

Managing Devices

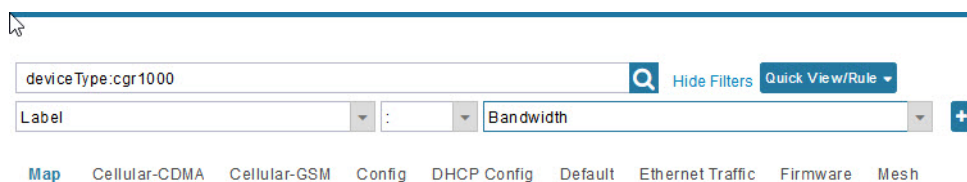
This section describes how to manage devices in IoT FND, and includes the following topics:

- [Overview](#)
- [Managing Routers](#)
- [Managing Endpoints](#)
- [Managing the Cisco Industrial Compute \(IC3000\) Gateway](#)
- [Managing the Cisco Wireless Gateway for LoRaWAN](#)
- [Managing Cisco IR510 WPAN Industrial Routers](#)
- [Managing Head-End Routers](#)
- [Managing External Modules](#)
- [Managing Servers](#)
- [Tracking Assets](#)
- [Common Device Operations](#)
- [Configuring Rules](#)
- [Configuring Devices](#)
- [Monitoring a Guest OS](#)
- [Managing Files](#)
- [Managing Work Orders](#)
- [Demo and Bandwidth Operation Modes](#)
- [Device Properties](#)

Overview

Use the following IoT FND pages to monitor, add and remove devices, and perform other device management tasks that do not include device configuration:

Figure 1 Devices menu options



- To work with Field Devices such as Routers (CGR1000, C800, IR800, SBR (C5921)) and Endpoints (meters and IR500 gateways), and IoT Gateways (such as the LoRaWAN gateway and IC3000), use the **DEVICES > Field Devices** page.
 - **Note:** In some textual displays of the IoT FND, routers may display as “FAR” rather than the router model (cgr1000, etc).
- To work with Head-end Routers (ASR1000, ISR3900, ISR4000) use the **DEVICES > Head-End Routers** page.
- To work with FND NMS and database servers, use the **DEVICES > Servers** page.
- To view Assets associated with the Cisco Wireless Gateway for LoRaWAN (IXM-LPWA-900), use the **DEVICES > Assets** page.

Note: Refer to the [Managing Firmware Upgrades](#) chapter of this book for details on firmware updates for Routers and Gateways mentioned in this chapter.

Managing Routers

You manage routers on the Field Devices page (**DEVICES > Field Devices**). Initially, the page displays devices in the Default view. This section includes the following topics:

- [Working with Router Views](#)
- [Managing Embedded Access Points on Cisco C819 and Cisco IR829 ISRs](#)
- [Using Router Filters](#)
- [Refreshing the Router Mesh Key](#)
- [Managing Embedded Access Points on Cisco C819 and Cisco IR829 ISRs](#)
- [Displaying Router Configuration Groups](#)
- [Displaying Router Firmware Groups](#)
- [Displaying Router Tunnel Groups](#)

Working with Router Views

Unless you select the **Default to map view** option in user preferences (see [Figure 2 Setting User Preferences for User Interface Display](#)) the Field Devices page defaults to the List view, which contains basic device properties. Select a router or group of routers in the **Browse Devices** pane (left pane) to display tabs in the main pane.

The router or routers you select determine which tabs display.

Note: Listed below are all the possible tabs. You can select to view the Map option from the List view.

- Map
- Cellular-CDMA
- Cellular-GSM
- Config
- DHCP Config
- Default
- Ethernet Traffic

Managing Routers

- Firmware
- Group
- LoRaWAN
- Mesh
- Mesh Config
- Physical
- PLC Mesh
- RF Mesh
- Tunnel
- WiMAX

Each of the tab views above displays different sets of device properties. For example, the Default view displays basic device properties, and the Cellular-GSM view displays device properties particular to the cellular network.

For information on how to customize router views, see [Customizing Device Views](#).

For information about the device properties that display in each view, see [Device Properties](#).

For information about common actions performed in these views (for example, adding labels and changing device properties), see [Common Device Operations](#).

Viewing Routers in Map View

To view routers in Map view, check the **Enable map** check box in `<user> > Preferences` (see [Figure 2](#)), and then click the **Map** tab (see [Figure 3](#)) in the main pane.

Figure 2 Setting User Preferences for User Interface Display

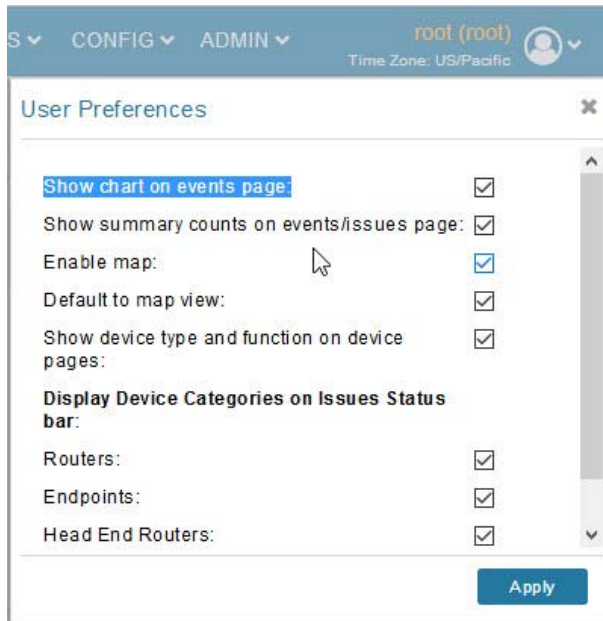
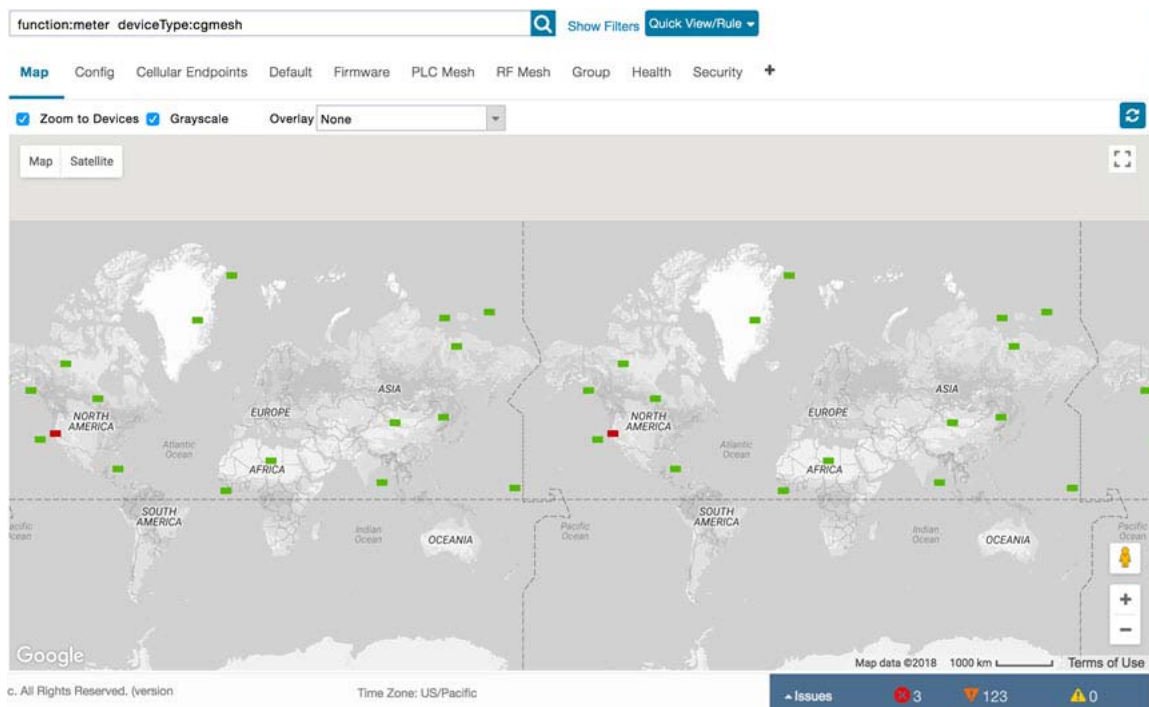


Figure 3 Map View



Note: You can view any RPL tree by clicking the device in Map view, and closing the information popup window.

The RPL tree connection displays data traffic flow as blue or orange lines, as follows:

- Orange lines indicate that the link is an uplink: data traffic flows in the up direction on the map.
- Blue lines indicate that the link is a downlink: data traffic flows in the down direction on the map.

Migrating Router Operating Systems

You can migrate CGR operating systems from CG-OS to Cisco IOS on the **CONFIG > Firmware Update** page, using the procedure in [Performing CG-OS to Cisco IOS Migrations](#).

Refreshing the Router Mesh Key

If you suspect unauthorized access attempts to a router, refresh its mesh key.

Caution: Refreshing the router mesh key can result in mesh endpoints being unable to communicate with the router for a period of time until the mesh endpoints re-register with the router, which happens automatically.

To refresh the router mesh key, select a router or group of routers in the Browse Devices pane, and then in Default view:

1. Check the check boxes of the routers to refresh.
2. Choose **More Actions > Refresh Router Mesh Key** from the drop-down menu.
3. Click **Yes** to continue.

Managing Embedded Access Points on Cisco C819 and Cisco IR829 ISRs

IoT Field Network Director allows you to manage the following embedded access point (AP) attributes on C819 and IR829 ISRs:

Note: IoT Field Network Director can only manage APs when operating in Autonomous mode.

- Discovery
- AP configuration
- Periodic inventory collection
- Firmware update of APs when operating in Autonomous Mode
- Event Management over SNMP

Note: Not all C800 Series and IR800 routers have embedded APs. A C800 ISR features matrix is [here](#). The IR800 ISR features matrix is [here](#).

Using Router Filters

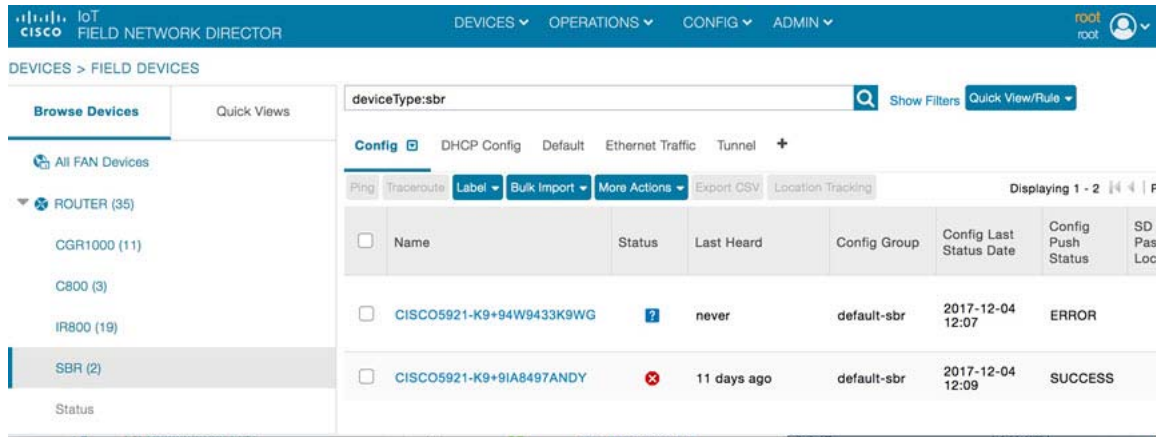
To refine the list of displayed routers, use the built-in router filters under ROUTERS in the Browse Devices pane or saved custom searches in the Quick View pane (left pane). For example, to display all operational routers, click the **Up** group under ROUTERS in the Browse Devices pane. Click a filter to insert the corresponding search string in the Search Devices field. For example, clicking the **Up** group under ROUTERS inserts the search string **status:up** in the Search Devices field.

Displaying Router Configuration Groups

At the **DEVICES > Field Devices** page, use the Browse Devices pane to display routers that belong to one of the groups (such as CGR1000) listed under ROUTER.

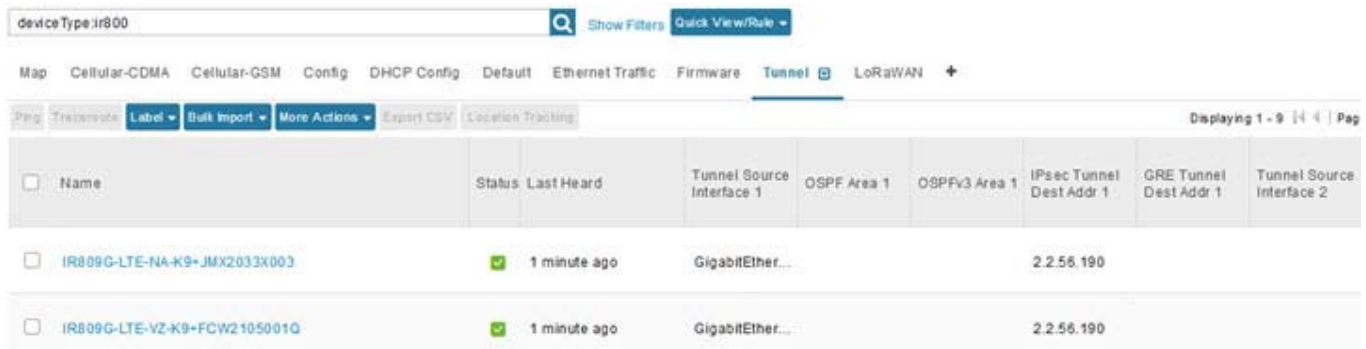
Displaying Router Firmware Groups

1. At the **CONFIG > Firmware Update** page, select the **Groups** tab (left pane) and then choose one of the ROUTER Groups (such as Default-c800, Default-cgr1000, Default-lorawan, Default-ir800 or Default-sbr).
2. The firmware image available for the router displays under the Name field in the right-pane. In the case of the Default-ir800, it includes both the IR809 and IR829, so there are two different firmware images listed.



Displaying Router Tunnel Groups

Use the Browse Devices pane to display the router devices that belong to one of the groups listed under ROUTER TUNNEL GROUPS.



Managing Endpoints

To manage endpoints, view the **DEVICES > Field Devices** page. By default, the page displays the endpoints in List view. This section includes the following topics:

- [Viewing Endpoints in Default View](#)
- [Viewing Mesh Endpoints in Map View](#)
- [Blocking Mesh Devices](#)
- [Displaying Mesh Endpoint Configuration Groups](#)
- [Displaying Mesh Endpoint Firmware Groups](#)

Viewing Endpoints in Default View

When you open the **DEVICES > Field Devices** page in Default view, IoT FND lists All FAN Devices such as Routers, Endpoints (meters, gateways), and IoT Gateway and their basic device properties.

When you select an ENDPOINT device or group in the Browse Devices pane, IoT FND provides tabs to display additional endpoint property views:

Note: Listed below are all the possible tabs (left to right as they appear on the screen).

- Map
- Config
- Cellular Endpoints
- Default
- Firmware
- PLC Mesh
- RF Mesh
- Group
- Health
- Security
- + (Allows you to define a new View (tab))

Each one of these views displays a different set of device properties.

For information on how to customize endpoint views, see [Customizing Device Views](#).

For information about the device properties displayed in each view, see [Device Properties](#).

For information about the common actions in these views (for example, adding labels and changing device properties) that also apply to other devices, see [Common Device Operations](#).

Viewing Mesh Endpoints in Map View

To view mesh endpoints in Map view, select Enable map in *<user>* > **Preferences**, and click the **Map** tab.

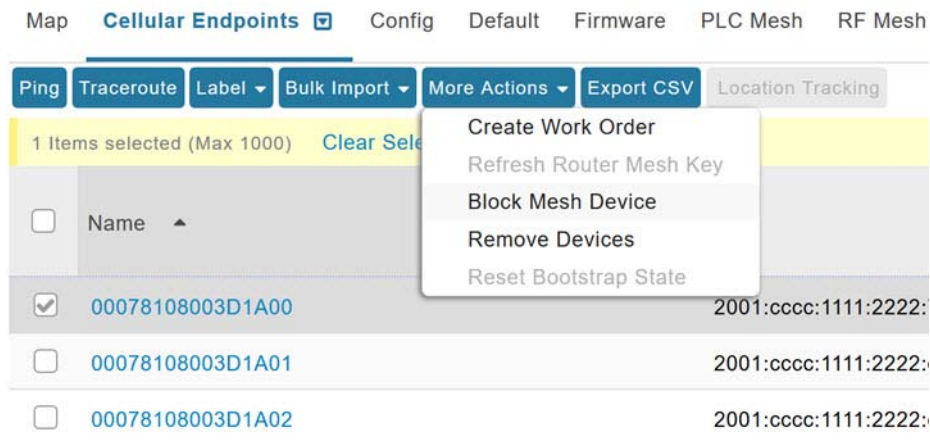
Blocking Mesh Devices

If you suspect unauthorized access attempts to a mesh device, block it from accessing IoT FND.

Caution: If you block a mesh endpoint, you cannot unblock it using IoT FND. To re-register the mesh endpoints with IoT FND, you must escalate and get your mesh endpoints administrator involved.

To block a mesh endpoint device, in Default view (**DEVICES > Field Devices > ENDPOINTS > METER-MESH**):

1. Check the check boxes of the mesh devices to refresh.
2. Choose **More Actions > Block Mesh Device** from the drop-down menu.



3. Click **Yes** in the Confirm dialog box.

4. Delete the mesh endpoint from the NPS server to prevent the device from rejoining the mesh network.

Displaying Mesh Endpoint Configuration Groups

You can view available defined configuration groups for mesh endpoints at the **CONFIG > Device Configuration** page.

Displaying Mesh Endpoint Firmware Groups

You can use the Browse Devices pane to display the mesh endpoint devices that belong to one of the groups listed under ENDPOINTS.

Managing the Cisco Industrial Compute (IC3000) Gateway

Prerequisite

IMPORTANT: Before you can manage the IC3000 Gateway using IoT FND 4.3.1, you must first Deploy Pre-built IOx Applications via the App tab within FND 4.3.1.

For details, refer to the Phase 2 section (summarized below) within the [Cisco IC3000 Industrial Compute Gateway Deployment Guide](#).

■ Phase 2: Deploy Pre-Built IOx Applications via FND

The Phase 2 section within the Cisco IC3000 Industrial Compute Gateway Deployment Guide addresses the following actions, specific to IC3000:

Step 1: Installing FND (This action will most likely already be complete)

Step 2: Adding Devices List to FND

Step 3: Device Registration and DHCP Server Settings

Step 4: Understanding the Device Configuration Template

Step 5: Uploading the Firmware to FND

Step 6: Upgrading Firmware with FND

Step 7: Deploying the IOx Applications via the APP Tab

Overview

IC3000 supports edge computing and communicates with IoT FND through the IOx application, [Cisco Fog Director \(FD\)](#) which accessible via IoT FND.

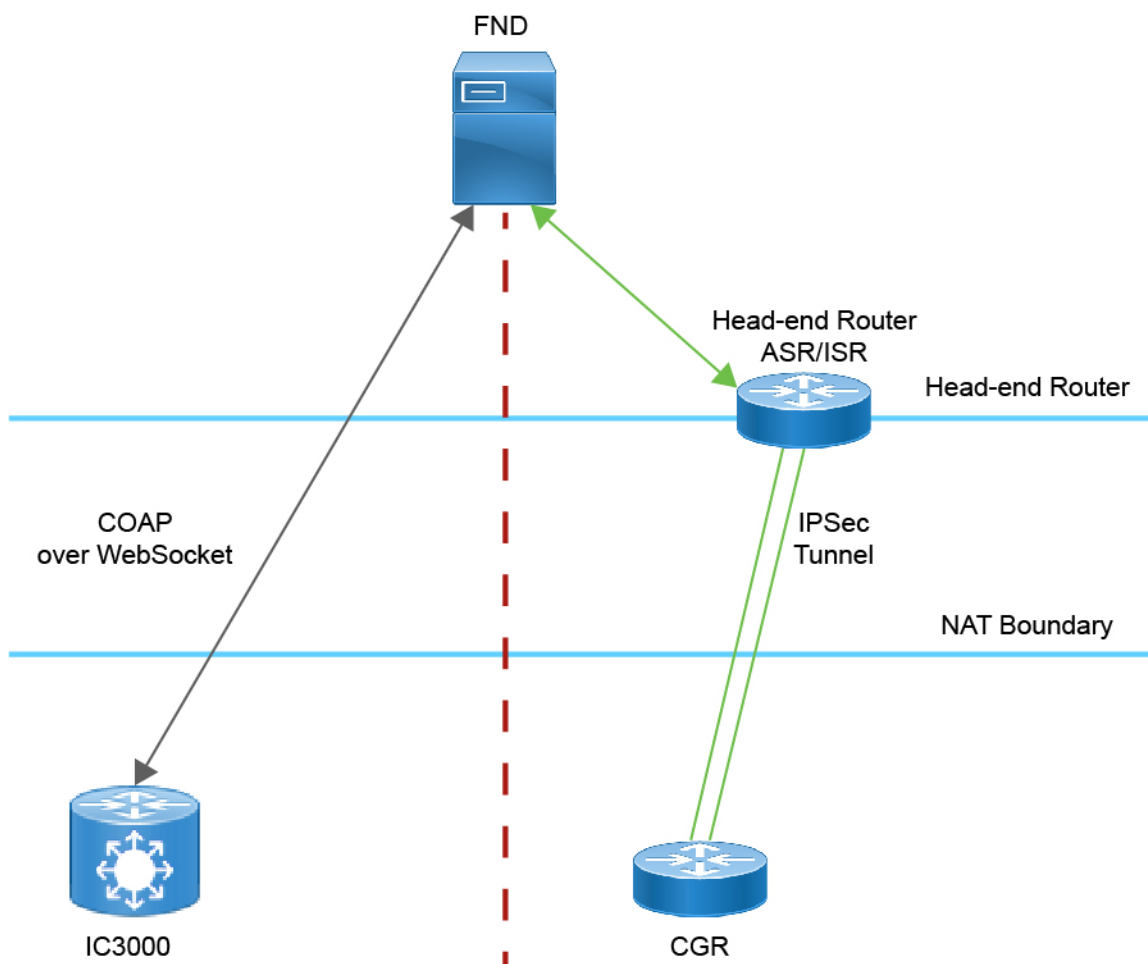
When the IC3000 starts up, it registers with IoT FND. FND then pushes the configuration to the device. Information pushed includes: metric periodic profile interface settings, user management settings and the heartbeat time interval of the device.

Initial communication occurs by establishing a secure HTTPs session. This connection is then upgraded to a WebSocket connection after initial setup.

Using the WebSocket protocol allows the client and server to talk to each other as well as operate independently of each other (see [Figure 4](#)). The client does not need to make a request to connect to the server (see left side of network diagram).

Once established, the client and server communicate over the same TCP connection for the lifecycle of the WebSocket connection.

Figure 4 IC3000 Communicates with FND using CoAP over WebSocket



You can perform the following actions for an IC3000 device type on demand:

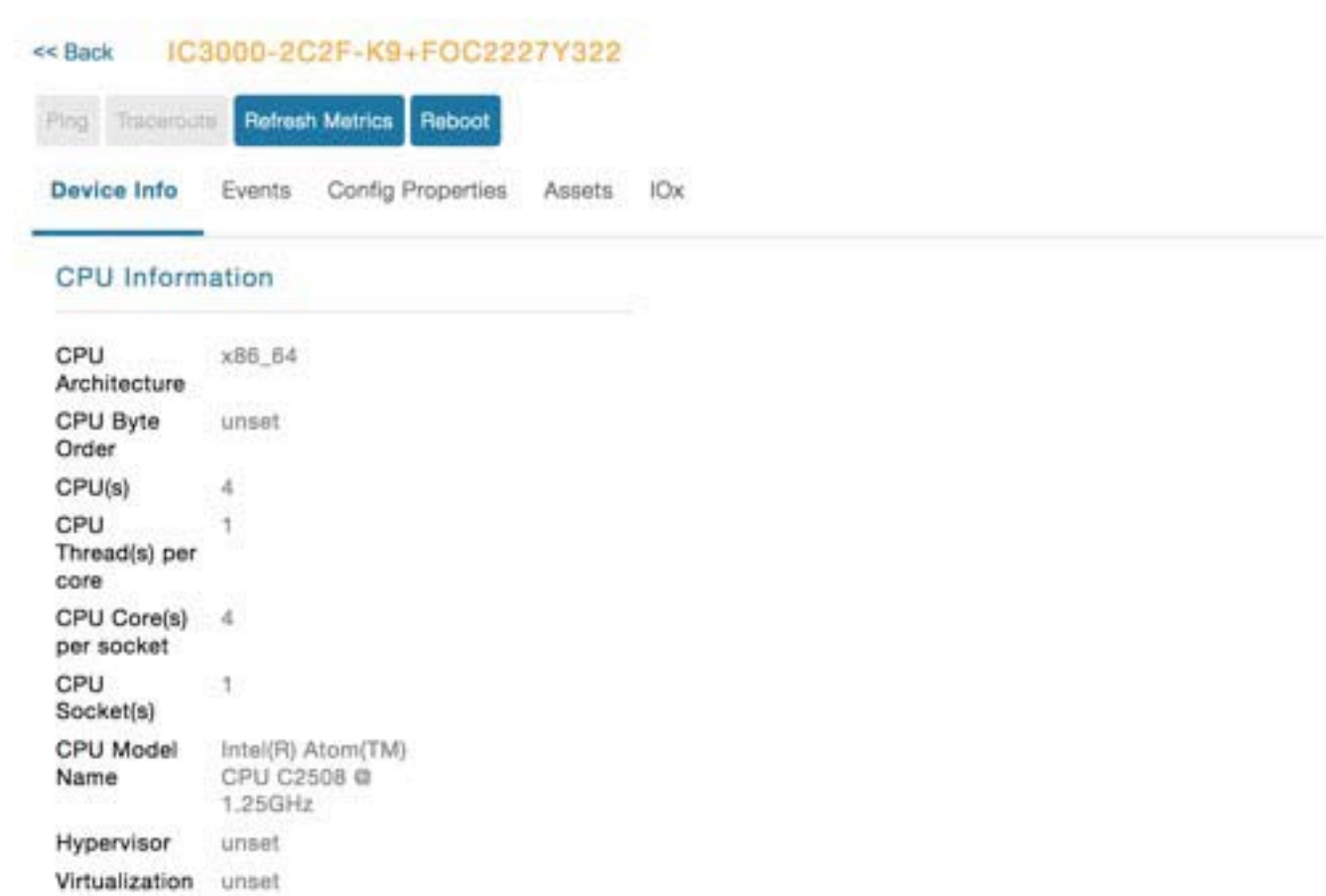
- Refresh Metrics
- Reboot

Device Category: GATEWAY (in Browse Devices pane)

To view the IC3000 Gateway details:

1. Choose **DEVICES > Field Devices**.
2. Select a IC3000 device under GATEWAY in the left-pane. The device info for the gateway appears (Figure 5). At the Device Info page, you can Refresh Metrics and Reboot the IC3000.

Figure 5 Device Info Page for an IC3000 Device



You can view the following information on the Application Management Servers Fog Director.

Managing the Cisco Wireless Gateway for LoRaWAN

You can use the Browse Devices pane to display the Cisco Wireless Gateway for LoRaWAN devices (IXM-LPWA-800 and IXM-LPWA-900) that belongs to the IoT Gateway group.

The two Cisco Wireless Gateway for LoRaWAN products are:

Managing the Cisco Wireless Gateway for LoRaWAN

- A virtual interface (IXM-LPWA-800-16-K9) of the Cisco 809 and 829 Industrial Integrated Service Routers (IR809, IR829) to provide LoRa radio access with the IR809 and IR829 providing an IP backhaul (Gigabit Ethernet, Fiber, 4G/LTE, and Wi-Fi). In this case, LoRaWAN has an Operating Mode of *IOS Interface* and displays the Hosting Device ID for the IR800 system to which it connects. See [Managing External Modules](#)
- A standalone unit (IXM-LPWA-900-16-K9) using its own built-in Fast Ethernet backhaul to access LAN switches, routers, Wi-Fi AP or other IP interfaces. When functioning as a standalone gateway, LoRaWAN has an Operating Mode of *Standalone*.

Device Category: GATEWAY (in Browse Devices pane)

To view the LoRaWAN Gateway:

1. Choose **DEVICES > Field Devices**.
2. Select a device under GATEWAY > default-lorawan or Cisco LoRa in the left-pane.
3. Click on the desired IXM-LPWA-900 or IXM-LPWA-800 system listed in the Name column to display Device Info, Events, Config Properties, Running Config, and Assets for the gateway.

Note: You can view Device details for the IXM-LPWA-800 system at both the ROUTER > IR800 page and the GATEWAY page.

To perform supported actions for the GATEWAY, at the Device Info page use the following buttons:

- Map, Default, + (Plus icon allows you to add a new view)

Figure 6 IoT Gateway Device Info Page, 1 of 2

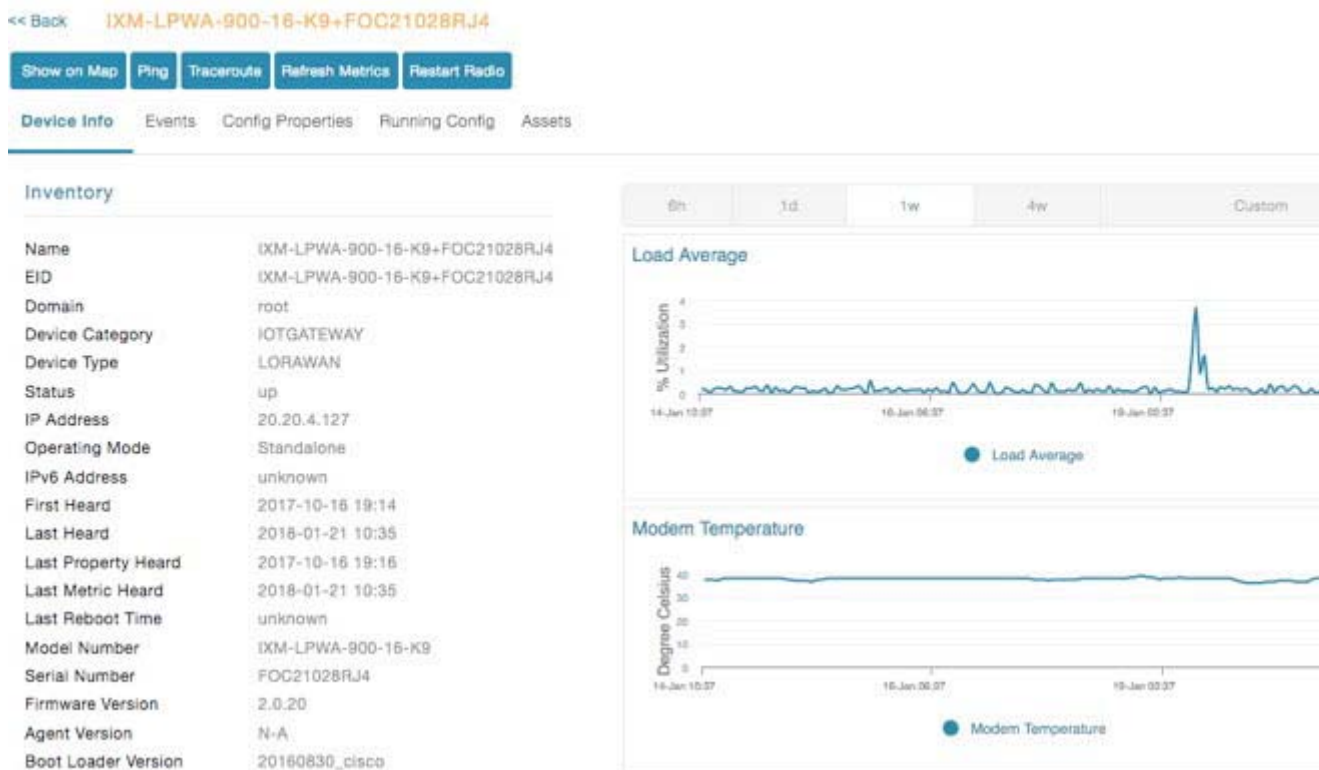


Figure 7 IoT Gateway Device Info Page, 2 of 2

Gateway Health	
Uptime	1d 22hr 37min
Door Status	closed
Modem Temperature	37.0 Celsius
Load Average	1min 0.54 5min 0.23 15min 0.17
System LED	unknown

FPGA Information	
FPGA Version	61
HAL Version	5.1.0
SPI Speed	speed set to 2000000
LoRaWAN Chip 1 Type	SX1301
LoRaWAN Chip 1 Version	103
LoRaWAN Chip 1 ID	1
LoRaWAN Chip 2 Type	SX1301
LoRaWAN Chip 2 Version	103
LoRaWAN Chip 2 ID	1
FPGA Version Check	OK

Packet Forwarder Information	
Packet Forwarder Status	Running
Packet Forwarder Firmware	Installed
Packet Forwarder Version	1.6.11
Packet Forwarder Public Key	Installed
Packet Forwarder Id	6596c3e0

Gateway Properties	
Location	10.6, 10.0
GPS Info Time	unknown
RF Chip ID	LSB = 0x2876f90f MSB = 0x00f14212
Tx Power Calibration	<NA,NA,NA,54,35,108,99,91,82,74,66,56,47,38,29,20-NA,NA,NA,51,32,106,97,89,80,72,64,55,46,37,28,19>
Antenna 1 RSSI Offset(dBm)	-205.00
Antenna 2 RSSI Offset(dBm)	-205.00

Managing Cisco IR510 WPAN Industrial Routers

Cisco IR510 Industrial Router (formerly known as Cisco 500 Series wireless personal area network (WPAN) industrial routers) provides unlicensed 902–928MHz, ISM-band IEEE 802.15.4g/e/v WPAN communications to diverse Internet of Things (IoT) applications such as smart grid, distribution automation (DA), and supervisory control and data acquisition (SCADA). As the next generation of the DA gateway, IR510 provides higher throughput, distributed intelligence, GPS, and enhanced security. unlicensed 915-MHz industrial, scientific, and medical band WPAN communications.

Note: IR510 is identified and managed as an ENDPOINT in IoT FND.

Adaptive Modulation

Adaptive Modulation allows IR510 to dynamically adapt to changes in channel conditions to maximize throughput.

Based on the channel conditions, the node may run on OFDM or FSK mode. FND retrieves info on both modes at the same time and then selects which modulation the IR510 runs on.

To edit the configuration template for the IR510, you enter:

0- Adaptive Modulation

1-FSK

2-OFDM

1. Choose CONFIG > Device Configuration.> Edit Configuration Template

- a. To add a new Adaptive PHY Mode setting for the IR510, select an option from Available Columns panel and click the left-arrow to move the value into the Active Columns panel.
- b. To remove an Adaptive PHY Mode setting for the IR510, select an option from Active Columns panel and click the right-arrow to move the value into the Available Columns panel.

2. Select Default-ir510

Based on the channel conditions, the node may run on OFDM mode or FSK mode, this info should be retrieved by FND, at the same time, FND can select which modulation the node run on.

Profile Instances

IoT FND employs Profile-based configuration for IR510s. This allows you to define a specific Profile instance (configuration) that you can assign to multiple IR500 configuration groups.

“Table 1Pre-defined Profiles for IR510” task on page -75 lists the supported Profile types.

Note the following about the Profiles:

- Each Profile type has a default profile instance. The default Profile instance cannot be deleted.
- You can create a Profile instance and associate that profile with multiple configuration groups on the IR510.
- A ‘None’ option is available for all the Profile types that indicates that the configuration does not have any settings for that Profile type.
- When a configuration push is in progress for a configuration group, all the associated Profiles will be locked (lock icon displays) and Profiles cannot be updated or deleted during that time.
- A lock icon displays for a locked Profile.

Create, Delete, Rename or Clone any Profile at the Config Profiles Page



To create a new profile:

1. Choose **CONFIG > DEVICE CONFIGURATION > Config Profiles** tab

2. Click the **+** (plus icon) at the top of the configuration panel to open the Add Profile entry panel.
3. Enter a **Name** for the new profile and select the **Profile Type** from the drop-down menu.
4. Click **Add** button. A new entry for the Profile entry appears in the left pane under the Profile Type sub-heading.

To delete a profile:

1. Choose **CONFIG > DEVICE CONFIGURATION > Config Profiles** tab.
2. Select the Profile name (excluding Default-Profile) that you want to delete. Click on the trash icon to remove the Profile.
3. In the pop up window that appears, click **Yes** to confirm deletion.

To rename a profile:

1. Choose **CONFIG > DEVICE CONFIGURATION > Config Profiles** tab.
2. Select the Profile name (excluding Default-Profile) that you would to rename. Click on the pencil icon to open the Rename Profile pop up window.
3. Make your edit and click **OK**. New name appears in the left pane.

To clone a profile:

1. Choose **CONFIG > DEVICE CONFIGURATION > Config Profiles** tab.
2. Select the Profile name that you want to clone. Click on the overlapping squares icon to open the Clone Profile pop up window.
3. Enter a **Name** for the new profile and select the **Profile** type from the drop-down menu.
4. Click **Add** button. A new Profile entry appears in the left pane under the Profile Type sub-heading.

Table 1 Pre-defined Profiles for IR510

Profile Name	Description	Properties Configurable in CSV File
<p>Access Control List (ACL) Profile</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > ACL PROFILE > Config Profiles tab</p> <p>Interface configuration</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > Default-ir500 > Edit Configuration Template</p>	<p>Perform packet filtering to control which packets move through the network for increased security.</p> <p>You can define up to 20 ACL Profiles. Each defined ACL has one associated Access Control Entry (ACE) for a maximum of 20 ACEs.</p> <p>The check process goes through ACL from 1 to 20.</p> <p>There is an implicit deny for all ACL at the end of 20 ACL unless configured differently.</p> <p>To configure the interface for the Default-IR500, with Groups tab selected:</p> <p>In right-pane, choose Edit Configuration Template tab and select the Enable Interface ACL check box.</p>	---
<p>Forward Mapping Rule (FMR) Profile</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > FMR PROFILE > Config Profiles tab</p>	<p>Processes IPv4 traffic between MAP nodes that are in two different MAP domains.</p> <p>Each FMR rule has IPv4 Prefix, IPv4 Prefix Length and EA Bits Length.</p> <p>You can define up to 10 FMR Profiles.</p> <p>FMR settings are pushed to the device as a part of MAP-T Settings during configuration push.</p>	<p>Forward Mapping Rule IPv6 Prefix: fmrlIPv6Prefix0 to fmrlIPv6Prefix9</p> <p>Forward Mapping Rule IPv6 Prefix Length: fmrlIPv6PrefixLen0 to fmrlIPv6PrefixLen9</p>
<p>DSCP profile</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > DSCP PROFILE > Config Profiles tab</p>	<p>Sets the DSCP marking for the Ethernet QoS configuration.</p> <p>DSCP marking has three priority levels (low, normal, and medium).</p> <p>You can specify a maximum of 10 IPv4 addresses and associated DSCP markings.</p>	---
<p>MAP-T Profile</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > DSCP PROFILE > Config Profiles tab</p>	<p>Configures endUser properties.</p>	<p>endUserIPv6Prefix bmrlIPv6PrefixLen</p>

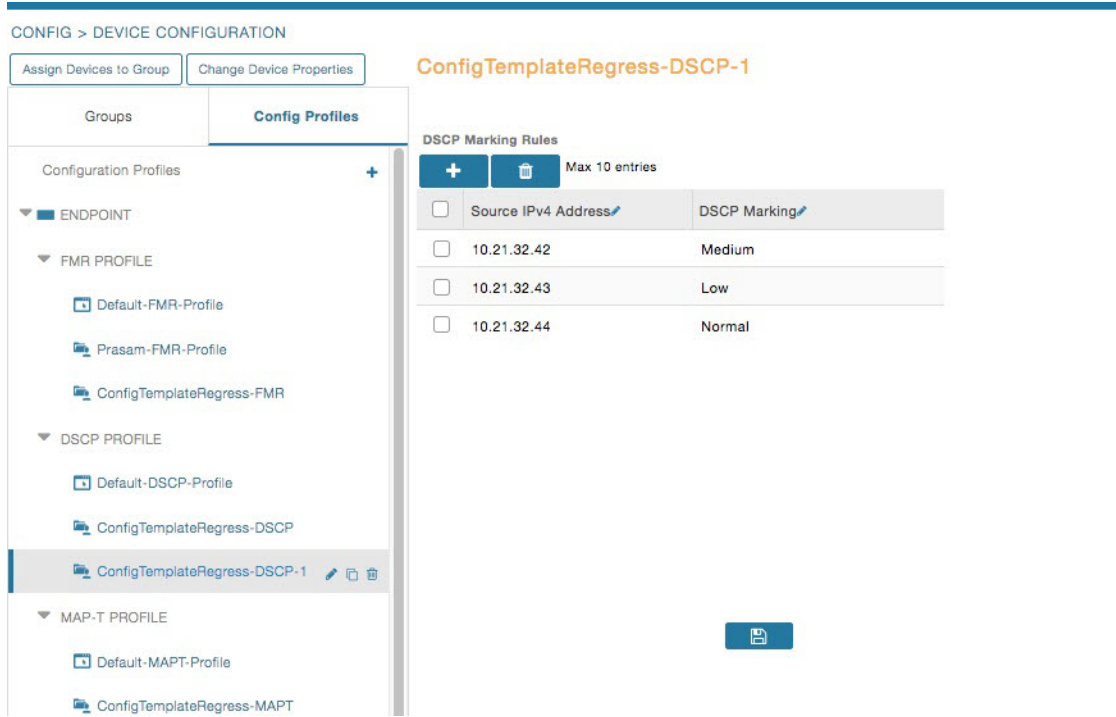
Table 1 Pre-defined Profiles for IR510

Profile Name	Description	Properties Configurable in CSV File
<p>Serial Port Profile (DCE and DTE)</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > SERIAL PROFILE > Config Profiles tab</p>	<p>You can use different serial port profiles for DCE and DTE serial port settings).</p> <p>You can configure the following settings on the serial interface:</p> <ul style="list-style-type: none"> Port affinity Media Type Data Bits Parity Flow Control DSCP Marking Baud rate Stop Bit <p>Note: You can also configure Raw Socket Sessions settings at the this page.</p>	<p>---</p>

Table 1 Pre-defined Profiles for IR510

Profile Name	Description	Properties Configurable in CSV File
<p>DHCP Client Profile</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > DHCP CLIENT PROFILE > Config Profiles tab</p>	<p>The DHCPv4 server allocates an address to each client according to a static binding between a client-id and an IPv4 address.</p> <p>FND configures this static binding supports up to 10 client mappings.</p> <p>The DHCP Client ID binding profile configuration associates a client ID to an IPv4 Host address.</p> <p>The Client-id of each Client is expected to be unique within a single IR510.</p> <p>Any string can be used as client-id (for example, client-id="iox") can be mapped to a binding address in the pool.</p>	<p>---</p>
<p>DHCP Server Profile</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > DHCP SERVER PROFILE > Config Profiles tab</p>	<p>Information that the DHCPV4 Server returns as part of DHCP Options in the response, can be configured in the</p> <p>DHCP server profile configuration includes:</p> <ol style="list-style-type: none"> 1. Lease Time 2. DNS server list 	<p>---</p>
<p>NAT44 Profile</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > NAT 44 PROFILE > Config Profiles tab</p>	<p>You can use one of the following methods to configure the NAT44 properties for the IR500 device:</p> <ul style="list-style-type: none"> - CSV import method - NAT44 profile instance within FND user interface <p>You configure three fields for NAT44: Internal Address, Internal Port and External Port</p> <p>You can configure up to fifteen NAT 44 Static Map entries</p> <p>Note: Before you push the configuration, be sure to:</p> <ol style="list-style-type: none"> 1. Enable Ethernet on the configuration group to which the device belongs (select check box) 2. Save Configuration Group 	<p>---</p>

Figure 8 Configuration Template for a Profile



Configuration Notes:

- Set DSCP (QoS) markings for all interfaces - Ethernet, DTE and DCE. Options: Low Priority (0), Normal Priority (10), Medium Priority (18).
- DSCP is applied on interfaces. Default values for DCE and DTE are Low Priority (0). There are no default values for Ethernet. Traffic will flow unmarked if you do not configure any value on the Configuration Template.
- Only one Raw Socket session can flow through DCE and DTE interfaces at a time. The DSCP value will be the same throughout.

Configuration Profile for a Group

- You can view Profile details in the Configuration Group Template page (Figure 9).
- You can save configuration templates and push the configuration to all devices in the Configuration Group.
- Any of the Profile associations within a Configuration Group are optional. For example, a Configuration Group may not require Serial DCE settings, so you may select 'None' for Serial DCE settings.

Figure 9 Configuration Template for a Group

default-ir500

Sync Membership

Group Members **Edit Configuration Template** Push Configuration Group Properties Transmis

Current Configuration revision #87 - Last Saved on 2017-12-06 00:54

Active Columns

OFDM-800Kbps

Available Columns

OFDM-50kbps

OFDM-200kbps

OFDM-1200kbps

Note: This settings is applicable for **IR510** devices only.

FMR Profile:	ConfigTemplate_FMR	▼	
DSCP Profile:	ConfigTemplate_DSCP	▼	
Map-T Domain Profile:	Default-MAPT-Profile	▼	
DHCP Client Profile:	sce_DHCPClient	▼	
NAT44 Profile:	sce_2	▼	
DHCP Server Profile:	sce_DHCPServerProfile	▼	
Serial Port Profile (DCE):	sce_1_Dce	▼	
Serial Port Profile (DTE):	sce_2_dte	▼	

Managing Head-End Routers

To manage Head-end routers (HERs), open the Head-End Routers page by choosing Devices > Head-End Routers (Figure 10). Unless Enable Map is selected in user preferences, by default, the page displays the HERs in List view. When you open the Head-End Routers page in List view, IoT FND displays the Default list view. This view displays basic HER device properties. In addition, IoT FND provides these tabs to display additional HER property views:

- Tunnel 1
- Tunnel 2

Each one of these views displays different sets of device properties. These views display information about the HER tunnels.

Figure 10 Head-End Routers Page

For information on how to customize HER views, see [Customizing Device Views](#).

For information about the device properties displayed in each view, see [Device Properties](#).

For information about the common actions in these views (for example, adding labels and changing device properties) that also apply to other devices, see [Common Device Operations](#).

Managing External Modules

To manage devices that connect to Field Devices such as routers, choose **Devices > Field Devices**. By default, the page displays all known FAN Devices in List view.

You can manage the following external modules using IoT FND:

Itron CAM Module

You can install an Itron CAM Module within a CGR, **after** you meet the following requirements:

Guest OS (GOS) **must** be running on a CGR before you install the Itron CAM module.

1. ACTD driver **must** be installed and running within the CGR Guest OS **before** you can use IoT FND to deploy, upgrade or monitor ACTD. This ensures that FND can reach the CGR Guest OS to manage the ACTD driver. This can be done by configuring NAT on the CGR or setup a static route on CGR and HER as follows:

A) In the cgms.properties file, you **must** set the “manage-actd” property to *true* as follows:

```
manage-actd=true
```

B) Two new device properties are added for the user to specify the Guest OS external reachable IP address and the IOx access port in case port mapping is used.

```
gosIpAddress <external IP address of Guest OS>
ioxAccessPort <default=8443>
```

2. From within IoT FND, do the following to upload the ACTD driver:

A) Choose **CONFIG > FIRMWARE UPDATE > Images** tab.

B) Select CGR-Default profile from under the Groups panel and click the **Upload Image** button.

C) Click **+** to open the Upload Image panel and Select Type ACTD-CGR and select the appropriate Image from the drop-down menu such *app-actd-ver-x.y.z.tar*.

- D) Click **Upload Image**.
- E) Click **Yes** to confirm upload.

LoRaWAN Gateway Module

- LoRaWAN (IXM-LPWA-800) interface to IR800 router.

There are two ways to upload the LRR image for a LoRaWAN module to the IR800 router: during Zero Touch Deployment (ZTD) and by on-demand configuration push.

Note: IoT FND does not support discovery for the LoRaWAN module. Rather, IoT FND recognizes it as an IR800 module and will communicate with it via Cisco IOS.

- To view LoRaWAN modules in a Device List, choose an IR800 router in the **Browse Devices** list and select the **LoRaWAN** tab.



- To reboot the modem on the LoRaWAN module:
 - a. Click on the relevant IXM-LORA link under the **Name** column to display the information seen below:

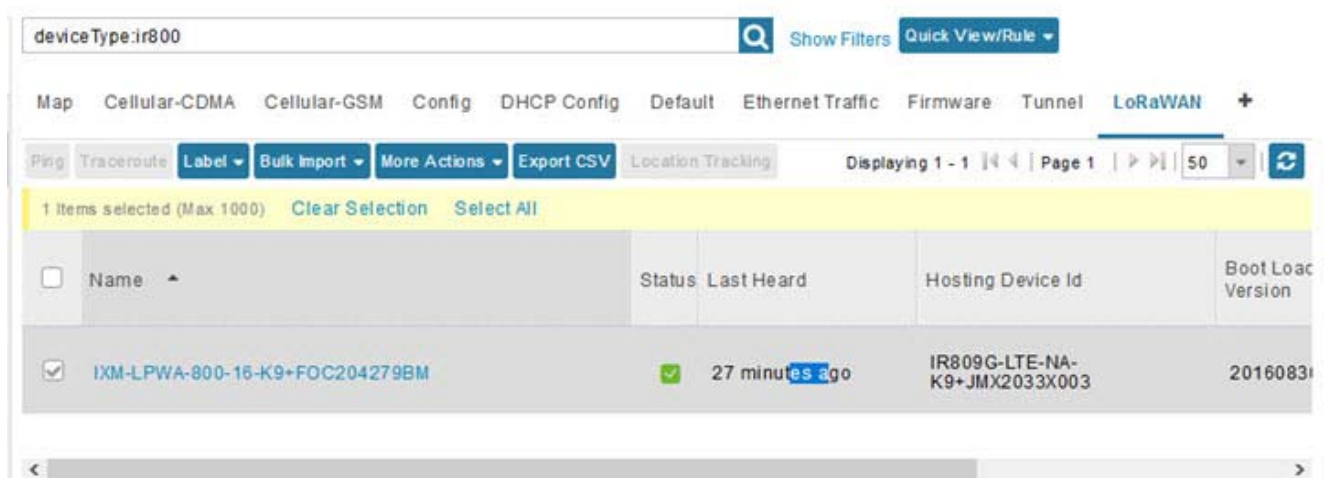


- b. Click **Reboot Modem**. When the reboot completes, the date and time display in the **Last Reboot Time** field in the Device Info pane for the LoRaWAN module. You can only process one modem reboot at a time.

The Reboot Modem action generates two events: LoRa Modem Reboot Initiated and LoRa Modem Reboot Success.

- To remove a LoRaWAN module from the IR800 router inventory:
 - a. In the **Browse Devices** pane, select the IR800, which has the LoRAWAN module that needs to be disabled and removed from inventory.

- b. Select the **LoRaWAN** tab and check the box next to the LoRaWAN module to be removed.



- c. At the More Actions drop-down menu, select **Remove Devices**.
- To create a user-defined LoRaWAN (IXM) Tunnel, choose **CONFIG > Tunnel Provisioning**.
 - a. In the left-pane, under GATEWAY, select the LoRaWAN system for which you want to configure a tunnel.
 - b. Select the **Gateway Tunnel Addition** tab.
 - c. In the Add Group window that appears, enter a **Name** for the LoRaWAN (IXM) Tunnel and select **Gateway** as the Device Category. Click **Add**. The new tunnel appears under the GATEWAY heading in the left-pane.

Managing Servers

To manage servers, open the Servers page by choosing **Devices > Servers**. By default, the page displays the servers in List view. When you open the Servers page in List view, IoT FND displays the Default list view. This view displays basic server device properties. To obtain information about a server, click its name.

To add additional views, see [Customizing Device Views](#).

For more information about the device properties displayed in each view, see [Device Properties](#).

For information about the common actions in this view, see [Common Device Operations](#).

Managing NMS and Database Servers

In the Browse Devices pane, both NMS and Database servers appear under the All Server Devices heading.

In single NMS or Database server deployments, only one server appears under the NMS and/or Database Servers heading. In cluster deployments, multiple NMS servers appear under the NMS Servers heading. To filter the list pane:

- To display all NMS servers, click **Devices > Servers** in the top-level menu and then select NMS Servers within the Browse Devices pane. In single NMS server deployments, only one server appears under the NMS Servers heading. In cluster deployments, multiple NMS servers appear under the NMS Servers heading.
- To display all Database servers, click **Devices > Servers** in the top-level menu and then select Database Servers within the Browse Devices pane. In single-server deployments, only one database server appears under Database Servers. If a secondary database is configured, it also appears under the same entry.

Note: By default, only those NMS and Database Servers in an Up state display.

Managing Application Management Servers

To display details on the Fog Director, click **Devices > Services** in the top-level menu and then select Application Management Servers. Details include: Host System Information, Host Disk Information and Service Information. Graphs displays details on CPU Usage and Memory Usages

Tracking Assets

Assets represent non-Cisco equipment that is associated with an FND-managed Cisco device.

You can view Assets associated with specific routers (**DEVICES > Field Devices**) at the Device Detail pages of CGR1000, IR800, C800, and SBR (Cisco 5921).

You can view a summary of all assets being tracked for all devices at the **DEVICES > Assets** page.

You can perform the following actions on Assets at the **DEVICES > Assets** page, using **Bulk Operation**:

- Add Assets: Use to upload a CSV file of assets to FND. A history of past file uploads displays at the bottom of the page.

Example of Asset content in CSV file:

```
assetName,assetType,deviceEid,assetDescription,vin, hvacNumber,housePlate,attachToWO  
asset1,RDU,00173bab01300000,Sample description,value1, value2, value3,no
```

Note: Asset Name and Asset Type are the mandatory fields in the CSV file. All other fields are optional.

- Change Asset Property (CSV file): Use to make changes to existing assets.
- Remove Assets (CSV file): Use to remove specific assets.
- Add Files to Assets (zip/tar file): Use to append additional information to Asset content.

Guidelines for Adding or Associating an Asset with a Device:

- One or more assets can be mapped to a particular device.
- A limit of five assets can be associated to a single device, and there is also a limit of five files per asset.
- An asset can be mapped to only one device at any point in time.
- The mapped assets can also be useful when creating Work orders for the device.

Common Device Operations

This section describes how to use IoT FND to manage and view information about devices, and includes the following topics:

- [Selecting Devices](#)
- [Customizing Device Views](#)
- [Viewing Devices in Map View](#)
- [Configuring Map Settings](#)

- [Changing the Sorting Order of Devices](#)
- [Exporting Device Information](#)
- [Pinging Devices](#)
- [Tracing Routes to Devices](#)
- [Managing Device Labels](#)
- [Removing Devices](#)
- [Displaying Detailed Device Information](#)
- [Using Filters to Control the Display of Devices](#)
- [Performing Bulk Import Actions](#)

Selecting Devices

In List view, IoT FND lets you select devices on a single page and across pages. When you select devices, a yellow bar displays that maintains a count of selected devices and has the **Clear Selection** and **Select All** commands. The maximum number of devices you can select is 1000. Perform the following to select devices:

- To select all devices listed on a page, check the check box next to **Name**.
- To select devices across all pages, click **Select All**.
- To select a group of devices, check the check boxes of individual devices listed on a page and across pages. The count increments with every device selected, and selections on all pages are retained.

Customizing Device Views

IoT FND lets you customize device views. For List views you can:

- Add and delete tabs
- Specify the properties to display in the columns for each view (see [Device Properties by Category](#) for available properties)
- Change the order of columns

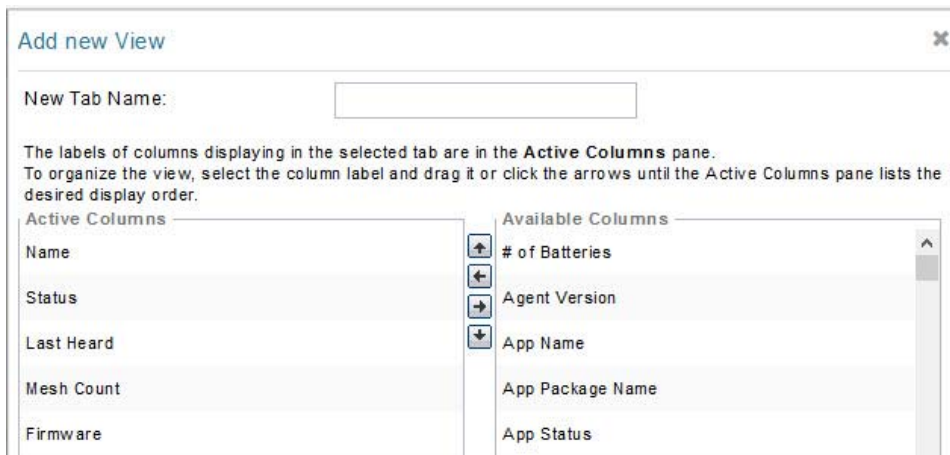
Adding Device Views

To add a custom device view tab to a device page in list view:

1. Click the + tab.



2. In the **Add New View** dialog box, enter the name of the new tab.



3. Add properties to the Active Columns list by selecting them from the Available Columns list, and then clicking the left arrow button, or dragging them into the Active Columns list.

- To change column order, use the up and down arrow buttons or drag them to the desired position.
- To remove properties from the Active Columns list, select those properties and click the right arrow button, or drag them out of the list.

Tip: Hold the Shift key to select multiple column labels and move them to either list.

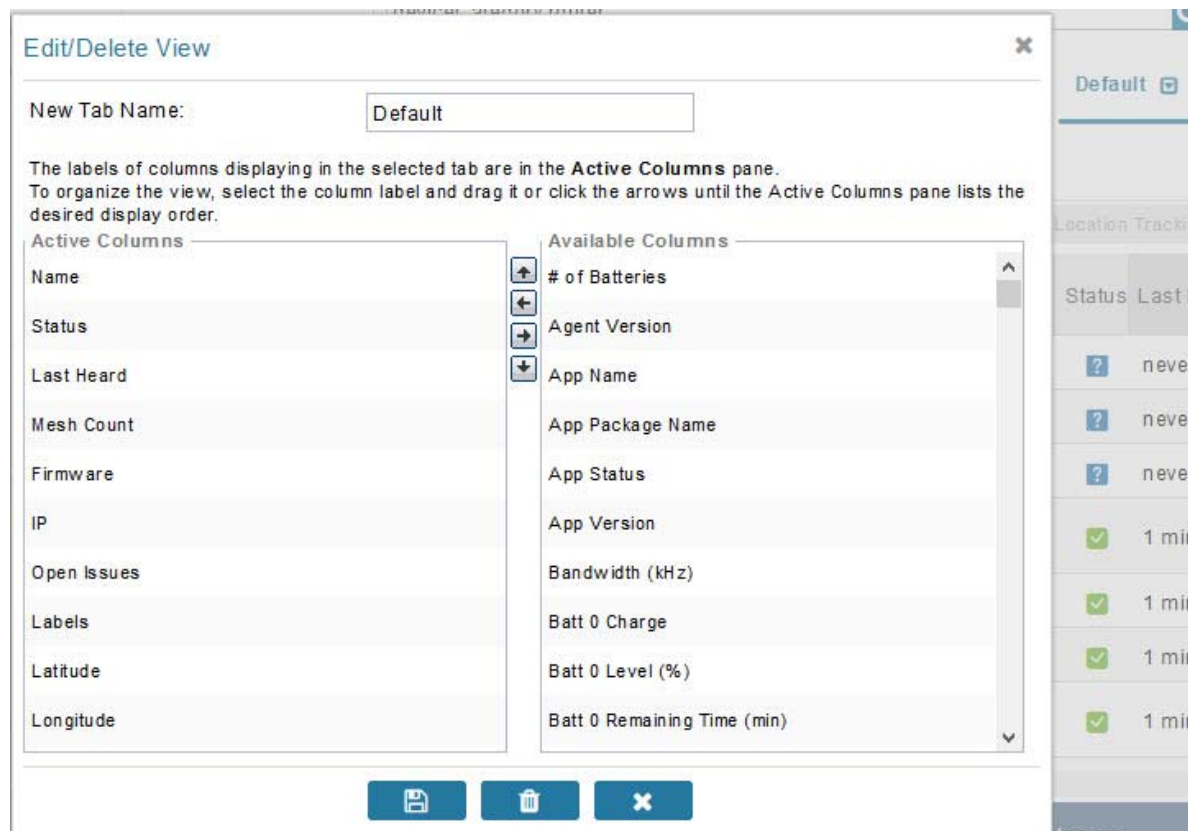
4. Click **Save View**.

Editing Device Views

To edit a device view:

1. Select a device type under the Browse Devices pane, and click the **Default** drop-down arrow to open the Edit/Delete View.
2. In the Edit/Delete View dialog box:
 - a. To remove properties from the Active Columns list, select those properties and click the right-arrow button or drag them out of the Active Columns list.
 - b. To add properties to the Active Columns list, select those properties from the Available Columns list and click the left-arrow button, or drag them into position in the Active Columns list.
 - c. To change the sort order of the active columns, use the up- and down-arrow buttons, or drag them to the desired position.

To close the View without making any changes, select **X** icon.



3. Click disk image to **Save View**.

Deleting a Device View

To remove a View entirely:

1. Select a device type under the Browse Devices pane, and click the **Default** drop-down arrow to open the Edit/Delete View.
2. In the Edit/Delete View dialog box, select the desired label in the Active Columns pane.
3. To delete the view, click the trash icon.

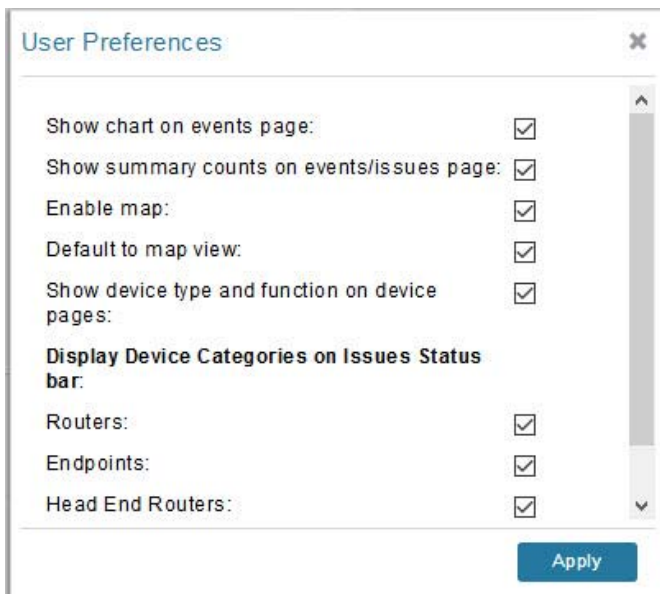
Viewing Devices in Map View

IoT FND provides a map view for visualizing device information based on geographic location. In Map view, IoT FND displays a Geographic Information System (GIS) map and uses GIS Map services to show device icons on the map based on the latitude and longitude information of the device. When this information is not defined for a device, IoT FND does not display the device on the map.

To view devices in Map view:

1. Choose `<user>` > **Preferences** (upper-right hand corner).

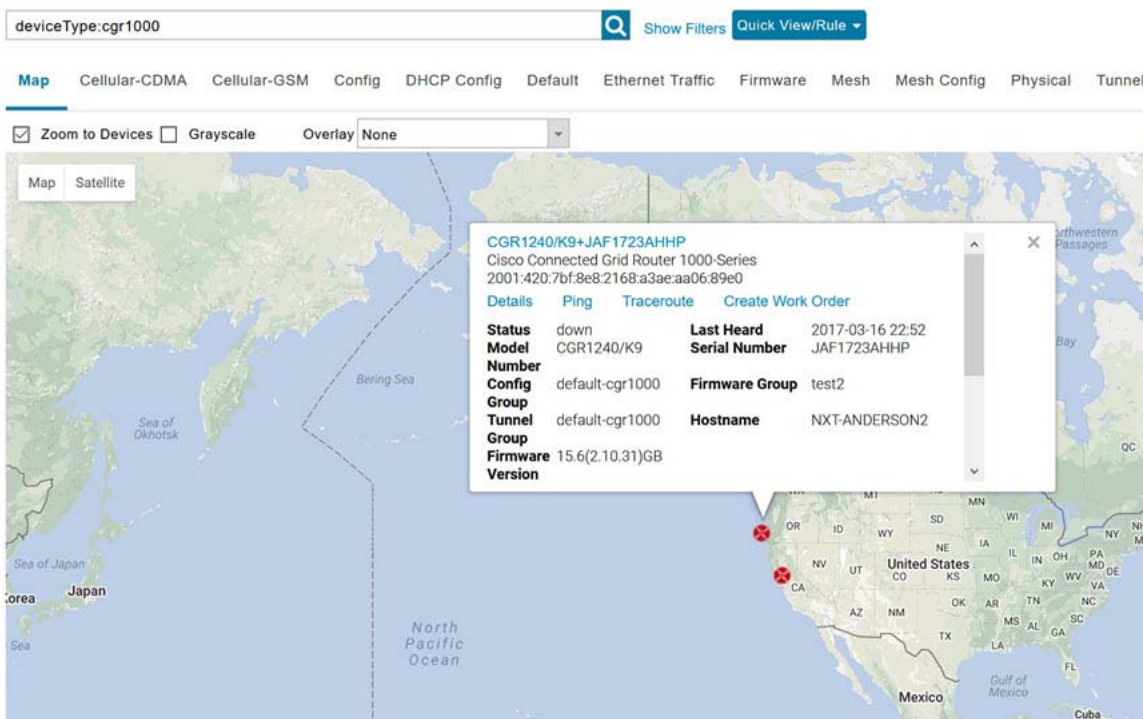
2. Select the **Enable map** check box, and click **Apply**.



3. Choose **DEVICES > Field Devices**.

4. Click the **Map** tab.

By default, IoT FND displays all devices registered in its database on the map. Depending on the zoom level of the map and the device count, individual device icons might not display. Instead, IoT FND displays device group icons.



To view individual devices, zoom in until the device icons appear. You can also click on a device to display a popup window that includes the **Zoom In** link to move the map display to the device level.

IoT FND displays the device count next to each device group or category in the Browse Devices pane (left pane).

- To display a subset of all devices, click one of the filters listed in the Browse Devices pane.
IoT FND changes the map region based on your selection and displays the devices found by the filter. For example, you can use the **Routers > Up** filter to display all routers that are up and running. You can also use saved custom filters in the Quick View pane (left pane) to filter the device view. For information about creating custom filters, see [Creating a Quick View Filter](#).
- To display information about a device or group, click its icon on the map.

A popup window displays listing basic device or group information.

- To view device specifics, click **Details** or the device EID link in the Device popup window.

You can also ping the device, perform a trace route, and create a work order from this window.

5. Close the Device popup window to view the RPL tree associated with the device. See [Configuring RPL Tree Polling](#).

The RPL tree connection displays as blue or orange lines; where blue indicates that the link is down, and orange indicates that the link is up.

6. Click the refresh button to update the Map view.

Configuring Map Settings

In Map view, IoT FND lets you configure these settings for maps:

- Automatically zoom to devices
- Display the map in grayscale
- Default map location (set to North America by default)

To configure map settings:

1. Choose **DEVICES > Field Devices**.

2. Click the **Map** tab.

- To automatically zoom to devices, check the **Zoom to Devices** check box.
- To display the map in grayscale, check the **Grayscale** check box.

Using the Overlay drop-down menu:

- For Routers you can overlay: None, All, or Associated Endpoints on the map.
- For Endpoints you can overlay: None, All, All Associated Routers, All Modulations, Active Link Type.
- To set the map location to open to a certain area, display the area of the map to display by default, and then click **Quick View/Rule** (top of page).

3. Click **OK**.

Changing the Sorting Order of Devices

To change the sorting order of devices, click the arrowhead icon in the column heading to list the entries in an ascending (upward pointing) or descending manner (downward pointing).

Exporting Device Information

IoT FND lets you export the device properties of the selected devices in List view. IoT FND exports only properties in the current view.

To export device information displayed in the current view, in List view:

1. Select the devices to export by checking their corresponding check boxes.
2. Click **Export CSV**.
3. Click **Yes** in the confirmation dialog box.

IoT FND creates a CSV file, `export.csv`, containing the information that displays in the List view pane. By default, IoT FND saves this file to your default download directory. When a file with the same name exists, IoT FND adds a number to the default filename (for example, `export-1.csv` and `export-2.csv`).

The `export.csv` file consists of one header line defining the exported fields followed by one or more lines, each representing a device. Here is an example of an export of selected devices from the Field Devices page:

```
name,lastHeard,meshEndpointCount,uptime,runningFirmwareVersion,openIssues,labels,lat,lng
CGR1240/K9+JSJLABTES32,2012-09-19 00:58:22.0,,,,Door Open|Port Down,,50.4,-130.5
sgbuA1_cgr0,,,,,42.19716359,-87.93733641
sgbuA1_cgr1,,,,,44.3558597,-114.8060403
```

Pinging Devices

When troubleshooting device issues, ping registered devices to rule out network connectivity issues. If you can ping a device, it is accessible over the network.

To ping selected devices, in List view:

1. Check the check boxes of the devices to ping.
Note: If the status of a device is Unheard, a ping gets no response.
2. Click **Ping** button in heading above List view entries.

A window displays the ping results. If you check the check box for **Auto Refresh**, IoT FND pings the device at predefined intervals until you close the window. Click the **Refresh** button (far right) to ping the device at any time.

3. To close ping display, click **X** icon.

Tracing Routes to Devices

The Traceroute command lets you determine the route used to reach a device IP address.

Note: You cannot use the Traceroute command with the Itron OpenWay RIVA CAM module or the Itron OpenWay RIVA Electric devices and Itron OpenWay RIVA G-W (Gas-Water) devices.

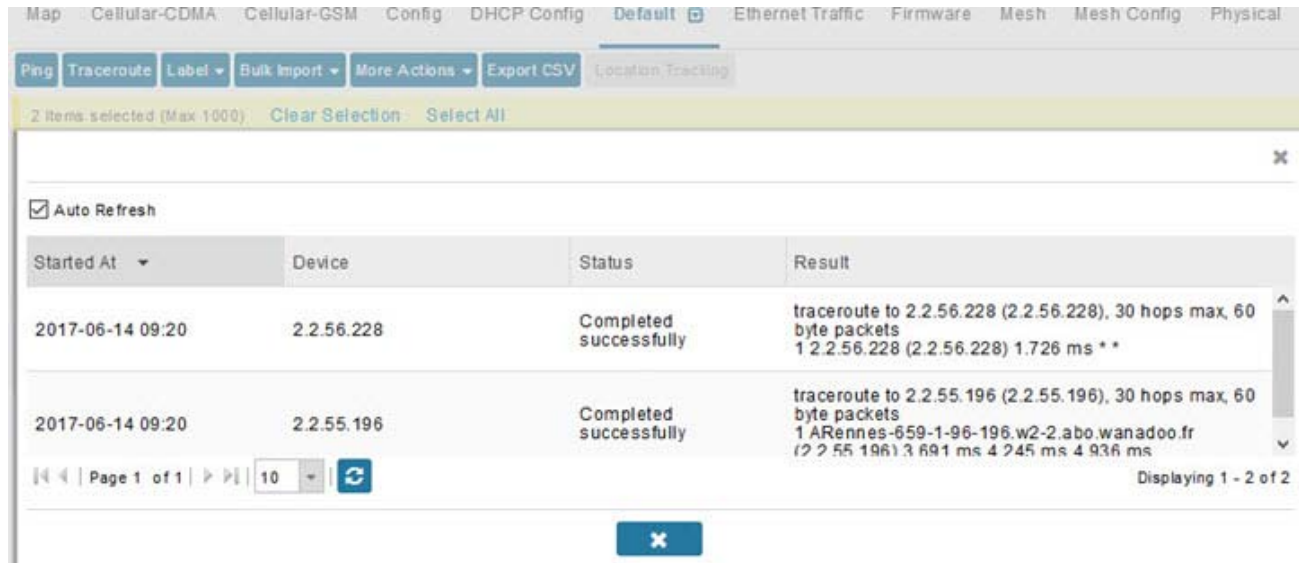
To trace routes to selected devices, in List view:

1. Check the check boxes of the devices to trace.

Note: You can only trace routes to devices registered with IoT FND. If the status of a device is Unheard, you cannot trace the route to it.

2. Click **Traceroute**.

A window displays with the route-tracing results.



Expand the Result column to view complete route information.

Click the **Refresh** button to resend the Traceroute command. Check the **Auto Refresh** check box to resend the Traceroute command at predefined intervals until you close the window.

3. Click **X** to close the window.

Managing Device Labels

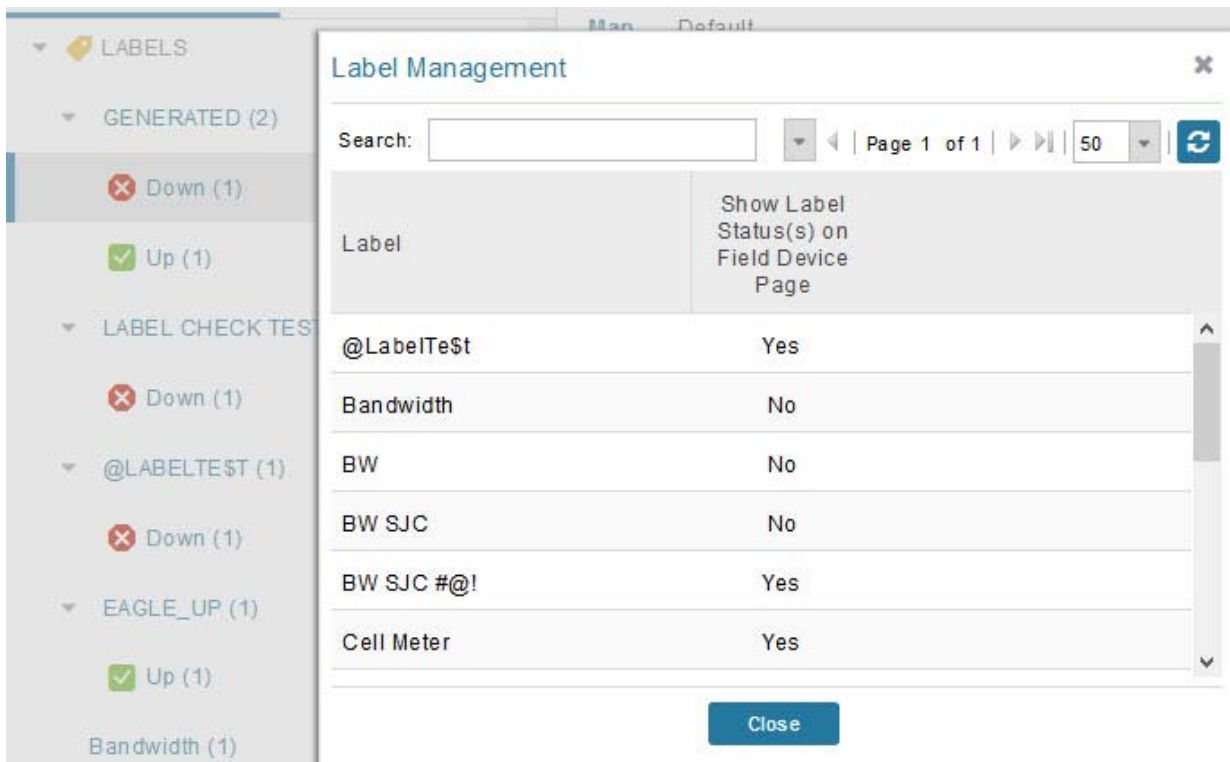
You use labels to create logical groups of devices to facilitate locating devices and device management.

Managing Labels

You use the Label Management window to display all custom labels, label properties, and search for custom labels.

To manage labels, in the Browse Device pane on any devices page:

1. Hover your mouse over LABELS and click the edit (pencil) icon.



- To find a specific label, enter the label name in the **Search** field.
- **Tip:** Click the arrowhead icon next to the Search field to reverse label name sort order.
- To change label properties, double-click a label row and edit the label name and device status display preference.

2. Click **Update** to accept label property changes or **Cancel** to retain label properties.

3. Click **Close**.

Adding Labels

To add labels to selected devices, in List view:

1. Check the check boxes of the devices to label.

Choose **Label > Add Label**.

2. Enter the name of the label or choose an existing label from the drop-down menu.
3. Click **Add Label**.

Tip: You can add multiple labels to one device.

4. Click **OK**.

To add labels in bulk, see [Adding Labels in Bulk](#).

Removing Labels

To remove labels from selected devices, in List view:

1. Check the check boxes of the devices from which to remove the label.
2. Choose **Label > Remove Label**.
3. Click **OK**.

To remove labels in bulk, see [Removing Labels in Bulk](#).

Removing Devices

Caution: When you remove routers, IoT FND returns all the leased IP addresses associated with these devices to the Cisco Network Registrar (CNR) server and removes the corresponding tunnels from the head-end routers.

To remove devices, in List view:

1. Check the check boxes of the devices to remove

2. Choose **More Actions > Remove Devices**.
3. Click **Yes**.

Displaying Detailed Device Information

IoT FND keeps detailed information about every device in the system. To access detailed information about a device, click its name or EID.

- [Detailed Device Information Displayed](#)
- [Actions You Can Perform from the Detailed Device Information Page](#)

Detailed Device Information Displayed

- [Server Information](#)
- [Head-end Router, Router, and Endpoint Information](#)

Note: IoT FND automatically refreshes the detailed device information without the need to reload the page.

Server Information

Select **DEVICES > Servers** and click the Name of the server to open a page to display the following information about the NMS servers.

Table 2 NMS Server Pane Areas

Area and Field Name	Description
Host System Information	
Hostname	Hostname of the IoT FND server.
Host Operating System	Operating system.
CPU	CPU specifications and CPU Usage graph.
Total Memory	Total amount of RAM memory (GB) available on the system and Memory Usage graph.
Current System Time	Current system time.
Host Disk Information	
File System	File system.
Size	Size of file system disk space (GB).
Used	Amount of file system disk space used (GB).
Available	Available file system disk space (GB).
Use %	Percentage of file system disk space used.
Mounted On	The directory in which the file system is mounted.
IoT FND Application Information	
EID	EID of the server.
Start Time	Time when the IoT FND server started.
Number of Restarts	The number of times the IoT FND application has restarted.
Memory Allocation	Memory space allocation in GB for the IoT FND application.
Graphs	
CPU usage	Displays usage information during set and custom-defined intervals.
Memory Usage	Memory usage plotted in MB.
CSMP	CoAP Simple Management Protocol (CSMP) message statistics.

Head-end Router, Router, and Endpoint Information

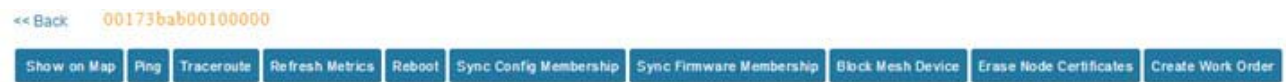
Select **DEVICES > Field Devices** and then select a device type (router, head-end router or endpoint) from the Browse Devices pane. Then, click on the Name of a specific system from the device list to see the available information (such as Device Info, Events, Config Properties, etc.) for that system type as shown in the screen shot below.

A detailed summary for each device is summarized in the table below.



Information Category	Description
Device Info (all)	Displays detailed device information (see Device Properties). For routers and endpoints, IoT FND also displays charts (see Viewing Device Charts).
Events (all)	Displays information about events associated with the device.
Config Properties (routers, endpoints: meter-cgmesh, gateway-IR500, meter-cellular)	Displays the configurable properties of a device (see Device Properties). You can configure these properties by importing a CSV file specifying the properties to configure and their new values, as described in Changing Device Configuration Properties .
Running Config (routers)	Displays the running configuration on the device.
Routing Tree (CGR1000, endpoints: gateway-IR500, meter-cgmesh, meter-OW Riva)	Displays the routing tree. For routers, the pane displays all the possible routers from the endpoints to the router. For endpoints, the Routing Tree pane displays the mesh route to the router.
Link Traffic (routers)	Displays the type of link traffic over time in bits per second.
Router Files (routers)	Lists files uploaded to the .../managed/files/ directory.
Raw Sockets (routers)	Lists metrics and session data for the TCP Raw Sockets (see Table 29 on page 153).
Embedded AP (IR829 only)	Lists inventory (configuration) details and metrics for the attached access point.
AP Running Config (C800 and IR8829 only)	Lists the running configuration file for the attached access point.

Actions You Can Perform from the Detailed Device Information Page



Depending on device type, the Detailed Device Information page lets you perform the actions summarized in the table below:

Action	Description
Show on Map (C800, endpoints)	Displays a popup window with a map location of the device. This is the equivalent of entering eid:Device_EID in the search field in Map View.
Ping	Sends a ping to the device to determine its network connectivity. See Pinging Devices .
Traceroute	Traces the route to the device. See Tracing Routes to Devices .

Common Device Operations

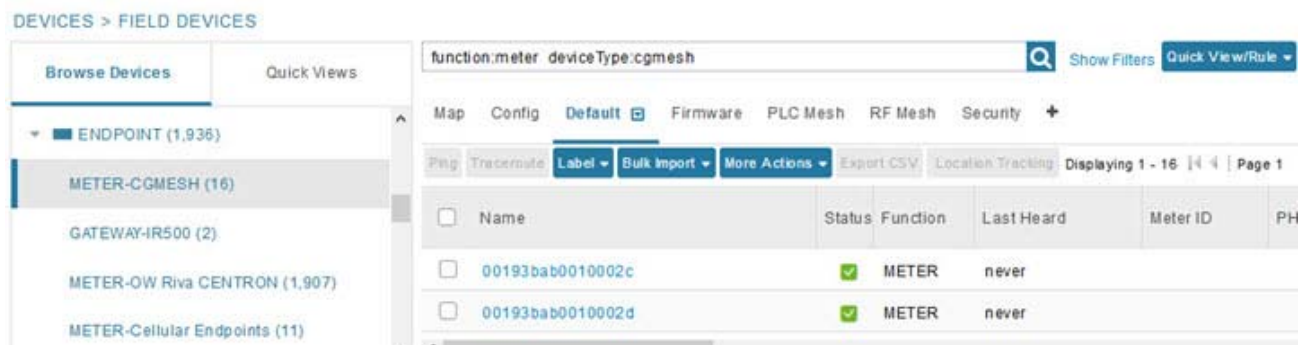
Action	Description
Refresh Metrics (Head-end routers and routers only)	Instructs the device to send metrics to IoT FND. Note: IoT FND assigns historical values for metrics for each device. To access historical metric values, use the GetMetricHistory North Bound API call.
Reboot	Enables a reboot of the modem on LoRaWAN.
Sync Config Membership (Mesh endpoints only)	Synchronizes the configuration membership for this device. See Synchronizing Endpoint Membership .
Sync Firmware Membership (Mesh endpoints only)	Click Sync Firmware Membership to synchronize the firmware membership for this device, and then click Yes to complete the process.
Block Mesh Device (Mesh endpoints only)	Blocks the mesh endpoint device. Caution: This is a disruptive operation. Note: You cannot use Block Mesh Device with the Itron OpenWay RIVA CAM module or the Itron OpenWay RIVA Electric devices and Itron OpenWay RIVA G-W (Gas-Water) devices.
Erase Node Certificates	Removes Node certificates.
Create Work Order (Routers and DA Gateway only)	Creates a work order. See Creating Work Orders .

Using Filters to Control the Display of Devices

Depending on your deployment, the number of devices managed by IoT FND can be very large (IoT FND supports up to 10 million devices). To facilitate locating and displaying devices in Map View and List view, IoT FND provides filters and lets you add customized filters. Filters are listed in the Browse Devices and Quick View tabs.

Browse Devices Filters

Built-in device filters display in the Browse Devices pane. These filters control the display of devices in List and Map views. For every filter entry, IoT FND provides a device count in parenthesis. IoT FND automatically updates the device count without having to reload the page. In the example in [Figure 11](#), the top-level Endpoints label is selected, which inserts the following built-in filter in the Search Devices field: `deviceType:cgmesh firmwareGroup:default-cgmesh`.

Figure 11 Built-in Filter to Search for Mesh Endpoints

Creating and Editing Quick View Filters

The Quick View pane displays custom filters. Click a filter in this pane to view the devices that fulfill the search criteria defined in the filter.

Creating a Quick View Filter

To create a Quick View filter:

1. On any device page, click **Show Filters** and add filters to the Search field.
For more information about adding filters, see [Adding a Filter](#).
2. From the **Quick View/Rule** drop-down menu, choose **Create Quick View**.
3. In the Create Quick View dialog box that opens, enter a Name for the view.
4. Click the disk icon to save the view. To close without saving, click the **X**.

Editing a Quick View Filter

To edit or delete a Quick View filter:

1. Click the Quick View tab and select the filter to edit.
2. From the **Quick View/Rule** drop-down menu, choose **Edit Quick View**.
3. In the **Update Quick View** dialog box, make the necessary modifications, and then click **Save**.
4. To delete the Quick View, click the **Delete** button.

Adding a Filter

To add a filter to the Search field:

1. If the Add Filter fields are not present under the Search field, click **Show Filters**.
2. From the **Label** drop-down menu, choose a filter.

The drop-down menu defines filters for all device information categories. For more information about these categories, see [Working with Router Views](#).

3. From the **Operator** (:) drop-down menu, choose an operator.

For more information about operators, see [Table 3](#). If you choose a numeric metric from the Label menu (for example, **Transmit Speed**), you can specify a range of values in the filter you are adding. For date/time filters, “between” is the operator. Use the calendar buttons to specify the date range for the filter.

4. In the **Value** field, enter a value to match or a range of values in the case of numeric metrics or select an available value from the drop-down menu.
5. Click the Add (+) button to add the filter to the existing filter syntax in the Search field.
6. (Optional) Repeat the process to continue adding filters.

Filter Operators

[Table 3](#) describes the operators you can use to create filters.

Table 3 Filter Operators

Operator	Description
:	Equal to
>	Greater than
>=	Greater than or equal to
<	Less than
<=	Less than or equal to
<>	Not equal to

Search Syntax

IoT FND supports this simple query language syntax:

Search := filter [filter ...]

Filter := fieldname operator value

operator := < | <= | > | >= | <> | = | :

Note the following when creating filters to search fields:

- Each field has a data type (String, Number, Boolean, and Date).
- String fields can contain a string, and you can search them using string equality (“:”).
- Numeric fields can contain a decimal number (stored as a double-precision float), and you can search them using the numeric comparison operators (“>”, “>=”, “<”, “<=”, “<>”).
- Boolean fields can contain the strings “true” or “false”.
- Date fields can contain a date in this format: yyyy-MM-dd HH:mm:ss:SSS. You can search dates using numeric comparison operators.

[Table 4](#) describes filter examples.

Table 4 Filter Examples

Filter	Description
configGroup: "default-cgr1000"	Finds all devices that belong to the default-cgr1000 group.

Table 4 Filter Examples

Filter	Description
configGroup:"default-c800"	Finds all devices that belong to the default-c800 group.
name:00173*	Finds all routers with a name starting with 00173.
deviceType:cgr1000 status:up label:"Nevada"	Finds all CGR 1000s in the Nevada group that are up and running.

Performing Bulk Import Actions

In IoT FND, you can perform these bulk import device actions:

- [Adding Routers, Head-End Routers, IC3000 Gateway, Endpoint and Extenders and IR500 in Bulk](#)
- [Adding HERs to IoT FND](#)
- [Changing Device Properties in Bulk](#)
- [Adding Labels in Bulk](#)
- [Removing Labels in Bulk](#)

Adding Routers, Head-End Routers, IC3000 Gateway, Endpoint and Extenders and IR500 in Bulk

The **Add Devices** option in the Bulk Operation drop-down menu lets you add devices to IoT Field Network Director in bulk using a CSV file.

To add devices in bulk:

1. On any Device page (such as **DEVICES > FIELD DEVICES**), choose **Add Devices**.
2. In the Add Devices window, click **Browse** to locate the CSV file containing the device information to import, and then click **Add**.

For more information about adding gateways, see [Adding an IC3000 Gateway](#)

For more information about adding HERs, see [Adding HERs to IoT FND](#).

For more information about adding routers, see [Adding Routers to IoT FND](#).

Note: For routers, you can also use the Notice-of-Shipment XML file provided by your Cisco partner to import routers.

3. Click **Add**.
4. Click **Close**.

Adding an IC3000 Gateway

To add a gateway to IoT FND, create a CSV file like the following example that consists of a header line followed by one or more lines, each representing a separate gateway:

```
eid,deviceType,lat,lng,I0xUserName,I0xUserPassword
IC3000+FOC2219Y47Z,ic3000,10,10,system,

r6Bx/jSWuFi2vs9U1Zh21NSILakPJNwS1CY/jQBYYRcxSH8qLpgUtOn7nqywr/v0kVPYbNPAFXj4Pbag6m1spjZLR6oc1
PkT9eF6108frFXy+eI2FFaUZ1SCKTdjSqfur5EwEu1E5u54ckMi1e07X8INZuNdFNfU7ZgElt3es8yrpR3i/EgD0dSb5dqw
0u3lOeVrEtPY0xBHraYgPv+dBh3XtW4i2Kv/sveiTBpx2FiNRvuLWil7Qm+D7b11Fh4ZJCivapy7EYZirwHHAVJlQh6bWYr
GAccNpkY+KqIZDCyX/Ck5psmgzyAHKmj8Dq7K0nBsnq2+b2VKReEhsj9+Fw==
```

Adding HERs to IoT FND

Configuring HERs Before Adding them to IoT FND

Before you can add an HER to IoT FND, configure the HER to allow management by IoT FND using Netconf over SSH as follows:

```
hostname <her_hostname>
ip domain-name <domain.com>
aaa new-model
no ip domain-lookup
ip ssh time-out 120
ip ssh version 2
crypto key gen rsa
netconf ssh
netconf max-sessions 16
```

Where <her_hostname> is the hostname or IP address of the IoT FND server, and <domain.com> is the name of the domain name where the HER and IoT FND reside. The time-out value of 120 is required for large networks.

After configuring the HER to allow management by IoT FND, ensure that you can:

- Ping the management interface of the HER.
- Access the management interface of the HER over SSH and vice versa.

Adding HERs

To add HERs, create a CSV file like the following example that consists of a header line followed by one or more lines, each representing an HER:

```
eid,deviceType,lat,lng,ip,netconfUsername,netconfPassword
ASR1001+JAE15460070,asr1000,40.0,-132.0,172.27.166.57,admin,cisco
ASR1001+JAE15460071,asr1000,40.0,-132.0,172.27.166.58,admin,cisco
```

Table 5 describes the fields to include in the CSV file.

Note: For device configuration field descriptions, see [Device Properties](#).

Table 5 HER Import Fields

Field	Description
eid	The element identifier (EID) of the device, which consists of the product ID (PID), a plus sign, and the serial number (SN) of the HER (for example, <i>HER_PID+HER_SN</i>).
deviceType	The device type must be asr1000 or isr3900.
lat	(Optional) The location (latitude and longitude) of the HER.
lng	
ip	The IP address of the HER. The address must be reachable from the IoT FND server.
netconfAddress	
netconfUsername	The SSH username and password that IoT FND uses to connect to the HER.
netconfPassword	

When you add an HER, IoT FND displays its status as Unheard. IoT FND changes the status to Up after it polls the HER. IoT FND polls HERs in the background every 15 minutes to collect device metrics, so it should take no more than 15 minutes for the status of HERs to change to Up after you add them to IoT FND. However, you can trigger the polling of HERs by clicking **Refresh Metrics** ([Refresh Metrics](#)).

Adding Routers to IoT FND

Typically, when adding routers to IoT FND, you use the Notice-of-Shipment XML file sent to you by your Cisco partner. This file contains an <R> record for every router shipped to you. This is an example of an <R> record for a CGR:

```
<AMI>
  <Relays>
    <DCG deviceClass=?10.84.82.56?>
      <PID>CGR1240/K9</PID>
      <R>
        <ESN>2.16.840.1.114416.3.2286.333498</ESN>
        <SN>FIXT:SG-SALTA-10</SN>
        <wifiSsid>wifi ssid 1</wifiSsid>
        <wifiPsk>wifi psk 1</wifiPsk>
        <adminPassword>ppswd 1</adminPassword>
        <type6PasswordMasterKey>secret 1</type6PasswordMasterKey>
        <tunnelSrcInterface1>Ethernet2/3</tunnelSrcInterface1>
      </R>
    </DCG>
  </Relays>
</AMI>
```

Note: For a list of all Device Properties that you can configure using the XML configuration template go to [Device Properties, page 139](#).

Table 6 describes the router properties defined in the <R> record used in this example:

Table 6 Router Import Fields

Field	Description
PID	The product ID, as supplied by Cisco. This is not printed on the product.
SN	The router serial number. Note: IoT FND forms the router EID by combining the PID and SN.
ESN	A serial number assigned by your Cisco partner to the WPAN mesh card inside the router. This field is not used by IoT FND.
wifiSsid	This information is configured on the router by your Cisco partner during the manufacturing configuration process. IoT FND stores this information in its database for future use. Note: For CG-OS CGRs, a maximum of two SSIDs is allowed.
wifiPsk	
adminPassword	
adminUsername	
type6PasswordMasterKey	
tunnelSrcInterface1	

Mapping Routers to HERs

After you determine the Router-to-HER mapping, which is essential for tunnel provisioning, you can configure the mapping in IoT FND in one of two ways:

- Adding the mapping information to every router record in the Notice-of-Shipment XML file.
- Creating a CSV file specifying the mapping of routers to HERs.

Adding Router-to-HER Mappings to the Notice-of-Shipment XML File

To map a router to an HER, add the tunnelHerEid and ipsecTunnelDestAddr1 HER properties to the router record in the Notice-of-Shipment XML file.

- The tunnelHerEid property specifies the EID of the HER
- The ipsecTunnelDestAddr1 property specifies the tunnel IP address of the HER.

For example:

```
...
    <tunnelHerEid>ASR1001+JAE15460070</tunnelHerEid>
    <ipsecTunnelDestAddr1>172.27.166.187</ipsecTunnelDestAddr1>
  </R>
</DCG>
```

Adding Router-to-HER Mappings to a CSV File

To map routers to HERs using a CSV file, add a line for every router-to-HER mapping. The line must specify the EID of the router, the EID of the corresponding HER, and the tunnel IP address of the HER, as in this example for a CGR:

```
eid,tunnelHerEid,ipsecTunnelDestAddr1
CGR1240/K9+FIXT:SG-SALTA-10,ASR1001+JAE15460070,172.27.166.187
```

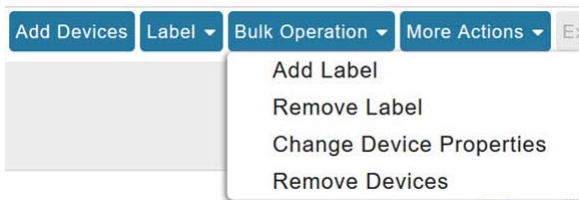
Removing Devices in Bulk

You can remove devices in bulk using a CSV file listing the EIDs of the devices to remove.

Caution: When you remove routers, IoT FND returns all the leased IP addresses associated with these devices to CNR and removes the corresponding tunnels from the HERs.

To remove devices in bulk:

1. Choose **Devices** > *Device Type*.
2. Choose **Bulk Operation** > **Remove Devices**.



3. Click **Browse** to locate the CSV file containing the devices to delete, and then click **Choose**.



Status

This is an example of the CSV format expected. In this case, the CSV file specifies three CGRs and one HER:

```
eid
cgr1000-CA-107
cgr1000-CA-108
cgr1000-CA-109
asr1000-CA-118
```

4. Click **Remove**.

The Status section of the Remove Devices window displays the status of the operation. The History section describes additional information about the operation. If there was any failure, click the corresponding link in the Failure# column to get more information about the error.

5. Click **Close** when done.

Changing Device Properties in Bulk

IoT FND lets you configure device properties in bulk using a CSV file. For example, this CSV file changes the latitude and longitude for the specified HER:

```
eid,lat,lng,ip,  
ASR1001+JAE15460070,42.0,-120.0
```

To configure device properties in bulk:

1. On any device page, choose **Bulk Operation > Change Device Properties**.
2. Click **Browse** to locate the CSV containing the list of devices and corresponding properties to configure, and then click **Open**.
3. Click **Change**.
4. Click **Close** when done.

Adding Labels in Bulk

You can group devices logically by assigning them labels. Labels are independent of device type, and devices of any type can belong to any label. A device can also have multiple labels. Unlike configuration groups and firmware groups, there are no policies or metadata associated with labels.

IoT FND lets you add labels in bulk using a CSV file. In the CSV file, specify the list of devices to be labeled.

To add device labels:

1. On any device page, choose **Bulk Operation > Add Label**.
2. Click **Browse** to locate the CSV file that contains the list of devices to label, and then click *Open*.

This is an example of the expected CSV format:

```
eid  
cgr1000-CA-107  
cgr1000-CA-108  
cgr1000-CA-109  
asr1000-CA-118
```

3. In the **Label** field, enter the label or choose one from the drop-down menu.
4. Click **Add Label**.

The label appears in the Browse Devices tab (left pane) under LABELS.

5. Click **Close** when done.

Removing Labels in Bulk

IoT FND lets you delete labels in bulk using a CSV file.

To delete device labels:

1. On any device page, choose **Bulk Operation > Remove Label**.
2. Click **Browse** to locate the CSV containing the list of devices to remove the label from, and then click **Open**.
3. From the drop-down menu, choose the label to remove.
4. Click **Remove Label**.
5. Click **Close**.

Configuring Rules

A IoT FND rule defines a filter and actions that IoT FND performs after an event or after it receives metrics that match the search criteria defined in the filter. Rules can check for event conditions and metric thresholds.

For example, whenever the status of a router in a configuration group changes to Up, you can add a custom message to the server log (server.log) and add the appropriate labels to the device. This helps you automate the process of adding labels to devices.

When working with rules, you can do the following:

- Add rules with conditions and actions.
- Define a rule with a condition using a device search query, which matches devices according to properties and metrics.
- Define a rule with an action that adds labels to matching devices or to the devices that sent a matching event.
- Define a rule with an action that removes a label from a matching device or the device that sent a matching event.
- Define a rule with an action that places a *user alert* event into the log, which includes a user-defined message.

Viewing and Editing Rules

To view rules:

1. Choose **CONFIG > Rules**.

IoT FND displays the list of rules stored in its database. [Table 7](#) describes the fields displayed in the list.

Table 7 Rule Fields

Field	Description
Name	The name of the rule.
Active?	Whether the rule is active. Rules are not applied until you activate them.
Rule definition	The syntax of the rule. For example, IoT FND executes this rule when a device battery 0 level drops below 50%: <code>battery0Level<50</code>

Table 7 Rule Fields

Field	Description
Rule Actions	<p>The actions performed by the rule. For example:</p> <p>Log Event With: CA-Registered , Add Label: CA-Registered</p> <p>In this example, the actions:</p> <ul style="list-style-type: none"> ■ Set the eventMessage property of the Rule Event generated by this rule to CA-Registered. ■ Add the label CA-Registered to the matching device.
Updated By	The username of user who last updated the rule.
Updated At	The date and time when the rule was last updated.

2. To edit a rule, click its name.

For information on how to edit rules, see [Creating a Rule](#).

Creating a Rule

To add a rule:

1. Choose **CONFIG > Rules**.
2. Click **Add**.
3. Enter a name for the rule.

Note: If you enter invalid characters (for example, "=", "+", and "~"), IoT FND displays a red alert icon, highlights the field in red, and disables the **OK** button.

4. To activate the rule, check the **Active** check box.
5. In the Construct Rule panel, enter the syntax of the rule.

Use the same syntax used for creating filters. See [Search Syntax](#).

The screenshot shows the 'Create Rule' interface. At the top, there is a 'Name' field and an 'Active' checkbox. Below this is a large text area labeled 'Construct Rule' containing an example rule: 'example: deviceType:cgr1000 status:up ...'. The 'Actions' section at the bottom contains three main options, each with a checkbox and associated input fields:

- Log event with: [Text field]
- Severity: [Dropdown menu]
- User-defined Event Name: [Text field]
- Add Label: [Dropdown menu]
- Show label status on Field Device page: [Text field]
- Remove Label: [Dropdown menu]

A blue save icon is located at the bottom center of the panel.

6. In the Create Rule panel, check the check box of at least one action:

- **Log event with**—Specify the message to add to the log entry of the event in the server log, the severity, and event name.
 - **Severity**—Select the severity level to assign to the event.
 - **User-defined Event**—Assign a name to the event (see [Searching By Event Name, page 197](#)).

For example, if you enter Red Alert in this field, set the Severity to CRITICAL and enter CHECK ROUTER in the Event Name field, the eventMessage field in the logged entry for the event that matches the rule is set to Red Alert, as shown in this sample entry from the server log (server.log):

```
16494287: NMS-200-5: May 02 2017 22:32:41.964 +0000: %CGMS-7-UNSPECIFIED:
 %[ch=EventProducer][sev=DEBUG][tid=com.espertech.esper.Outbound-CgmsEventProvider-1]: Event
 Object which is send = EventObject [netElementId=50071, eventTime=1335997961962,
 eventSeverity=0, eventSource=cgr1000, eventType=UserEventType, eventMessage=Red Alert,
 eventName=CHECK ROUTER, lat=36.319324, lng=-129.920815, geoHash=9n7weedx3sdydv1b6ycjw,
 eventTypeId=1045, eid=CGR1240/K9+JAF1603BBFF]
```

In IoT FND, the message you define in the **Log event with** field appears in the Message field of the matching event entries listed on the Events page (**Operations > Events**), and the new Event Name is a new search filter.

- **Add Label**—Enter the name of a new label or choose one from the **Add Label** drop-down menu.
- **Show label status on Field Devices page**—Shows the status of the device that triggered this rule in the LABELS section of the Browse Devices pane.
- **Remove Label**—Choose the label to remove from the **Remove Label** drop-down menu.

7. Click the **disk** icon to save changes.

Activating Rules

IoT FND only applies rules that you activate.

To activate a rule:

1. Choose **CONFIG > Rules**.
2. Check the check boxes of the rules to activate.
3. Click **Activate**.
4. Click **Yes** to activate the rule.
5. Click **OK**.

Deactivating Rules

If you deactivate a rule, IoT FND does not apply it.

To deactivate rules:

1. Choose **CONFIG > Rules**.
2. Check the check boxes of the rules to deactivate.
3. Click **Yes** to deactivate the rule.
4. Click **OK**.

Deleting Rules

To delete rules:

1. Choose **CONFIG > Rules**.
2. Check the check boxes of the rules to delete.
3. Click **Delete**.
4. Click **Yes** to delete the rule.
5. Click **OK**.

Configuring Devices

This section describes how to configure devices in IoT FND, including:

- [Configuring Device Group Settings](#)
- [Editing the ROUTER Configuration Template](#)
- [Editing the ENDPOINT Configuration Template](#)
- [Pushing Configurations to Routers](#)
- [Pushing Configurations to Endpoints](#)

Configuring Device Group Settings

IoT FND uses groups to manage devices in bulk. When you add routers to IoT Field Network Director, IoT FND automatically adds them to the appropriate default ROUTER configuration groups, for example, **default-cgr1000** or **default-c800**. When you add MEs (meters and range extenders), IoT FND adds them to the default ENDPOINT configuration group, **default-cgmesh**. When you add IR500s, CG-NMS adds them to the default ENDPOINT configuration group, **default-ir500**.

- [Creating Device Groups](#)
- [Changing Device Configuration Properties](#)
- [Moving Devices to Another Group](#)
- [Listing Devices in a Configuration Group](#)
- [Configuring Periodic Inventory Notification and Mark-Down Time](#)
- [Renaming a Device Configuration Group](#)
- [Deleting Device Groups](#)

Creating Device Groups

By default, IoT FND defines the following device groups listed on the **CONFIG > Device Configuration** page left tree as follows:

Group Name	Description
Default-act	By default, all Itron OpenWay RIVA Electric devices (ENDPOINT) are members of this group. <ul style="list-style-type: none"> Individual RIVA electric devices listed under the Group heading display as <i>OW Riva CENTRON</i>.
Default-bact	By default, all Itron OpenWay RIVA G-W (Gas-Water) devices (ENDPOINT) are members of this group. <ul style="list-style-type: none"> Individual RIVA water meters listed under the Group heading display as <i>OW Riva G-W</i>. Individual RIVA gas meters listed under the Group heading display as <i>OW Riva G-W</i>.
Default-cam	By default, all Itron OpenWay RIVA CAM modules (ENDPOINT) are members of this group. <ul style="list-style-type: none"> Individual RIVA CAM modules listed under the CAM heading display as <i>OW Riva CAM</i>.
Default-c800	By default, all C800s and ISRs (ROUTER) are members of this group.
Default-ir800	By default, all IR807s, IR809s, and IR829s (ROUTER) are members of this group.
Default-cgmesh	By default, all cgmesh endpoints (ENDPOINT) are members of this group.
Default-cgr1000	By default, all CGRs (ROUTER) are members of this group.
Default-sbr	By default, all ESRs (ROUTER) are members of this group. This product is also identified as C5921.
Default-ir500	By default, all IR500s (ENDPOINT) are members of this group.
Default-lorawan	By default all LoRaWAN Gateways (IOT GATEWAY) are members of this group.
default-c800	By default, all ISR 800s are members of this group.
default-ir500	By default, all IR500s are members of this group.

Each default group defines a default configuration template that you can push to all devices in that group. However, if you need to apply a different template to a group of devices, create a new group and modify its default configuration template as needed.

Note: You cannot delete the default groups, but you can change their names, although we do not recommend it. Also, the default ROUTER and ENDPOINT groups use the same icon, while custom groups use a different icon. See [Table 5](#) for icon definitions.

- [Creating ROUTER Groups](#)
- [Creating Endpoint Groups](#)

Creating ROUTER Groups

Note: CGRs, IR800s, C800s, and C5921s (SBR) can coexist on a network; however, you must create custom templates that include all router types.

To create a ROUTER configuration group:

1. Choose **CONFIG > Device Configuration**.
2. Select the default Configuration Group: Default-cgr1000, Default-ir800 or **default-c800.**, Default-c800 or Default-sbr.
3. With the Groups tab selected (top, left pane of page), click the **+** icon (under the heading) to open the **Add Group** entry panel.



4. Enter the name of the group. The Device Category auto-fills *router* by default.

Note: If you enter invalid characters (for example, “=”, “+”, and “~”), IoT FND displays a red alert icon, highlights the field in red, and disables the **Add** button.

5. Click **Add**.

The new group entry appears in the ROUTER list (left pane).

- To change the name of a group, see [Renaming a Device Configuration Group](#).
- To remove a group, see [Deleting Device Groups](#).

Creating Endpoint Groups

To create an Endpoint configuration group:

1. Choose **CONFIG > Device Configuration**.
2. Select the default group (Default-act, Default-bact, Default-cam, Default-cgmesh, Default-ir500)
3. With the Groups tab selected (top, left panel of page), click the **+** icon (under the heading) to open the **Add Group** entry panel. **Note:** The device category (such as endpoint or router) auto-populates.
4. Enter a name for the group. The device category (endpoint, gateway, or router) auto-populates.

Note: If you enter invalid characters (for example, “=”, “+”, and “~”), IoT FND displays a red alert icon, highlights the field in red, and disables the **OK** button.

5. Click **Add**.

The new group entry appears in the appropriate device category list (left pane).

- To change the name of a group, see [Renaming a Device Configuration Group](#).
- To remove a group, see [Deleting Device Groups](#).

Changing Device Configuration Properties

You can change the configurable properties of devices by uploading a Device Properties CSV file with modified values for the devices.

To change device configuration properties:

1. Choose **CONFIG > Device Configuration**.
2. Click **Change Device Properties**.



3. Click **Browse** and select the Device Properties CSV or XML file to upload.
 4. Click **Change**.
 5. Click **Close** when done.
- For a list of configurable device properties in IoT FND, see [Device Properties](#).

Moving Devices to Another Group

There are two ways to move devices from one configuration group to another:

- [Moving Devices to Another Configuration Group Manually](#)
- [Moving Devices to Another Configuration Group in Bulk](#)

Moving Devices to Another Configuration Group Manually

To move devices to another configuration group:

1. Choose **CONFIG > Device Configuration**.

2. Select a group from the list of configuration groups (left pane).
3. Select the check box of the devices to move.
4. Click **Change Configuration Group**.



5. From the drop-down menu in the dialog box, choose the target group for the devices.
6. Click **Change Config Group**.
7. Click **OK**.

Moving Devices to Another Configuration Group in Bulk

To move a large number of devices from one group to another, you can import a CSV file containing the list of the devices to move.

For example, this CSV file specifies the EIDs of three CGRs to move:

```
eid
CGR1120/k9+JS1
CGR1120/k9+JS2
CGR1120/k9+JS3
```

To move devices to another configuration group in bulk:

1. Choose **CONFIG > Device Configuration**.
2. Click **Assign Devices to Group**.



3. Click **Browse** to locate the CSV or XML file containing the list of devices to move, and then click **Open**.
4. From the Group drop-down menu, choose the target group for the devices.
5. Click **Assign to Group**.
6. Click **OK**.

Listing Devices in a Configuration Group

To list the devices in a configuration group:

1. Choose **CONFIG > Device Configuration**.
2. Select a group from the list of configuration groups (left pane).
3. To get more information about a device in the list, click its EID (for example: CGR1240/K9+JAF1723AHGD).

Configuring Periodic Inventory Notification and Mark-Down Time

You can change the periodic inventory notification interval for a configuration group of routers without affecting the logic that IoT FND uses to mark those routers as **Down**. However, for this to happen, you must enable the periodic configuration notification frequency for the router group so that it is less than the mark-down timer.

You can configure the mark-down timer by clicking the Group Properties tab for the group and modifying the value of the Mark Routers Down After field.

- [Configuring Periodic Inventory Notification](#)
- [Configuring the Mark-Down Timer](#)

Configuring Periodic Inventory Notification

To configure the periodic inventory notification interval for a ROUTER configuration group:

1. Click **CONFIG > Device Configuration**.
2. Select a ROUTER configuration group.
3. Click **Edit Configuration Template**.

Group Members
Edit Configuration Template
Push Configuration
Group Properties

Current Configuration revision #10 - Last Saved on 2014-05-07 14:05

```

<#if far.isRunningIos()>
<!--
If a Loopback0 interface is present on the device (normally configured
during tunnel provisioning) then use that as the source interface for
the HTTP client and SNMP traps. The source for the HTTP client is not
changed during tunnel provisioning because usually the addresses assigned
to the loopback interface are only accessible through the tunnels.
Waiting insures the tunnel is configured correctly and comes up.
-->

<!-- Enable periodic inventory notification every 1 hour to report metrics. -->
cgna profile cg-nms-periodic
  interval 15
exit

<!-- Enable periodic configuration (heartbeat) notification every 15 min. -->
cgna heart-beat interval 5]

<#elseif far.isRunningCgOs() <--
<!-- Enable periodic inventory notification every 6 hours to report metrics. -->
callhome
  periodic-inventory notification frequency 360
exit

<!-- Enable periodic configuration (heartbeat) notification every 1 hour. -->
<#if far.supportsHeartbeat()>
callhome
  periodic-configuration notification frequency 60
exit
</#if>

```

347219

4. This step is OS-specific:

- For Cisco IOS CGRs, change the value of the **cgna heart-beat interval** parameter. The time is in minutes. For example, to enable periodic inventory notification to report metrics every 20 minutes for a Cisco IOS CGR, add these lines to the template:


```

<!-- Enable periodic configuration (heartbeat) notification every 20 min. -->
cgna heart-beat interval 20
exit

```
- For CG-OS CGRs, change the value of the **periodic-inventory notification frequency** parameter to the new value. The time unit is minutes.

5. Click disk icon to save changes.

Configuring the Mark-Down Timer

To configure the mark-down timer for a ROUTER configuration group:

1. Click **CONFIG > Device Configuration**.
2. Select a ROUTER configuration group.
3. Click **Group Properties**.

CGOS-IOS

Group Members Edit Configuration Template Push Configuration **Group Properties**

Mark Routers Down After (secs):	<input type="text" value="1800"/>
Number of Periodic Notifications between RPL Tree Polls:	<input type="text" value="2"/>
Maximum Time between RPL Tree Polls (minutes):	<input type="text" value="480"/>

- In the **Mark Routers Down After** field, enter the number of seconds after which IoT FND marks the routers as down if they do not send periodic configuration notifications (heartbeats) to IoT FND during that time.

Note: We recommend a 1:3 ratio of heartbeat interval to mark-down timer.

- Click the disk icon to save changes.
- Ensure that the periodic-configuration notification frequency in the configuration template is less than the value you entered the **Mark Routers Down After** field:
 - Click **Edit Configuration Template**.
 - Ensure that the value of the periodic-configuration notification frequency parameter is less than the **Mark Routers Down After** value.

Use a notification value that is at most one-third of the mark-down value. For example, if you choose a mark-down value of 3600 seconds (60 minutes), set the periodic-configuration notification frequency parameter to 20 minutes:

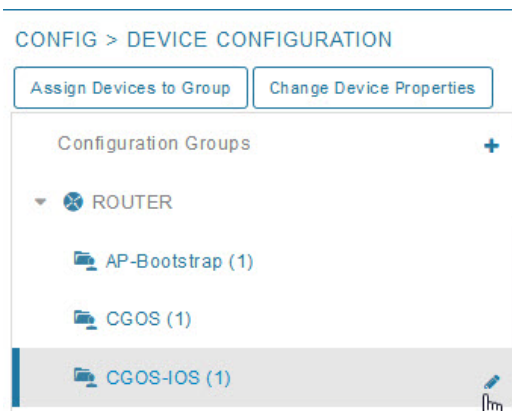
```
<!-- Enable periodic configuration (heartbeat) notification every 20 minutes. -->
<#if far.supportsHeartbeat()>
callhome
  periodic-configuration notification frequency 20
exit
</#if>
```

Note: The ability to control the periodic inventory notification interval and the periodic-configuration notification frequency applies to CGR image version 3.2.

Renaming a Device Configuration Group

To rename a device configuration group:

- Choose **CONFIG > Device Configuration**.
- Select a group from the list of configuration groups (left pane).
- Hover over the name of the group in the list. A pencil icon appears.
- Click on the pencil icon to open the **Edit Group** panel.



5. Enter the new name in the **Rename Group** dialog box, and then click **OK**.

Note: If you enter invalid characters (for example, “=”, “+”, and “~”), IoT FND displays a red alert icon, highlights the field in red, and disables the **OK** button.

Deleting Device Groups

Note: Before deleting a group, move all devices in that group to another group. You cannot delete a non-empty group.

To delete a configuration group:

1. Choose **CONFIG > Device Configuration**.
2. Select a group from the list of configuration groups (left pane).
3. Ensure that the group is empty.
4. Click **Delete Group (-)**.

The Delete icon displays as a red minus sign when you hover over the name of the group in the list.

5. Click **Yes** to confirm, and then click **OK**.

Synchronizing Endpoint Membership

Endpoints maintain information about the IoT FND group to which they belong. If the group information changes, the endpoint becomes out of sync. For example, if you rename an endpoint group, the members of the group might not be modified immediately (for example, due to a packet loss). If a device is out of sync, any operation you perform on the group through IoT FND does not reach the device. To ensure that the endpoints remain in sync, use the Sync Membership button to push the group information to group members.

Note: Devices sync for the first time after they register with IoT FND.

To send group information to endpoints:

1. Choose **CONFIG > Device Configuration**.
2. Select an ENDPOINT group (left pane).
3. In the Group Members pane, click on the name of an endpoint.
4. Click **Sync Config Membership** button on the page that appears.
5. When prompted, click **Yes** to confirm synchronization.

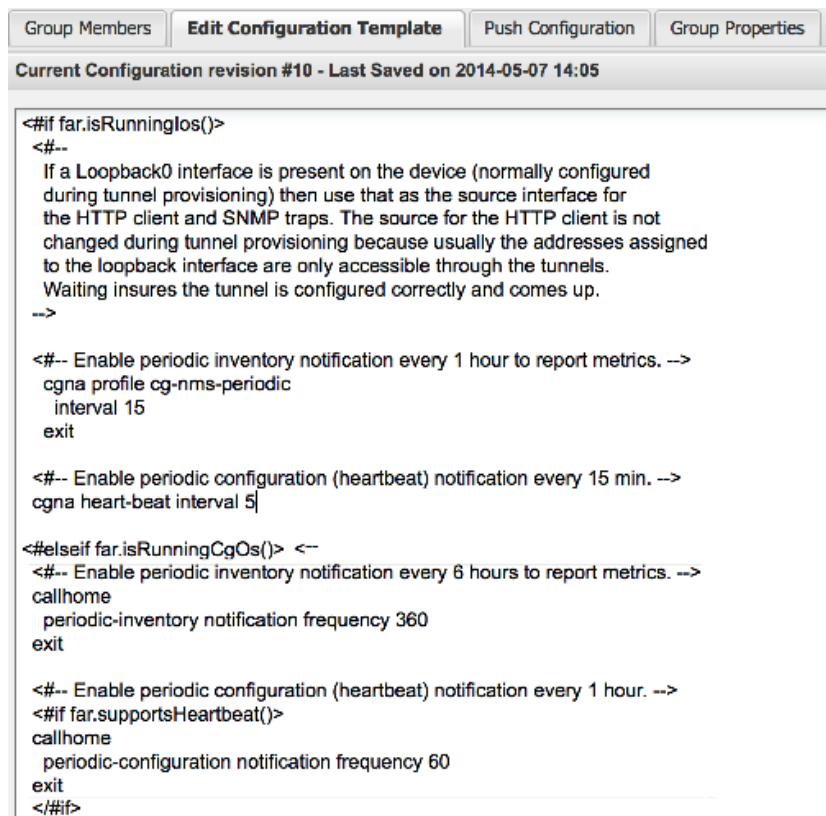
6. Click **OK**.

Editing the ROUTER Configuration Template

IoT FND lets you configure routers in bulk using a configuration template. When a router registers with IoT FND, IoT Field Network Director pushes the configuration defined in the default template to the device and commits the changes to the router startup configuration. IoT FND then retrieves the running configuration from the router before changing the device status to **Up**.

To edit a ROUTER group configuration template:

1. Choose **CONFIG > Device Configuration**.
2. Under CONFIGURATION GROUPS (left pane), select the group with the template to edit.
3. Click **Edit Configuration Template**.



```

<#if far.isRunningIos()>
<#--
If a Loopback0 interface is present on the device (normally configured
during tunnel provisioning) then use that as the source interface for
the HTTP client and SNMP traps. The source for the HTTP client is not
changed during tunnel provisioning because usually the addresses assigned
to the loopback interface are only accessible through the tunnels.
Waiting insures the tunnel is configured correctly and comes up.
-->
-->

<#-- Enable periodic inventory notification every 1 hour to report metrics. -->
cgna profile cg-nms-periodic
  interval 15
exit

<#-- Enable periodic configuration (heartbeat) notification every 15 min. -->
cgna heart-beat interval 5]

<#elseif far.isRunningCgOs() <--
<#-- Enable periodic inventory notification every 6 hours to report metrics. -->
callhome
  periodic-inventory notification frequency 360
exit

<#-- Enable periodic configuration (heartbeat) notification every 1 hour. -->
<#if far.supportsHeartbeat()>
callhome
  periodic-configuration notification frequency 60
exit
</#if>

```

4. Edit the template.

The template is expressed in FreeMarker syntax.

Note: The router configuration template does not validate the configuration data entered. Verify the configuration before saving.

5. Click **Save Changes**.

IoT FND commits the changes to the database and increases the template version number.

Editing the AP Configuration Template

IoT FND lets you configure APs in bulk using a configuration template. When the AP registers with IoT FND, it pushes the configuration defined in the default template to devices and commits the changes to the startup configuration. IoT FND then retrieves the running configuration from the AP before changing the device status to **Up**.

To edit a AP group configuration template:

1. Choose **CONFIG > Device Configuration**.
2. Under CONFIGURATION GROUPS (left pane), select the C800 device group with embedded AP devices with the template to edit.
3. Click **Edit AP Configuration Template**.

<< Back **CGR1240/K9+JAF1623BNLD**

Ping Traceroute Refresh Metrics Reboot Refresh Router Mesh Key Create Work Order

Device Info Events Config Properties Running Config Mesh Routing Tree Mesh Link Traffic Router Files Raw Sockets **Guest OS**

Restart GOS

Name:	CGR1000_JAF1623BNLD-GOS-1
Status:	up
IP Address:	192.168.168.2
OS Version:	1.6.1.1
OS Family:	Linux
External IP Address:	unset
IOx Access Port:	8443

4. Edit the template.

The template is expressed in FreeMarker syntax. For more information about FreeMarker go to <http://freemarker.org/>.

AP TEMPLATE EXAMPLE

```
ip dhcp pool TEST_POOL
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
 lease infinite
!
dot11 ssid GUEST_SSID
 authentication open
 authentication key-management wpa
 wpa-psk ascii 0 12345678
 guest-mode
!
interface Dot11Radio0
 no ip address
 encryption mode ciphers aes-ccm
 ssid GUEST_SSID
!
interface Dot11Radio0
 no ip address
 encryption mode ciphers aes-ccm
 ssid GUEST_SSID
```

Note: The AP configuration template does not validate the configuration data entered. Verify the configuration before saving.

5. Click **Save Changes**.

IoT FND commits the changes to the database and increases the template revision number.

Enabling Dual PHY Support on IoT FND

You can configure CGR master and slave interfaces. For more information about configuring a dual-PHY WPAN interface, refer to [Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide \(Cisco IOS\)](#).

Configuring IoT FND for Dual-PHY

For Dual-PHY CGRs, you must configure all Dual-PHY WPAN modules—master and slaves—by setting the Dual-PHY WPAN Properties (see [Table 22](#)). The parameters to set in the appropriate device addition file are **masterWpanInterface** and **slaveWpanInterface**. For slave Dual-PHY WPAN devices, you must also set the **slave-mode** parameter.

EXAMPLE

The following instructs IoT FND which WPAN devices to allocate as the master interface and slave interface during the configuration push:

```
deviceType, eid, ip, meshPrefixConfig, meshPrefixLengthConfig, meshPanidConfig, meshAddressConfig,
dhcpV4LoopbackLink, dhcpV4TunnelLink, dhcpV6LoopbackLink, dhcpV6TunnelLink, tunnelSrcInterface1,
tunnelHerEid, adminUsername, adminPassword, certIssuerCommonName, ipsecTunnelDestAddr1,
masterWpanInterface, slaveWpanInterface, lat, lng
cgr1000, CGR1240/K9+JAF1741BFQS, 2.2.56.253, 2319:EXTRA:BEEF:CAFE::, 64, 1233,
2319:EXTRA:BEEF:CAFE::, 20.211.0.1, 20.211.0.1, 2001:420:7bf:7e8::1,
2001:420:7bf:7e8::1, GigabitEthernet2/1, cg-isr900, cg-nms-administrator,
0ERIF+cKsLwyT0YTFd0k+NpVAAPxcIvFfoX1sogAXVksOAczUFT8TG0U58ccJuhds52KXL4dtu5iljZsQNH+
pEQ1aIQvIGuIas9wp9MKUARYpNErXRiHEnpeH044Rfa4uSgsWXEyrVNXHyuvSefB5j6H0uA7tIQwEHDxOiq
/d0yxvfd4IYos7NzPXlJNiR+Cp6bwx7dG+d9Jo+JuNXLXpi8Fo5n88usjMoXPNbyrqvgn7SS4f+VYgXxliyDNP0k
+70EE8uSTVeUJXe7UXkndz5CaU17yk94UxOxamv2i1KEQxTFgw/UvrkCwPQoDMiJPstDBXpFv8dqtA0xDGKuaRg
==, cenbursaca-cenbu-sub-ca, 2.2.55.198, Wpan3/1, Wpan5/1, 41.413324, -120.920315
```

The following is a typical template for configuring the master/slave interface on CGR WPAN modules:

```
interface ${device.masterWpanInterface}
  no shut
  ipv6 address ${device.meshAddressConfig}/${device.meshPrefixLengthConfig}
  ieee154 panid ${device.meshPanidConfig}
  outage-server ${device.relayDest}
exit

interface ${device.slaveWpanInterface}
  no ip address
ip broadcast-address 0.0.0.0
no ip route-cache
ieee154 beacon-async min-interval 10 max-interval 10 suppression-coefficient 0
ieee154 ssid cisco_muruga_dual
ieee154 txpower 21
slave-mode 3
rpl dag-lifetime 240
rpl dio-min 21
rpl version-incr-time 240
authentication host-mode multi-auth
authentication port-control auto
ipv6 dhcp relay destination global 2001:420:7BF:5F::705
dot1x pae authenticator
  ieee154 panid ${device.meshPanidConfig}
exit
```

```
end
```

Mesh Security Keys for Dual-PHY Devices

Note: Do not configure mesh security keys on slave WPAN devices.

With master/slave mode configured correctly in IoT FND, IoT FND automatically detects the master WPAN and sets its the mesh security keys. When configuring an existing CGR and adding another WPAN interface, remove all mesh security keys from both interfaces, and then configure master/slave mode through IoT FND. If CGRs are connected, all meters go through re-authentication.

You can remove mesh keys using the command:

```
mesh-security expire mesh-key interface wpan <slot>/<slot number>
```

Configuration Details for WPAN Devices

The following examples retrieve the current Dual-PHY WPAN device RPL slot tree, RPL slot table, RPL IP route info table, and configuration information for slots 4/1 and 3/1.

```
cisco-FAR5#show run int wpan 4/1
Building configuration...
Current configuration : 320 bytes
!
interface Wpan4/1
  no ip address
  ip broadcast-address 0.0.0.0
  no ip route-cache
  ieee154 beacon-async min-interval 100 max-interval 600 suppression-coefficient 1
  ieee154 panid 5552
  ieee154 ssid ios_far5_plc
  ipv6 address 2001:RTE:RTE:64::4/64
  ipv6 enable
  ipv6 dhcp relay destination 2001:420:7BF:5F::500
end
```

```
cisco-FAR5#show run int wpan 3/1
Building configuration...
Current configuration : 333 bytes
!
interface Wpan3/1
  no ip address
  ip broadcast-address 0.0.0.0
  no ip route-cache
  ieee154 beacon-async min-interval 120 max-interval 600 suppression-coefficient 1
  ieee154 panid 5551
  ieee154 ssid ios_far5_rf
  slave-mode 4
  ipv6 address 2001:RTE:RTE:65::5/64
  ipv6 enable
  ipv6 dhcp relay destination 2001:420:7BF:5F::500
end
```

```
cisco-FAR5#show wpan 4/1 rpl stree
```

```
----- WPAN RPL SLOT TREE [4] -----
```

```
[2001:RTE:RTE:64::4]
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1800    // SY RF nodes
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1801
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A00
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1802
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1803
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1804
\--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1805
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A03
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A07
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1806
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1807
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1808
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1809
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:180A
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:180B
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A01
      \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C05
      \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C06
      \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C07
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A02
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A04
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A05
      \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C03
      \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C08
      \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C09
      \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C0A
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A06
      \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C02
      \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C04
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A08
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A09
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A0A
      \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C00
      \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C01
      \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C0B
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A0B
  \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E00    // CY PLC nodes
  \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E01
  \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E02
  \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E03
  \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E04
  \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E05
  \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E06
  \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E07
```

RPL SLOT TREE: Num.DataEntries 44, Num.GraphNodes 45 (external 0) (RF 36) (PLC 8)

```
cisco-FAR5#ping 2001:RTE:RTE:64:217:3BCD:26:4E01
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:RTE:RTE:64:217:3BCD:26:4E01, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 254/266/294 ms
```

```
cisco-FAR5#ping 2001:RTE:RTE:64:207:8108:3C:1C00
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:RTE:RTE:64:207:8108:3C:1C00, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 272/441/636 ms
cisco-FAR5#
```

```
cisco-FAR5#show wpan 4/1 rpl stable
```

```
----- WPAN RPL ROUTE SLOT TABLE [4] -----
```

Configuring Devices

NODE_IPADDR	NEXTHOP_IP	SSLOT	LAST_HEARD
2001:RTE:RTE:64:207:8108:3C:1800	2001:RTE:RTE:64::4	3	17:49:12
// SY RF nodes			
2001:RTE:RTE:64:207:8108:3C:1801	2001:RTE:RTE:64::4	3	18:14:05
2001:RTE:RTE:64:207:8108:3C:1802	2001:RTE:RTE:64::4	3	18:14:37
2001:RTE:RTE:64:207:8108:3C:1803	2001:RTE:RTE:64::4	3	17:56:56
2001:RTE:RTE:64:207:8108:3C:1804	2001:RTE:RTE:64::4	3	17:48:53
2001:RTE:RTE:64:207:8108:3C:1805	2001:RTE:RTE:64::4	3	17:47:52
2001:RTE:RTE:64:207:8108:3C:1806	2001:RTE:RTE:64::4	3	17:49:54
2001:RTE:RTE:64:207:8108:3C:1807	2001:RTE:RTE:64::4	3	17:46:38
2001:RTE:RTE:64:207:8108:3C:1808	2001:RTE:RTE:64::4	3	18:22:01
2001:RTE:RTE:64:207:8108:3C:1809	2001:RTE:RTE:64::4	3	17:50:02
2001:RTE:RTE:64:207:8108:3C:180A	2001:RTE:RTE:64::4	3	17:50:02
2001:RTE:RTE:64:207:8108:3C:180B	2001:RTE:RTE:64::4	3	18:24:00
2001:RTE:RTE:64:207:8108:3C:1A00	2001:RTE:RTE:64:207:8108:3C:1801	3	17:56:34
2001:RTE:RTE:64:207:8108:3C:1A01	2001:RTE:RTE:64:207:8108:3C:180B	3	18:27:34
2001:RTE:RTE:64:207:8108:3C:1A02	2001:RTE:RTE:64:207:8108:3C:180B	3	18:03:06
2001:RTE:RTE:64:207:8108:3C:1A03	2001:RTE:RTE:64:207:8108:3C:1805	3	18:25:18
2001:RTE:RTE:64:207:8108:3C:1A04	2001:RTE:RTE:64:207:8108:3C:180B	3	17:57:15
2001:RTE:RTE:64:207:8108:3C:1A05	2001:RTE:RTE:64:207:8108:3C:180B	3	18:23:39
2001:RTE:RTE:64:207:8108:3C:1A06	2001:RTE:RTE:64:207:8108:3C:180B	3	18:04:16
2001:RTE:RTE:64:207:8108:3C:1A07	2001:RTE:RTE:64:207:8108:3C:1805	3	17:55:00
2001:RTE:RTE:64:207:8108:3C:1A08	2001:RTE:RTE:64:207:8108:3C:180B	3	18:19:35
2001:RTE:RTE:64:207:8108:3C:1A09	2001:RTE:RTE:64:207:8108:3C:180B	3	18:02:02
2001:RTE:RTE:64:207:8108:3C:1A0A	2001:RTE:RTE:64:207:8108:3C:180B	3	18:18:00
2001:RTE:RTE:64:207:8108:3C:1A0B	2001:RTE:RTE:64:207:8108:3C:180B	3	18:02:46
2001:RTE:RTE:64:207:8108:3C:1C00	2001:RTE:RTE:64:207:8108:3C:1A0A	3	18:22:03
2001:RTE:RTE:64:207:8108:3C:1C01	2001:RTE:RTE:64:207:8108:3C:1A0A	3	18:24:03
2001:RTE:RTE:64:207:8108:3C:1C02	2001:RTE:RTE:64:207:8108:3C:1A06	3	18:25:03
2001:RTE:RTE:64:207:8108:3C:1C03	2001:RTE:RTE:64:207:8108:3C:1A05	3	18:15:05
2001:RTE:RTE:64:207:8108:3C:1C04	2001:RTE:RTE:64:207:8108:3C:1A06	3	18:24:05
2001:RTE:RTE:64:207:8108:3C:1C05	2001:RTE:RTE:64:207:8108:3C:1A01	3	18:10:02
2001:RTE:RTE:64:207:8108:3C:1C06	2001:RTE:RTE:64:207:8108:3C:1A01	3	18:05:03
2001:RTE:RTE:64:207:8108:3C:1C07	2001:RTE:RTE:64:207:8108:3C:1A01	3	18:11:03
2001:RTE:RTE:64:207:8108:3C:1C08	2001:RTE:RTE:64:207:8108:3C:1A05	3	18:15:05
2001:RTE:RTE:64:207:8108:3C:1C09	2001:RTE:RTE:64:207:8108:3C:1A05	3	18:15:04
2001:RTE:RTE:64:207:8108:3C:1C0A	2001:RTE:RTE:64:207:8108:3C:1A05	3	18:15:04
2001:RTE:RTE:64:207:8108:3C:1C0B	2001:RTE:RTE:64:207:8108:3C:1A0A	3	18:24:03
2001:RTE:RTE:64:217:3BCD:26:4E00	2001:RTE:RTE:64::4	4	18:21:40
// CY PLC nodes			
2001:RTE:RTE:64:217:3BCD:26:4E01	2001:RTE:RTE:64::4	4	17:47:23
2001:RTE:RTE:64:217:3BCD:26:4E02	2001:RTE:RTE:64::4	4	18:20:16
2001:RTE:RTE:64:217:3BCD:26:4E03	2001:RTE:RTE:64::4	4	17:49:07
2001:RTE:RTE:64:217:3BCD:26:4E04	2001:RTE:RTE:64::4	4	18:21:49
2001:RTE:RTE:64:217:3BCD:26:4E05	2001:RTE:RTE:64::4	4	18:22:06
2001:RTE:RTE:64:217:3BCD:26:4E06	2001:RTE:RTE:64::4	4	18:22:51
2001:RTE:RTE:64:217:3BCD:26:4E07	2001:RTE:RTE:64::4	4	18:24:04

Number of Entries in WPAN RPL ROUTE SLOT TABLE: 44 (external 0)
 cisco-FAR5#show wpan 4/1 rpl itable

```

----- WPAN RPL IPROUTE INFO TABLE [4] -----

```

NODE_IPADDR	RANK	VERSION	NEXTHOP_IP	ETX_P	ETX_LRSSIR	RSSIF	HOPS	PARENTS	SSLT
2001:RTE:RTE:64:207:8108:3C:1800	835	1	2001:RTE:RTE:64::4		0	762	-67	-71	1 1 3
// SY RF nodes									
2001:RTE:RTE:64:207:8108:3C:1801	692	2	2001:RTE:RTE:64::4		0	547	-68	-67	1 1 3
2001:RTE:RTE:64:207:8108:3C:1802	776	2	2001:RTE:RTE:64::4		0	711	-82	-83	1 1 3
2001:RTE:RTE:64:207:8108:3C:1803	968	2	2001:RTE:RTE:64::4		0	968	-72	-63	1 1 3
2001:RTE:RTE:64:207:8108:3C:1804	699	1	2001:RTE:RTE:64::4		0	643	-71	-66	1 1 3
2001:RTE:RTE:64:207:8108:3C:1805	681	1	2001:RTE:RTE:64::4		0	627	-70	-64	1 1 3
2001:RTE:RTE:64:207:8108:3C:1806	744	1	2001:RTE:RTE:64::4		0	683	-69	-68	1 1 3
2001:RTE:RTE:64:207:8108:3C:1807	705	1	2001:RTE:RTE:64::4		0	648	-76	-63	1 1 3
2001:RTE:RTE:64:207:8108:3C:1808	811	2	2001:RTE:RTE:64::4		0	811	-68	-69	1 2 3
2001:RTE:RTE:64:207:8108:3C:1809	730	1	2001:RTE:RTE:64::4		0	692	-68	-70	1 1 3
2001:RTE:RTE:64:207:8108:3C:180A	926	1	2001:RTE:RTE:64::4		0	926	-66	-68	1 1 3
2001:RTE:RTE:64:207:8108:3C:180B	602	2	2001:RTE:RTE:64::4		0	314	-74	-69	1 1 3

Configuring Devices

2001:RTE:RTE:64:207:8108:3C:1A00	948	1	2001:RTE:RTE:64:207:8108:3C:1801	692	256	-73	-75	2	1	3
2001:RTE:RTE:64:207:8108:3C:1A01	646	2	2001:RTE:RTE:64:207:8108:3C:180B	323	256	-73	-75	2	3	3
2001:RTE:RTE:64:207:8108:3C:1A02	948	1	2001:RTE:RTE:64:207:8108:3C:180B	602	256	-73	-75	2	2	3
2001:RTE:RTE:64:207:8108:3C:1A03	803	2	2001:RTE:RTE:64:207:8108:3C:1805	503	256	-68	-78	2	3	3
2001:RTE:RTE:64:207:8108:3C:1A04	858	1	2001:RTE:RTE:64:207:8108:3C:180B	602	256	-65	-69	2	1	3
2001:RTE:RTE:64:207:8108:3C:1A05	646	2	2001:RTE:RTE:64:207:8108:3C:180B	323	256	-71	-69	2	2	3
2001:RTE:RTE:64:207:8108:3C:1A06	858	1	2001:RTE:RTE:64:207:8108:3C:180B	602	256	-73	-75	2	2	3
2001:RTE:RTE:64:207:8108:3C:1A07	979	1	2001:RTE:RTE:64:207:8108:3C:1805	627	352	-71	-73	2	1	3
2001:RTE:RTE:64:207:8108:3C:1A08	646	2	2001:RTE:RTE:64:207:8108:3C:180B	390	256	-75	-70	2	3	3
2001:RTE:RTE:64:207:8108:3C:1A09	948	1	2001:RTE:RTE:64:207:8108:3C:180B	602	256	-70	-69	2	3	3
2001:RTE:RTE:64:207:8108:3C:1A0A	646	2	2001:RTE:RTE:64:207:8108:3C:180B	390	256	-75	-71	2	2	3
2001:RTE:RTE:64:207:8108:3C:1A0B	858	1	2001:RTE:RTE:64:207:8108:3C:180B	602	256	-68	-68	2	2	3
2001:RTE:RTE:64:207:8108:3C:1C00	902	2	2001:RTE:RTE:64:207:8108:3C:1A0A	646	256	-70	-74	3	1	3
2001:RTE:RTE:64:207:8108:3C:1C01	902	2	2001:RTE:RTE:64:207:8108:3C:1A0A	646	256	-71	-72	3	1	3
2001:RTE:RTE:64:207:8108:3C:1C02	1114	1	2001:RTE:RTE:64:207:8108:3C:1A06	858	256	-74	-73	3	1	3
2001:RTE:RTE:64:207:8108:3C:1C03	1114	1	2001:RTE:RTE:64:207:8108:3C:1A05	858	256	-76	-77	3	1	3
2001:RTE:RTE:64:207:8108:3C:1C04	902	2	2001:RTE:RTE:64:207:8108:3C:1A06	646	256	-75	-68	3	2	3
2001:RTE:RTE:64:207:8108:3C:1C05	1114	1	2001:RTE:RTE:64:207:8108:3C:1A01	858	256	-66	-74	3	1	3
2001:RTE:RTE:64:207:8108:3C:1C06	1114	1	2001:RTE:RTE:64:207:8108:3C:1A01	858	256	-74	-72	3	1	3
2001:RTE:RTE:64:207:8108:3C:1C07	1114	1	2001:RTE:RTE:64:207:8108:3C:1A01	858	256	-70	-75	3	1	3
2001:RTE:RTE:64:207:8108:3C:1C08	1114	1	2001:RTE:RTE:64:207:8108:3C:1A05	858	256	-74	-70	3	1	3
2001:RTE:RTE:64:207:8108:3C:1C09	1114	1	2001:RTE:RTE:64:207:8108:3C:1A05	858	256	-70	-74	3	1	3
2001:RTE:RTE:64:207:8108:3C:1C0A	1114	1	2001:RTE:RTE:64:207:8108:3C:1A05	858	256	-70	-69	3	1	3
2001:RTE:RTE:64:207:8108:3C:1C0B	902	2	2001:RTE:RTE:64:207:8108:3C:1A0A	646	256	-76	-74	3	1	3
2001:RTE:RTE:64:217:3BCD:26:4E00	616	2	2001:RTE:RTE:64::4	0	616	118	118	1	1	4
nodes										// CY PLC
2001:RTE:RTE:64:217:3BCD:26:4E01	702	1	2001:RTE:RTE:64::4	0	646	118	118	1	1	4
2001:RTE:RTE:64:217:3BCD:26:4E02	557	2	2001:RTE:RTE:64::4	0	557	118	118	1	1	4
2001:RTE:RTE:64:217:3BCD:26:4E03	626	1	2001:RTE:RTE:64::4	0	579	118	118	1	1	4
2001:RTE:RTE:64:217:3BCD:26:4E04	609	2	2001:RTE:RTE:64::4	0	609	118	118	1	1	4
2001:RTE:RTE:64:217:3BCD:26:4E05	602	2	2001:RTE:RTE:64::4	0	602	118	118	1	1	4
2001:RTE:RTE:64:217:3BCD:26:4E06	594	2	2001:RTE:RTE:64::4	0	594	118	118	1	1	4
2001:RTE:RTE:64:217:3BCD:26:4E07	584	2	2001:RTE:RTE:64::4	0	584	118	118	1	1	4

Number of Entries in WPAN RPL IPRROUTE INFO TABLE: 44

Enabling Router GPS Tracking

You can enable GPS traps to trigger an event if the router moves a distance threshold, after a time threshold, or both. For example, you can configure stationary, pole-top CGR monitoring for a distance threshold, to detect movement from theft or pole incident; for mobile routers, set both thresholds to determine distance over time. The recommended distance threshold is 100 feet (30 m).

To enable GPS traps, uncomment these lines in the default configuration template.

```
<#--
Enable the following configurations to generate events that track if the router
moves by a certain distance (unit configurable) or within a certain time (in minutes)
-->
<#-- cgna geo-fence interval 10 -->
<#-- cgna geo-fence distance-threshold 100 -->
<#-- cgna geo-fence threshold-unit foot -->
<#-- cgna geo-fence active -->
```

Tip: Because GPS traps only generate Informational logs, we recommend that you create a rule-based event with high severity (such as CRITICAL) to inform the administrator of router movement. An example of this type of rule definition is: configGroup:name eventName:deviceLocChanged (see [Creating a Rule](#)).

Configuring SNMP v3 Informational Events

For Cisco IOS routers you configure SNMP v3 Informational Events to replace the default SNMP v3 traps. In CG-OS by default, SNMP v3 traps are configured for any IoT FND event-related changes that generate a trap on the router. IoT FND maps these traps to the corresponding event. For Cisco IOS routers, converting these SNMP v3 traps to SNMP v3 Informational Events sends an acknowledgment to the router for every event received from the router. The router then verifies that the trap was received by IoT FND. To enable SNMP v3 Informational Events, uncomment the following lines in the default configuration file and push the new configuration file to all router(s) in the group:

```
<#-- Enable the following configurations for the nms host to receive informs instead of traps -->
<#-- no snmp-server host ${nms.host} traps version 3 priv ${far.adminUsername} -->
<#-- snmp-server engineID remote ${nms.host} ${nms.localEngineID} -->
```

```
<!-- snmp-server user ${far.adminUsername} cgnms remote ${nms.host} v3 auth sha ${far.adminPassword}
priv aes 256 ${far.adminPassword} -->
<!-- snmp-server host ${nms.host} informs version 3 priv ${far.adminUsername} -->
```

Editing the ENDPOINT Configuration Template

To edit an ENDPOINT configuration template:

1. Choose **CONFIG > Device Configuration**.
2. Under CONFIGURATION GROUPS (left pane), select the **ENDPOINT group** with the template to edit.
3. Click **Edit Configuration Template**.
4. Edit the template.

For example, in the **Report Interval** field, you can enter the number of seconds between data updates. By default, mesh endpoints send a new set of metrics every 28,800 seconds (8 hours).

You can change the following values on the Edit Configuration Template tab:

- **Report Interval:** The number of seconds between data updates.
- **BBU Settings:** Enable this option to configure BBU Settings for range extenders with a battery backup unit.
- **Enable Ethernet:** Check this check box to enable Ethernet for selected devices or configure NAT 44 settings on selected DA Gateway devices.

Note: For NAT 44 configuration, you must specify values for all three fields in a CSV file. The default values are 127.0.0.1, 0, 0, respectively. You do not need to configure any other settings for a particular map index. If these settings are invalid for that map index, they are ignored during a configuration push.
- **MAP-T Settings:** The IPv6 and IPv4 settings for the device.

Note: For Cisco IOS CGRs, MAP-T rules are set by indicating the MAP-T IPv6 basic mapping rule (BMR), IPv4 BMR, and IPv6 default mapping rule (DMR). On Cisco IR509 devices, the MAP-T IPv6 is an IPv6 prefix that integrates the MAP-T BMR IPv6 rules, IPv4 suffix value, and length being based on the BMR EA length value.
- **Serial Interface 0 (DCE) Settings:** The data communications equipment (DCE) communication settings for the selected device.

Note: There can be only one session per serial interface. You must configure the following parameters for all TCP Raw Socket sessions (for each virtual line and serial port) for the selected DA Gateway device(s):

 - Initiator - Designates the device as the client/server.
 - TCP idle timeout (min) - Sets the time to maintain an idle connection.
 - Local port - Sets the port number of the device.
 - Peer port - Sets the port number of the client/server connected to the device.
 - Peer IP address - Sets the IP address of the host connected to the device.
 - Connect timeout - Sets the TCP client connect timeout for Initiator DA Gateway devices.
 - Packet length - Sets the maximum length of serial data to convert into the TCP packet.
 - Packet timer (ms) - Sets the time interval between each TCP packet creation.
 - Special Character - Sets the delimiter for TCP packet creation.
- **Serial Interface 1 (DTE) Settings:** The data terminal equipment (DTE) communication settings for the selected device.

Note: The IPv6 prefix must valid. Maximum prefix lengths are:

- IPv6: 0-128
- IPv4: 0-32

5. Click **Save Changes**.

IoT FND commits the changes to the database and increases the version number.

Pushing Configurations to Routers

Note: CGRs, C800s, IR800s, and ISR 800s can coexist on a network; however, you must create custom configuration templates that include both router types.

To push the configuration to routers:

1. Choose **CONFIG > Device Configuration**.
2. Select the group or subset of a group to push the configuration to in the CONFIGURATION GROUPS pane.
3. Click the **Push Configuration** tab to display that window.
4. In the **Select Operation** drop-down menu, choose **Push Router Configuration**.

For C800 and IR800 groups with embedded AP devices, choose **Push AP Configuration** to push the AP configuration template.

5. In the Select Operation drop-down menu, choose **Push Endpoint Configuration**. Click **Start**.
6. Click **Start**.

The Push Configuration page displays the status of the push operation for every device in the group. If an error occurs while pushing configuration to a device, the error and its details display in the relevant columns.

In the Status column, one of these values appears:

- NOT_STARTED—The configuration push has not started.
- RUNNING—The configuration push is in progress.
- PAUSED—The configuration push is paused. Active configuration operations complete, but those in the queue are not initiated.
- STOPPED—The configuration push was stopped. Active configuration operations complete, but those in the queue are not initiated.
- FINISHED—The configuration push to all devices is complete.
- STOPPING—The configuration push is in the process of being stopped. Active configuration operations complete, but those in the queue are not initiated.
- PAUSING—The configuration push is in the process of being paused. Active configuration operations complete, but those in the queue are not initiated.

Tip: To refresh the status information, click the **Refresh** button.

Enabling CGR SD Card Password Protection

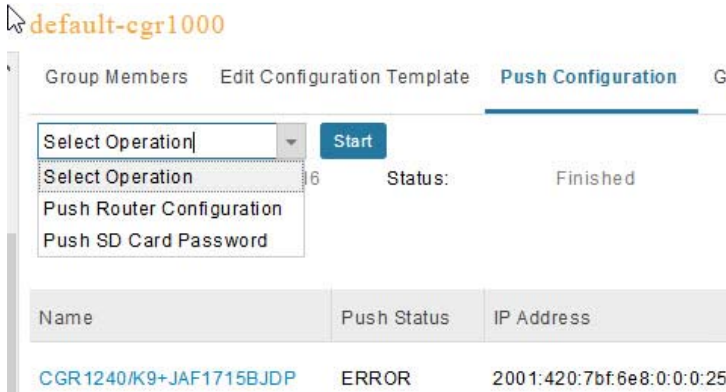
Password protection for the SD card in the CGR helps prevent unauthorized access and prevents transference of the CGR SD card to another system with a different password.

Note: This does not apply to C800s or IR800s.

The Device Info pane displays CGR SD card password protection status in the Inventory section. The Config Properties tab displays the SD card password in the Router Credentials section.

To enable CGR SD card password protection:

1. Choose **CONFIG > Device Configuration**.
2. Select the CGR group or CGRs to push the configuration to in the Configuration Groups pane.
3. Select the **Push Configuration** tab.



4. In the **Select Operation** drop-down menu, choose **Push SD Card Password**.
5. Click **Start**. Click **Yes** to confirm action or **No** to stop action.
6. Select **SD Card protection > Enable**.



7. Select the desired protection method:
 - Property: This password is set using a CSV or XML file, or using the Notification Of Shipment file.
 - Randomly Generated Password: Enter the password length.
 - Static Password: Enter a password.
8. Click **Push SD Card Password**.

Pushing Configurations to Endpoints

To push configuration to mesh endpoints:

1. Choose **CONFIG > Device Configuration**.
2. Select the group or subset of a group to push the configuration to in the **ENDPOINT** list.
3. Click the **Push Configuration** tab.

Note: The Push Configuration tab supports a subnet view for cgmesh Endpoints that summarizes:

Pan ID	Identifies the Personal Area Network Identifier for a group of endpoints (nodes).
Subnet Prefix	Identifies the IPv6 subnet prefix for the endpoint.
Nodes in Group (Total in Subnet)	Number of nodes within the group and the number of nodes in the subset.
Config Synced	Shows how many nodes within a Pan ID are in the process of or have finished a configuration push out of the total nodes in that Pan.

4. In the **Select Operation** drop-down menu, choose **Push Endpoint Configuration**.
5. Click **Start**. Confirm action by clicking the **Yes** button or stop the action by clicking the **No** button.

The Push Configuration page displays the status of the push operation for every device in the group. If an error occurs while pushing configuration to a device, the error and its details display in the relevant columns.

In the Status column, one of these values appears:

- **NOT_STARTED**—The configuration push has not started.
- **RUNNING**—The configuration push is in progress.
- **PAUSED**—The configuration push is paused. Active configuration operations complete, but those in the queue are not started.
- **STOPPED**—The configuration push was stopped. Active configuration operations complete, but those in the queue are not started.
- **FINISHED**—The configuration push to all devices is complete.
- **STOPPING**—The configuration push is in the process of being stopped. Active configuration operations complete, but those in the queue are not started.
- **PAUSING**—The configuration push is in the process of being paused. Active configuration operations complete, but those in the queue are not started.

To refresh the status information, click the **Refresh** button.

Monitoring a Guest OS

Cisco IOS CGR1000s and IR800s support a virtual machine to run applications on a Guest OS (GOS) instance running beside the Cisco IOS virtual machine. The GOS is Linux. Applications running on the GOS typically collect statistics from the field for monitoring and accounting purposes. The Cisco IOS firmware bundle installs a reference GOS on the VM instance on the CGR or IR800s. IoT FND supports the following role-based features on the GOS:

- Monitoring GOS status
- Upgrading the reference GOS in the Cisco IOS firmware bundle

Note: IoT FND only supports the reference GOS provided by Cisco.

You monitor a GOS on the **DEVICES > Field Devices** on the CGR1000 or IR829 configuration page.

Installing a GOS

Depending on CGR factory configuration, a GOS may be present in the VM instance. The GOS installs with the Cisco IOS firmware bundle (see [“Router Firmware Updates” section on page -159](#)). The GOS, Hypervisor, and Cisco IOS all upgrade when you perform a Cisco IOS image bundle installation or update.

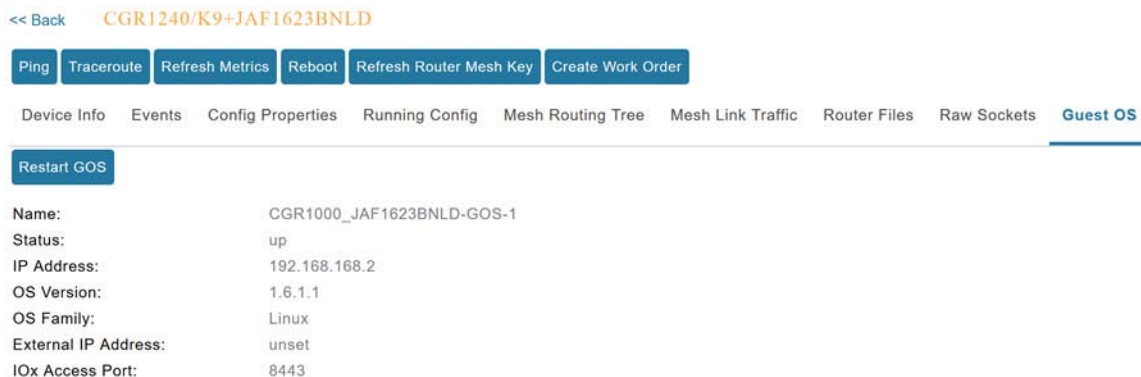
After any Cisco IOS install or upgrade, when IoT FND discovers a GOS, it checks if the initial communications setup is complete before it performs the required setup. The CGR must have a DHCP pool and Gigabit Ethernet 0/1 interface configured to provide an IP address and act as the gateway for the Guest OS. See the [Cisco 1000 Series Connected Grid Routers Configuration Guides](#) web portal for information on configuring the CGR.

Note: if the router is configured with Guest-OS CLI during the router’s registration with FND, FND detects that Guest-OS is running and will populate a new **Guest OS** tab on the Device Info page for that particular router. From that page, we could also trigger a Guest-OS restart. Once the Guest-OS is restarted a pop-up with the status of the operation would be seen on the UI and messages would be logged in the server.log file.

Restarting a GOS

You can trigger a Guest-OS restart from the Guest OS tab. Select the **Restart GOS** button and select **Yes** to confirm restart. Once the Guest-OS restarts, a pop-up with the status of the operation appears in the UI and messages are logged in the server.log file.

Figure 12 DEVICES > Field Devices Information Page Showing Guest OS tab and Restart GOS Button



This section includes the following topics:

- [Pushing GOS Configurations](#)

Pushing GOS Configurations

You can push the GOS configuration to the CGR using the IoT FND config template. This is the only way to configure the DHCP pool.

Managing Files

Use the **CONFIG > Device File Management** page to transfer and execute dual backhaul and Embedded Event Manager (EEM) scripts on the router. The Template module performs file validation. This section includes the following topics:

- [File Types and Attributes](#)
- [Adding a File to IoT FND](#)
- [Transferring Files](#)
- [Viewing Files](#)
- [Monitoring Files](#)
- [Monitoring Actions](#)
- [Deleting Files](#)

Note: File management is role-dependent and may not be available to all users. See [Managing Roles and Permissions](#).

File Types and Attributes

Two types of EEM scripts are used on the router: an embedded applet, and Tool Command Language (TCL) scripts that execute on the router individually. You can upload and run new EEM TCL scripts on the router without doing a firmware upgrade. EEM files upload to the *eem* directory in router flash memory. These scripts display in the **Import File** page File Type column as *eem script*. You must edit the configuration template file to activate the EEM TCL scripts (see [Editing the ROUTER Configuration Template](#)). This feature works with all router OS versions currently supported by IoT FND.

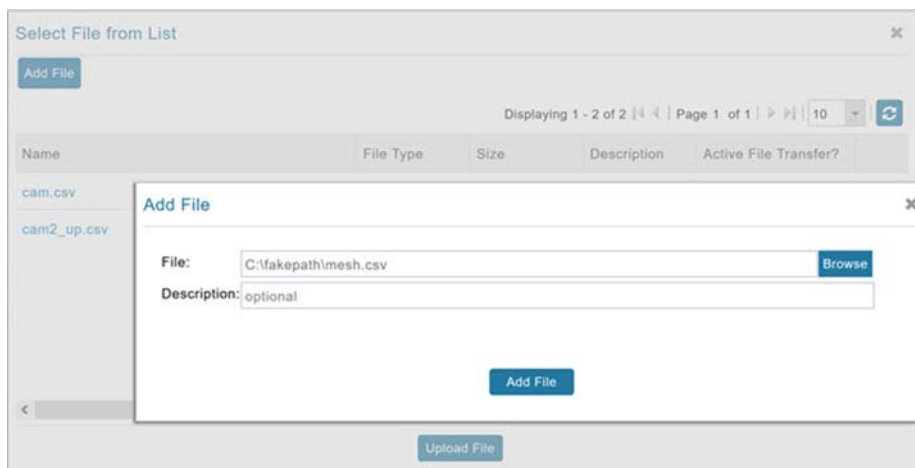
You can also transfer other file types to the router for better file management capability. You must first import the files to IoT FND to upload files to the router. IoT FND processes the file and stores it in the IoT FND database with the following attributes:

- Filename
- Description
- Import Date/Time
- Size
- Sha1 Checksum
- MD5 Checksum
- File Content

Adding a File to IoT FND

To add a file to IoT FND:

1. On the **CONFIG > Device File Management** page, click **Import Files** (far-left pane) or **Upload** (Actions tab) to open a Select File from List dialog box.
2. Click on the file you want to add (import) to FND.



3. Click **Add File** and browse to the file location.

Note: The maximum import file size is 200 MB.

4. (Optional) Type a description for the file.
5. Click **Add File**.

When the upload completes, the file name displays in the Select File From List dialog box.

6. Repeat steps 2 through 5 to add another file, or see [Transferring Files](#) to upload the file to the selected device or group, or close the Select File From List dialog box.

Deleting a File from IoT FND

You can also delete imported files from the IoT FND database if the file is **not** in an active file transfer. This action only removes the file from the IoT FND database, not from any routers that contain the file. Click the Name hyperlink to view uploaded text files (file size must be less than 100KB).

To delete a file from IoT FND:

1. On the **CONFIG > Device File Management** page, select a file from the List dialog box (far-left panel).
2. At the Actions tab, click **Delete** button.
3. At the Delete from List panel, select a file and click **Delete File**.

Transferring Files

You can transfer files from the NMS database to any firmware, configuration or tunnel provisioning group, or to individual routers. The maximum import file size is 200 MB.

To perform a file transfer:

1. On the **CONFIG > Device File Management** page, select the group to transfer the file to from the **Browse Devices** left pane.
2. Click **Import Files** or **Upload** on the **Actions** tab. The **Select File from List** dialog box displays.

3. Select the file to transfer to the routers in the selected group.

4. Click **Upload File**.

The **Upload File to Routers** dialog box displays.

5. Check the check boxes of the routers to which you want to transfer the file.

6. Click **Upload**.

If there is no file transfer or deletion, configuration push, firmware upload, or install or reprovision operations in progress for the group, the upload starts.

You can choose to transfer files to all routers in the selected group or select only a subset of the routers in the group. You can also select another group and file to perform a separate file transfer or deletion simultaneously.

All files transferred from IoT FND reside on the router in `flash:/managed/files/` for Cisco IOS CGRs, and `bootflash:/managed/files/` for CG-OS CGRs.

The status of the last file transfer is saved with the group, as well as the operation (firmware update, configuration push, and so on) and status of the group.

The following file transfer status attributes are added to all group types:

- File Operation: upload
- Start Date/Time of the last transfer
- End Date/Time
- File name
- Allow overwrite: Select True to allow overwrite of file on the CGR
- Success Count
- Failure Count
- Total Count: The number of CGRs selected for the operation
- Status: NOTSTARTED, RUNNING, FINISHED, STOPPING, STOPPED

Viewing Files

To view imported text file content:

1. Select **CONFIG > Device File Management**.
2. Click the EID link (such as CGR1240/K9+JAF1626BLDK) listed under the Name column to display the Device Info pane.
3. Click the **Router Files** tab.
4. Click the file name link to view the content in a new window.

Note: IoT FND only displays files saved as plain text that are under 100 KB. You cannot view larger text files or binary files of any size. Those file types do not have a hyperlink.

Monitoring Files

On the **CONFIG > Device File Management** page, click the **Managed Files** tab to view a list of routers and the files uploaded to their `.../managed/files/` directories. Devices listed in the main pane are members of the selected group.

The following information is included in this list:

- EID link (Name) to the Device Info page
- Number of files (#Files) stored on the device
- File Names uploaded

You can use the **Filter By File Name** drop-down menu to only view devices that contain a particular file. Select **All** from the menu to include all devices in the group. Click the refresh button to update the list during file transfer or deletion processes.

Monitoring Actions

On the **CONFIG > Device File Management** page, click the **Actions** tab to view the status of the last file transfer or last file deleted for routers in the selected group. You can click the Cancel button to terminate any active file operation.

The Actions tab lists the following attributes:

- Start Time and Finish time of the last transfer
- File name
- Status of the process: UNKNOWN, AWAITING_DELETE, DELETE_IN_PROGRESS, DELETE_COMPLETE, CANCELLED, FINISHED, NONE, NOTSTARTED, UPLOAD_IN_PROGRESS, UPLOAD_COMPLETE, STOPPING, STOPPED
- Completed Devices: Displays the following total number of (upload complete/total number of target devices)
- Error/Devices: Number of errors and errored device count
- File Path
- Status: Icon displays: ?, X or check mark
- Name: EID link to Device Info page
- Last Status Time
- Activity: UPLOAD, DELETE, NONE
- File: Name of file
- Status: Text description of status
- Progress: Percentage number
- Message: Describes any issues discovered during the process
- Error: Description of the error type

Deleting Files

To delete files from routers:

1. On the **CONFIG > Device File Management** page, within the **Browse Devices** pane, select the file that you want to delete.
2. On the **Actions** tab, click **Delete**.
3. In the **Delete file from List** dialog, select a file to delete.

You can delete the file from all routers in the selected group or any subset of routers in the group.

4. Click **Delete File**.

The **Delete File from Routers** dialog box displays.

5. Check the check boxes of the routers from which you want to delete the file.
 - You can click **Change File** to select a different file to delete from the selected routers.
 - You can select multiple routers.
 - Only one file can be deleted at a time.
 - You can click Clear Selection and (x) close the windows to stop deletion.
6. Click **Delete**.

If there are no file transfer or deletion, configuration push, firmware upload, or install or reprovision operations in progress for the group, the delete operation begins. IoT FND searches the `.../managed/files/` directory on the devices for the specified file name.

Note: On deletion, all file content is purged from the selected devices, but not from the IoT FND database. File clean-up status displays for the selected group.

You can select another group and file to perform a separate file deletion while file transfer or deletion processes are in progress for this group. When you cancel file deletion process before it completes, the currently running file deletion process completes and all waiting file deletion processes are cancelled.

The following file deletion status attributes are added to all group types:

- File Operation: delete
- Start Date/Time of the last transfer
- End Date/Time
- File name
- Success Count
- Failure Count
- Total Count: The number of CGRs selected for the operation.
- Status: UNKNOWN, AWAITING_DELETE, DELETE_IN_PROGRESS, DELETED, CANCELLED
- Percentage Completed
- Error Message

- Error Details

Managing Work Orders

CGR1000, IR800, and IR500 routers support work orders. The IoT FND Work Order feature works with IoT-DM Release 3.0 or later.

For integration instructions, see [“Accessing Work Authorizations”](#) in the *Cisco Connected Grid Device Manager Installation and User Guide, Release 3.1*, or [“Managing Work Orders”](#) in the *Cisco Connected Grid Device Manager Installation and User Guide (Cisco IOS), Release 4.0 and 4.1* or *Cisco IoT Device Manager Installation and User Guide (Cisco IOS), Release 5.0*.

Note: For more details on actions supported by platform and minimum software releases required and configuration details, refer to following documents, respectively:

- [Release Notes for Cisco IoT Device Manager 5.4](#)
- [Cisco IoT Device Manager Installation and User Guide, Release 5.x](#)

Note: If you are using CGDM Release 3.1 and later, you must enable SSLv3 for IoT-DM-IoT FND connection authentication as follows:

1. Stop IoT FND:

```
service cgms stop
```

2. For IoT-DM Release 3.x and later, in the following files, replace **protocol="TLSv1"** attribute:

- /opt/cgms/standalone/configuration/standalone.xml
- /opt/cgms/standalone/configuration/standalone-cluster.xml

For CGDM 3.x

- Replace the attribute with: **protocol="TLSv1,SSLv3"**

For CGDM 4.x and IoT-DM 5.x

- Replace the attribute with: **protocol="TLSv1.x,SSLv3"**

3. Start IoT FND:

```
service cgms start
```

- [Creating User Accounts for Device Manager \(IoT-DM\) Users](#)
- [Creating Work Orders](#)
- [Downloading Work Orders](#)
- [Editing Work Orders](#)
- [Deleting Work Orders](#)

Creating User Accounts for Device Manager (IoT-DM) Users

Before creating work orders, you must create user accounts in IoT FND for the field technicians who use IoT-DM to download work orders from IoT FND.

To create a Device Manager user account:

1. If not defined, create a Device Manager User role:
 - a. Choose **ADMIN > Access Management > Roles**.
 - b. Click **Add**.
 - c. (CG-OS only) In the Role Name field, enter a name for the role.
 - d. Check the check box for **Device Manager User**, and click the disk icon to save the changes.
2. Create the user account:
 - a. Choose **ADMIN > Access Management > Users**, and then click + to add a user.
 - b. Enter the user name, new password, confirm password and time zone information.
 - c. Select **Time Zone**.
 - d. Click **Assign Domain**. In the panel that appears, check the check boxes for **Monitor Only** and the Device Manager User role you created in Step 1.
 - e. Click **Assign**.

Creating Work Orders

Create work orders in IoT FND to deploy field technicians for device inspections. Field technicians use the IoT-DM client to connect to IoT FND and download the work order.

CGR1000, IR800, and IR500 support work orders.

Before you can create a work order:

- Your user account must have the Work Order Management permissions enabled. See [Managing Roles and Permissions](#).
- To provide a signed work order to IoT-DM on request, you must import IoT-DM certificates to cgms_keystore using the alias cgms.
- Create the user account for the field technician.

To create a work order for an IR500:

1. In the **Browse Devices** panel under ENDPOINT, select GATEWAY-IR500.
2. In the **Inventory** view (right-pane):
 - a. Select the check box of the faulty GATEWAY-IR500.
 - b. From the drop-down menu options, select **More Actions > Create Work Order**.

The Operations > Work Orders page appears. IoT Field Network Director adds the names of the selected field device to the Field Device Names/EIDs field as a comma-separated list.

For more information about work orders, see [Managing Work Orders](#).

Viewing Work Orders

To view work orders in IoT FND, choose **OPERATIONS > Work Orders**.

Table 8 lists the fields that display on the Work Orders page.

Table 8 Work Orders Page Fields

Field	Description
Work Order Number	Unique identifier of the work order.
Work Order Name	Name of the work order.
Role	(CG-OS only) Role of the user assigned to the work order: tech, admin, or viewer.
Device Type	EID of the system associated with the work order.
FAR Name/EID	Product name such as CGR1240 followed by EID.
Technician User Name	User name of the assigned technician.
Time Zone	The time zone where the router is located— <i>not</i> the user's time zone. This value is deployment dependent, and can match the user's time zone.
Start Date	Project start date allotted to the field technician.
End Date	Project start date allotted to the field technician.
Last Update	Time of last work order status update.
Status	Work order status. Valid status values are: New, Assigned, InService, Completed, Incomplete, or Expired.

Creating Work Orders

DETAILED STEPS

To create a work order for an existing Router (CGR1000) or Endpoint (GATEWAY-IR500) in the network:

1. At the **DEVICES > FIELD DEVICES** page, select the **ROUTER** or **ENDPOINT** heading within the Browse Devices panel.
2. Locate the device on the Inventory page (right panel) and select the box next to the Name of that device.
3. Select **More Actions > Create Work Order**.
4. At the **OPERATIONS > WORK ORDERS** page that appears, click **Add Work Order**.
5. In the **Work Order Name** field, enter the name of the work order.
6. In the **Field Device Names/EIDs** field, enter a comma-separated list of router names or EIDs.
For every router in the list, IoT FND creates a separate work order.
7. **Device Type** (Router or Endpoint) and **CGR OS** version (CG-OS or IOS) auto-populate.
8. Enter the IoT-DM system name in the **Device Username** field.
Select the **Technician User Name** for the IoT-DM from the drop-down menu. This menu only lists users with IoT-DM User permissions enabled.
9. From the **Status** drop-down menu, choose the status of the work order (**New, Assigned, In Service, Completed, or InComplete**). The **New** option auto-populates.

Note: For a IoT-DM user to retrieve a work order, the work order must be in the **Assigned** state in IoT FND for that user. If the work order is in any other state, IoT-DM cannot retrieve the signed work order.

Note: After the work order has been successfully requested by the IoT-DM user, the state of work order changes to **In Service**.

10. In the **Start Date** and **End Date** fields, specify the starting and ending dates for which the work order is valid.

If the work order is not valid, the technician cannot access the router.

11. In the **Device Time Zone** field, choose the time zone of the device from the drop-down menu.

12. To save your entries, click the disk icon. (To cancel your entries, click **x**.)

13. Click **OK**.

You can also create work orders on the Field Devices page (**DEVICES > Field Devices > More Actions** menu), as described in [Creating Work Orders](#), and on the Device Info page.

Downloading Work Orders

To download the work orders created by IoT FND, a field technician uses Cisco IoT-DM, which is a Windows-based application used to manage a single Cisco CGR 1000 router. The technician can download all work orders in the *Assigned* state.

Field technicians use IoT-DM to update work order status, which is sent to IoT FND.

Note: Certificates are not included in the work order and are preinstalled on the IoT-DM field laptop prior to downloading work orders from IoT FND.

For more information about IoT-DM, see the [Cisco IoT Device Manager User Guide](#) for Release 5.2.

Editing Work Orders

To edit work order details:

- 1.** Choose **OPERATIONS > Work Orders**.
- 2.** Click the box next to the work order you want to edit. Click **Edit Work Order**.

Alternatively, click the work order number to open the page displaying the work order details.

- 3.** After editing the work order, click **Save**.

Deleting Work Orders

To delete work orders:

- 1.** Choose **OPERATIONS > Work Orders**.
- 2.** Check the check box of the work order(s) to delete.
- 3.** Click **Delete Work Order**.
- 4.** Click **Yes** to confirm or to cancel action click **No**.

Demo and Bandwidth Operation Modes

The Demo and Bandwidth Operation Modes allow you define the application protocol (HTTP or HTTPS) to use for communication between FND and the router to minimize setup and bandwidth requirements, respectively. The two modes do not affect or change the way that FND communicates with meters or other endpoints. Secure communication between FND and endpoints devices will continue to be secured by using a hardware secure module (HSM) or software secure module (SSM).

- **Demo Mode:** Allows users to quickly set up a small network with FND for demos by minimizing the setup requirements. It eliminates the need for router certificates or the need to set up SSL.
- **Bandwidth optimization mode:** Reduces network bandwidth requirements for a network by using HTTP to send periodic metrics between routers and FND while preserving security for other operations. All other router communications will employ HTTPS.

Table 9 Communication Method Given FND Operation Mode

Process	Demo Mode	Bandwidth Optimization Mode	Default Mode
IOS Registration	All communications over HTTP	HTTPS	All communications over HTTPS
AP Registration		HTTPS	
LoRA Registration		HTTPS	
AP Bootstrap		HTTPS	
IOS Tunnel Provisioning		HTTPS	
Configuration Push		HTTPS	
File Transfer		HTTPS	
Metrics		HTTP and HTTPS	

Demo Mode Configuration

FND Configuration Changes

In order to change FND router Management mode to Demo mode, you **must**:

1. Add the following to the **cgms.properties** file:

```
fnd-router-mgmt-mode=1 <---where 1 represents Demo Mode
```

2. Add the following to the **tpsproxy.properties** file:

```
inbound-proxy-destination=http://<FND-IP/Hostname>:9120 <---where 9120 represents Inbound proxy
tps-proxy-enable-demo-mode=true <---Enables the TPS proxy to accept HTTP connections
```

3. For the AP registration process, you must add the following two properties to the **cgms.properties** file:

```
rtr-ap-com-protocol=http
rtr-ap-com-port=80
```

Router Configuration Changes

In order to manage routers in Demo mode:

1. Manually change the URL for all the profiles to use HTTP protocol:

```
url http://nms.iot.cisco.com:9121/cgna/ios/registration
url http://nms.iot.cisco.com:9121/cgna/ios/metrics
```

2. Update WSMA profile URL to use HTTP protocol (Only Required in Demo Mode)

```
wsma profile listener config
transport http path /wsma/config
wsma profile listener exec
transport http path /wsma/exec
```

3. Update URL of iot-fnd-register, iot-fnd-metric and iot-fnd-tunnel profiles to use HTTP protocol on Cisco Wireless Gateway for LoRaWAN (IXM-LPWA)

```
configure terminal
igma profile iot-fnd-register
url http://fnd.iok.cisco.com:9121/igma/register
exit
exit
configure terminal
igma profile iot-fnd-metric
url http://fnd.iok.cisco.com:9121/igma/metric
exit
exit
configure terminal
igma profile iot-fnd-tunnel
url http://fnd.iok.cisco.com:9121/igma/tunnel
exit
exit
```

Bandwidth Optimization Mode Configuration

Only periodic metrics will go over HTTP protocol in the Bandwidth Optimization Mode. So, you have to manually change the metric profile URL as follows:

```
url http://nms.iot.cisco.com:9124/cgna/ios/metrics
```

Manually change the URL of metrics profiles to use HTTP protocol, by entering:

```
configure terminal
igma profile iot-fnd-metric
url http://fnd.iok.cisco.com:9124/igma/metrics
exit
exit
```

Note: When operating In Bandwidth Optimization Mode, all WSMA requests **must** go over HTTPS. Therefore, you must ensure that the WSMA profile listener is set to HTTPS at the config and exec command modes.

Configuring Demo Mode in User Interface

Note: By default, all communications between FND and the router will be over HTTPS.

To setup Demo Mode for FND and router communications:

1. Choose **ADMIN > SYSTEM MANAGEMENT > Provisioning Settings**.
2. In the Provisioning Process panel, enter the IoT FND URL in the following format: `http:// <ip address:9121>` in **both** the IoT FND URL and Periodic Metrics URL fields.

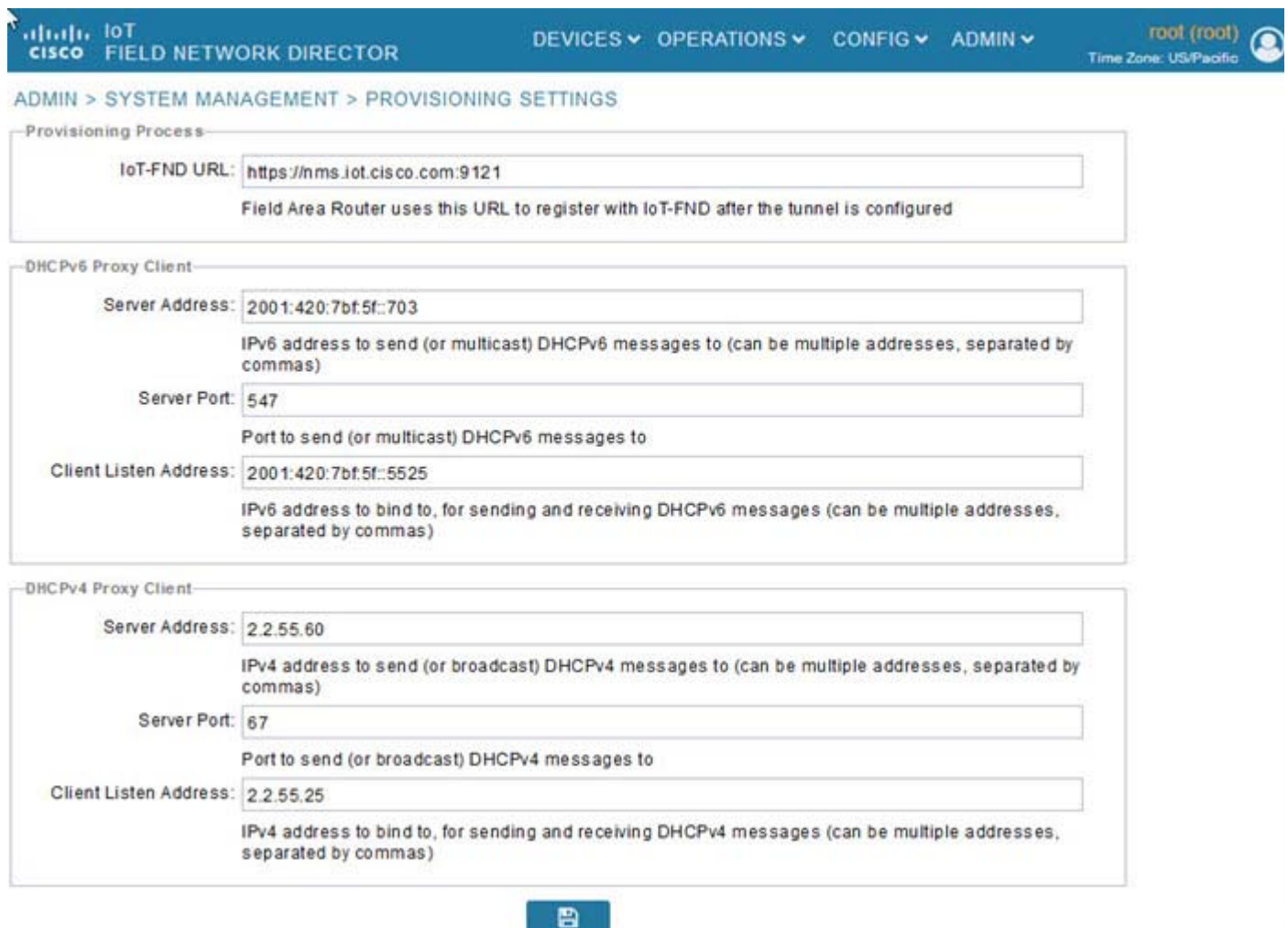
Note: The FAR uses the IoT FND URL to communicate with IoT FND after the tunnel is configured and uses the Periodic Metrics URL to report periodic metrics and notifications with IoT FND.

Configuring Bandwidth Optimization Mode in User Interface

Note: By default, all communications between FND and the router will be over HTTPS.

To setup Bandwidth Optimization Mode for FND and router communications:

1. Choose **ADMIN > SYSTEM MANAGEMENT > Provisioning Settings**.
2. In the Provisioning Process panel:
 - Enter your IoT FND URL in the following format: "https:// FND IP/HostName:9121" in the IoT FND URL field. FAR uses this URL to communicate with IoT FND after the tunnel is configured.
 - Enter the following URL in the Periodic Metrics URL field: http:// <ip address:9124> FAR uses this URL to report periodic metrics and notifications with IoT FND.



Device Properties

This section describes the device properties that you can view in IoT FND. Some of these properties are configurable; others are not.

- [Types of Device Properties](#)
- [Device Properties by Category](#)

Types of Device Properties

IoT FND stores two types of device properties in its database:

- **Actual device properties**—These are the properties defined by the device, such as IP Address, Transmit Speed, and SSID.
- **IoT FND device properties**—These are properties defined by IoT FND for devices, such as Latitude and Longitude properties, which IoT FND uses to display device locations on its GIS map.

Note: The Key column provides the version of the property name in the IoT FND database that you can use in filters. For example, to search for the device with an IP address of 10.33.0.30, enter **ip:10.33.0.30** in the Search Devices field.

Device Properties by Category

This section presents IoT FND device properties by category:

- [Cellular Link Settings](#)
- [Cellular Link Metrics for CGRs](#)
- [DA Gateway Properties](#)
- [Dual PHY WPAN Properties](#)
- [Embedded Access Point \(AP\) Credentials](#)
- [Embedded AP Properties](#)
- [Ethernet Link Metrics](#)
- [Guest OS Properties](#)
- [Head-End Routers > Netconf Config](#)
- [Head-End Routers > Tunnel 1 Config](#)
- [Head-End Routers > Tunnel 2 Config](#)
- [Inventory](#)
- [Mesh Link Config](#)
- [Device Health](#)
- [Mesh Link Keys](#)
- [Link Settings](#)
- [Link Metrics](#)
- [NAT44 Metrics](#)
- [PLC Mesh Info](#)
- [Raw Sockets Metrics and Sessions](#)

Device Properties

- Router Battery
- Router Config
- Router Credentials
- Router DHCP Proxy Config
- Router Health
- Router Tunnel Config
- Router Tunnel 1 Config
- Router Tunnel 2 Config
- SCADA Metrics
- User-defined Properties
- WiFi Interface Config
- WiMAX Config
- WiMAX Link Metrics
- WiMAX Link Settings

Every device in IoT FND presents a list of fields, which are used for device searches. The available fields for a device are defined in the **Device Type** field. Fields are either configurable or discovered. Configurable fields are set using XML and CSV files; the device EID is the lookup key. Discovered fields are presented from the device. Fields are also accessible in the device configuration templates for routers.

Cellular Link Settings

Table 10 lists the fields in the Cellular Link area of the Device Detail page for all Cellular interfaces.

Note: Beginning with IoT FND 3.2, Cisco routers IR829, CGR1240, CGR1120, and Cisco 819 4G LTE ISRs (C819) support a new dual-active radio module that supports dual modems and 2 physical interfaces (interfaces 0 and 1, interfaces 2 and 3) per modem. See SKUs below:

- IR829GW-2LTE-K9
- CGM-LTE-LA for CGR 1000 routers
- C819HG-LTE-MNA-K9

Cellular properties supported on the dual modems and their two physical interfaces (and four logical interfaces 0, 1, 2 and 3), display as follows:

Cellular Link Settings	Interface 0 and Interface 1	Interface 2 and Interface 3

Additionally, the 4G LTE dual-active radio module does not support or display all fields summarized in Table 10.

Table 10 Cellular Link Settings Fields

Field	Key	Configurable?	Description
Cellular Network Type	N/A	Yes	Defines the type of cellular network for example, GSM or CDMA.
Module Status	cellularStatus	No	Displays whether the cellular interface module is active in the network. There is also an unknown state for the module.
Network Name	–	Yes	Defines the service provider name, for example, AT&T or Verizon.
APN	cellularAPN	No	Displays the Access Point Name (APN) of the AP to which the cellular interface connects.
Cell ID	cellularID	No	Displays the cell ID for the cellular interface. This value must exist to activate the interface.
Cellular SID	cellularSID	No	Displays the System Identification Number for the CDMA cellular area.
Cellular NID	cellularNID	No	Displays the Network Identification Number for the CDMA cellular area.
Cellular Roaming Status	cellularRoamingStatus	No	Indicates whether the modem is in the Home network or Roaming.
Cellular Modem Serial Number	N/A	No	Displays the serial number of the connected modem.
Cellular Modem Firmware Version	cellularModemFirmwareVersion	No	Displays the version of the modem firmware on the module installed within the CGR.
Connection Type	connectionType	No	Displays the connection type as: <ul style="list-style-type: none"> ■ Packet switched ■ Circuit switched ■ LTE
Location Area Code	locationAreaCode	No	Displays the Location Area Code (LAC) given by the base station.
Routing Area Code	routingAreaCode	No	Displays the routing area code given by the base station.
APN	cellularAPN	No	Displays the Access Point Name (APN) of the AP to which the cellular interface connects.
Cellular Modem Firmware Version	cellularModemFirmwareVersion	No	Displays the version of the modem firmware on the Cellular module installed within the CGR.

Table 10 Cellular Link Settings Fields (continued)

Field	Key	Configurable?	Description
Connection Type	connectionType	No	Displays the connection type as: <ul style="list-style-type: none"> ■ Packet switched ■ Circuit switched
IMSI	cellularIMSI	No	The International Mobile Subscriber Identity (IMSI) identifies an individual network user as a 10-digit decimal value within a GSM and CDMA network. <p>Possible values are:</p> <ul style="list-style-type: none"> ■ 10-digit decimal value ■ Unknown
IMEI	cellularIMEI	No	Displays the International Mobile Equipment Identity (IMEI) for the cellular interface within a GSM network only. The IMEI value is a unique number for the cellular interface.

Cellular Link Metrics for CGRs

Table 11 describes the fields in the Cellular Link Metrics area of the Device Info view.

Table 11 Cellular Link Metrics Area Fields

Field	Key	Description
Transmit Speed	cellularTxSpeed	Displays the current speed (bits/sec) of data transmitted by the cellular interface over the cellular uplink for a defined period (such as an hour).
Receive Speed	cellularRxSpeed	Displays the average speed (bits/sec) of data received by the cellular uplink network interface for a defined period (such as an hour).
RSSI	cellularRssi	Indicates the radio frequency (RF) signal strength of the cellular uplink. Valid values are 0 to -100. <p>The LED states on the cellular interface and corresponding RSSI values are:</p> <ul style="list-style-type: none"> ■ Off: RSSI < = -110 ■ Solid amber: -100 < RSSI <= -90 ■ Fast green blink: -90 < RSSI <= -75 ■ Slow green blink: -75 < RSSI <= -60 ■ Solid green: RSSI > -60
Bandwidth Usage (Current Billing Cycle)	CellBwPerCycle (bytes)	Displays current bandwidth usage (in bytes) of a particular route for the current billing cycle.

Table 11 Cellular Link Metrics Area Fields (continued)

Field	Key	Description
Cell Module Temperature	cellModuleTemp	Internal temperature of 3G module.
Cell ECIO	cellularEcio	Signal strength of CDMA at the individual sector level.
Cell Connect Time	cellConnectTime	Length of time that the current call lasted. This field only applies only to CDMA.

DA Gateway Properties

[DA Gateway Metrics Area Fields](#) describe the fields in the DA Gateway area of the Device Info view.

Table 12 DA Gateway Metrics Area Fields

Field	Key	Description
SSID	-	The mesh SSID.
PANID	-	The subnet PAN ID.
Transmit Power	-	The mesh transmit power.
Security Mode	-	Mesh Security mode: <ul style="list-style-type: none"> ■ 0 indicates no security mode set ■ 1 indicates 802.1x with 802.11i key management
Meter Certificate	meterCert	The subject name of the meter certificate.
Mesh Tone Map Forward Modulation	toneMapForwardModulation	Mesh tone map forward modulation: <ul style="list-style-type: none"> ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Tone Map Reverse Modulation	-	Mesh tone map reverse modulation: <ul style="list-style-type: none"> ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Device Type	-	The primary function of the mesh device (for example, meter, range extender, or DA gateway).
Manufacturer of the Mesh Devices	-	Manufacturer of the mesh device as reported by the device.
Basic Mapping Rule End User IPv6 Prefix	-	End-user IPv6 address for basic rule mapping for the device.
Basic Mapping Rule End User IPv6 Prefix Length	-	Specified prefix length for the end-user IPv6 address.
Map-T IPv6 Address	-	IPv6 address for MAP-T settings.

Table 12 DA Gateway Metrics Area Fields (continued)

Field	Key	Description
Map-T IPv4 Address	-	IPv4 address for MAP-T settings.
Map-T PSID	-	MAP-T PSID.
Active Link Type	-	Link type of the physical link over which device communicates with other devices including IoT FND.

Dual PHY WPAN Properties

Table 13 describes the fields in the Dual PHY area of the Device Info view.

Table 13 Dual PHY Metrics Area Fields

Field	Key	Description
SSID	ssid	The mesh SSID.
PANID	panid	The subnet PAN ID.
Transmit Power	txpower	The mesh transmit power.
Security Mode	-	Mesh Security mode: <ul style="list-style-type: none"> ■ 0 = No security mode set ■ 1 = 802.1x with 802.11i key management
Meter Certificate	meterCert	The subject name of the meter certificate.
Mesh Tone Map Forward Modulation	toneMapForwardModulation	Mesh tone map forward modulation: <ul style="list-style-type: none"> ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Tone Map Reverse Modulation	-	Mesh tone map reverse modulation: <ul style="list-style-type: none"> ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Device Type	-	The primary function of the mesh device (for example, meter, range extender, or DA gateway).
Manufacturer of the Mesh Devices	-	Manufacturer of the mesh device as reported by the device.
Basic Mapping Rule End User IPv6 Prefix	-	End-user IPv6 address for basic rule mapping for the device.
Basic Mapping Rule End User IPv6 Prefix Length	-	Specified prefix length for the end-user IPv6 address.
Map-T IPv6 Address	-	IPv6 address for Map-T settings.

Table 13 Dual PHY Metrics Area Fields (continued)

Field	Key	Description
Map-T IPv4 Address	-	IPv4 address for Map-T settings.
Map-T PSID	-	MAP-T PSID.
Active Link Type	-	Link type of the physical link over which device communicates with other devices including IoT FND.

Embedded Access Point (AP) Credentials

Table 14 describes the fields in the Embedded Access Point Credentials area of the Device Info view.

Table 14 Embedded Access Point Credentials Fields

Field	Key	Configurable?	Description
AP Admin Username	-	Yes	The user name used for access point authentication.
AP Admin Password	-	Yes	The password used for access point authentication.

Embedded AP Properties

Table 15 describes the fields on the Embedded AP tab of the C800 or IR800 Device Info view.

Table 15 Embedded AP Properties

Field	Key	Description
Inventory	-	Summary of name, EID, domain, status, IP address, hostname, domain name, first heard, last heard, last property heard, last metric heard, model number, serial number, firmware version, and uptime details.
Wi-Fi Clients	-	Provides client MAC address, SSID, IPv4 address, IPv6 address, device type, state, name, and parent.
Dot11Radio 0 Traffic	-	Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps), and Rx speed (bps).
Dot11Radio 1 Traffic	-	Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps,) and Rx speed (bps).
Tunnel3	-	Provides admin status (up/down), operational status (up/down), Tx speed (bps), Tx drops (bps), and Rx speed (bps).
BV11	-	Provides admin status (up/down), operational status (up/down), IP address, physical address, Tx speed (bps), Tx drops (bps) and Rx speed (bps).
GigabitEthernet0	-	Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps), and Rx speed (bps).

Ethernet Link Metrics

Table 16 describes the fields in the Ethernet link traffic area of the Device Info view.

Table 16 Ethernet Link Metrics Area Fields

Field	Key	Description
Transmit Speed	ethernetTxSpeed	Indicates the average speed (bits/sec) of traffic transmitted on the Ethernet interface for a defined period of time.
Receive Speed	ethernetRxSpeed	Indicates the average speed (bits/sec) of traffic received on the Ethernet interface for a defined period of time.
Transmit Packet Drops	ethernetTxDrops	Indicates the number of packets dropped (drops/sec) when the transmit queue is full.

Guest OS Properties

Table 17 describes the fields in the Guest OS Properties area of the Config Properties page.

Table 17 Guest OS Properties Fields

Field	Key	Description
GOS Password	-	Password to access the GOS.
DHCPv4 Link for Guest OS Gateway	-	The DHCPv4 gateway address.
Guest OS IPv4 Subnet mask	-	The IPv4 subnet mask address.
Guest OS Gateway IPv6 Address	-	The IPv6 gateway address.
Guest OS IPv6 Subnet Prefix Length	-	The IPv6 subnet prefix length.

Head-End Routers > Netconf Config

Table 18 describes the fields in the Netconf Client area of the **Head-End Routers > Config Properties** page.

Table 18 Head-End Routers > Netconf Config Client Fields

Field	Key	Configurable?	Description
Netconf Username	netconfUsername	Yes	Identifies the username to enter when establishing a Netconf SSH session on the HER.
Netconf Password	netconfPassword	Yes	Identifies the password to enter when establishing a Netconf SSH session on the HER.

Head-End Routers > Tunnel 1 Config

Table 19 describes the fields in the Tunnel 1 Config area of the **Head-End Routers > Config Properties** page.

Table 19 Head-End Routers > Tunnel 1 Config Fields

Field	Key	Configurable?	Description
IPsec Tunnel Source 1	ipsecTunnelSrc1	Yes	Identifies the source interface or IP address of IPsec tunnel 1.

Table 19 Head-End Routers > Tunnel 1 Config Fields (continued)

Field	Key	Configurable?	Description
IPsec Tunnel Dest Addr 1	ipsecTunnelDestAddr1	Yes	Identifies the destination interface or IP address of IPsec tunnel 1.
GRE Tunnel Source 1	greTunnelSrc1	Yes	Identifies the source interface or IP address of GRE tunnel 1.
GRE Tunnel Dest Addr 1	greTunnelDestAddr1	Yes	Identifies the destination interface or IP address of GRE tunnel 1.

Head-End Routers > Tunnel 2 Config

[Table 20](#) describes the fields in the Tunnel 2 Config area of the **Head-End Routers > Config Properties** page.

Table 20 Head-End Routers > Tunnel 2 Config Device Fields

Field	Key	Configurable?	Description
IPsec Tunnel Source 2	ipsecTunnelSrc2	Yes	Identifies the source interface or IP address of IPsec tunnel 2.
IPsec Tunnel Dest Addr 2	ipsecTunnelDestAddr2	Yes	Identifies the destination interface or IP address of IPsec tunnel 2.
GRE Tunnel Source 2	greTunnelSrc2	Yes	Identifies the source interface or IP address of GRE tunnel 2.
GRE Tunnel Dest Addr 2	greTunnelDestAddr2	Yes	Identifies the destination interface or IP address of GRE tunnel 2.

Inventory

[Table 21](#) describes the fields in the Inventory area of the Device Info page.

EXAMPLE PATH to Device Info page which summarizes the Inventory details: DEVICES> Field Devices > ROUTERS > CGR1000 > EID Name

Table 21 Inventory Fields

Field	Key	Configurable?	Description
Config Group	configGroup	Yes	The name of the configuration group to which the device belongs.
Device Category	deviceCategory	No	This field lists the type of device.
Device Type	deviceType	No	This field determines all other fields, as well as how the device communicates, and how it displays in IoT FND.
Domain Name	domainName	Yes	The domain name configured for this device.
EID	eid	No	The primary element ID of the device, which is used as the primary unique key for device queries.
Firmware Group	firmwareGroup	Yes	The name of the firmware group to which the device belongs.
Firmware Version	runningFirmwareVersion	No	The firmware version running on the device.
Hardware Version	vid	No	The hardware version of the device.
Hypervisor Version	hypervisor	No	(Cisco IOS CGRs running Guest OS only) The version of the Hypervisor.

Table 21 Inventory Fields (continued)

Field	Key	Configurable?	Description
Hostname	hostname	No	The hostname of the device
IP Address	ip	Yes	The IP address of the device. Use this address for the IoT FND connection through a tunnel.
Labels	label	Yes	Custom label assigned to the device. A device can have multiple labels. Labels are assigned through the UI or API, but not through a XML or CSV file.
Last Heard	lastHeard	No	The last date and time the device contacted IoT FND.
Last Metric Heard	N/A	No	The time of last polling (periodic notification).
Last Property Heard	N/A	No	The time of last property update for the router.
Last RPL Tree Update	N/A	No	The time of last RPL tree poll update (periodic notification).
Location	N/A	No	The latitude and longitude of the device.
Manufacturer	-	No	The manufacturer of the endpoint device.
Function	cgmesh	No	Function of the mesh device. Valid values are Range Extender and Meter.
Meter Certificate	meterCert	No	The global or unique certificate reported by the meter.
Meter ID	meterId	No	ME meter ID.
Model Number	pid	No	The product ID of the device.
Name	name	Yes	The unique name assigned to the device.
SD Card Password Lock	-	Yes	(CGRs only) The state of the SD card password lock (on/off).
Serial Number	sn	No	The serial number of the device.
Status	status	No	The device status.
Tunnel Group	tunnelGroup	Yes	The name of the tunnel group to which the device belongs.

Mesh Link Config

Table 22 describes the fields in the Mesh Link Config area of the **Routers > Config Properties** page.

Table 22 Mesh Link Config Fields

Field	Key	Configurable?	Description
Mesh Prefix Config	meshPrefixConfig	Yes	The subnet prefix address.
Mesh Prefix Length Config	meshPrefixLengthConfig	Yes	The subnet prefix address length.
Mesh PAN ID Config	meshPanidConfig	Yes	The subnet PAN ID.
Mesh Address Config	meshAddressConfig	Yes	The IP address of the mesh link.
Master WPAN Interface	masterWpanInterface	Yes	(Dual-PHY CGRs only) The interface on which the device is master.
Slave WPAN Interface	slaveWpanInterface	Yes	(Dual-PHY CGRs only) The interface on which the device is slave.

Device Health

Table 23 describes the fields in the Device Health area of the Device Info view.

Table 23 Device Health Fields

Field	Key	Description
Uptime	uptime	The amount of time in days, hours, minutes and seconds that the device has been running since the last boot. <i>Unknown</i> appears when the system is not connected to the network.

Mesh Link Keys

Table 24 describes the fields in the Mesh Link Keys area of the Device Info view.

Table 24 Mesh Link Keys Fields

Field	Key	Configurable?	Description
Key Refresh Time	meshKeyRefresh	No	The last date the mesh link keys were uploaded.
Key Expiration Time	meshKeyExpire	Yes	The date the mesh link keys expire.

Link Settings

Table 25 describes the fields in the Link Settings area of the Device Info view.

Table 25 Link Settings Fields

Field	Key	Description
Firmware Version	meshFirmwareVersion	The Cisco Resilient Mesh Endpoint (RME) firmware version.
Mesh Interface Active	meshActive	The status of the RME.
Mesh SSID	meshSsid	The RME network ID.
PANID	meshPanid	The subnet PAN ID.
Transmit RF Power	meshTxPower	The RME transmission power (dBm).
Security Mode	meshSecMode	The RME security mode.
Transmit PLC TX Level	tx_level dBuV	The PLC level for Itron OpenWay RIVA CAM module and Itron OpenWay RIVA Electric devices (dBuV) <i>where u = micro</i>

Table 25 Link Settings Fields (continued)

Field	Key	Description
RPL DIO Min	meshRplDioMin	An unsigned integer used to configure the lmin of the DODAG Information Object (DIO) Trickle timer.
RPL DIO Double	meshRplDioDbI	An unsigned integer used to configure the lmax of the DIO Trickle timer.
RPL DODAG Lifetime	meshRplDodagLifetime	An unsigned integer used to configure the default lifetime (in minutes) for all downward routes that display as Directed Acyclic Graphs (DAGs).
RPL Version Incr. Time	meshRplVersionIncrementTime	An unsigned integer used to specify the duration (in minutes) between incrementing the RPL version.

Link Metrics

Table 26 describes the fields in the Link Metrics area of the Device Info page.

Table 26 Link Metrics Fields

Field	Key	Description
Active Link Type	activeLinkType	Determines the most recent active RF or PLC link of a meter.
Meter ID	meterId	The meter ID.
PANID	meshPanid	The endpoint PANID.
Mesh Endpoints	meshEndpointCount	Number of RMEs.
Mesh Link Transmit Speed	meshTxSpeed	The current speed of data transmission over the uplink network interface (bits/sec) averaged over a short element-specific time period (for example, an hour).
Mesh Link Receive Speed	meshRxSpeed	The rate of data received by the uplink network interface (bits/sec) averaged over a short element-specific time period (for example, an hour).
Mesh Link Transmit Packet Drops	-	The number of data packets dropped in the uplink.
Route RPL Hops	meshHops	The number of hops that the element is from the root of its RPL routing tree.
Route RPL Link Cost	linkCost	The RPL cost value for the link between the element and its uplink neighbor.
Route RPL Path Cost	pathCost	The RPL path cost value between the element and the root of the routing tree.
Transmit PLC Level	tx_level dBuV	Supported on the PLC and the Itron OpenWay RIVA Electric devices and the Itron OpenWay RIVA G-W (Gas-Water) devices only (u within dBuV = micro)

NAT44 Metrics

Table 27 describes the fields in the NAT44 area of the Device Info page.

Table 27 NAT44 Metrics Fields

Field	Key	Description
NAT44 Internal Address	nat44InternalAddress0	The internal address of the NAT 44 configured device.
NAT 44 Internal Port	nat44InternalPort0	The internal port number of the NAT 44 configured device.
NAT 44 External Port	nat44ExternalPort0	The external port number of the NAT 44 configured device.

PLC Mesh Info

Table 28 describes the fields in the PLC Mesh Info area of the Device Info view.

Table 28 PLC Mesh Info Fields

Field	Key	Description
Mesh Tone Map Forward Modulation	toneMapForwardModulation	Mesh tone map forward modulation: <ul style="list-style-type: none"> ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Tone Map Forward Map	toneMapForward	Indicates the number of usable subcarriers in the channel, shown as a binary octet (for example, 0011 1111). Ones indicate viable channels. The more ones on the map, the higher the channel capacity.
Mesh Tone Map Reverse Modulation	toneMapRevModulation	Mesh tone map reverse modulation: <ul style="list-style-type: none"> ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Tone Map Reverse Map	toneMapReverse	Indicates the number of usable subcarriers in the channel, shown as a binary octet (for example, 0011 1111). Ones indicate viable channels. The more ones in the map, the higher the channel capacity. The reverse map information and RSSI combine to determine viable channels.
Mesh Absolute Phase of Power	-	Mesh absolute phase of power is the relative position of current and voltage waveforms for a PLC node.
LMAC Version	-	Version of LMAC firmware in use by the PLC module DSP processor, which provides lower media access functionality for PLC communications compliant with the IEEE P1901.2 PHY standard.

Raw Sockets Metrics and Sessions

Table 29 describes the fields in the TCP Raw Sockets area of the **Field Devices > Config Properties** page.

Table 29 Raw Sockets Metrics and Sessions View

Field	Key	Description
Metrics		
Tx Speed (bps)	rawSocketTxSpeedS[portNo]	The transmit speed of packetized streams of serial data in bits per second.
Rx Speed (bps)	rawSocketRxSpeedS[portNo]	The receive speed of packetized streams of serial data in bits per second.
Tx Speed (fps)	rawSocketTxFramesS[portNo]	The transmit speed of packetized streams of serial data in frames per second.
Rx Speed (fps)	rawSocketRxFramesS[portNo]	The receive speed of packetized streams of serial data in frames per second.
Sessions		
Interface Name	-	The name of the serial interface configured for Raw Socket encapsulation.
TTY	-	The asynchronous serial line on the router associated with the serial interface.
VRF Name	-	Virtual Routing and Forwarding instance name.
Socket	-	The number identifying one of 32 connections.
Socket Mode	-	Client or server. The mode in which the asynchronous line interface is set up.
Local IP Address	-	The IP address that either the server listens for connections on (in Server Socket Mode), or to which the client binds to initiate connections to the server (in Client Socket Mode).
Local Port	-	The port that either the server listens to for connections (in Server Socket Mode), or to which the client binds to initiate connections to the server (in Client Socket Mode).
Dest. IP Address	-	The destination IP address of the remote TCP Raw Socket server.
Dest. Port	-	Destination port number to use for the connection to the remote server.
Up Time	-	The length of time that the connection has been up.
Idle Time	-	The length of time that no packets were sent.
Time Out	-	The currently configured session idle timeout, in minutes.

Router Battery

Table 30 describes the fields in the Router Battery (Battery Backup Unit (BBU) area of the Device Info page.

Table 30 Router Battery Device View

Field	Key	Configurable?	Description
Battery 0 Charge	battery0Charge	No	Shows the battery voltage of BBU 0.
Battery 0 Level (%)	battery0Level	No	Displays the percentage of charge remaining in BBU 0 as a percentage of 100.
Battery 0 Remaining Time	battery0Runtime	No	How many hours remain before the BBU 0 needs to be recharged.

Table 30 Router Battery Device View (continued)

Field	Key	Configurable?	Description
Battery 0 State	battery0State	No	How long BBU 0 has been up and running since its installation or its last reset.
Battery 1 Level (%)	battery1Level	No	Displays the percentage of charge remaining in BBU 1 as a percentage of 100.
Battery 1 Remaining Time	battery1Runtime	No	How many hours remain before BBU 1 needs to be recharged.
Battery 1 State	battery1State	No	How long BBU 1 has been up and running since its installation or its last reset.
Battery 2 Level (%)	battery2Level	No	Displays the percentage of charge remaining in BBU 2 as a percentage of 100.
Battery 2 Remaining Time	battery2Runtime	No	How many hours remain before BBU 2 needs to be recharged.
Battery 2 State	battery2State	No	How long BBU 2 has been up and running since its installation or its last reset.
Battery Total Remaining Time	batteryRuntime	No	The total aggregate charge time remaining for all batteries.
Number of BBU	numBBU	No	The number of battery backup units (BBUs) installed in the router. The router can accept up to three BBUs (battery 0, battery 1, battery 2).
Power Source	powerSource	No	The router power source: AC or BBU.

Router Config

[Table 31](#) describes the fields in the Router Config area of the **Field Devices > Config Properties** page.

Table 31 Router Config Device View

Field	Key	Configurable?	Description
Use GPS Location	useGPSLocationConfig	Yes	The internal GPS module provides the router location (longitude and latitude).

Router Credentials

[Table 32](#) describes the fields in the Router Credentials area of the **Field Devices > Config Properties** page.

Table 32 Router Credentials Fields

Field	Key	Configurable?	Description
Administrator Username	-	Yes	The user name used for root authentication.
Administrator Password	-	Yes	The password used for root authentication.
Master key	-	Yes	The master key used for device authentication.
SD Card Password	-	No	SD card password protection status.
Token Encryption Key	-	Yes	The token encryption key.
CGR Username	-	Yes	The username set for the CGR.
CGR Password	-	Yes	The password set on the CGR for the associated username.

Router DHCP Info

Table 33 describes the fields in the DHCP Info area of the Device Info page.

Table 33 Router DHCP Fields

Field	Key	Description
DHCP Unique ID (DUID)	-	A DHCP DUID in hex string format (for example, 0xHHHH).

Router DHCP Proxy Config

Table 34 describes the fields in the DHCP Proxy Config area of the **Field Devices > Config Properties** page.

Table 34 DHCP Proxy Config Fields

Field	Key	Configurable?	Description
DHCPv4 Link for Loopback Interfaces	dhcpV4LoopbackLink	Yes	Refers to the IPv4 link address to use within DHCP DISCOVER messages when requesting a lease for loopback interfaces.
DHCPv4 Link for Tunnel Interfaces	dhcpV4TunnelLink	Yes	Refers to the IPv4 link address to use within DHCP DISCOVER messages when requesting a lease for tunnel interfaces.
DHCPv6 Link for Loopback Interfaces	dhcpV6LoopbackLink	Yes	The IPv6 link address to use in DHCPv6 Relay-forward messages when requesting a lease for loopback interfaces.
DHCPv6 Link for Tunnel Interfaces	dhcpV6TunnelLink	Yes	The IPv6 link address to use in DHCPv6 Relay-forward messages when requesting a lease for tunnel interfaces.

Router Health

Table 35 describes the Router Health fields in the Device Info view.

Table 35 Router Health Device View

Field	Key	Configurable?	Description
Uptime	uptime	No	Indicates the length of time (in seconds) that the router has been up and operating since its last reset.
Door Status	doorStatus	No	Options for this field are: <ul style="list-style-type: none"> ■ “Open” when the door of the router is open ■ “Closed” after the door is closed
Chassis Temperature	chassisTemp	No	Displays the operating temperature of the router. You can configure alerts to indicate when the operating temperature falls outside of the customer-defined temperature range.

Router Tunnel Config

[Table 36](#) describes the fields in the Router Tunnel Config area of the **Field Devices > Config Properties** page.

Table 36 Router Tunnel Config Device View

Field	Key	Configurable?	Description
Tunnel Config	tunnelHerEid	Yes	Displays the EID number of the HER that the router connects with through secure tunnels.
Common Name of Certificate Issuer		No	Displays the name of the certificate issuer.
NMBA NHS IPv4 Address		Yes	Displays the Non-Broadcast Multiple Access (NBMA) IPv4 address.
NMBA NHS IPv6 Address		Yes	Displays the NBMA IPv6 address.
Use FlexVPN Tunnels		Yes	Displays the FlexVPN tunnel setting.

Router Tunnel 1 Config

[Table 37](#) describes the fields in the Router Tunnel 1 Config area of the **Field Devices > Config Properties** page.

Table 37 Router Tunnel 1 Config Device View

Field	Key	Configurable?	Description
Tunnel Source Interface 1	tunnelSrcInterface1	Yes	Defines the interface over which the first tunnel is built to provide WAN redundancy.
OSPF Area 1	ospfArea1	Yes	Defines the OSPFv2 Area 1 in which the router (running IPv4) is a member.
OSPFv3 Area 1	ospfv3Area1	Yes	Defines OSPFv3 Area 1 in which the router (running IPv6) is a member.
OSPF Area 2	ospfArea1	Yes	Defines the OSPFv2 Area 2 in which the router (running IPv4) is a member.
OSPFv3 Area 2	ospfv3Area1	Yes	Defines OSPFv3 Area 2 in which the router (running IPv6) is a member.
IPsec Dest Addr 1	ipsecTunnelDestAddr1	Yes	Defines the destination IP address for IPsec tunnel 1.
GRE Dest Addr 1	greTunnelDestAddr1	Yes	Defines the destination IP address for GRE tunnel 1.

Router Tunnel 2 Config

[Table 38](#) describes the fields in the Router Tunnel 2 Config area of the **Field Devices > Config Properties** page.

Table 38 Router Tunnel 2 Config Device View

Field	Key	Configurable?	Description
Tunnel Source Interface 2	tunne2SrcInterface1	Yes	Defines the interface over which the second tunnel is built to provide WAN redundancy.
OSPF Area 2	ospfArea2	Yes	Defines the OSPFv2 Area 2 in which the router (running IPv4) is a member.
OSPFv3 Area 2	ospfv3Area2	Yes	Defines OSPFv3 Area 2 in which the router (running IPv6) is a member.
IPsec Dest Addr 2	ipsecTunnelDestAddr2	Yes	Defines the destination IP address for IPsec tunnel 2.
GRE Dest Addr 2	greTunnelDestAddr2	Yes	Defines the destination IP address for GRE tunnel 2.

SCADA Metrics

Table 39 describes the fields on the SCADA tab of the Device Info page.

Table 39 SCADA Metrics View

Field	Key	Configurable?	Description
Channel Name	channel_name	No	Identifies the channel on which the serial port of the router communicates to the RTU.
Protocol Type	protocol	No	Identifies the Protocol Translation type.
Messages Sent	-	No	The number of messages sent by the router.
Messages Received	-	No	The number of messages received by the router.
Timeouts	-	No	Displays the timeout value for connection establishment.
Aborts	-	No	Displays the number of aborted connection attempts.
Rejections	-	No	Displays the number of connection attempts rejected by IoT FND.
Protocol Errors	-	No	Displays the number of protocol errors generated by the router.
Link Errors	-	No	Displays the number of link errors generated by the router.
Address Errors	-	No	Displays the number of address errors generated by the router.
Local IP	-	No	Displays the local IP address of the router.
Local Port	-	No	Displays the local port of the router.
Remote IP	-	No	Displays the remote IP address of the router.
Data Socket	-	No	Displays the Raw Socket server configured for the router.

User-defined Properties

The User-defined Properties area of the Routers > Config Properties page displays any customer defined properties.

WiFi Interface Config

Table 40 describes the fields in the WiFi Interface Config area of the **Field Devices > Config Properties** page.

Table 40 WiFi Interface Config Fields

Field	Key	Configurable?	Description
SSID	wifiSsid	No	The service set identifier (SSID) assigned to the WiFi interface on the router.
Pre-Shared Key	type6PasswordMasterKey	No	The key used to encrypt other pre-shared keys stored on the router.

WiMAX Config

Table 41 describes the fields in the WiMAX Config area of the Device Info page. Use these properties to set up a username and password for the Pairwise Key Management (PKM) of a CGR 1000.

Note: The WiMAX module must be installed and running. CGR1000s that ship with a pre-installed WiMAX module have a pre-installed WiMAX configuration.

Table 41 WiMAX Config Fields

Field	Key	Description
PkmUsername	PkmUsername	Pairwise Key Management (PKM) Username for WiMAX.
PkmPassword	PkmPassword	Pairwise Key Management (PKM) Password for WiMAX

WiMAX Link Metrics

Table 42 describes the fields in the WiMAX Link Health area of the Device Info page.

Table 42 WiMAX Link Health Fields

Field	Key	Description
Transmit Speed	wimaxTxSpeed	The current speed of data transmission over the WiMAX uplink network interface, measured in bits per second, averaged over a short element-specific time period (for example, an hour).
Receive Speed	wimaxRxSpeed	The rate of data that has been received by the WiMAX uplink network interface, measured in bits per second, averaged over a short element-specific time period (for example, an hour).
RSSI	wimaxRssi	The measured RSSI value of the WiMAX RF uplink (dBm).
CINR	wimaxCinr	The measured CINR value of the WiMAX RF uplink (dB).

WiMAX Link Settings

Table 43 describes the fields in the WiMAX Link Settings area of the Device Info page.

Table 43 WiMAX Link Settings Fields

Field	Key	Description
BSID	wimaxBsid	The ID of the base station connected to the WiMAX device.
Hardware Address	wimaxHardwareAddress	The hardware address of the WiMAX device.
Hardware Version	wimaxHardwareVersion	The hardware version of the WiMAX device.
Microcode Version	wimaxMicrocodeVersion	The microcode version of the WiMAX device.
Firmware Version	wimaxFirmwareVersion	The firmware version of the WiMAX device.
Device Name	wimaxDeviceName	The name of the WiMAX device.
Link State	wimaxLinkState	The link state of the WiMAX device.
Frequency	wimaxFrequency	The frequency of the WiMAX device.
Bandwidth	wimaxBandwidth	The bandwidth the WiMAX device is using.