Konfigurieren von Field Network Director zur Verwendung von Plug and Play auf dem IR800

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie mit Field Network Director (FND) und Plug and Play (PNP) beginnen und dabei mindestens eine Reihe von Komponenten verwenden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Erfahrung mit Linux und Wissen, um laufende Konfigurationsdateien auf einem Linux-Computer zu bearbeiten
- Mindestens einer der unterstützten Router wird vom FND verwaltet. Beispiel: IR809 oder IR829. KonsolenzugriffIOS® Mindestversion 15.7(3)M1
- OVA-Datei wird auf einem Hypervisor bereitgestellt (Beispiel: VMWare ESXi). Die OVA-Datei kann heruntergeladen werden (falls vorhanden) unter: https://software.cisco.com/download/home/286287993/type/286320249

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und

Hardwareversionen:

- OVA-Datei für die FND-Version 4.5.0-122 (CISCO-IOTFND-V-K9-4.5.0-122.zip)
- VMWare ESX
- IR809 mit IOS® Version 15.8(3)M2

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

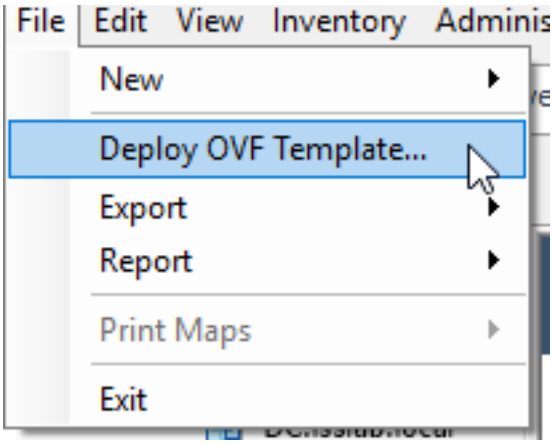
Da FND über viele verschiedene Bereitstellungsoptionen verfügt, soll eine minimale, aber funktionierende Installation für FND eingerichtet werden können. Diese Konfiguration kann dann als Ausgangspunkt für weitere Anpassungen dienen und zusätzliche Funktionen hinzufügen. Die hier beschriebene Konfiguration wird mit der Open Virtual Appliance (OVA)-FND-Installation als Startpunkt verwendet. Der einfache Modus verhindert die Bereitstellung von Public Key Infrastructure (PKI) und Tunneln. Verwenden Sie PNP, um die Installation zu vereinfachen und Geräte hinzuzufügen.

Das Ergebnis dieses Leitfadens ist nicht für die Verwendung in der Produktion vorgesehen, da es aufgrund von Plan-Text-Passwörtern und dem Fehlen von Tunneln und PKI möglicherweise einige Sicherheitsrisiken geben kann.

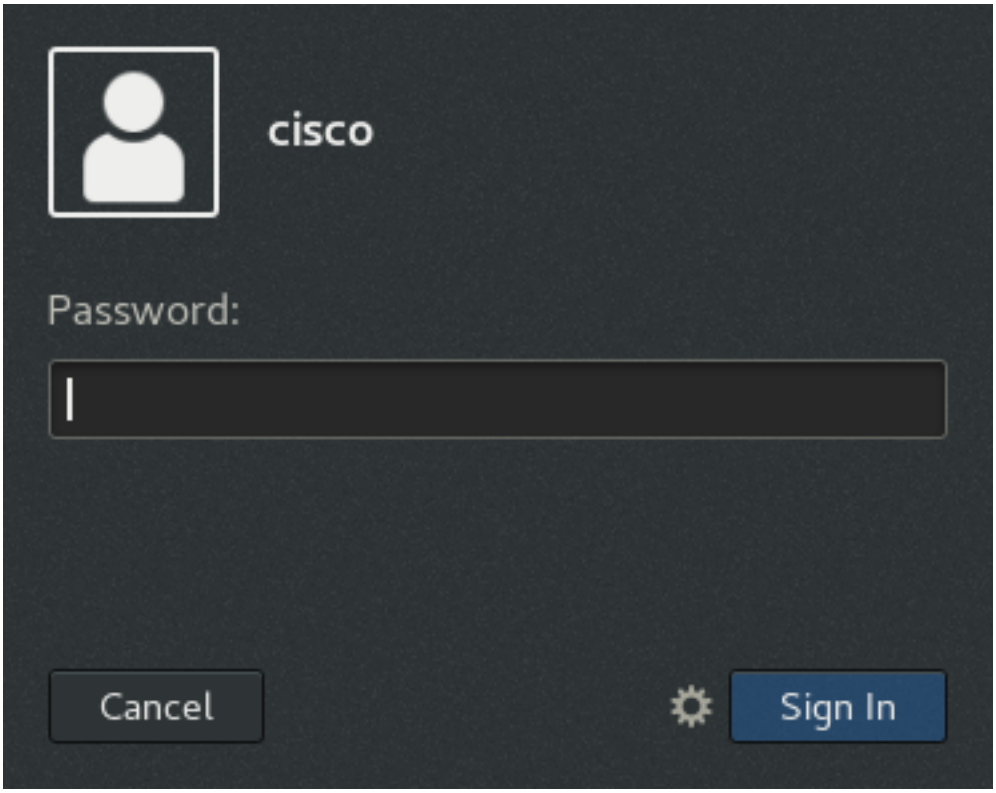
Konfigurieren

Bereitstellung und Konfiguration der FND OVA

Schritt 1: Laden Sie die FND OVA-Datei herunter, und stellen Sie sie auf Ihrem Hypervisor bereit. Für VMWare erfolgt dies beispielsweise über **Datei > OVF-Vorlage bereitstellen** wie im Bild gezeigt.



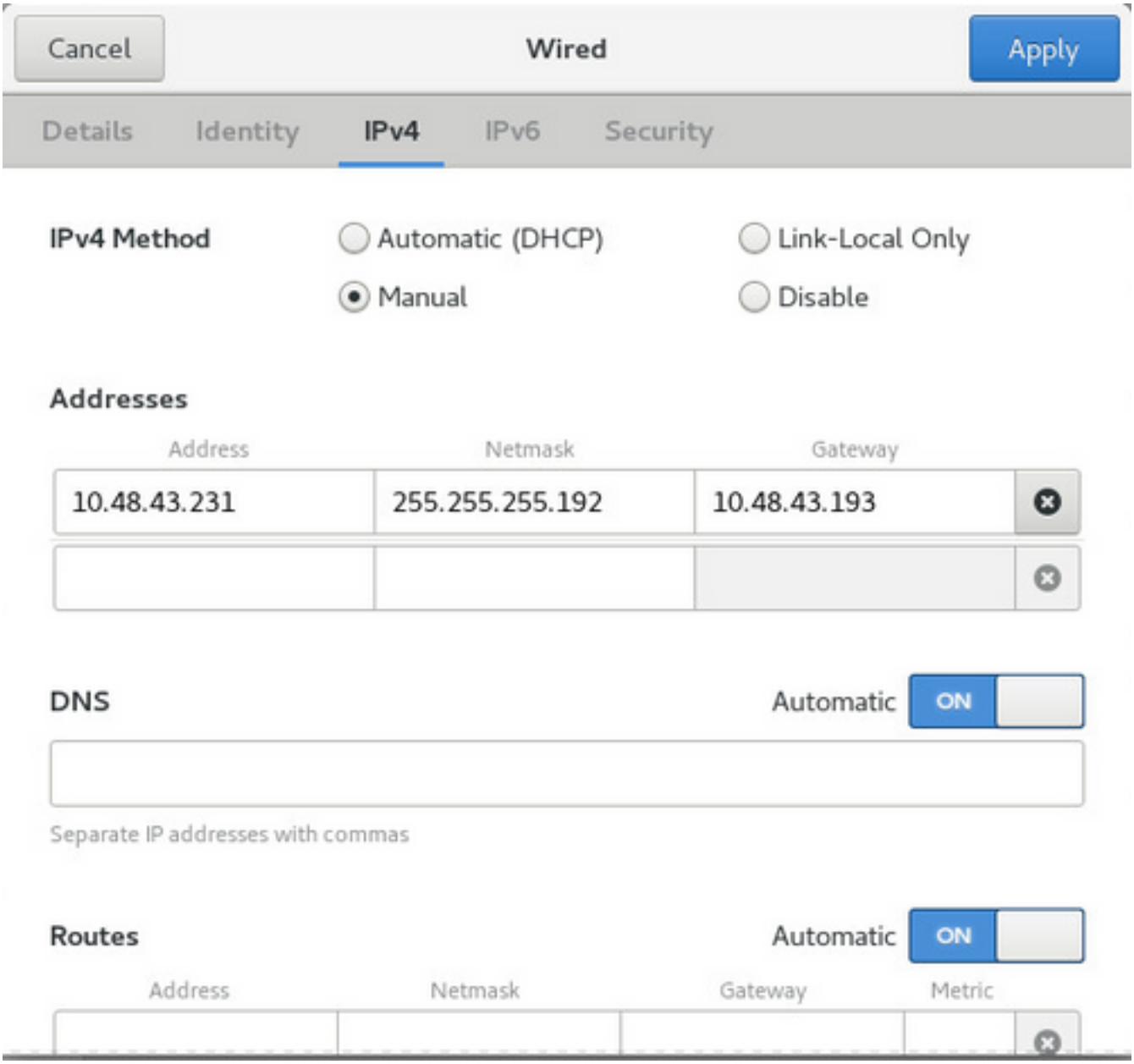
Schritt 2: Nach der Bereitstellung können Sie das virtuelle System starten. Es wird ein Anmeldebildschirm angezeigt, der im Abbild angezeigt wird.



Die Standardkennwörter für die OVA-Datei sind:

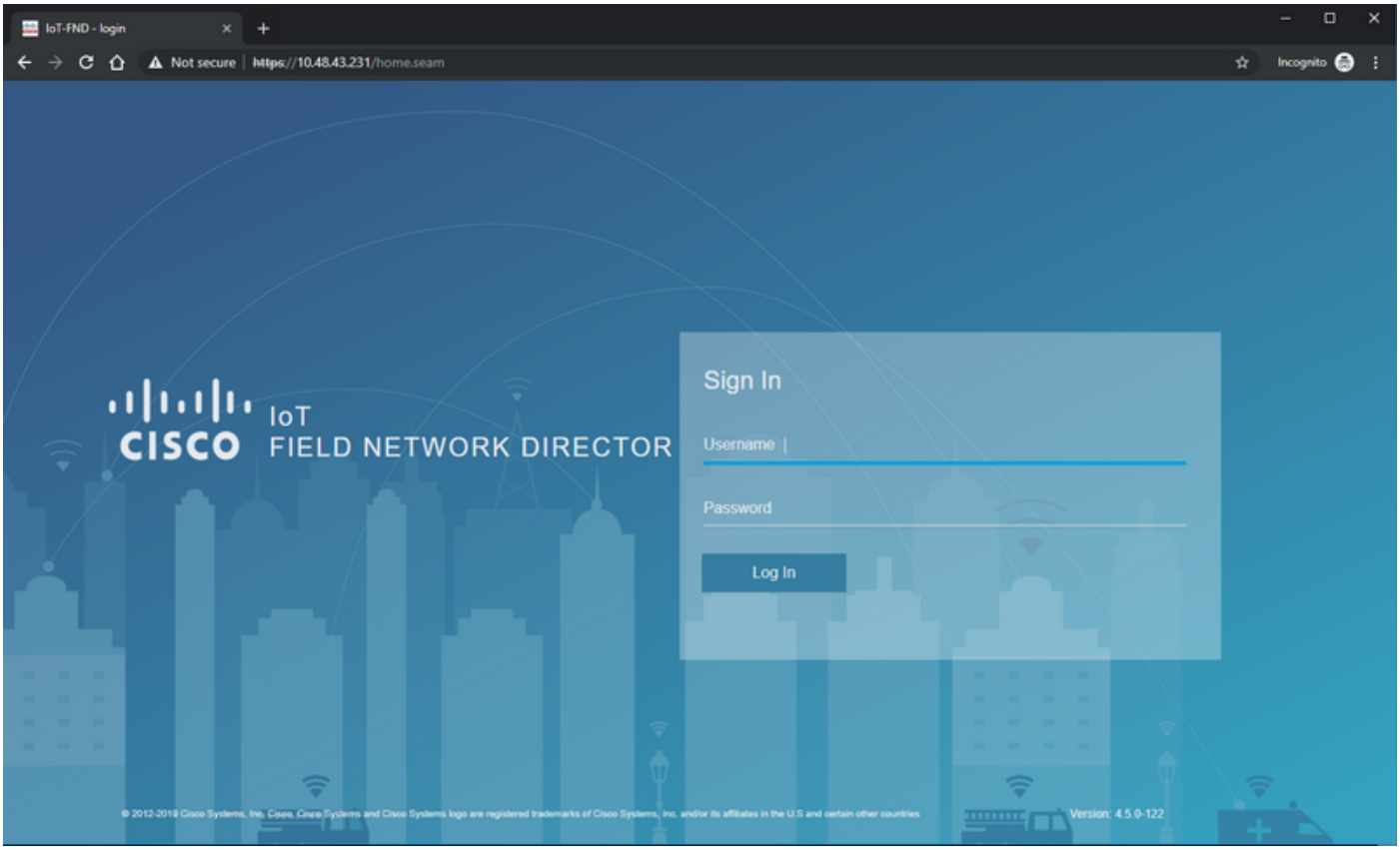
- Benutzername: root-Kennwort: **Cisco 123**
- Benutzername: Cisco Kennwort: **C_Scan123**

Schritt 3: Melden Sie sich mit dem Cisco Benutzer und Kennwort an, und navigieren Sie zu **Applications > System Tools > Settings > Network.** Fügen Sie ein verkabeltes Profil hinzu, und legen Sie auf der Registerkarte IPv4 die gewünschte IP-Adresse oder DHCP wie im Bild gezeigt fest.



Schritt 4: Klicken Sie auf **Übernehmen** und schalten Sie die Verbindung ein bzw. aus, um sicherzustellen, dass die neuen Einstellungen angewendet werden.

An diesem Punkt sollten Sie mit Ihrem Browser zur **FND-GUI** navigieren können und die IP-Adresse konfigurieren können, wie im Bild gezeigt.



Schritt 5: Melden Sie sich mit dem Standardbenutzernamen und -kennwort bei der GUI an: **root / root123**

Sie werden aufgefordert, Ihr Kennwort sofort zu ändern und anschließend erneut zur Anmeldung umzuleiten.

Wenn alles gut geht, sollten Sie sich mit Ihrem neuen Passwort anmelden und durch die FND GUI navigieren können.

Darüber hinaus werden der PNP- und der Demomodus beschrieben, gefolgt von der Konfiguration von FND.

Über PNP

PNP ist die aktuellste Cisco Methode zur Bereitstellung ohne Benutzereingriff (Zero Touch Deployment, ZTD). Bei Verwendung von PNP kann ein Gerät vollständig konfiguriert werden, sodass die Konfiguration nicht manuell vorgenommen werden muss.

Bei FND wird bei Verwendung von PNP vermieden, dass der Router zuerst mit einem Bootstrap gestartet werden muss. Tatsächlich leitet PNP das Gerät auf sichere Weise an den FND um und ruft die Bootstrap-Konfiguration ab.

Sobald die Bootstrap-Konfiguration im Gerät vorhanden ist, wird der übrige Prozess wie bei einem klassischen Bootstrapper fortgesetzt.

PNP kann auf verschiedene Weise verwendet werden:

- Über den Cisco PNP-Service (device.cisco.com) unter Verwendung eines Smart Accounts. Auf bestimmten Geräten standardmäßig werkseitig aktiviert

- Bei Verwendung der DHCP-Option 43, um die IP oder den Hostnamen für die Verbindung zum Bootstrapping bereitzustellen
- Durch manuelles Einstellen des PNP-Servers in der Konfiguration

Für diese Konfiguration wird die PNP-Server-IP manuell festgelegt, d. h. die IP-Adresse des FND-Servers und der Port am Gerät. Wenn Sie dies mit DHCP tun möchten, sollten Sie die folgenden Informationen angeben:

Für Cisco IOS® sollte der DHCP-Server wie folgt konfiguriert werden:

```
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"
!
```

Für DHCPd unter 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";
}
```

In dieser Konfiguration für Option 43 oder anbietergekapselte Optionen müssen Sie die folgenden ASCII-Zeichenfolgen angeben:

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

Sie kann wie folgt angepasst werden:

- 5 - DHCP-Typcode 5
- A - Aktiver Funktionsfunktionscode
- K4 = HTTP Transport Protocol
- B2 - Der IP-Adresstyp des PnP-Servers/TPS/FND-Servers lautet IPv4.
- I10.48.43.231 - IP-Adresse des FND-Servers
- J9125 - Portnummer 9125 (Port für PNP auf FND-Server)

Weitere Informationen zu PNP mit DHCP finden Sie unter https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/guide/4_3/iot_fnd_ug4_3/sys_mgmt.html#31568 im Abschnitt: **Konfigurieren der DHCP-Option 43 auf dem Cisco IOS® DHCP-Server**

Info zu EasyMode

Der einfache Modus wurde seit FND 4.1 eingeführt, obwohl er damals als Demo-Modus bezeichnet wurde und Ihnen ermöglicht, FND auf eine weniger sichere Art und Weise auszuführen. Obwohl dies nicht für die Produktion empfohlen wird, ist es eine gute Möglichkeit, zu beginnen.

Mit dem einfachen Modus können Sie sich auf den PNP-Prozess, das Bootstrapping und die Konfiguration des Routers konzentrieren. Falls etwas nicht funktioniert, müssen Sie die Tunneleinrichtung oder Zertifikate nicht vermuten.

Änderungen, die bei der Konfiguration von FND für die Ausführung im einfachen Modus auftreten:

- Kein Headend-Router (HER) oder Tunnel zum FND-Server erforderlich.
- Keine Einrichtung einer Public Key Infrastructure (PKI) und Simple Certificate Enrollment Protocol (SCEP) erforderlich.
- Router-Zertifikate, Trustpoint- und SSL-Zertifikate sind nicht erforderlich.
- Die gesamte Kommunikation erfolgt über HTTP statt HTTPS.

Weitere Informationen zum Easy Mode finden Sie hier:

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

Konfigurieren von FND für PNP und Easy Mode

Nun wissen Sie, was der Demomodus/PNP ist und warum er in diesem Zusammenhang verwendet wird. Ändern wir die FND-Konfiguration, um sie zu aktivieren:

Stellen Sie auf der FND VM, die von der OVA-Datei stammt, eine Verbindung mit SSH her, und bearbeiten Sie die **cgms.properties** wie folgt:

```
[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
```

Die letzten drei Zeilen haben sich in der Konfigurationsdatei geändert.

- Zeile 10: Ermöglicht einfachen Modus
- Zeile 11: aktiviert PNP
- Zeile 12: legt die IP-Adresse des FND-Servers für die Verbindung fest

Nachdem Sie die Datei geändert haben, starten Sie den FND-Container neu, um die vorgenommenen Änderungen anzupassen:

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

Nach dem Neustart kann die restliche Konfiguration über die Benutzeroberfläche vorgenommen werden.

Vorbereiten des CSV und Hinzufügen des Routers zum FND

Es mag etwas unlogisch klingen, das Gerät zu diesem Zeitpunkt des Konfigurationsprozesses hinzuzufügen, aber leider sind Teile der Konfiguration erst verfügbar, wenn bestimmte Gerätetypen hinzugefügt wurden.

Dies geschieht, um zu verhindern, dass die Benutzeroberfläche zu überwältigend ist, da verschiedene Geräte unterschiedliche Optionen einführen.

Lassen Sie uns an dieser Stelle versuchen, eine IR809 zu FND hinzuzufügen.

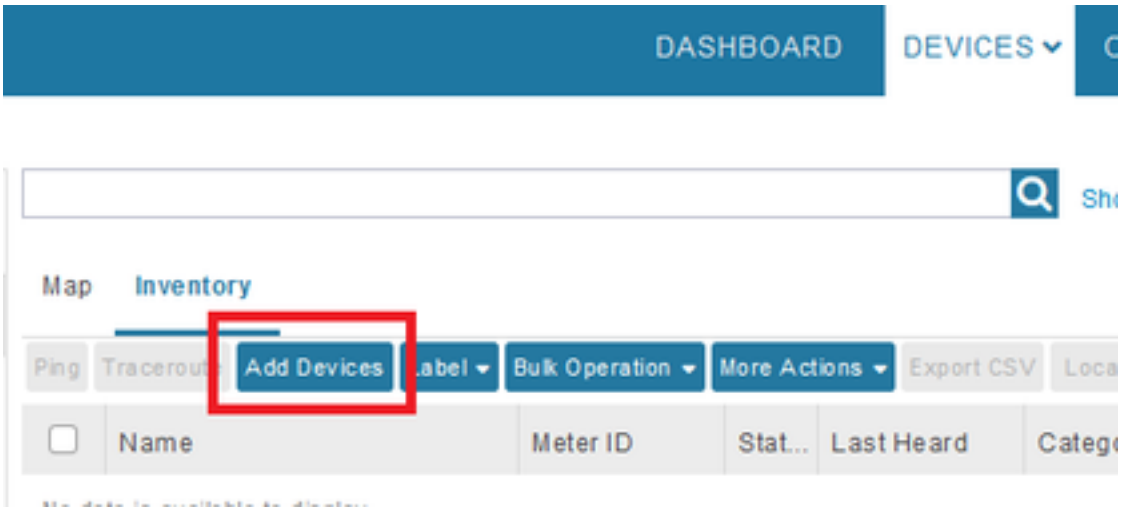
Der CSV sieht wie folgt aus:

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

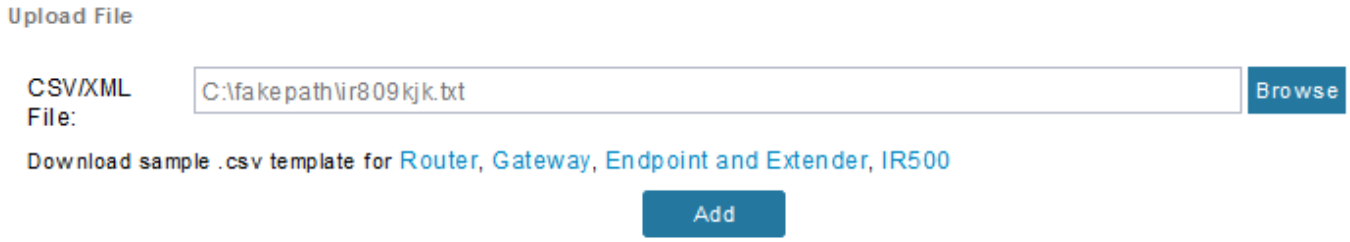
Die Felder im CSV sind:

- **Gerätetyp**: 800
- **eid**: PID und seriell zusammen mit +
- **adminBenutzername**: Dieser Benutzername wird der Router-Konfiguration hinzugefügt und später zum Abschluss des Registrierungsprozesses verwendet.
- **adminPasswort**: Kennwort für adminBenutzername
- **ip**: die IP-Adresse, die nach der Bereitstellung bei der Konfiguration des Geräts ersetzt werden soll

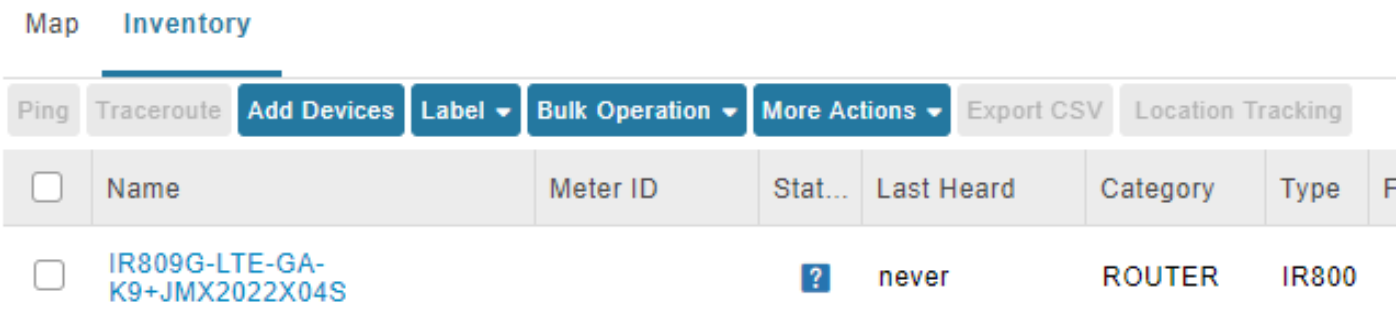
Um dieses Gerät hinzuzufügen, stellen Sie eine Verbindung zur Benutzeroberfläche her, und navigieren Sie zu **Devices > Field Devices > Inventory > Add Devices (Geräte hinzufügen),** wie im Bild gezeigt.



Geben Sie im Dialogfeld den Speicherort Ihrer CSV-Datei an, und klicken Sie auf **Hinzufügen**, um die Datei wie im Bild gezeigt zu FND hinzuzufügen.



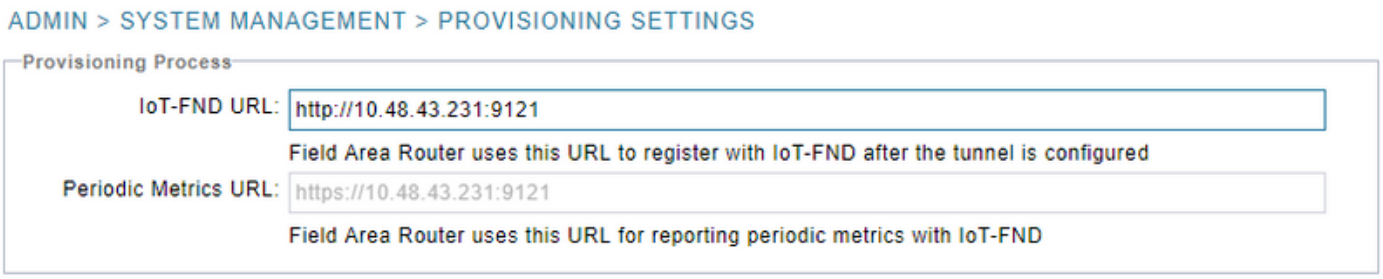
Wenn alles gut geht, sollten Sie das Verlaufselement sehen, um "Abgeschlossen" aufzulisten. Nach Schließen des Dialogfelds sollte das Gerät wie im Bild gezeigt im Inventar angezeigt werden.



Seit dem Hinzufügen des Geräts vom Typ ir800 sind die entsprechenden Vorlagen und Gruppen zu diesem Zeitpunkt in der GUI verfügbar.

Vorbereiten der Bereitstellungseinstellungen, der Bootstrap-Vorlage und der Konfigurationsvorlage

Da FND für den Demomodus konfiguriert ist, muss die Bereitstellungs-URL so geändert werden, dass sie stattdessen HTTP verwendet. Navigieren Sie zu **Admin > Provisioning Settings**, um Folgendes zu tun:



Ändern Sie die IoT-FND-URL in **http://<FND IP>:9121.**

Konfigurieren Sie anschließend zwei minimale Vorlagen für Bootstrapping und Konfiguration.

Die erste, die **Router Bootstrap Configuration**-Vorlage, ist die Konfiguration, die an den Router gesendet wird, sobald er mithilfe von PNP erfolgreich mit FND Kontakt aufnehmen kann.

Wenn PNP nicht verwendet wird, ist dies die Konfiguration, die zum Zeitpunkt des Bootstrap-Prozesses manuell auf dem Router oder werkseitig installiert wird. Diese Konfiguration enthält nur genügend Informationen, damit der Router den Registrierungsprozess in FND starten kann.

Die zweite Konfigurationsvorlage ist die Konfiguration, die der aktuell ausgeführten Konfiguration des Geräts hinzugefügt wird. Tatsächlich kann er als Inkrement der vorhandenen Konfiguration betrachtet werden.

In den meisten Fällen führt dies zu einer ungeraden Situation. Es wird daher empfohlen, zuerst alle Konfigurationen auf dem Router zu löschen, bevor Sie ihn zum FND hinzufügen.

Um die Vorlage zur Wiederherstellung der Werkseinstellungen für den Router festzulegen, navigieren Sie zu **Konfigurieren > Tunnelbereitstellung > Router Bootstrap-Konfiguration** und ersetzen Sie sie durch die folgende Vorlage:

```
<#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>
```

So legen Sie die Konfigurationsvorlage fest. Navigieren Sie zu **Konfiguration > Gerätekonfiguration > Konfigurationsvorlage bearbeiten,** und fügen Sie diese Vorlage hinzu:

```
<#-- 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
```

Diese Vorlage ist die aktuelle Konfiguration des Routers. Daher sollte hier jede spezifische Konfiguration für diese Konfigurationsgruppe hinzugefügt werden.

Am einfachsten ist es, mit dieser minimalen Vorlage zu beginnen. Nach dem erfolgreichen

Abschluss aktualisieren und anpassen Sie die Vorlage entsprechend Ihrer Anforderungen.

An diesem Punkt erfolgt die Konfiguration/Vorbereitung von FND. Sie können mit der Vorbereitung des Routers beginnen.

Vorbereitung der IR800 für Bereitstellung/PNP

Wenn das Gerät, das Sie bereitstellen möchten, bereits eine Konfiguration enthält oder bereits zuvor verwendet wurde, empfiehlt es sich, die Konfiguration des Routers vollständig zu löschen, bevor Sie es mit PNP zum FND hinzufügen.

Natürlich kann dieser Schritt übersprungen werden, wenn es sich um ein neues Gerät handelt.

Die einfachste Methode hierfür ist die Verwendung des Befehls **write erase** und das erneute Laden des Routers mithilfe der Konsole.

```
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
```

Nach einiger Zeit sollte die IR800 erneut mit der Aufforderung zum Ausführen des anfänglichen Konfigurationsdialogs angezeigt werden:

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

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


Press RETURN to get started!
```

Stellen Sie sicher, dass es keine weiteren PNP/ZTD-Versuche mehr gibt. Am besten müssen Sie das Archiv und das Verzeichnis neu erstellen und die **vor der Registrierung** vorgenommene **Konfiguration** auch auf dem Router entfernen:

```
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
```

Im Moment haben Sie entweder ein neues Gerät oder ein Gerät mit einer leeren Konfiguration. Wenn also erforderlich, kann eine minimale Konfiguration angewendet werden, damit der Router

FND erreichen kann.

Falls Sie einen DHCP-Server haben, sollte der Großteil automatisch ausgeführt werden.

Die folgende manuelle Konfiguration wird auf dem Gerät ausgewählt:

```
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#
```

Wie Sie sehen, wurde ein Quick Ping durchgeführt, um zu testen, ob der Router FND mit der angewendeten IP-Konfiguration erreichen konnte.

Bereitstellen des IR800-Routers

An diesem Punkt sind alle Voraussetzungen erfüllt, und Sie können den PNP-Prozess initiieren. In dieser Instanz wird dies manuell durchgeführt.

In einer Produktionsumgebung wird PNP höchstwahrscheinlich mit der DHCP-Option 43 verwendet. Dies bedeutet, dass der Router nach dem Start eine IP- und eine PNP-Konfiguration empfängt und Sie diesen und den nächsten Schritt überspringen können.

Um PNP auf dem IR800 ohne DHCP manuell zu konfigurieren, müssen Sie das Ziel für die Anfragen festlegen, d. h. den FND-Server.

Dies kann wie folgt erfolgen:

```
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
```

Sobald Sie die Zeile eingeben, die mit "transport" (Transport) beginnt, startet der Router den PNP-Prozess und versucht, mit FND über die angegebene IP und den Port Kontakt aufzunehmen.

Wenn alles gut geht, durchläuft das Gerät folgende Bereiche:

- [UPDATE_ODM]: Aktualisieren Sie die ODM-Dateien (Operational Data Model) auf dem Gerät, um sie mit den Dateien abzustimmen, die für die aktuelle FND-Version gültig sind.
- [UPDATE_ODM_VERIFY_HASH]: Überprüfen Sie, ob die aktualisierten Dateien korrekt sind
- [UPDATED_ODM]
- [COLLECTING_INVENTORY]: Sammeln der aktuellen Konfigurations- und Gerätedaten
- [COLLECTED_INVENTORY]

- [VALIDATING_CONFIGURATION]: versuchen Sie, die Konfiguration aus der Bootstrap-Konfiguration (ersetzte Router Factory Reprovisioning-Vorlage) anzuwenden.
- [VALIDATED_CONFIGURATION]
- [PUSHING_BOOTSTRAP_CONFIG_FILE]: Anwendung der validierten Konfiguration
- [PUSHING_BOOTSTRAP_CONFIG_VERIFY_HASH]: Überprüfen Sie, ob die angewendete Konfiguration richtig ist.
- [PUSHED_BOOTSTRAP_CONFIG_FILE]
- [CONFIGURING_STARTUP_CONFIG]:Konfiguration als Startkonfiguration schreiben
- [CONFIGURED_STARTUP_CONFIG]
- [APPLYING_CONFIG]: Anwenden der Startkonfiguration
- [APPLIED_CONFIG]
- [TERMINATION_BS_PROFILE]: Stoppen des Bootstrapings

Sie können den Prozess in FND server.log verfolgen.

In der GUI wird das Gerät verschoben, wenn Sie zu **Ungehört > Boostrapping > Bootstrapping** navigieren.

Nachdem das Bootstrapping abgeschlossen ist, verfügt der Router über die ersetzte Router-Factory-Reprovisionierungsvorlage und verhält sich wie ein reguläres Bootstrapper-Gerät ohne PNP.

Mit anderen Worten, ein CGNA-Profil auf dem IR800 versucht, sich beim FND-Server zu registrieren.

Überprüfen Sie den Status des CGNA-Profils:

```
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
```

Nach Ablauf von zehn Minuten versucht das Gerät, sich beim FND zu registrieren. Sie sehen, dass in dieser Ausgabe neun Minuten und dreißig Sekunden verbleiben, bevor der Router den Registrierungsprozess startet.

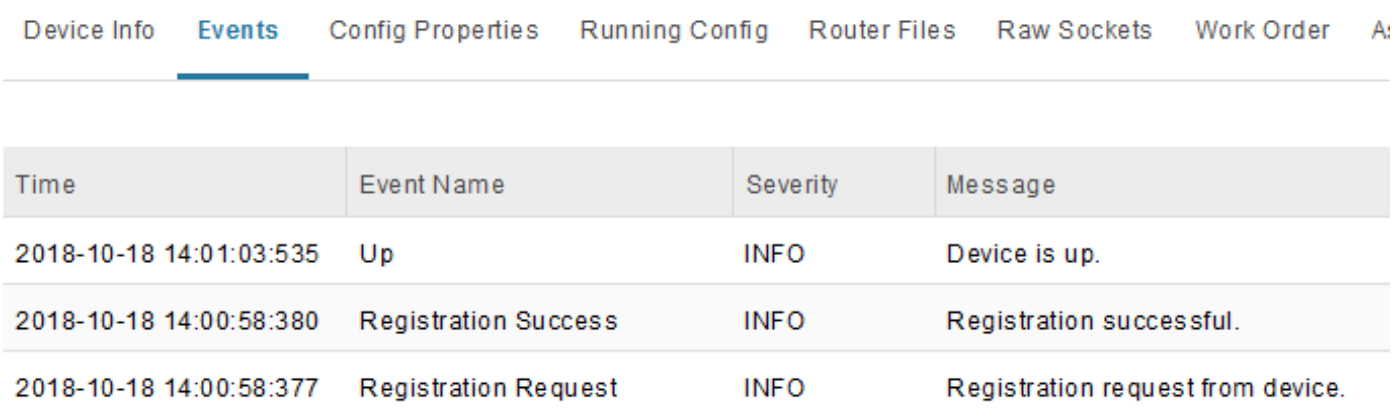
Sie können entweder warten, bis der Timer abgeschlossen ist, oder das **cg-nms-register-**Profil sofort manuell ausführen:

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

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Gerät sollte in den UP-Status in FND verschoben werden, wie im Bild gezeigt.



Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Überprüfen Sie zur Fehlerbehebung beim Bootstrapping folgende Punkte:

- Anmeldung beim FND-Server: **/opt/fnd/logs/server.log**
- Erhöhen Sie die Ausführlichkeit der Anmeldung: **Admin > Protokollierung > Einstellungen auf Protokollebene > Router-Bootstrapping > Debug**
- Von der IR800-Konsole: **show pnp ? oder debuggen pnp ?**
- In der FND-GUI: **Geräte > Bestand > Gerät auswählen > Ereignisse**
- Die meisten Probleme in dieser Phase stehen in Zusammenhang mit (Syntaxfehlern) in der Vorlage zur Wiederherstellung der Werkseinstellungen des Routers

Überprüfen Sie zur Fehlerbehebung beim Registrierungsprozess folgende Punkte:

- Anmeldung beim FND-Server: **/opt/fnd/logs/server.log**
- Von der IR800-Konsole:

  Alle Cgna-Profilzustände anzeigendebuggen cgna logging?debuggen wsma agent
- In der FND-GUI: **Geräte > Bestand > Gerät auswählen > Ereignisse**
- Überprüfung der WSMA-Verbindung über HTTP zum IR800 vom FND VM
  Von FND verwendeter URI: http://10.48.43.231:80/wsma/execMethode: POSTSicherheit: **Grundauth**