Configurare Field Network Director per l'utilizzo di Plug and Play su IR800

Sommario

Introduzione

In questo documento viene descritto come iniziare a utilizzare Field Network Director (FND) e Plug and Play (PNP) con l'utilizzo di un set minimo di componenti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Esperienza con Linux e conoscenze per modificare i file di configurazione di esecuzione su un computer Linux
- Almeno uno dei router supportati deve essere gestito da FND. Ad esempio, IR809 o IR829. Accesso consoleVersione minima IOS® 15.7(3)M1
- File OVA distribuito in un hypervisor (ad esempio: VMWare ESXi). Il file OVA, se intitolato, può essere scaricato da: https://software.cisco.com/download/home/286287993/type/286320249

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- File OVA per FND versione 4.5.0-122 (CISCO-IOTFND-V-K9-4.5.0-12.zip)
- VMWare ESX
- IR809 con IOS® versione 15.8(3)M2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

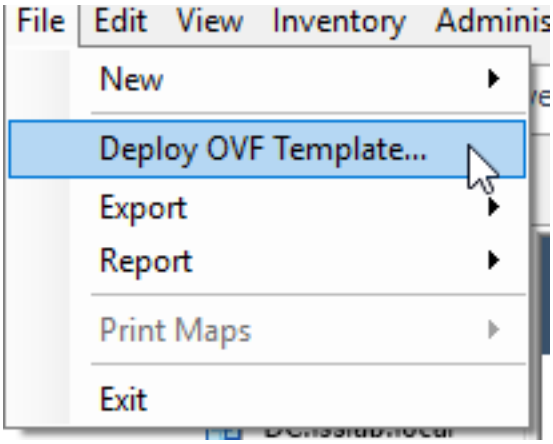
Poiché FND dispone di molte opzioni di installazione diverse, l'obiettivo è quello di poter impostare un'installazione minima ma funzionante per FND. Questa impostazione può quindi fungere da punto di partenza per ulteriori personalizzazioni e per aggiungere ulteriori funzionalità. La configurazione qui illustrata si basa sull'utilizzo dell'installazione Open Virtual Appliance (OVA) con pacchetto FND come punto di partenza e utilizza la modalità semplice per evitare la necessità di PKI (Public Key Infrastructure) e il provisioning del tunnel. Utilizzare PNP per semplificare e aggiungere dispositivi all'installazione.

Il risultato di questa guida non è destinato all'uso in produzione in quanto potrebbero esserci alcuni rischi di sicurezza dovuti alla password del testo del piano e all'assenza di tunnel e PKI.

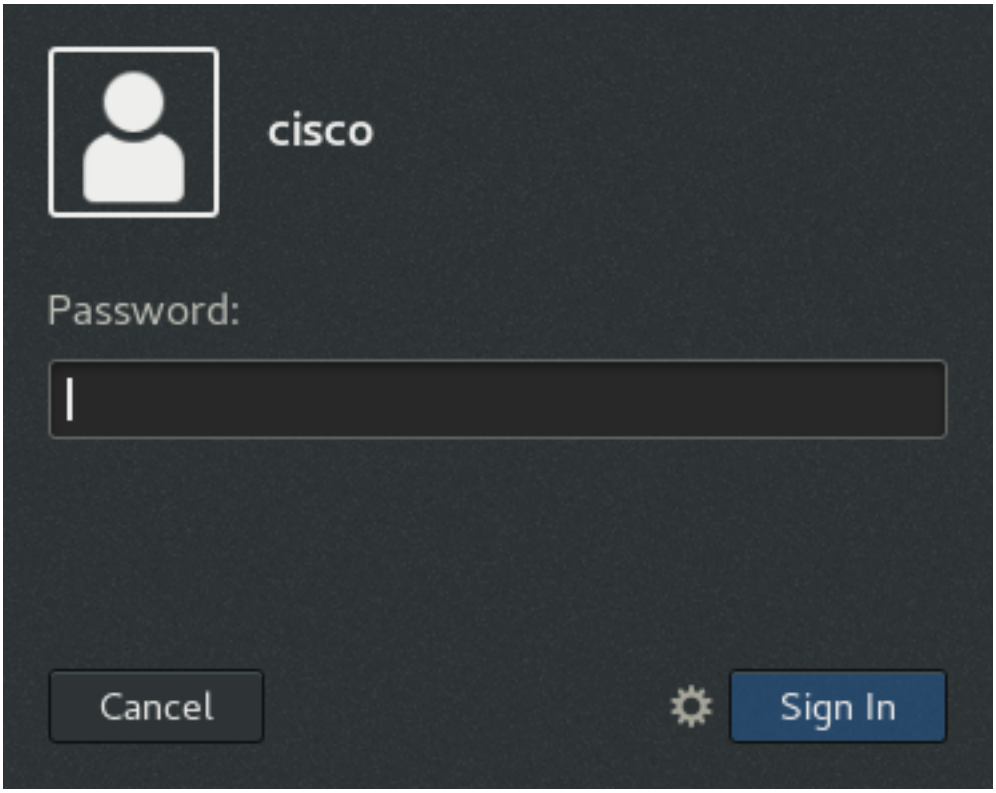
Configurazione

Distribuire e configurare gli OAV FND

Passaggio 1. Scaricare e distribuire il file OVA FND sull'hypervisor. Ad esempio, per VMWare, verrà utilizzato **File > Distribuisci modello OVF** come mostrato nell'immagine.



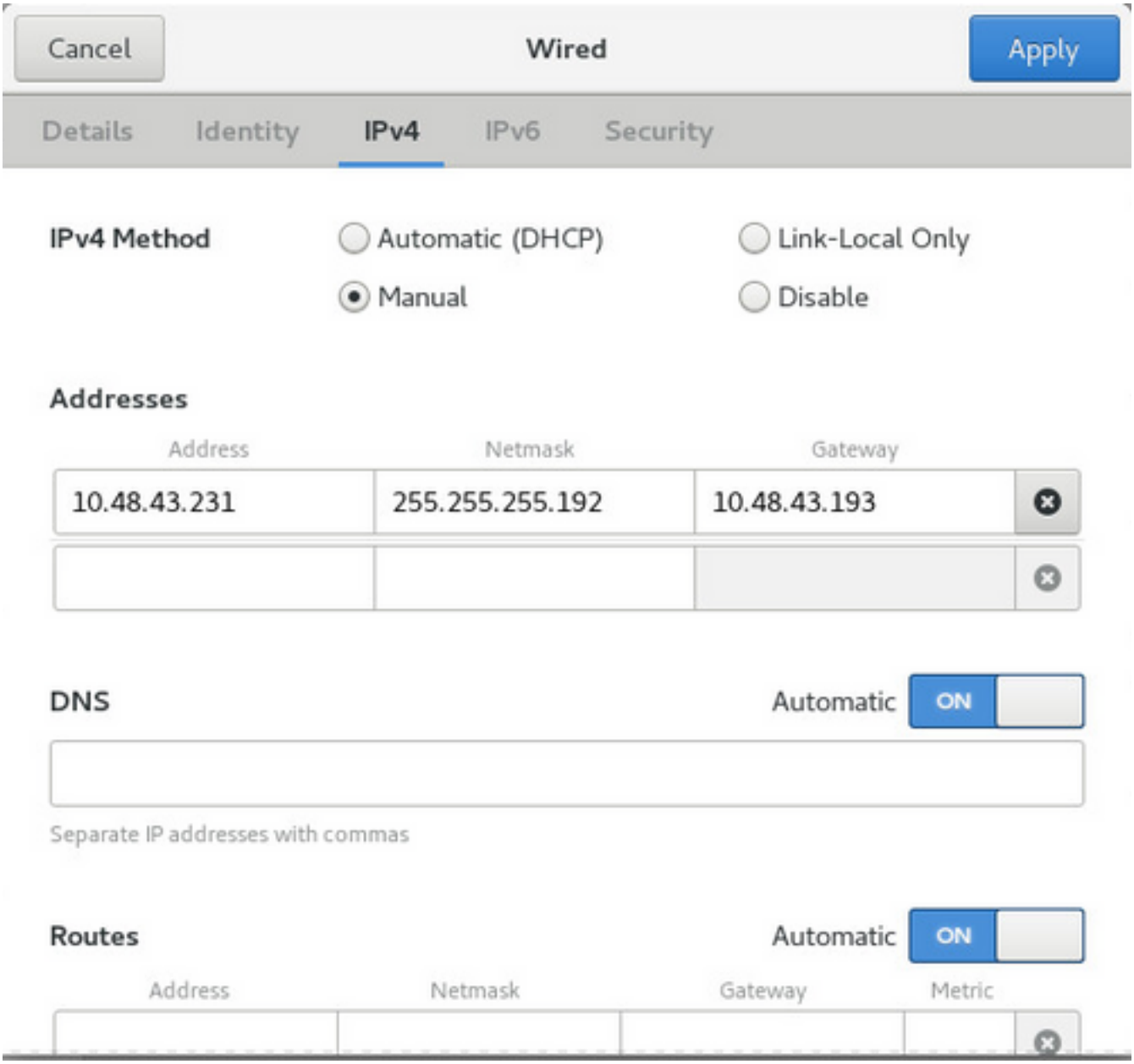
Passaggio 2. Una volta distribuita, è possibile avviare la VM e visualizzare una schermata di accesso, illustrata nell'immagine.



Le password predefinite per il file OVA sono:

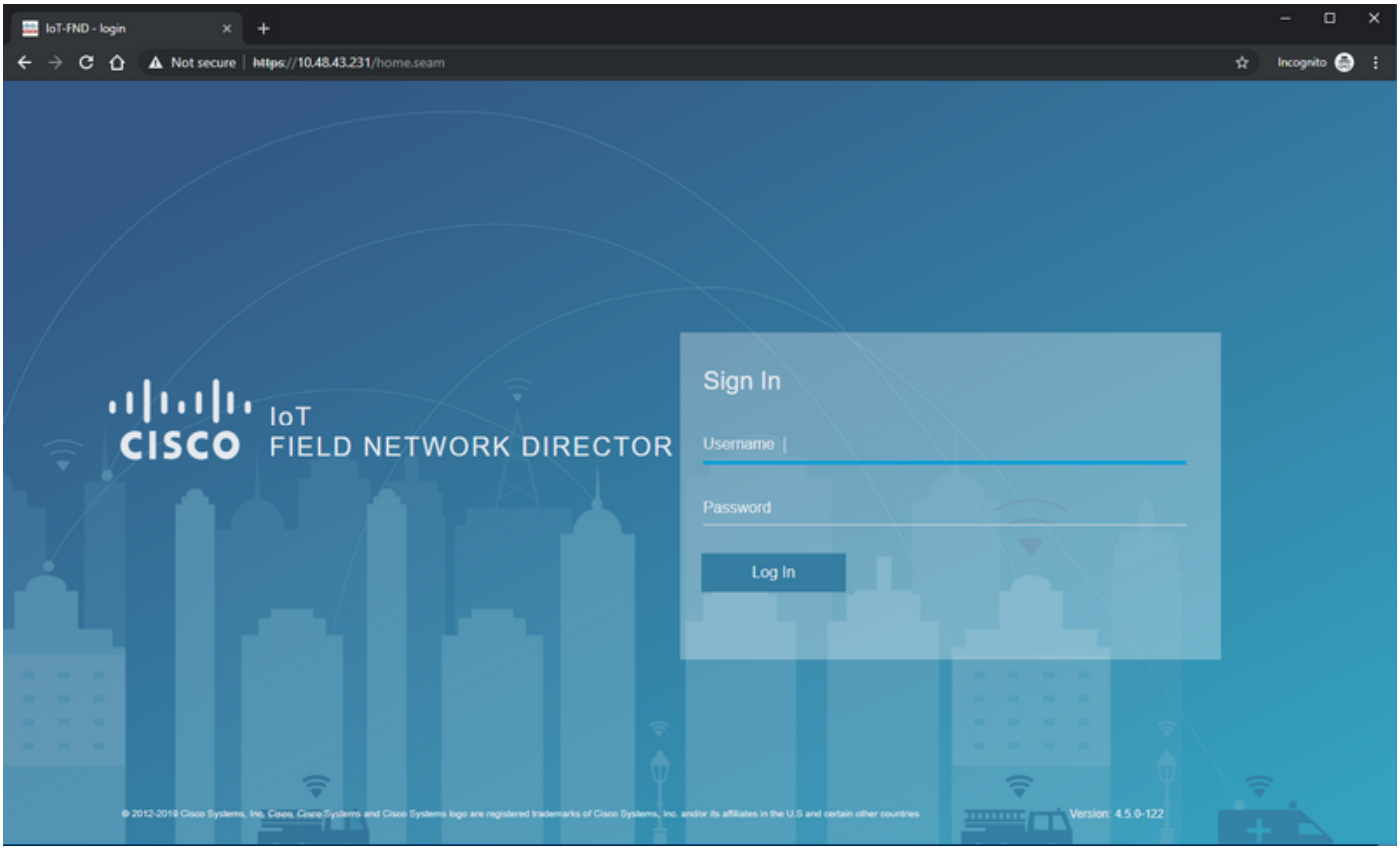
- username: password principale: **cisco 123**
- username: password cisco: **C_isco123**

Passaggio 3. Accedere con l'utente e la password cisco e selezionare **Applications > System Tools > Settings > Network.** Aggiungere un profilo cablato e nella scheda IPv4, impostare l'indirizzo IP o DHCP desiderato come mostrato nell'immagine.



Passaggio 4. Per verificare che le nuove impostazioni siano state applicate, fare clic su **Apply** (Applica) e attivare/disattivare la connessione.

A questo punto, dovrebbe essere possibile passare all'**interfaccia utente FND** con il browser e l'indirizzo IP configurato come mostrato nell'immagine.



Passaggio 5. Accedere alla GUI con il nome utente e la password predefiniti: **root / root123**

Viene richiesto di modificare immediatamente la password e quindi di reindirizzare nuovamente l'utente al login.

Se tutto va bene, si dovrebbe essere in grado di effettuare il login con la nuova password ed essere in grado di navigare attraverso la GUI FND.

Vengono inoltre descritte le modalità PNP e demo, seguite dalla configurazione di FND.

Informazioni su PNP

PNP è il metodo Cisco più recente per eseguire l'implementazione Zero Touch (ZTD). Con PNP, è possibile configurare completamente un dispositivo e non è necessario toccare manualmente la configurazione.

Per FND, con l'uso della rete PNP, è possibile evitare di dover prima eseguire il bootstrap del router. Infatti, tutto quello che fa PNP, lo reindirizza al FND, in modo sicuro, e recupera la configurazione del bootstrap.

Una volta che la configurazione bootstrap è presente nel dispositivo, il resto del processo continua come con un dispositivo bootstrap classico.

Esistono diversi modi per utilizzare PNP:

- Tramite il servizio PNP di Cisco (devicehelper.cisco.com), con l'utilizzo di uno Smart Account. Attivata per impostazione predefinita in alcuni dispositivi
- Usare l'opzione DHCP 43 per fornire l'IP o il nome host a cui connettersi per il bootstrap
- Impostando manualmente il server PNP nella configurazione

Per questa configurazione, l'indirizzo IP del server PNP viene impostato manualmente, ovvero l'indirizzo IP del server FND, e la porta sul dispositivo. Se si desidera eseguire questa operazione con DHCP, fornire le informazioni seguenti:

Per Cisco IOS®, il server DHCP deve essere configurato come segue:

```
ip dhcp pool pnp_pool
network 192.168.10.0 255.255.255.248
default-router 192.168.10.1
dns-server 8.8.8.8
option 43 ascii "5A;K4;B2;I10.48.43.231;J9125"
!
```

Per DHCPd su 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 questa configurazione dell'opzione 43 o delle opzioni incapsulate dal fornitore, è necessario specificare le seguenti stringhe ASCII:

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

Può essere personalizzato come segue:

- 5 - Codice tipo DHCP 5
- A - Codice operativo della feature attiva
- K4 - Protocollo di trasporto HTTP
- B2 - Il tipo di indirizzo IP del server PnP/TPS/FND è IPv4
- I10.48.43.231 - Indirizzo IP del server FND
- J9125 - Numero porta 9125 (porta per PNP su server FND)

Per ulteriori informazioni su PNP con DHCP, visitare il sito: https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/guide/4_3/iot_fnd_ug4_3/sys_mgmt.html#31568 nella sezione: **Configurazione dell'opzione DHCP 43 sul server DHCP Cisco IOS®**

Informazioni su EasyMode

La modalità Easy è stata introdotta a partire da FND 4.1, anche se all'epoca era chiamata modalità demo e consente di eseguire FND in modo meno sicuro. Sebbene non sia consigliato per la produzione, è un buon modo per iniziare.

Con l'uso della modalità semplice, è possibile concentrarsi sul processo PNP, sul bootstrap e sulla configurazione del router. Nel caso in cui qualcosa non funzioni, non è necessario sospettare la creazione del tunnel o i certificati.

Modifiche che si verificano quando si configura FND per l'esecuzione in modalità semplice:

- Non è necessario un router headend (HER) o un tunnel per il server FND.
- Non è necessario installare un'infrastruttura a chiave pubblica (PKI) e il protocollo SCEP (Simple Certificate Enrollment Protocol).
- Non sono necessari certificati router, trustpoint e certificati SSL.
- Tutte le comunicazioni avvengono tramite HTTP anziché tramite HTTPS.

Ulteriori informazioni sulla modalità semplice sono disponibili qui:

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

Configurare FND per PNP e Easy Mode

Ora, si sa cosa è la modalità demo/PNP e perché viene utilizzata in questo contesto. Modificare la configurazione FND per abilitarla:

Sulla VM FND, che ha avuto origine dal file OVA, collegarsi a SSH e modificare **cgms.properties** come segue:

```
[root@iot-fnd ~]# cat /opt/fnd/data/cgms.properties
cgms-keystore-password-hidden=dD5KmzJHa64Oyvpqdu8SCg==
use-router-ip-from-db=true
rabbit-broker-ip=
rabbit-broker-port=
rabbit-broker-username=
rabbit-broker-password=
fogd-ip=192.68.5.3
enable-reverse-dns-lookup=false
enableApiAuth=false
fnd-router-mgmt-mode=1
enable-bootstrap-service=true
proxy-bootstrap-ip=10.48.43.231
```

Le ultime tre righe sono state modificate nel file di configurazione.

- Riga 10: abilita la modalità semplice
- Riga 11: abilita PNP
- Riga 12: imposta l'indirizzo IP del server FND da contattare

Dopo aver modificato il file, riavviare il contenitore FND per adattare le modifiche apportate:

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

Dopo il riavvio, il resto della configurazione può essere eseguito usando la GUI.

Preparare il file CSV e aggiungere il router a FND

L'aggiunta del dispositivo a questo punto del processo di configurazione potrebbe sembrare un po' illogica, ma alcune parti della configurazione non sono disponibili finché non vengono aggiunti alcuni tipi di dispositivo.

Questa operazione viene eseguita per evitare che la GUI sia troppo complessa in quanto dispositivi diversi introducono opzioni diverse.

In questo caso, provare ad aggiungere un IR809 a FND.

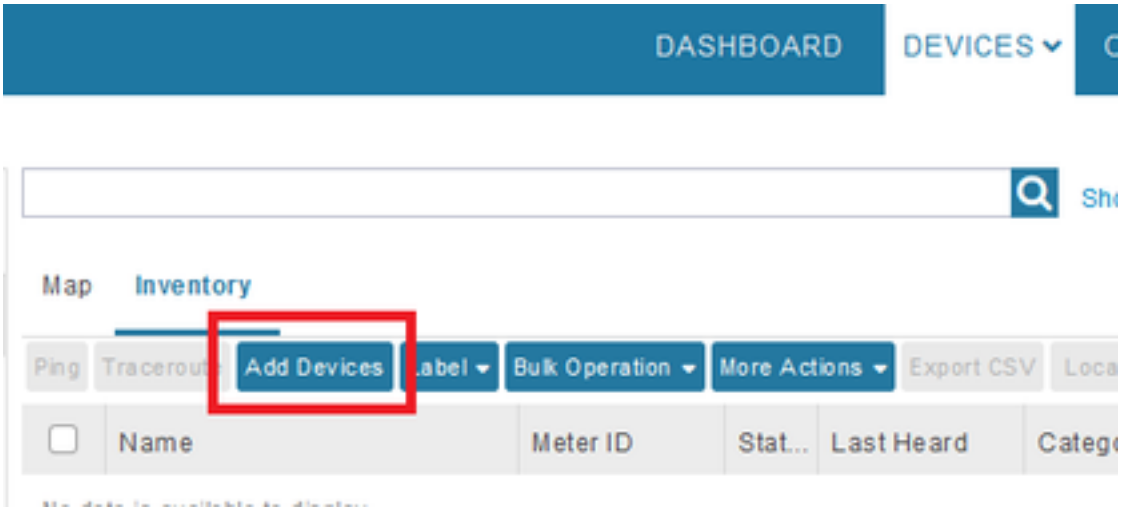
Il formato CSV è il seguente:

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

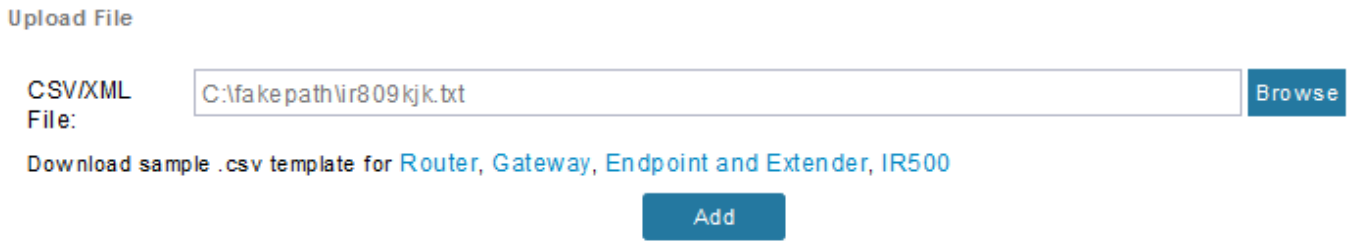
I campi nel file CSV sono:

- **TipoDispositivo**: ir800
- **eid**: PID e seriale con +
- **adminUsername**: questo nome utente verrà aggiunto alla configurazione del router e verrà usato in seguito per completare il processo di registrazione
- **password amministratore**: password per adminUsername
- **ip:** l'indirizzo IP da sostituire nella configurazione del dispositivo dopo l'installazione

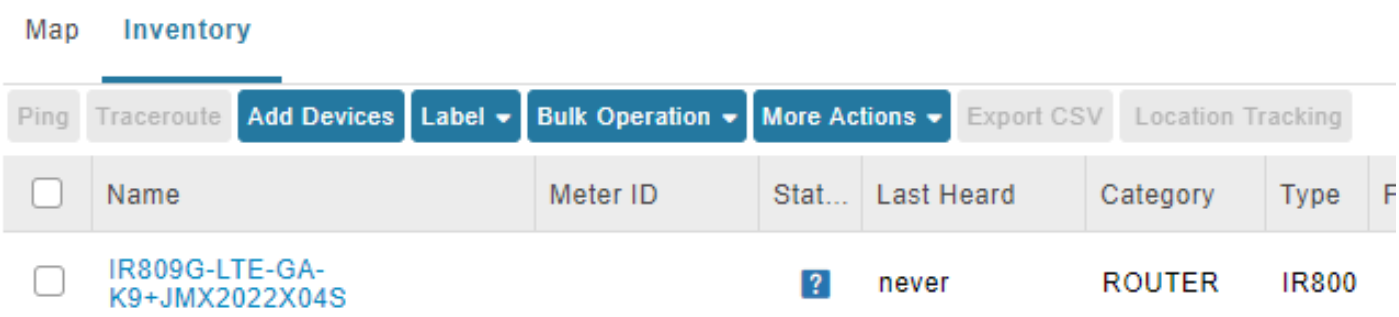
Per aggiungere questo dispositivo, collegarsi alla GUI e selezionare **Dispositivi > Dispositivi sul campo > Inventario > Aggiungi dispositivi**, come mostrato nell'immagine.



Nella finestra di dialogo, specificare il percorso del file CSV e fare clic su **Add** per aggiungerlo a FND, come mostrato nell'immagine.



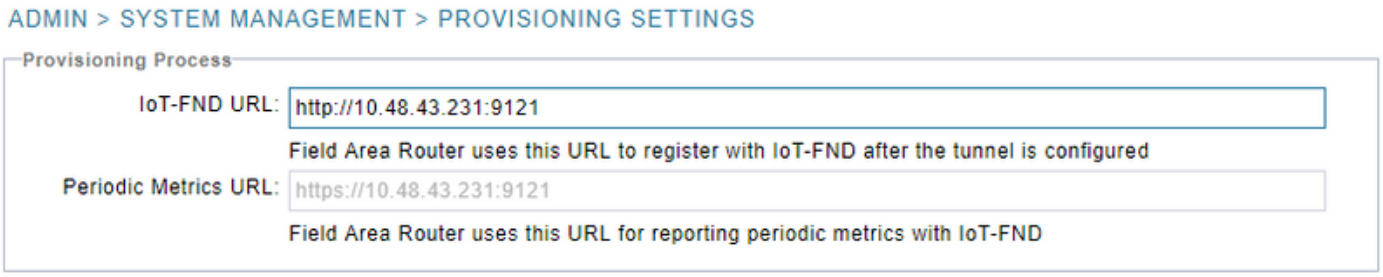
Se tutto va bene, dovrebbe vedere l'elemento della cronologia per elencare "COMPLETED". Dopo aver chiuso la finestra di dialogo, il dispositivo dovrebbe apparire nell'inventario come mostrato nell'immagine.



Poiché è stato aggiunto il dispositivo di tipo ir800, a questo punto i modelli e i gruppi applicabili saranno disponibili nella GUI.

Preparare le impostazioni di provisioning, il modello di bootstrap e il modello di configurazione

Poiché FND è configurato per la modalità demo, è necessario modificare l'URL di provisioning per utilizzare HTTP. A tale scopo, selezionare **Admin > Provisioning Settings** (Amministratore > Impostazioni di provisioning):



Modificare l'URL IoT-FND in **http://<FND IP>:9121**

Configurare quindi due modelli minimi per il bootstrap e la configurazione.

Il primo, denominato modello di **configurazione del bootstrap del router**, è la configurazione che viene inviata al router una volta in grado di contattare correttamente FND con la PNP.

Se il protocollo PNP non è in uso, sarà la configurazione a essere applicata sul router manualmente o in fabbrica al momento del processo di bootstrap. Questa configurazione contiene informazioni sufficienti per permettere al router di avviare il processo di registrazione in FND.

Il secondo, denominato modello di configurazione, sarà la configurazione aggiunta alla configurazione attualmente in esecuzione del dispositivo. Infatti, può essere visto come un incremento nella configurazione esistente.

Nella maggior parte dei casi, ciò porta a una situazione strana, quindi si consiglia di cancellare tutte le configurazioni sul router prima di aggiungerlo a FND.

Per impostare il modello Router Factory Reprovision, selezionare **Configura > Tunnel Provisioning > Configurazione bootstrap router** e sostituirlo con il seguente modello:

```
<#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>
```

Per impostare il modello di configurazione. Passare a **Configurazione > Configurazione dispositivo > Modifica modello di configurazione** e aggiungere questo modello:

```
<#-- 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
```

Questo modello sarà la configurazione di esecuzione del router risultante. Pertanto, qualsiasi configurazione specifica per questo gruppo di configurazione deve essere aggiunta qui.

Il metodo più semplice consiste nell'utilizzare questo modello minimo. Una volta completato, aggiornare e personalizzare il modello in base alle proprie esigenze.

A questo punto, la configurazione/preparazione di FND è completata ed è possibile iniziare con la preparazione del router.

Preparare IR800 per provisioning/PNP

Se il dispositivo di cui si desidera eseguire il provisioning contiene già una configurazione o è stato utilizzato in precedenza, è consigliabile cancellare completamente la configurazione del router prima di aggiungerlo a FND con PNP.

Ovviamente, se si tratta di un nuovo dispositivo, questo passaggio può essere ignorato.

Il modo più semplice per eseguire questa operazione è usare il comando **write erase** e ricaricare il router con il comando console.

```
ir809kjk#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
*Oct 18 11:42:54.367 UTC: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
ir809kjk#reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]

Starting File System integrity check
NOTE: File System will be deinited and later rebuilt
```

Dopo qualche tempo, IR800 dovrebbe tornare con la richiesta di eseguire la finestra di dialogo di configurazione iniziale:

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

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


Press RETURN to get started!
```

Accertarsi che non vi siano più residui di un precedente tentativo PNP/ZTD, è meglio ricreare l'archivio e la directory e rimuovere anche la configurazione **prima della registrazione** sul router:

```
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
```

Al momento, si ha un nuovo dispositivo o un dispositivo con una configurazione vuota, quindi, se necessario, questo è il momento in cui è possibile applicare una configurazione minima per consentire al router di raggiungere FND.

Nel caso si disponga di un server DHCP, la maggior parte di questo dovrebbe avvenire automaticamente.

Sul dispositivo è selezionata la seguente configurazione manuale:

```
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#
```

Come si può vedere, è stato eseguito un ping rapido per verificare se il router è stato in grado di raggiungere FND con la configurazione IP applicata.

Provisioning del router IR800

A questo punto, tutti i prerequisiti sono completi ed è possibile avviare il processo PNP. In questo caso viene eseguita manualmente.

In un ambiente di produzione, è molto probabile che PNP venga utilizzato con l'opzione DHCP 43. Ciò significa che una volta avviato il router, riceverà una configurazione IP e PNP e sarà possibile ignorare questo passaggio e quello successivo.

Per configurare manualmente PNP su IR800 senza DHCP, è necessario specificare la destinazione delle richieste, che sarà il server FND.

A tale scopo, eseguire le operazioni seguenti:

```
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
```

Non appena si immette la riga che inizia con "transport", il router avvia il processo PNP e proverà a contattare FND sull'IP e sulla porta specificati.

Se tutto va bene, il dispositivo passa attraverso questi:

- [ODM_AGGIORNAMENTO]: aggiornare i file ODM (Operational Data Model) nel dispositivo in modo che corrispondano a quelli validi per la versione FND corrente
- [UPDATING_ODM_VERIFY_HASH]: verificare che i file aggiornati siano corretti
- [ODM_AGGIORNATO]
- [INVENTARIO_RACCOLTA]: raccogli la configurazione corrente e le informazioni sul dispositivo
- [INVENTARIO_RACCOLTO]
- [CONFIGURAZIONE_CONVALIDA]: provare ad applicare la configurazione dalla configurazione del bootstrap (modello Router Factory Reprovision sostituito)
- [CONFIGURAZIONE_CONVALIDATA]
- [PUSHING_BOOTSTRAP_CONFIG_FILE]: applica la configurazione convalidata
- [PUSHING_BOOTSTRAP_CONFIG_VERIFY_HASH]: verificare che la configurazione applicata sia corretta
- [FILE_CONFIG_PUSHED_BOOTSTRAP]
- [CONFIGURING_STARTUP_CONFIG]:scrittura della configurazione come configurazione di avvio
- [CONFIGURED_STARTUP_CONFIG]
- [CONFIG_APPLICAZIONE]: applicare la configurazione di avvio
- [CONFIG_APPLICATA]

- [TERMINATING_BS_PROFILE]: interrompere il bootstrap.

Èpossibile tenere traccia del processo in FND server.log.

Nella GUI, lo spostamento del dispositivo è visibile quando si passa a **Unheard > Boostrapping > Bootstrapped**

Al termine del bootstrap, il router riceve il modello Router Factory Reprovision sostituito e si comporta come un normale dispositivo bootstrap senza PNP.

In altre parole, un profilo CGNA su IR800 tenta di eseguire la registrazione con il server FND.

Controllare lo stato del profilo 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 configurazione fornita, il dispositivo tenterà di eseguire la registrazione con FND dopo dieci minuti. Come si può notare, in questo output rimangono nove minuti e trenta secondi prima che il router inizi il processo di registrazione.

È possibile attendere il termine del timer o eseguire manualmente il profilo **cg-nms-register** immediatamente:

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

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Il dispositivo dovrebbe passare allo stato UP in FND, come mostrato nell'immagine.

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.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per risolvere i problemi relativi al processo di bootstrap, verificare quanto segue:

- Accesso al server FND: **/opt/fnd/logs/server.log**
- Aumentare il livello di dettaglio del log in: **Amministrazione > Registrazione > Impostazioni livello di log > Bootstrap router > Debug**
- Dalla console IR800: **visualizzare il protocollo pnp? o debug pnp?**
- Nell'interfaccia utente di FND: **Dispositivi > Inventario > Seleziona dispositivo > Eventi**
- La maggior parte dei problemi in questa fase sono correlati a errori di sintassi nel modello Router Factory Reprovision

Per risolvere i problemi relativi al processo di registrazione, verificare quanto segue:

- Accesso al server FND: **/opt/fnd/logs/server.log**
- Dalla console IR800:

  show cgna profile-state alldebug cgna logging?debug dell'agente wsma
- Nell'interfaccia utente di FND: **Dispositivi > Inventario > Seleziona dispositivo > Eventi**
- Verificare la connettività WSMA su HTTP per IR800 dalla macchina virtuale FND
  URI utilizzato da FND: http://10.48.43.231:80/wsma/execMetodo: POSTSecurity: **autenticazione di base**