IR800でプラグアンドプレイを使用するようにField Network Directorを設定します

内容

概要

このドキュメントでは、最小限のコンポーネントセットを使用して、Field Network Director(FND)およびプラグアンドプレイ(PNP)を使用する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Linuxマシンで実行コンフィギュレーションファイルを編集するためのLinuxと知識の経験
- FNDによって管理されるサポート対象ルータの少なくとも1つ。例：IR809またはIR829。 コンソールアクセスIOS®バージョン15.7(3)M1以降
- ハイパーバイザに展開されたOVAファイル(例：VMWare ESXi)。 OVAファイルは、https://software.cisco.com/download/home/286287993/type/286320249からダウンロードできます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- FNDバージョン4.5.0-122用のOVAファイル(CISCO-IOTFND-V-K9-4.5.0-122.zip)
- VMware ESX
- IOS®バージョン15.8(3)M2を搭載したIR809

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

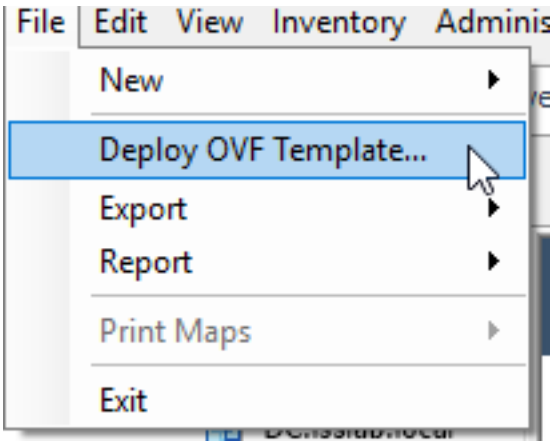
FNDには多くの異なる導入オプションがあるため、FND用に最小限の機能を備えたインストールを設定することが目標です。この設定は、さらにカスタマイズを行うための開始点として、さらに機能を追加するために役立ちます。ここで説明するセットアップは、Open Virtual Appliance(OVA)パッケージFNDを出発点として使用し、公開キーインフラストラクチャ(PKI)とトンネルプロビジョニングを回避するために簡易モードを使用します。PNPを使用して、デバイスを簡単に追加します。

このガイドの結果は、プレーンテキストのパスワードとトンネルとPKIが存在しないことによるセキュリティリスクが存在する可能性があるため、実稼働環境での使用を意図したものではありません。

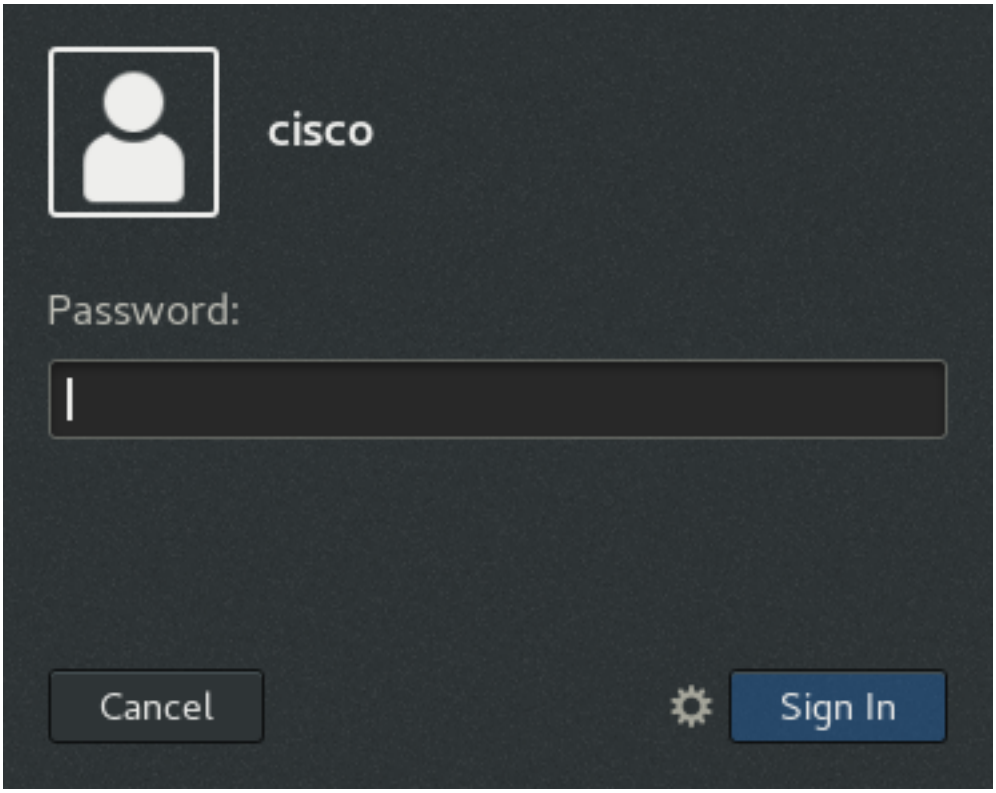
設定

FND OVAの導入と設定

ステップ1:FND OVAファイルをダウンロードし、ハイパーバイザに展開します。たとえば、VMWareの場合、図に示すように、**[File] > [Deploy OVF Template]を使用**します。



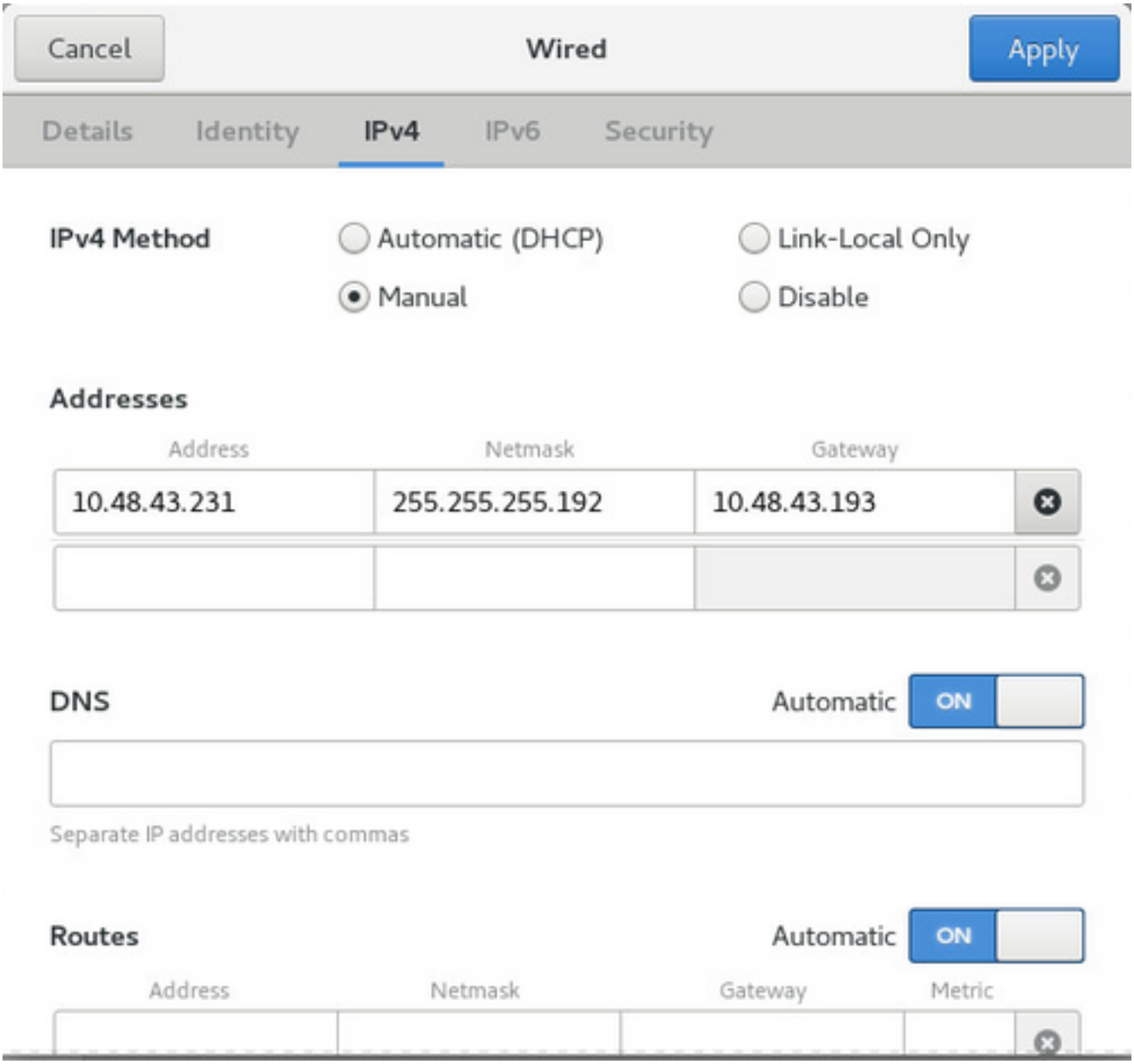
ステップ2:VMを導入したら、VMを起動できます。ログイン画面が表示されます（図を参照）。



OVAファイルのデフォルトパスワードは次のとおりです。

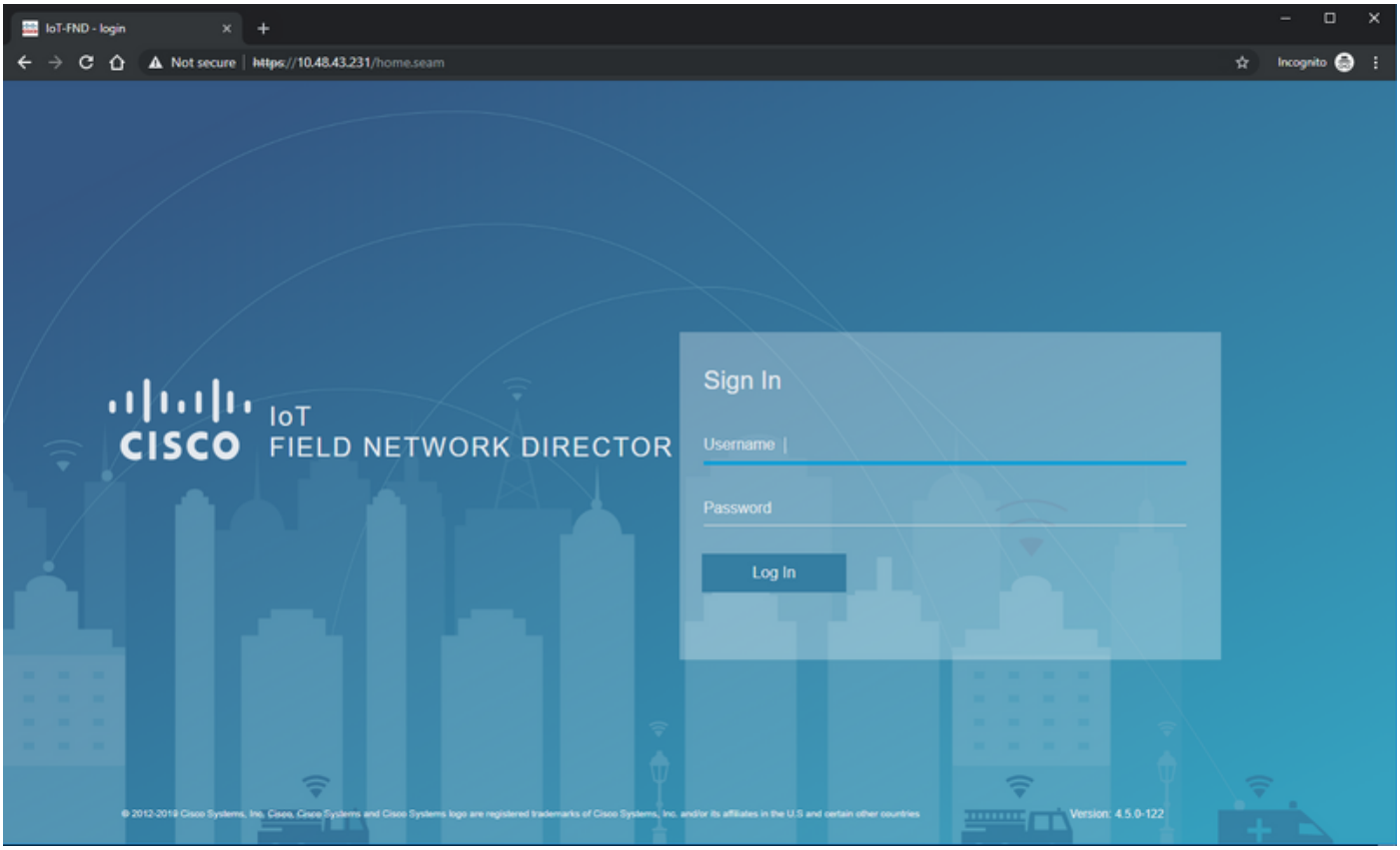
- username：ルートパスワード：**Cisco123**
- username：cisco password:**C_sco123**

ステップ3:ciscoユーザとパスワードを使用してログインし、**[Applications] > [System Tools] > [Settings] > [Network]に移動します**。有線プロファイルを追加し、[IPv4]タブで、図に示すように目的のIPアドレスまたはDHCPを設定します。



ステップ4:[Apply]をクリックし、接続をオフ/オンに切り替えて、新しい設定が適用されるようにします。

この時点で、図に示すように、ブラウザとIPアドレスが設定されたFND GUIに移動できます。



ステップ5：デフォルトのユーザ名とパスワードを使用してGUIにログインします。**ルート/ルート123**

すぐにパスワードを変更し、再度ログインにリダイレクトするように求められます。

すべてが正常に機能していれば、新しいパスワードでログインして、FND GUIをナビゲートできます。

さらに、PNPとデモモードについて説明し、その後FNDの設定を行います。

PNPについて

PNPは、ゼロタッチ導入(ZTD)を行うシスコの最新の方法です。PNPを使用すると、デバイスを完全に設定でき、手動で設定に触れる必要がなくなります。

FNDでは、PNPを使用することで、ルータを最初にブートストラップする必要がなくなります。実際には、PNPが行うすべてのことを、安全な方法でFNDにリダイレクトし、ブートストラップ設定を取得します。

ブートストラップ設定がデバイスに存在すると、残りのプロセスは従来のブートストラップされたデバイスと同様に続行されます。

PNPを使用する方法は次のとおりです。

- Cisco PNPサービス(devicehelper.cisco.com)を通じて、スマートアカウントを使用します。特定のデバイスで工場出荷時にデフォルトで有効
- DHCPオプション43を使用して、ブートストラッピングのために接続するIPまたはホスト名を指定する
- 設定でPNPサーバを手動で設定する

この設定では、PNPサーバのIPを手動で設定します。これはFNDサーバのIPであり、デバイスのポートです。DHCPでこれを行う場合は、次の情報を入力する必要があります。

Cisco IOS® の場合、DHCPサーバは次のように設定する必要があります。

```
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"
!
```

Linux上のDHCPdの場合：

```
[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";
}
```

オプション43またはvendor-encapsulated-optionsのこの設定では、次のASCII文字列を指定する必要があります。

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

次のようにカスタマイズできます。

- 5 - DHCPタイプコード5
- A – アクティブな機能操作コード
- K4:HTTPトランスポートプロトコル
- B2:PnPサーバ/TPS/FNDサーバのIPアドレスタイプはIPv4です。
- I10.48.43.231:FNDサーバのIPアドレス
- J9125 – ポート番号9125（FNDサーバのPNP用ポート）

DHCPを使用したPNPの詳細については、次のセクションの https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/guide/4_3/iot_fnd_ug4_3/sys_mgmt.html#31568を参照してください。**Cisco IOS® DHCPサーバでのDHCPオプション43の設定**

EasyModeについて

EasyモードはFND 4.1以降に導入されましたが、当時はデモモードと呼ばれていましたが、FNDをよりセキュアな方法で実行できます。これは実稼働には推奨されませんが、開始する良い方法です。

簡易モードを使用すると、ルータのPNPプロセス、ブートストラップ、および設定に焦点を当てることができます。何かが機能しない場合は、トンネルの構築や証明書を疑う必要はありません。

簡易モードで実行するようにFNDを設定すると発生する変更：

- ヘッドエンドルータ(HER)やFNDサーバへのトンネルは不要です。

- 公開キーインフラストラクチャ(PKI)のセットアップとSimple Certificate Enrollment Protocol(SCEP)は不要です。
- ルータ証明書、トラストポイント、およびSSL証明書は不要です。
- すべての通信は、HTTPSではなくHTTPで行われます。

簡易モードの詳細については、次のリンクを参照してください。

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

PNPおよびEasy Mode用のFNDの設定

ここで、デモモード/PNPが何で、このコンテキストで使用される理由を確認できます。FND設定を変更して有効にします。

OVAファイルから生成されたFND VMで、SSHを使用して接続し、次のように**cgms.propertiesを編集**します。

```
[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
```

コンフィギュレーションファイルで最後の3行が変更されました。

- 回線 10：イネーブルモードを有効にする
- 回線 11：PNPを有効にする
- 回線 12：接続するFNDサーバのIPを設定します

ファイルを変更した後、FNDコンテナを再起動して、変更を適用します。

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

再起動後、GUIを使用して残りの設定を行うことができます。

CSVの準備とFNDへのルータの追加

設定プロセスのこの時点でデバイスを追加することは少し論理的ではないように思えますが、残念ながら、特定のデバイスタイプが追加されるまで、設定の一部は使用できません。

これは、異なるデバイスが異なるオプションを導入する際に、GUIが過剰にならないようにするためです。

ここでは、IR809をFNDに追加してみましょう。

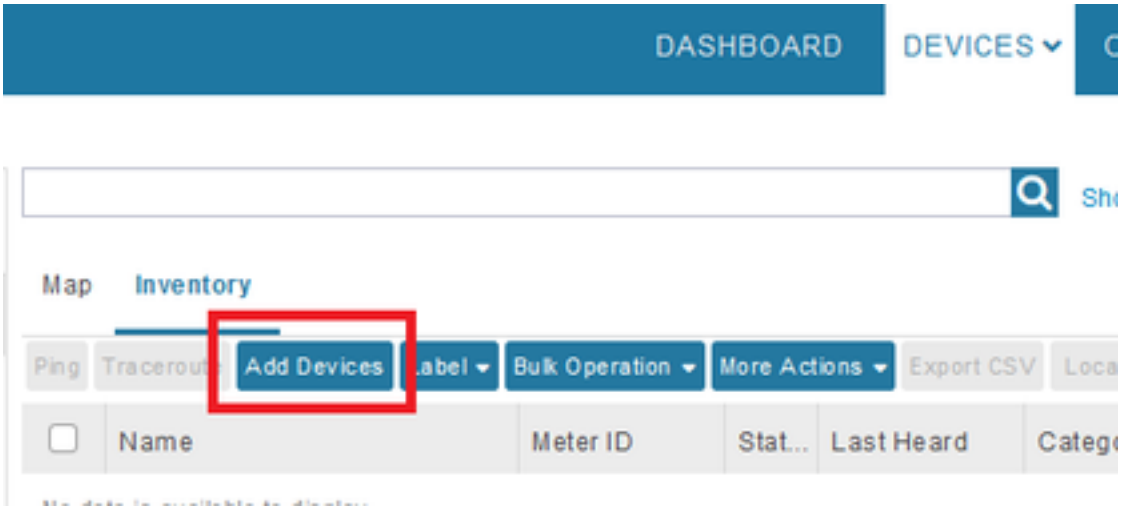
CSVは次のようになります。

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

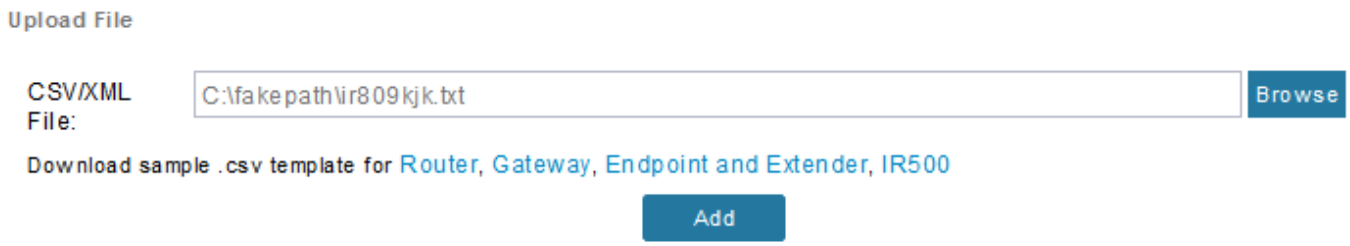
CSVのフィールドは次のとおりです。

- **deviceType**:ir800
- **eid**:PIDとシリアル+
- **adminUsername**:このユーザ名はルータの設定に追加され、後で登録プロセスを完了するために使用されます
- **adminPassword**:adminUsernameのパスワード
- **ip**：導入後にデバイスの設定に代わるIPアドレス

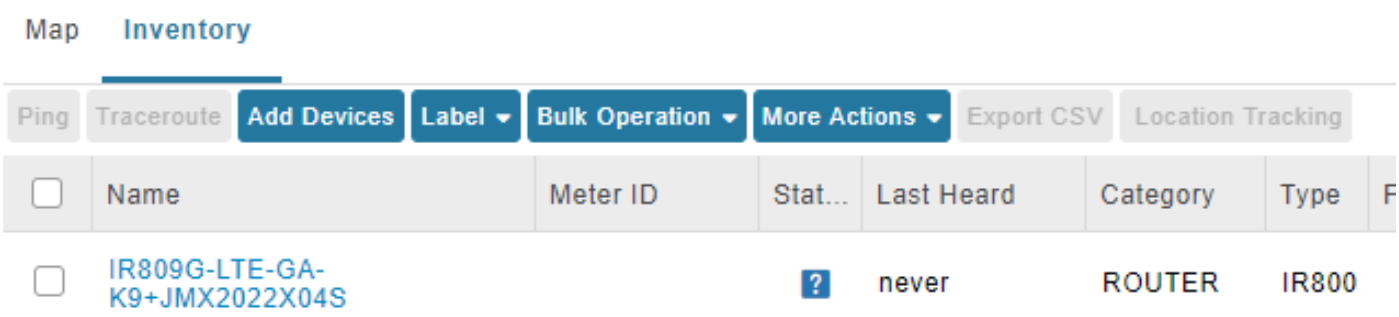
このデバイスを追加するには、GUIに接続し、図に示すように**[Devices] > [Field Devices] > [Inventory] > [Add Devices]に移動**します。



図に示すように、ダイアログでCSVファイルの場所を指定し、[追**加]をク**リックしてFNDに追加します。



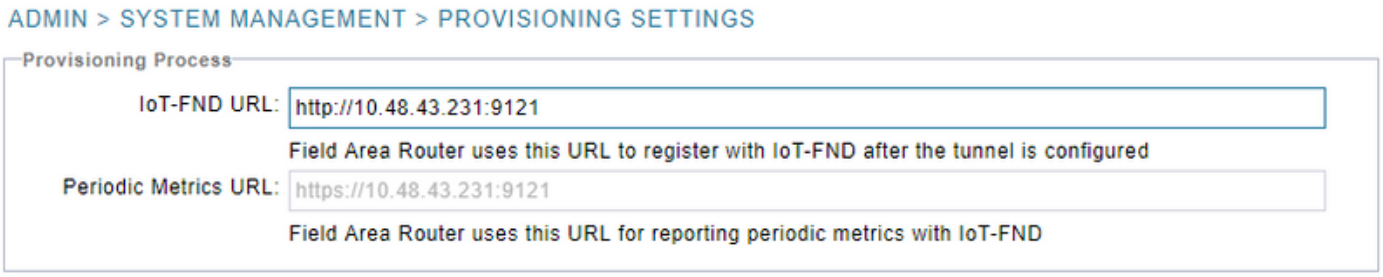
すべてが正常に動作している場合は、「完了」をリストする履歴項目が表示されます。 ダイアログを閉じると、デバイスがインベントリに表示されます（図を参照）。



deviceType ir800のデバイスが追加されたため、この時点で該当するテンプレートとグループがGUIで使用できるようになります。

プロビジョニング設定、ブートストラップテンプレート、および設定テンプレートの準備

FNDはデモモードに設定されているため、代わりにHTTPを使用するようにプロビジョニングURLを変更する必要があります。[Admin] > [Provisioning Settings]に移動して、次の操作を行います。



IoT-FND URLをhttp://<FND IP>:9121に変更します

次に、ブートストラッピングと設定用に2つの最小テンプレートを設定します。

1つ目の設定は、Router Bootstrap Configurationテンプレートと呼ばれ、PNPを使用してFNDに正常に接続できるようになった後にルータにプッシュされる設定です。

PNPが使用されていない場合は、ブートストラッププロセスの時点で手動または工場出荷時にルータに設定されます。この設定には、ルータがFNDで登録プロセスを開始するのに十分な情報が含まれています。

2つ目の設定テンプレートは、デバイスの現在実行されている設定に追加される設定です。実際には、既存の設定の増分として見ることができます。

ほとんどの場合、これは奇妙な状況を引き起こすため、ルータ上のすべての設定をFNDに追加する前に、最初に消去することを推奨します。

Router Factory Reprovisionテンプレートを設定するには、[Configure] > [Tunnel Provisioning] > [Router Bootstrap Configuration]に移動し、次のテンプレートに置き換えます。

```
<#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>
```

構成テンプレートを設定するには、[Config] > [Device Configuration] > [Edit Configuration Template]に移動して、次のテンプレートを追加します。

```
<#-- 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
```

このテンプレートが、ルータの実行コンフィギュレーションになります。したがって、この設定グループの特定の設定をここに追加する必要があります。

最も簡単なのは、この最小限のテンプレートから開始することです。成功したら、必要に応じてテンプレートを更新およびカスタマイズします。

これでFNDの設定と準備が完了し、ルータの準備から始めることができます。

IR800のプロビジョニング/PNPの準備

プロビジョニングするデバイスにすでに設定が含まれているか、以前に使用されている場合は、PNPを使用してFNDに追加する前に、ルータの設定を完全に消去することをお勧めします。

新しいデバイスの場合は、この手順をスキップできます。

これを行う最も簡単な方法は、write eraseコマンドを使用し、コンソールを使用してルータをリロードすることです。

```
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
```

しばらくすると、IR800に初期設定ダイアログを実行するプロンプトが表示されます。

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

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


Press RETURN to get started!
```

以前のPNP/ZTDの試行が残っていないことを確認します。アーカイブとディレクトリを再作成し、ルータの**before-registration-config**も削除することをお勧めします。

```
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
```

現在、新しいデバイスまたは空の設定のデバイスが存在するため、必要に応じて、ルータがFNDに到達するための最小限の設定を適用できる瞬間です。

DHCPサーバがある場合は、ほとんどの場合は自動的に行われます。

次の手動設定がデバイスで選択されます。

```
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#
```

このように、適用されたIP設定でルータがFNDに到達できるかどうかをテストするために、迅速なpingが実行されました。

IR800ルータのプロビジョニング

これで、すべての前提条件が完了し、PNPプロセスを開始できます。この場合は手動で行います。

実稼働環境では、PNPがDHCPオプション43とともに使用される可能性が高くなります。つまり、ルータが起動すると、IPとPNPの設定が受信され、このステップと次のステップは省略できます。

DHCPを使用せずにIR800でPNPを手動で設定するには、要求の宛先（FNDサーバ）を指定する必要があります。

これは次のように行うことができます。

```
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
```

「transport」で始まる行を入力すると、ルータはPNPプロセスを開始し、指定されたIPおよびポート上のFNDに接続しようとします。

すべてが正常に動作している場合、デバイスは次を通過します。

- [UPDATING_ODM]:デバイスのODM(Operational Data Model)ファイルを、現在のFNDバージョンで有効なファイルと一致するように更新します
- [UPDATING_ODM_VERIFY_HASH]:更新されたファイルが正しいかどうかを確認する
- [UPDATED_ODM]
- [COLLECTING_INVENTORY]:現在の設定とデバイス情報の収集
- [COLLECTED_INVENTORY]
- [VALIDATING_CONFIGURATION]:ブートストラップ構成(代替ルータファクトリー再プロビジョンテンプレート)から構成を適用します
- [VALIDATED_CONFIGURATION]
- [PUSH_BOOTSTRAP_CONFIG_FILE]:検証済みの設定を適用する
- [PUSH_BOOTSTRAP_CONFIG_VERIFY_HASH]:適用された設定が正しいかどうかを確認する
- [PUSH_BOOTSTRAP_CONFIG_FILE]
- [CONFIGURING_STARTUP_CONFIG]：スタートアップコンフィギュレーションとして設定を書き込みます。
- [CONFIGURED_STARTUP_CONFIG]
- [APPLYING_CONFIG]:スタートアップコンフィギュレーションの適用
- [APPLIED_CONFIG]
- [TERMINATING_BS_PROFILE]:ブートストラップを停止します。

プロセスはFND server.logで追跡できます。

GUIでは、[Unheard] > [Boostrapping] > [Bootstrap]に移動すると、デバイスが**移動します**

ブートストラッピングが完了すると、ルータは代替のRouter Factory Reprovisionテンプレートを持ち、PNPのない通常のブートストラップデバイスのように動作します。

つまり、IR800上のCGNAプロファイルはFNDサーバへの登録を試みます。

CGNAプロファイルのステータスを確認します。

```
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
```

指定された設定では、デバイスは10分後にFNDへの登録を試みます。この出力では、ルータが登録プロセスを開始するまでに9分30秒が残っていることがわかります。

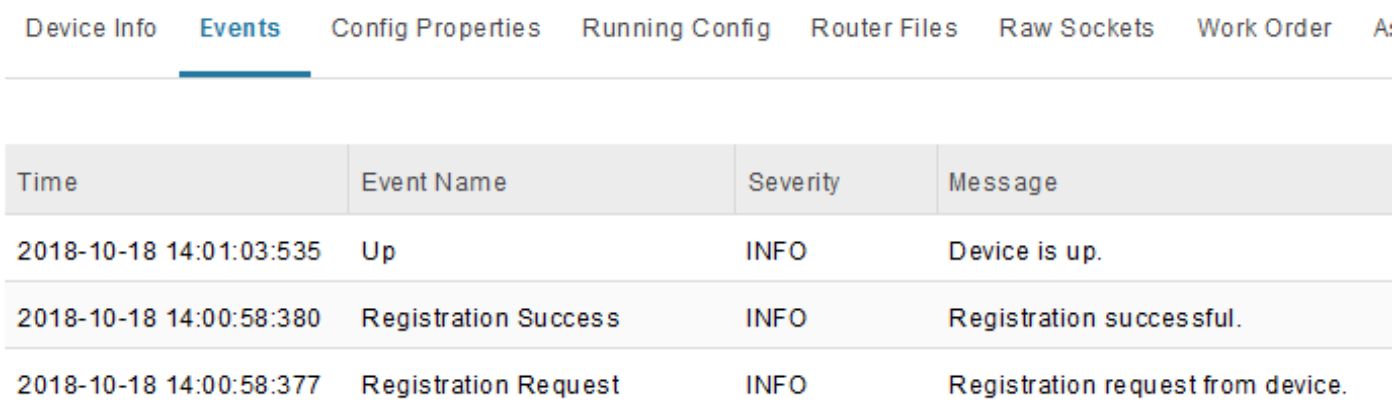
タイマーが終了するのを待つか、または**cg-nms-registerプロファイル**をすぐに手**動で実行する**ことができます。

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

確認

ここでは、設定が正常に機能しているかどうかを確認します。

図に示すように、デバイスはFNDのUPステータスに移動します。



トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ブートストラップ処理のトラブルシューティングを行うには、次の点を確認します。

- FNDサーバーログイン： **/opt/fnd/logs/server.log**
- ログインの冗長性を高めます。**Admin > Logging > Log Level Settings > Router Bootstrap > Debug**
- IR800コンソールから：**show pnp ?またはdebug pnp ?**
- FND GUIで次の操作を行います。**[Devices] > [Inventory] > [Select Device] > [Events]**
- この段階の問題のほとんどは、Router Factory Reprovisionテンプレートの（構文）エラーに関連しています

登録プロセスのトラブルシューティングを行うには、次の項目を確認します。

- FNDサーバーログイン：**/opt/fnd/logs/server.log**
- IR800コンソールから：

  show cgna profile-state alldebug cgna logging?debug wsma agent
- FND GUIで次の操作を行います。**[Devices] > [Inventory] > [Select Device] > [Events]**
- FND VMからIR800へのHTTP経由のWSMA接続を確認します
  FNDで使用されるURI: http://10.48.43.231:80/wsma/execMethod：POSTセキュリティ：**基本認証**