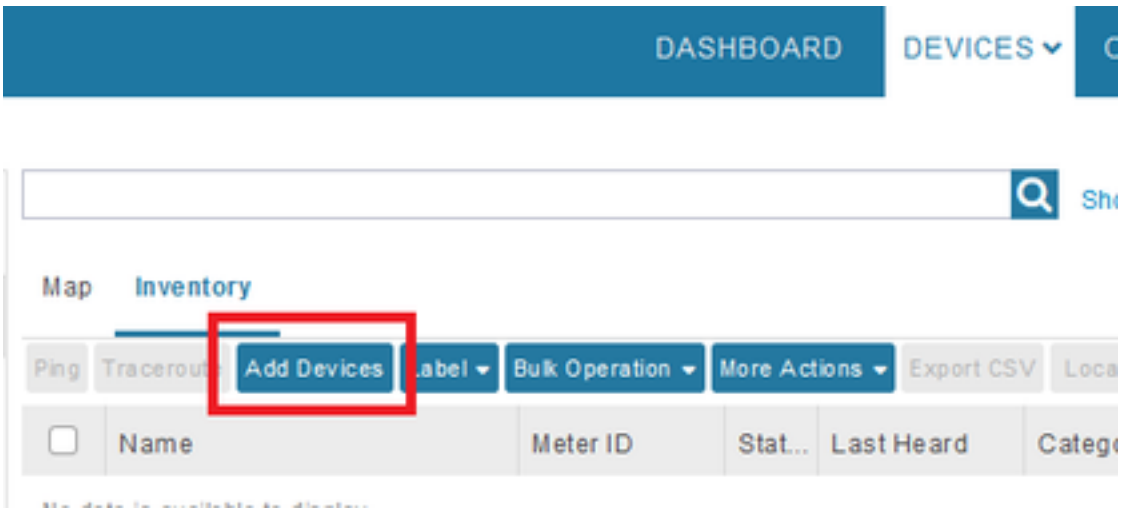
El CSV mira como sigue:

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

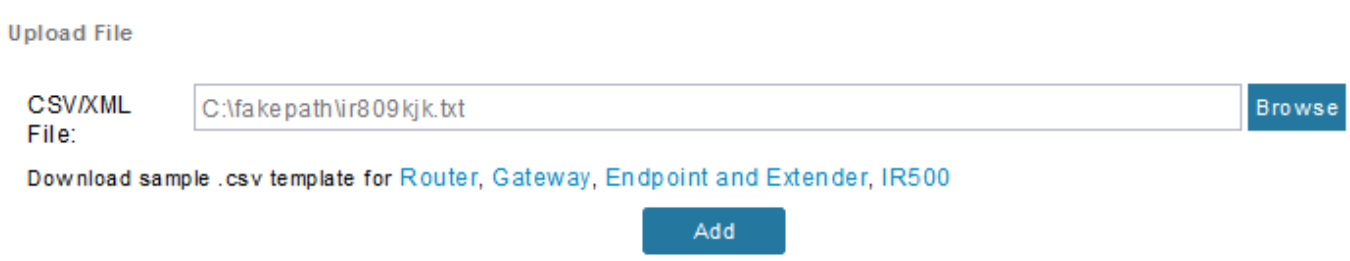
Los campos en el CSV son:

- **deviceType**: ir800
- **eid**: PID y serial así como +
- **adminUsername**: este nombre de usuario será agregado al router que los config y posterior serán utilizados para completar el proceso de inscripción
- **adminPassword**: contraseña para el adminUsername
- **IP**: la dirección IP al substitue en la configuración del dispositivo después del despliegue

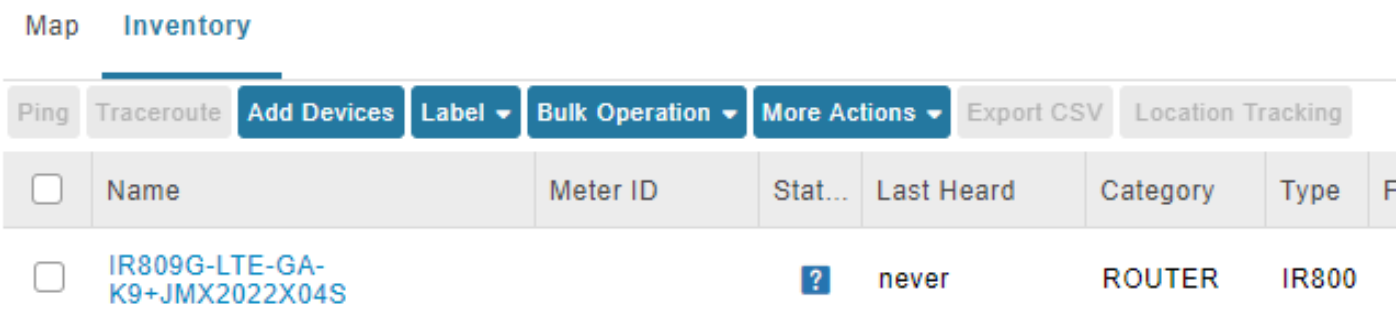
Para agregar este dispositivo, conecte con el GUI y navegue a los **dispositivos > a los dispositivos del campo > a los dispositivos del inventario > Add** tal y como se muestra en de la imagen.



En el diálogo, especifique la ubicación de su archivo CSV y el tecleo **agrega** para agregarla a FND tal y como se muestra en de la imagen.



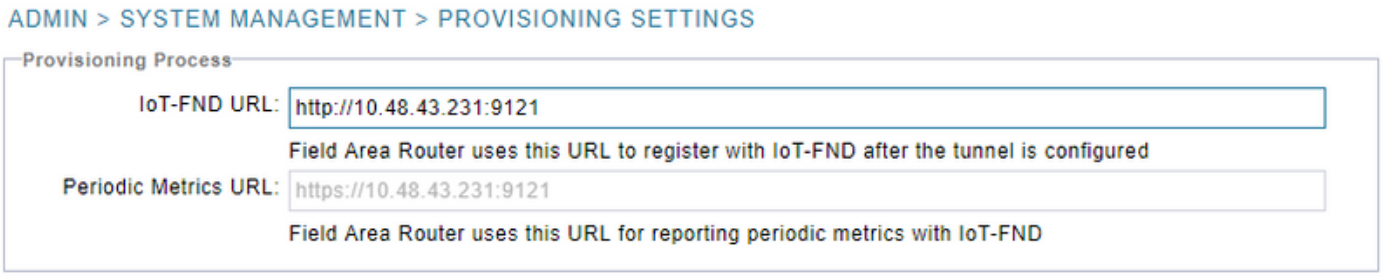
Si va todo bien, usted debe ver el elemento del historial para enumerar “COMPLETADO”. Después de que usted cierre el diálogo, el dispositivo debe aparecer en el inventario tal y como se muestra en de la imagen.



Puesto que el dispositivo del deviceType ir800 fue agregado, las plantillas y los grupos aplicables estarán disponibles en el GUI en este momento.

Prepare las configuraciones del aprovisionamiento, la plantilla de la carga inicial y la plantilla de configuración

Puesto que FND se configura para el modo de demostración, es necesario cambiar el URL de disposición para utilizar el HTTP en lugar de otro. Navegue a **Admin > las configuraciones del aprovisionamiento** para hacer tan:



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

Después, configure dos plantillas mínimas para atar con correa y la configuración.

Primer, llamado **plantilla de configuración de Router Bootstrap**, es la configuración que se avanza al router que puede una vez entrar en contacto con éxito FND con el uso de PNP.

Si PNP es parado, sería la configuración que se pone en el router manualmente o en la fábrica a la hora del proceso de la imagen de arranque. Esta configuración contiene la información bastante para que el router comience el proceso de inscripción en FND.

Segundo, llamado la plantilla de configuración, será la configuración que se agrega a la configuración actualmente que se ejecuta del dispositivo. De hecho, puede ser visto como incremento en la configuración existente.

En la mayoría de los casos, esto lleva a una situación impar, así que se recomienda a primero borra todas las configuraciones en el router antes de que usted lo agregue a FND.

Para fijar la plantilla de Reprovision de la fábrica del router, navegue **para configurar > aprovisionamiento del túnel > configuración de la carga inicial del router** y para substituirla por la plantilla siguiente:

```
<#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 fijar la plantilla de configuración. Navegue a los **Config > a la configuración del dispositivo > editan la plantilla de configuración y agregan 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 corriente del router resultante. Tan cualquier configuración específica para este grupo de configuración se debe agregar aquí.

El más fácil es comenzar con esta plantilla mínima. Una vez que es acertado, ponga al día y adapte la plantilla según sus necesidades.

En este momento, la configuración/la preparación de FND se hace y usted puede comenzar con la preparación del router.

Prepare el IR800 para Provisioning/PNP

Si el dispositivo que usted quiere provision ya contiene una configuración o se ha utilizado antes, es mejor borrar totalmente la configuración del router antes de que usted la agregue a FND con PNP.

Obviamente, si esto es un nuevo dispositivo, este paso puede ser saltado.

La manera más fácil de hacer esto está con el uso del comando write erase y de recargar al 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 una cierta hora, el IR800 debe volverse con el prompt para funcionar con 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 que no haya restos de una tentativa anterior PNP/ZTD, es el mejor reconstruir el archivo y el directorio y quitar los antes-registro-**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
```

Ahora, usted o tiene un nuevo dispositivo o un dispositivo con una configuración vacía, así pues, si es necesario, esto es el momento donde una configuración mínima para que el router alcance FND puede ser aplicada.

En caso de que usted tenga un DHCP-servidor, la mayor parte de éste debe ir automáticamente.

La configuración manual del siguiente se selecciona 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 usted ve, un ping rápido fue realizado para probar si el router podía alcanzar FND con la configuración IP aplicada.

Provision al router IR800

En este momento, todos los requisitos previos son completos y usted puede iniciar el proceso PNP. Es manualmente hecho en este caso.

En un entorno de producción, más probable, PNP será utilizado con la opción DHCP 43. Significa que una vez que encienden al router, él recibe un IP y la configuración PNP y usted puede saltar este paso y el siguiente.

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

Esto puede ser hecha como sigue:

```
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 usted ingrese la línea que comienza con el “transporte”, el router comienza el proceso PNP e intentará entrar en contacto FND en el IP dado y virar hacia el lado de babor.

Si va todo bien, los pasos de dispositivo con éstos:

- [UPDATING_ODM]: ponga al día los archivos ODM (modelo de datos de funcionamiento) en el dispositivo para hacer juego con los que está válidos para la versión actual FND
- [UPDATING_ODM_VERIFY_HASH]: marque si los archivos actualizados están correctos
- [UPDATED_ODM]
- [COLLECTING_INVENTORY]: recoja la configuración actual y la información del dispositivo
- [COLLECTED_INVENTORY]
- [VALIDATING_CONFIGURATION]: intente aplicar la configuración de los config de la carga inicial (la plantilla substituida de Reprovision de la fábrica del router)
- [VALIDATED_CONFIGURATION]
- [PUSHING_BOOTSTRAP_CONFIG_FILE]: aplique la configuración validada
- [PUSHING_BOOTSTRAP_CONFIG_VERIFY_HASH]: marque si la configuración aplicada está correcta
- [PUSHED_BOOTSTRAP_CONFIG_FILE]
- [CONFIGURING_STARTUP_CONFIG]: escriba la configuración como configuración de inicialización
- [CONFIGURED_STARTUP_CONFIG]
- [APPLYING_CONFIG]: aplique la configuración de inicialización
- [APPLIED_CONFIG]
- [TERMINATING_BS_PROFILE]: pare el atar con correa.

Usted puede seguir el proceso en el FND server.log.

En el GUI, usted verá el dispositivo moverse cuando usted navega a **inaudito > Boostrapping > atado con correa**

Después de que se complete el atar con correa, el router tiene la plantilla substituida de Reprovision de la fábrica del router y se comporta como un dispositivo atado con correa regular sin PNP.

Es decir un perfil CGNA en el IR800 intenta registrarse con el servidor FND.

Marque el estatus 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 con FND después de diez minutos. Usted puede ver eso en esta salida, nueve minutos y sigue habiendo treinta segundos antes de que el router comience el proceso de inscripción.

Usted puede esperar el temporizador para acabar o para ejecutar manualmente el perfil del CG-nanómetro-**registro** inmediatamente:

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

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

El dispositivo debe moverse al estatus ASCENDENTE en FND tal y como se muestra en de 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.

Troubleshooting

Esta sección brinda información que puede utilizar para la solución de problemas en su configuración.

Para resolver problemas el proceso que ata con correa, marque éstos:

- Login del servidor FND: **/opt/fnd/logs/server.log**
- Aumente la verbosidad del login: **Admin > registro > configuraciones llanas > router del registro que ata con correa > debug**
- De la consola IR800: **¿muestre el pnp? ¿o pnp del debug?**
- En el FND GUI: **Dispositivos > inventario > dispositivo selecto > Events**
- La mayor parte de los problemas en esta etapa se relacionan con los errores (del sintaxis) en la plantilla de Reprovision de la fábrica del router

Para resolver problemas el proceso de inscripción, marque éstos:

- Login del servidor FND: **/opt/fnd/logs/server.log**
- De la consola IR800:

  muestre el perfil-estado todo del cgna¿haga el debug del registro del cgna?haga el debug del agente del wsma
- En el FND GUI: **Dispositivos > inventario > dispositivo selecto > Events**
- Conectividad del control WSMA sobre el HTTP al IR800 del FND VM
  URI utilizó por FND: http://10.48.43.231:80/wsma/execMétodo: POSTSeguridad: **auth básico**