

Managing Devices

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

- [Managing Routers](#)
- [Managing Endpoints](#)
- [Managing Head-End Routers](#)
- [Managing Servers](#)
- [Common Device Operations](#)
- [Configuring Rules](#)
- [Configuring Devices](#)
- [Managing a Guest OS](#)
- [Managing Work Orders](#)
- [Device Properties](#)

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

- To work with FARs and Endpoints (MEs), use the Field Devices page (**Devices > Field Devices**).
- To work with HERs, use the Head-End Routers page (**Devices > Head-End Routers**).
- To work with database and NMS servers, use the Servers page (**Devices > Servers**).
- To configure the device properties of routers and MEs, use the Device Configuration page (**Config > Device Configuration**).

Managing Routers

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

- [Working with Router Views](#)
- [Creating Work Orders](#)
- [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 [Setting User Preferences](#)), 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:

- Cellular-CDMA
- Cellular-GSM
- Config
- DHCP Config
- Default
- Ethernet Traffic
- Firmware
- LoRaWAN
- Mesh
- Mesh Config
- Physical
- 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](#).

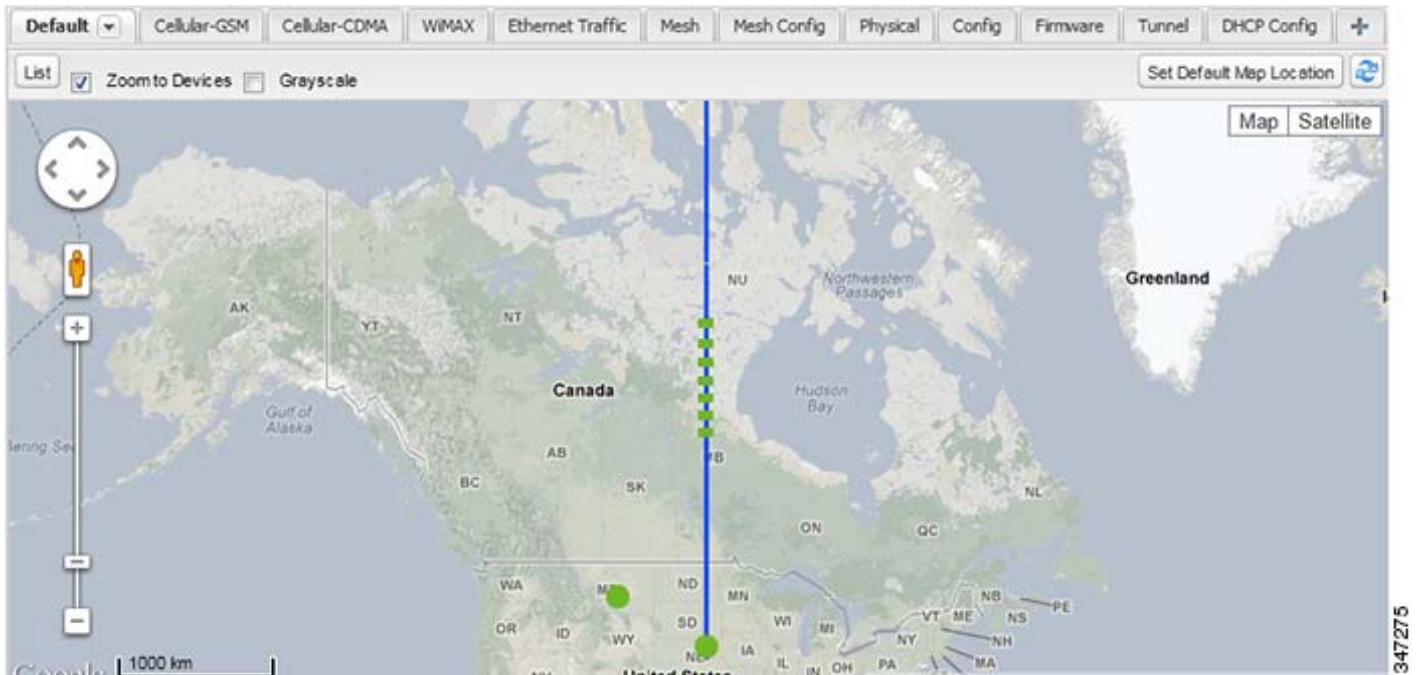
For information about common actions performed in these views (for example, adding labels and changing device properties), see [Common Device Operations](#).

Viewing Routers in Map View

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

Figure 1 Map View: Downlink Data Flow RPL Trees



Migrating Router Operating Systems

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

Creating Work Orders

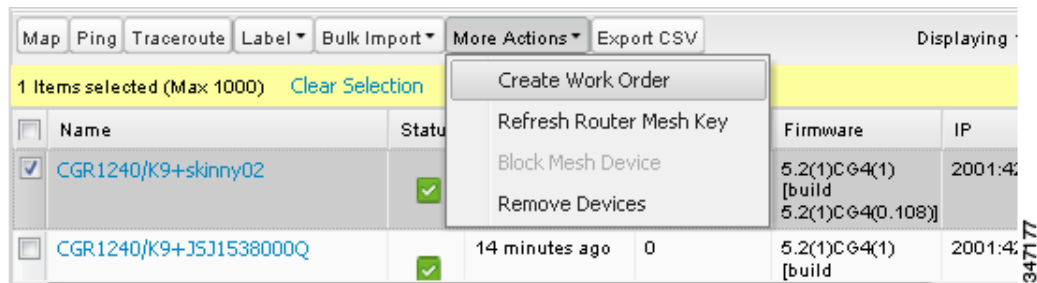
Create work orders in IoT FND to deploy field technicians for device inspections. Field technicians use the IoT-DM client to connect to IoT FND and download the work order.

Note: The Work Orders feature works with Release 3.0 or later of Device Manager (IoT-DM) only. See [“Accessing Work Authorizations”](#) in the [Cisco Connected Grid Device Manager Installation and User Guide, Release 3.1](#) for integration instructions for CG-OS installations. For Cisco IOS installations, please refer to the [Cisco Connected Grid Device Manager Installation and User Guide, Release 4.0](#) or later.

Note: Before you can create a work order, your user account must have Work Order Management permissions enabled. See [Managing Roles](#).

To create work orders for CGRs, select a router or group of routers in the **Browse Devices** pane, and then in **Default** view:

1. Check the check box of the faulty CGR.
2. Choose **More Actions > Create Work Order**.



The Work Orders page appears (**Config > Device Configuration > Work Orders**). On that page, IoT FND adds the names of the selected FARs to the List of FAR Names field as a comma-separated list.

- Follow the steps in [Creating Work Orders](#) to create the work order.

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

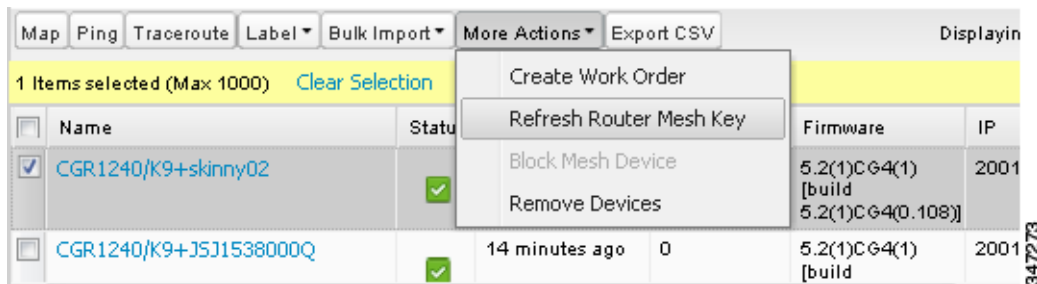
Refreshing the Router Mesh Key

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

Caution: Refreshing the router mesh key can result in MEs being unable to communicate with the FAR for a period of time until the MEs re-register with the FAR, 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:

- Check the check boxes of the of the FARs to refresh.



- Choose **More Actions > Refresh Router Mesh Key** from the drop-down menu.
- 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 FARs, 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

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

Displaying Router Firmware Groups

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

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 MEs 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 Field Devices page in Default view, IoT FND lists all FAN devices and 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:

- Map
- Config
- Default
- Firmware
- PLC Mesh
- RF Mesh
- Security
- Cellular Endpoints

Each one of these views displays different sets of device properties. For example, the Firmware view displays the device properties that fall under the firmware category, such as Hardware ID, Firmware Group, and FW Uploaded Version.

For information on how to customize ME 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 MEs 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 an ME, you cannot unblock it using IoT FND. To re-register the ME with IoT FND, you must escalate and get your ME administrator involved.

To block an ME device, in Default view:

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

Map Ping Traceroute Label Bulk Import More Actions Export CSV				Displaying
1 Items selected (Max 1000) Clear Selection				
Name	Status	Hops	Firmware	
<input type="checkbox"/> 00078108003C2600	✓	1	5.2.43	
<input checked="" type="checkbox"/> 00078108003C2601	✓	1	5.2.43	
<input type="checkbox"/> 00078108003C2602	✓	1	5.2.43	10 minutes ago
<input type="checkbox"/> 00078108003C2603	✓	1	5.2.43	10 minutes ago

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 use the Browse Devices pane to display the ME devices that belong to one of the groups listed under MESH DEVICE CONFIGURATION GROUPS.

Displaying Mesh Endpoint Firmware Groups

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

Managing Industrial Routers

You can use the configuration template to apply DSCP and Raw Socket settings to the IR509 Industrial Router.

DSCP Configuration

To configure DSCP on the IR509:

1. Choose **Config > Device Configuration**.
2. Select default-ir500 under ENDPOINT in the left-pane.
3. Choose **Edit Configuration Template** (Figure 2 and Figure 3)

Note: Refer to [Table 1](#) for a summary of configuration options.

Figure 2 Setting DSCP Markings on Ethernet Interface

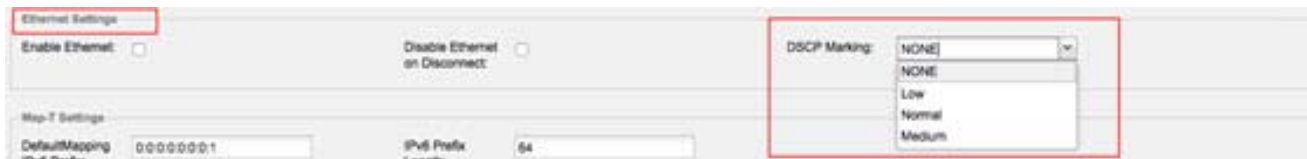
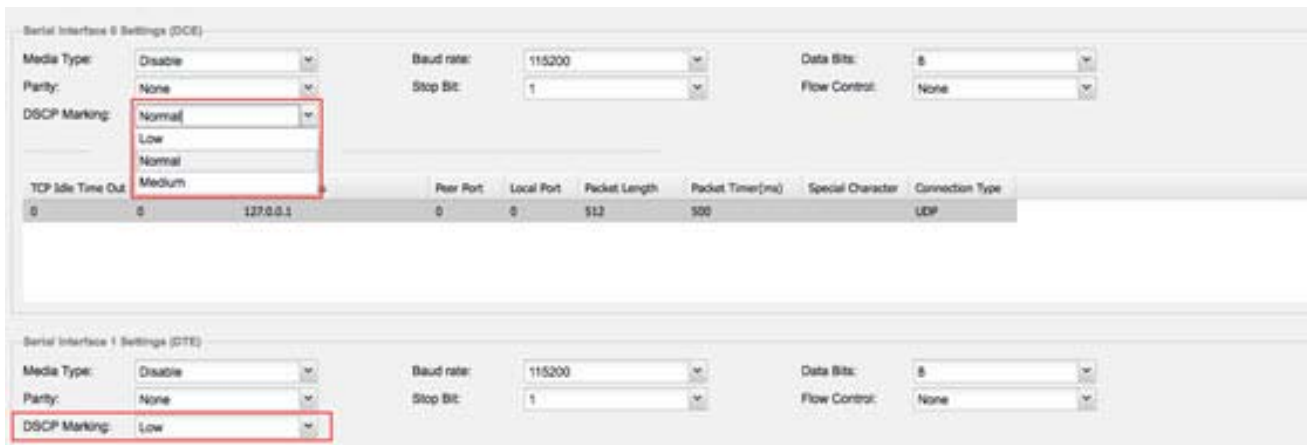


Figure 3 Setting DSCP Markings on DCE and DTEs



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 value 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.

Raw Socket Configuration

To configure Raw Socket on the IR509:

1. Choose **Config > Device Configuration**.
2. Select default-ir500 under ENDPOINT in the left-pane.
3. Choose **Edit Configuration Template ()**.

Note: Refer to [Table 1](#) for a summary of configuration options.

The screenshot displays the 'Raw Socket Configuration' interface. At the top, there is a 'Raw Socket Sessions' table with columns: TCP Idle Time Out, Connect Time Out, Peer IP Address, Peer Port, Local Port, Packet Length, Packet Timer(ms), Special Character, and Connection Type. The first row shows values: 0, 0, 127.0.0.1, 0, 0, 512, 500, and a dropdown menu for Connection Type with options: UDP (selected), TCP Client, TCP Server, and UDP. Below this is the 'Serial Interface 1 Settings (DTE)' section with fields for Media Type (Disable), Parity (None), DSCP Marking (Low), Baud rate (115200), Stop Bit (1), Data Bits (8), and Flow Control (None). At the bottom, there is another 'Raw Socket Sessions' table with columns: TCP Idle Time Out, Connect Time Out, Peer IP Address, Peer Port, Local Port, Packet Length, Packet Timer(ms), Special Character, and Connection Type. The first row shows values: 0, 0, 127.0.0.1, 0, 0, 512, 500, and a dropdown menu for Connection Type with options: TCP Server.

Configuration Notes:

- Update Raw Socket settings to support UDP sockets.
- Set stop bit values for serial devices. Values 1 to 4.
- Set minimum periodic notification interval for device. Values 1 to 5 minutes.

Table 1 Configuration Options for IR509

Interface	Settings
Ethernet	<ol style="list-style-type: none"> Ethernet Settings panel options (and required values): <ul style="list-style-type: none"> ■ Enable Ethernet: Leave option disabled (unchecked) ■ Disable Ethernet on Disconnect: Leave option disabled (unchecked) ■ DSCP Markings: Select NONE from the pull down menu. MAP-T Settings panel options: <ul style="list-style-type: none"> — Default Mapping IPv6 Prefix: 0:0:0:0:0:0:1 — IPv6 Prefix Length: 64
DCE	Serial Interface 0 Settings (DCE) panel options (and required values): <ul style="list-style-type: none"> ■ Media Type: Disable ■ Baud rate: 115200 ■ Data Bits: 8 ■ Parity: Normal ■ Stop Bit: 1 ■ Flow Control: None ■ DSCP Marking: Normal
DTE	Serial Interface 1 Settings (DTE) panel options (and required values): <ul style="list-style-type: none"> ■ Media Type: Disable ■ Baud rate: 115200 ■ Data Bits: 8 ■ Parity: None ■ Stop Bit: 1 ■ Flow Control: None ■ DSCP Marking: Low

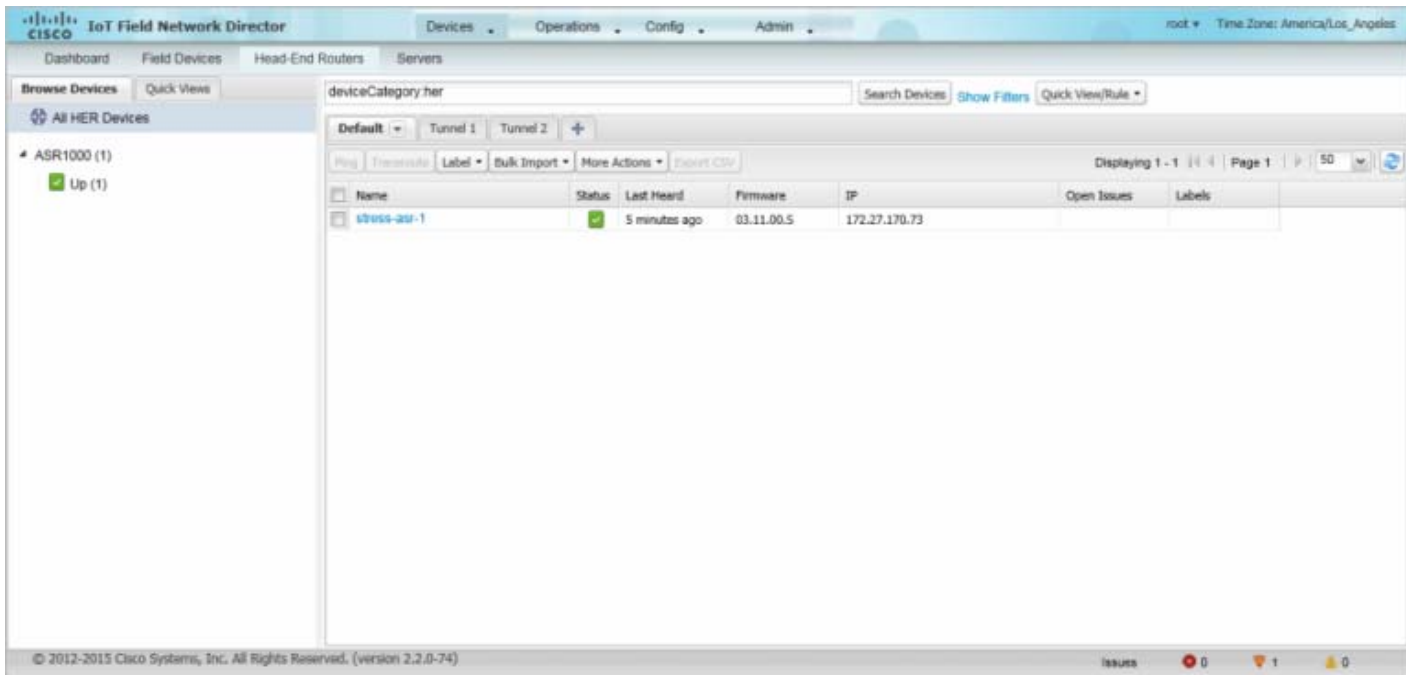
Managing Head-End Routers

To manage head-end routers (HERs), open the Head-End Routers page by choosing **Devices > Head-End Routers** (Figure 4). 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 4 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.

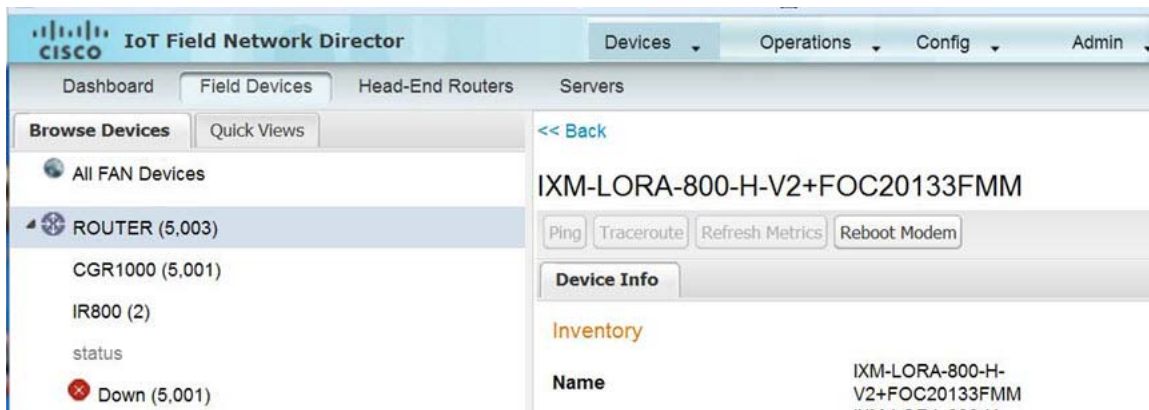


■ LoRaWAN

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

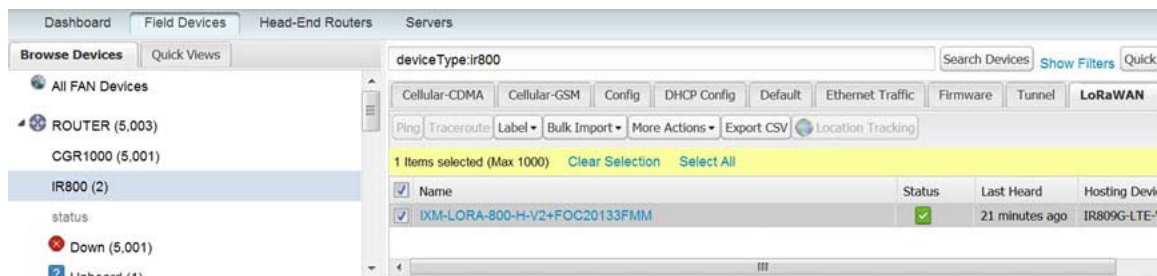
- To view LoRaWAN modules in a Device List, choose an IR800 router in the **Browse Devices** list and select the **LoRaWAN** tab.
- To reboot the modem on the LoRaWAN module:
 - a. Click on the relevant IXM-LORA link under the **Name** column to display the information seen below:



- 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 LoRa module which 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**.

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 Servers

In the Browse Devices pane, NMS servers appear under NMS Servers. In single-NMS server deployments, only one server appears under NMS Servers. In cluster deployments, multiple NMS servers appear under NMS Servers. To filter the list pane:

- To display all NMS servers, click **NMS Servers** in the Browse Devices pane.
- To display only operational servers, click **Up**.
- To display only non-operational servers, click **Down**.

Managing Database Servers

In the Browse Devices pane, IoT FND database servers appear under Database Servers. 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.

- To display all database servers in List view, click **Database Servers** in the Browse Devices pane.
- To only display servers that are operational, click **Up**.
- To only display servers that are non-operational, click **Down**.

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 devices across all pages, click **Select All**.

- To select all devices listed on a page, check the check box next to **Name**.
- 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

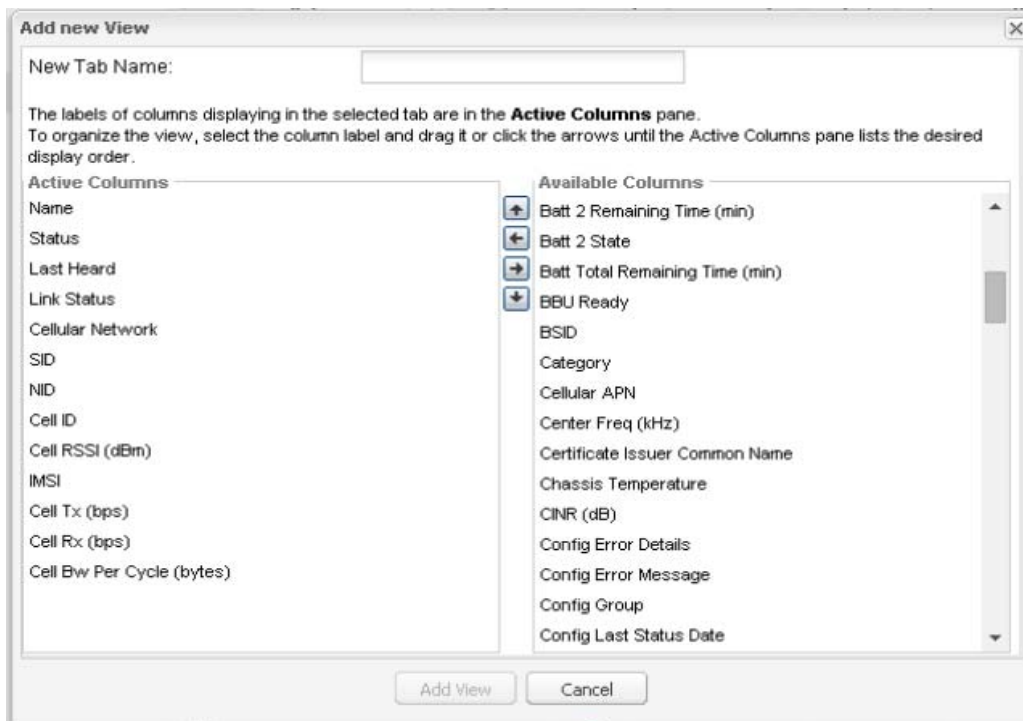
Adding Device Views

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.

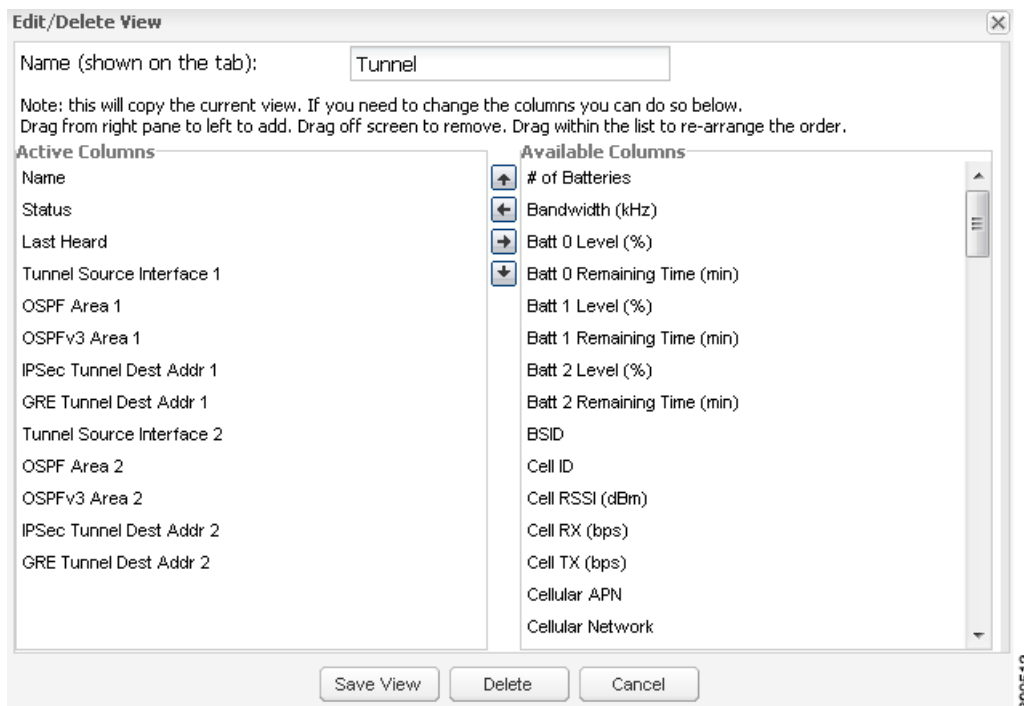
Tip: Hold the Shift key to select multiple column labels and move them to either list.

4. Click **Save View**.

Editing Device Views

To edit a device view:

1. Click the drop-down arrow on the desired tab.
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.

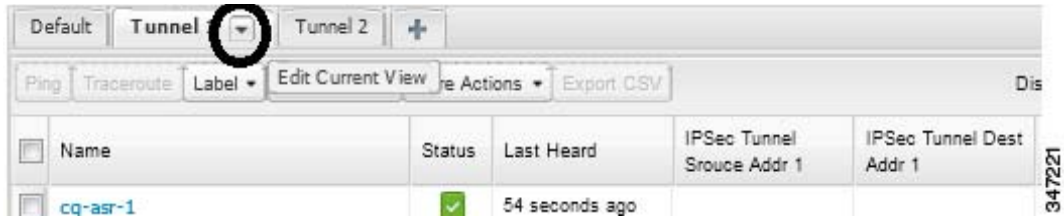


3. Click **Save View**.

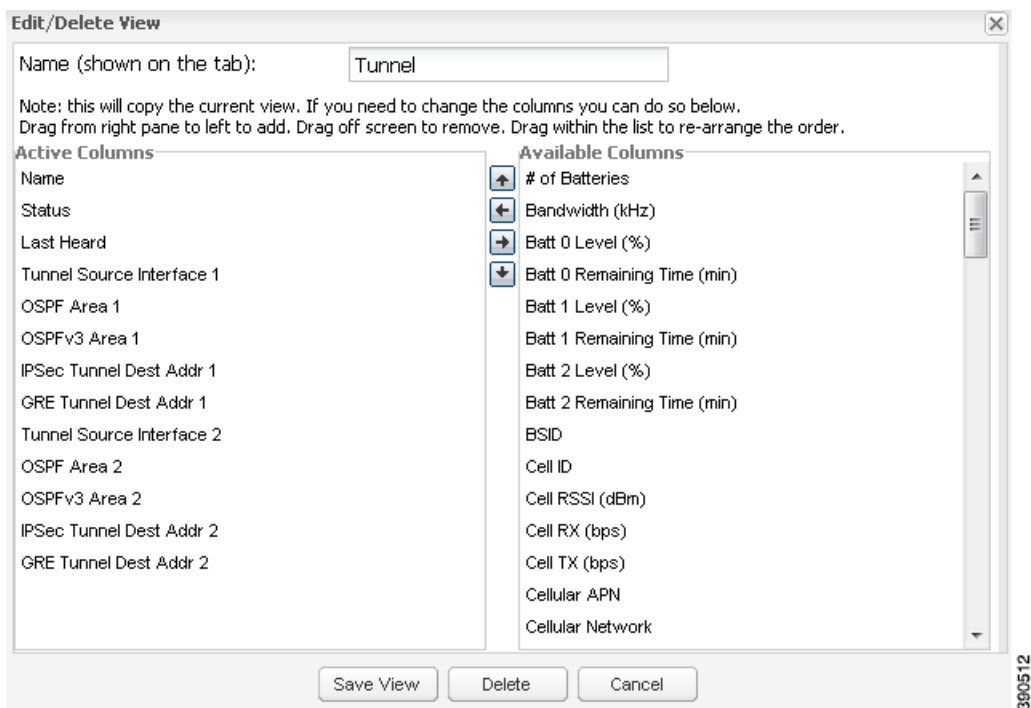
Deleting Device Views

To delete a device view:

1. Click the arrow on the tab of the device view to delete.



2. In the Edit/Delete View dialog box, select the desired label in the Active Columns pane.



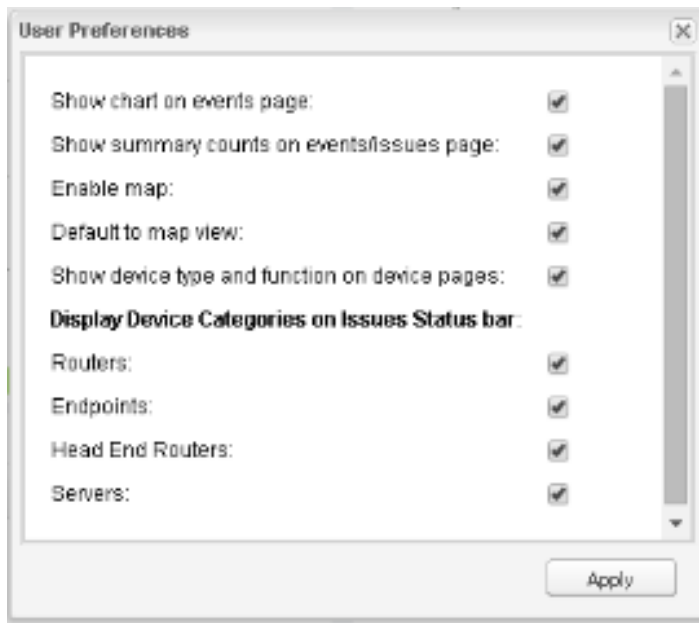
3. Click **Delete**.

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.

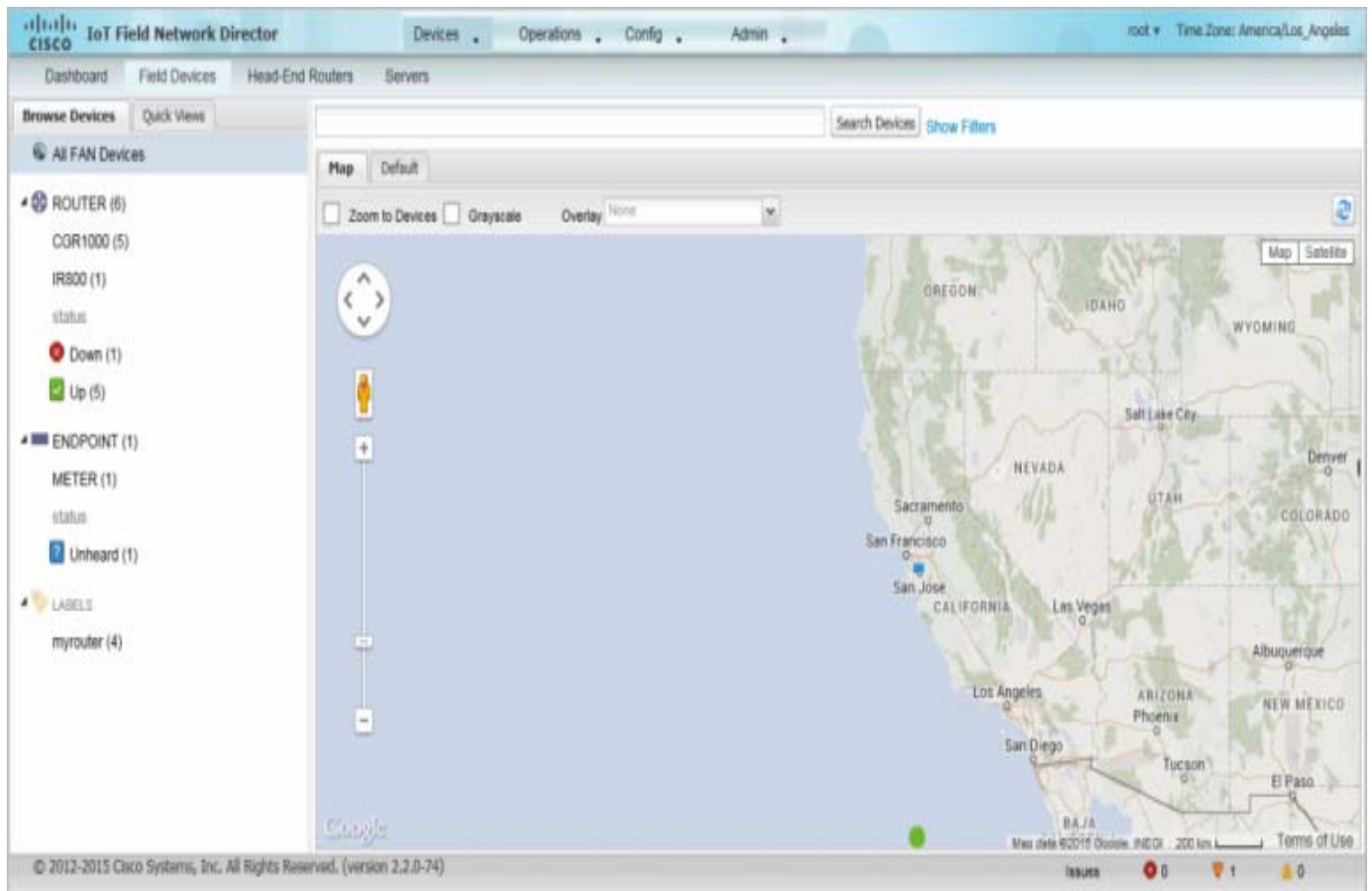
To view devices in Map view:

1. Choose **<user> > Preferences**, check the **Enable map** check box, and click **Apply**.

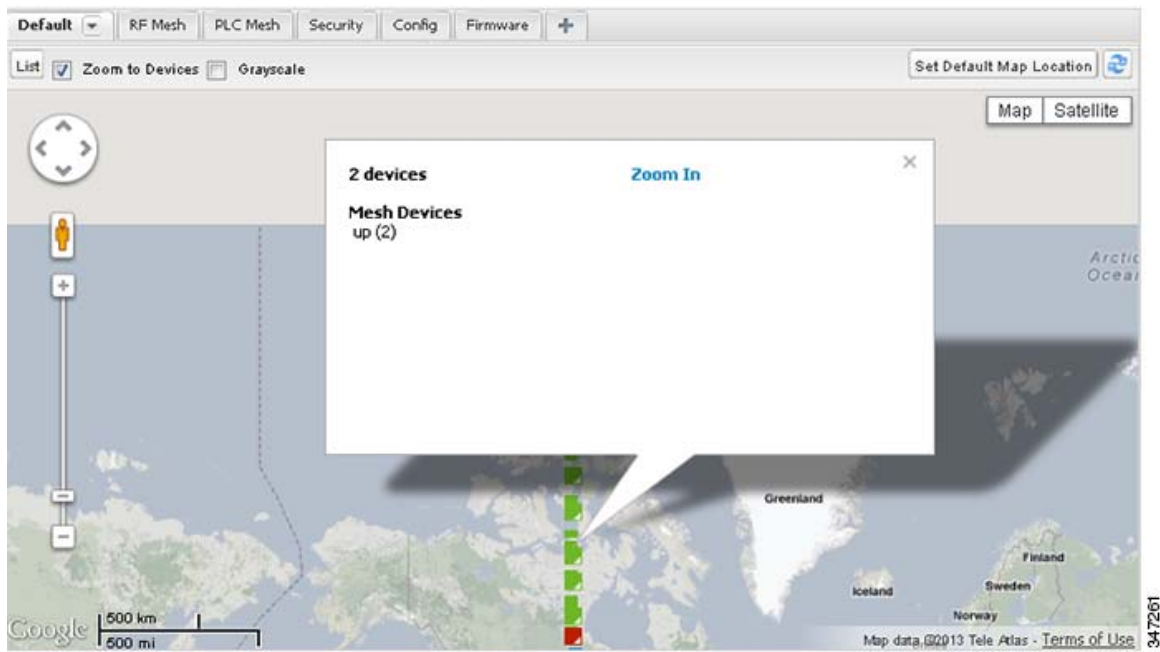


2. Choose **Devices > Field Devices**.
3. Click the **Map** tab.

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.

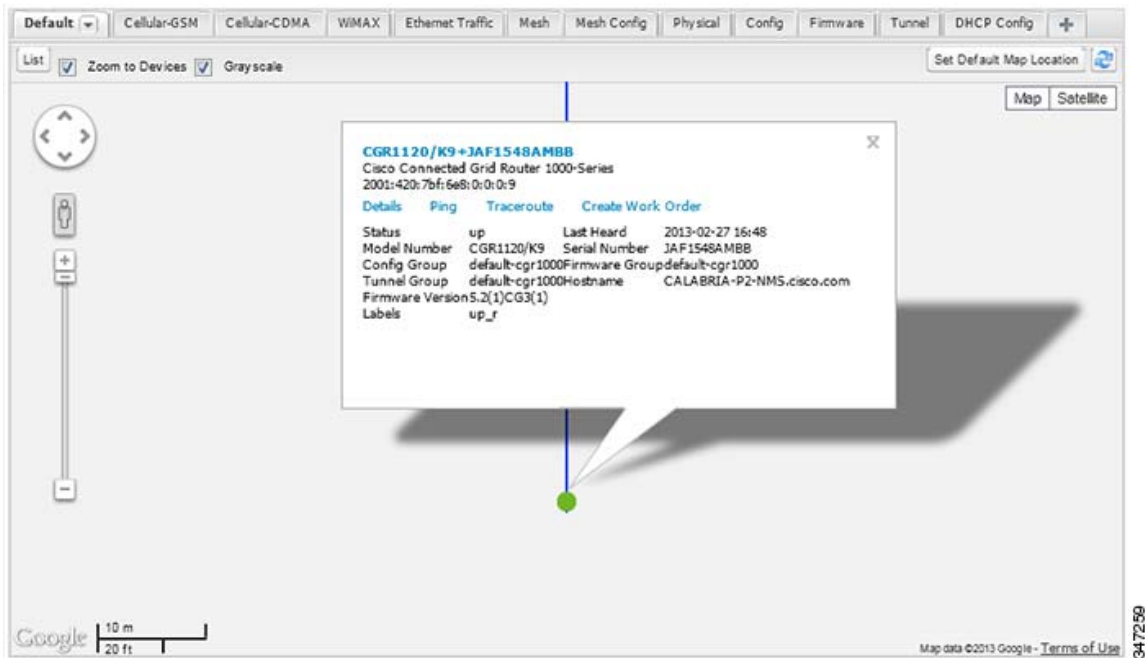


IoT FND displays the device count next to each device group or category in the Browse Devices pane (left pane).

- 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 FARs 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.

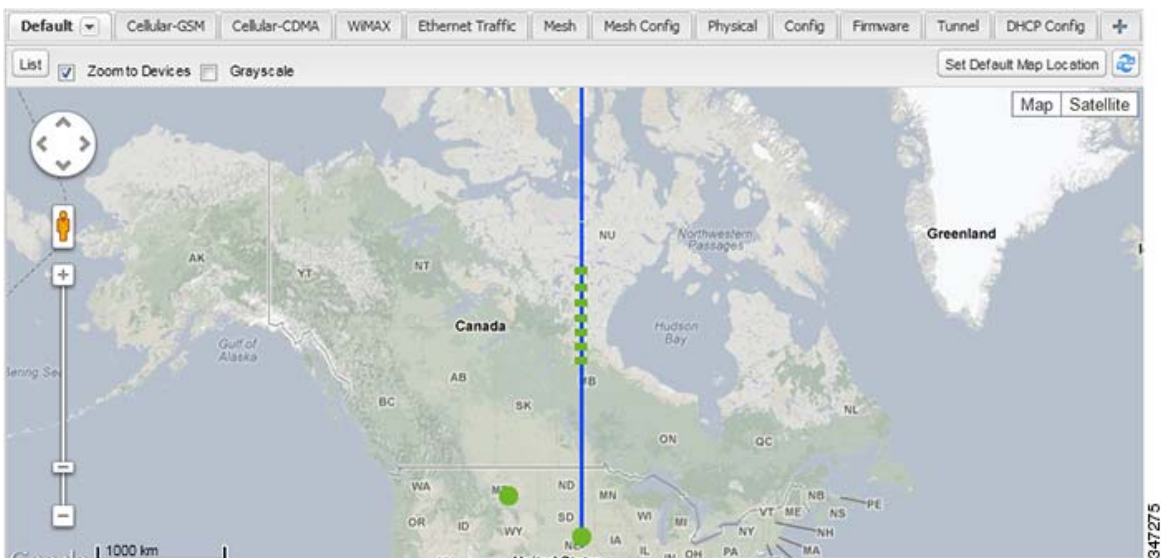


A popup window displays listing basic device or group information.


- 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.

4. 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.

5. Click the refresh button () to update the Map view.

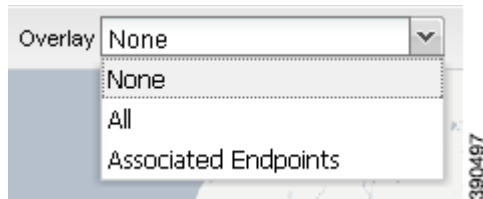
Configuring Map Settings

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:

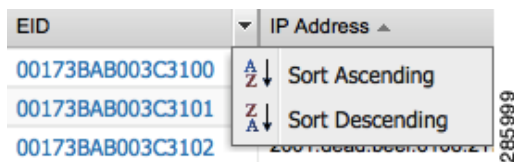
1. Choose **Devices > Field Devices**.
2. Click the **Map** tab.
 - To automatically zoom to devices, check the **Zoom to Devices** check box.
 - To display the map in grayscale, check the **Grayscale** check box.
 - To overlay all associated wireless personal area network (WPAN) endpoints on the map, select **Associated WPAN Endpoints** from the Overlay drop-down menu.



- To set the map location to always open to a certain area, display the area of the map to display by default, and then click **Set Default Map Location** (top right).
3. Click **OK**.

Changing the Sorting Order of Devices

To change the sorting order of devices, click the right side of the column heading and choose a sort command from the drop-down menu.



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**.

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 to ping the device at any time.

3. Click **Close** when done.

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.

Auto Refresh			
Started At	Device	Status	Result
2013-02-22 12:00	2004:cafe:aaaa:0:9fod:fed5	Completed successfully	tracert to 2004:cafe:aaaa:0:9fod:fed5 (2004:cafe:aaaa:0:9fod:fed5), 30 hops 1 2001:420:7b15f:710 (2001:420:7b15f:710) 0.721 ms 0.710 ms 0.710 ms 2 2001:420:7b15e8:9 (2001:420:7b15e8:9) 33.637 ms 34.132 ms 34.640 ms 3 2004:dead:aaaa:0:9fod:fed5 (2004:cafe:aaaa:0:9fod:fed5) 434.831 ms 580.117

Page 1 of 1 | 10 | Close

Displaying 1 - 1 of 1

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.

- Click **Close** when done.

Managing Device Labels

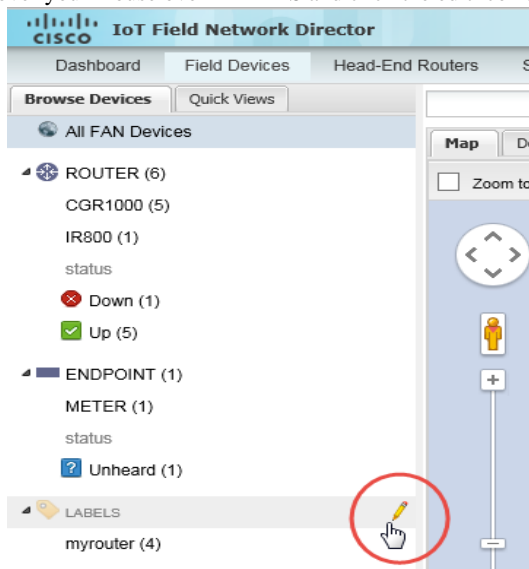
You use labels to create logical groups of devices to facilitate locating devices and device management.

Managing Labels

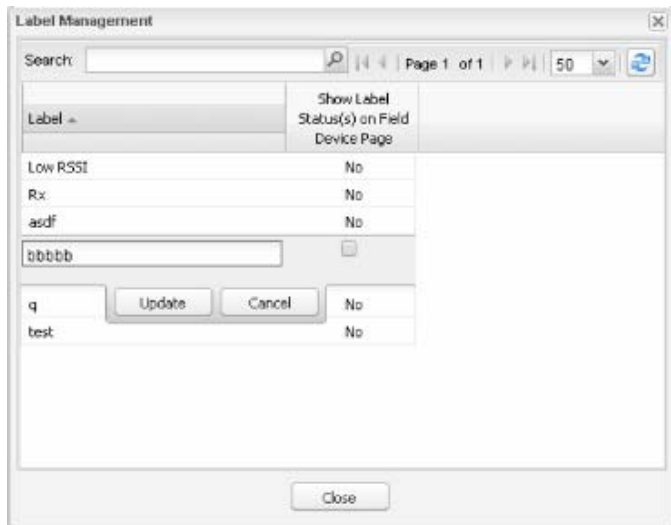
You use the Label Management window to display all custom labels, label properties, and search for custom labels.

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

- Hover your mouse over LABELS and click the edit icon (✎).



- To find a specific label, enter the label name in the **Search** field.



Tip: Click the Label column title to reverse label name sort order.

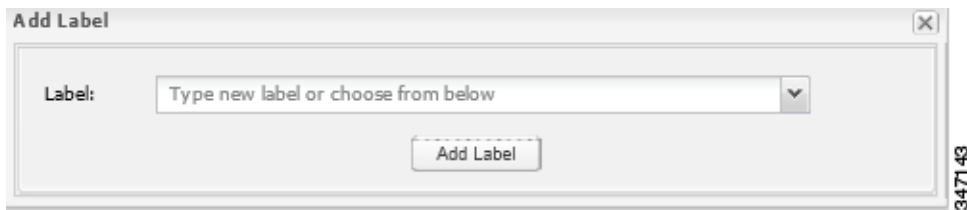
- To change label properties, double-click a label row, edit the label name and device status display preference.

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.
2. Choose **Label > Add Label**.



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

Tip: You can add multiple labels to one device.

5. 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**.

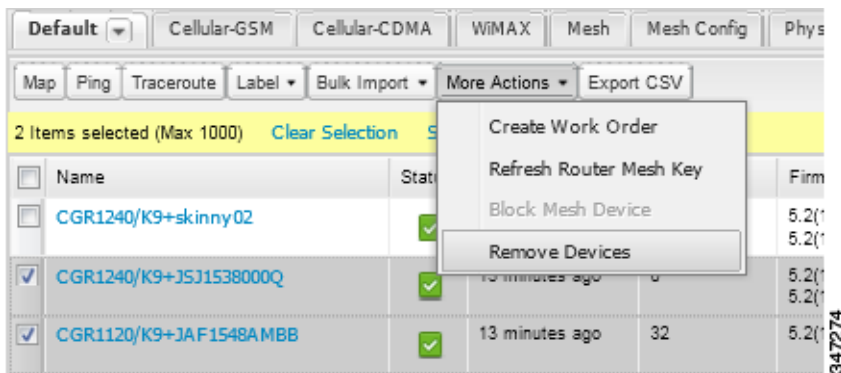
To remove labels in bulk, see [Removing Labels in Bulk](#).

Removing Devices

Caution: When you remove FARs, 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 HERs.

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

Detailed Information Displayed

- [Server Information](#)
- [HER, FAR, and Endpoint Information](#)

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

Server Information

IoT FND displays the following information about the system running the NMS and database 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.
Total Memory	Total amount of RAM memory (GB) available on the system.
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.

HER, FAR, and Endpoint Information

IoT FND groups the detailed device information it displays about HERs, FARs, and Endpoints into the following categories:

Information Category	Description
Device Info	Displays detailed device information (see Device Properties). For FARs and MEs, IoT FND also displays charts (see Viewing Device Charts).
Events	Displays information about events associated with the device.
Config Properties	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 (FARs)	Displays the running configuration on the device.
Mesh Routing Tree (FARs and MEs)	Displays the mesh routing tree. For FARs, the Mesh Routing Tree pane displays all the possible routers from the MEs to the FAR. For MEs, the Mesh Routing Tree pane displays the mesh route to the FAR.
Mesh Link Traffic (FARs)	Displays the type of mesh link traffic over time in bits per second.
Router Files (FARs)	Lists files uploaded to the .../managed/files/ directory.
Raw Sockets (FARs)	Lists metrics and session data for the TCP raw sockets (see Table 29 on page 250)

Information Category	Description
Embedded AP (IR829)	Lists inventory (configuration) details and metrics for the attached access point.
AP Running Config (C800 and IR800)	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 these actions:

Action	Description
Show on Map (MEs only)	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
Refresh Metrics (HERs and FARs 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.
Refresh Router Mesh Key (FARs only)	Refreshes the router ME key. See Refreshing the Router Mesh Key
Create Work Order (FARs and DA Gateway only)	Creates a work order. See Creating Work Orders
Sync Config Membership (MEs only)	Synchronizes the configuration membership for this device. See Synchronizing Endpoint Membership
Sync Firmware Membership (MEs only)	Click Sync Firmware Membership to synchronize the firmware membership for this device, and then click Yes to complete the process.
Block Mesh Device (MEs only)	Blocks the ME 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.

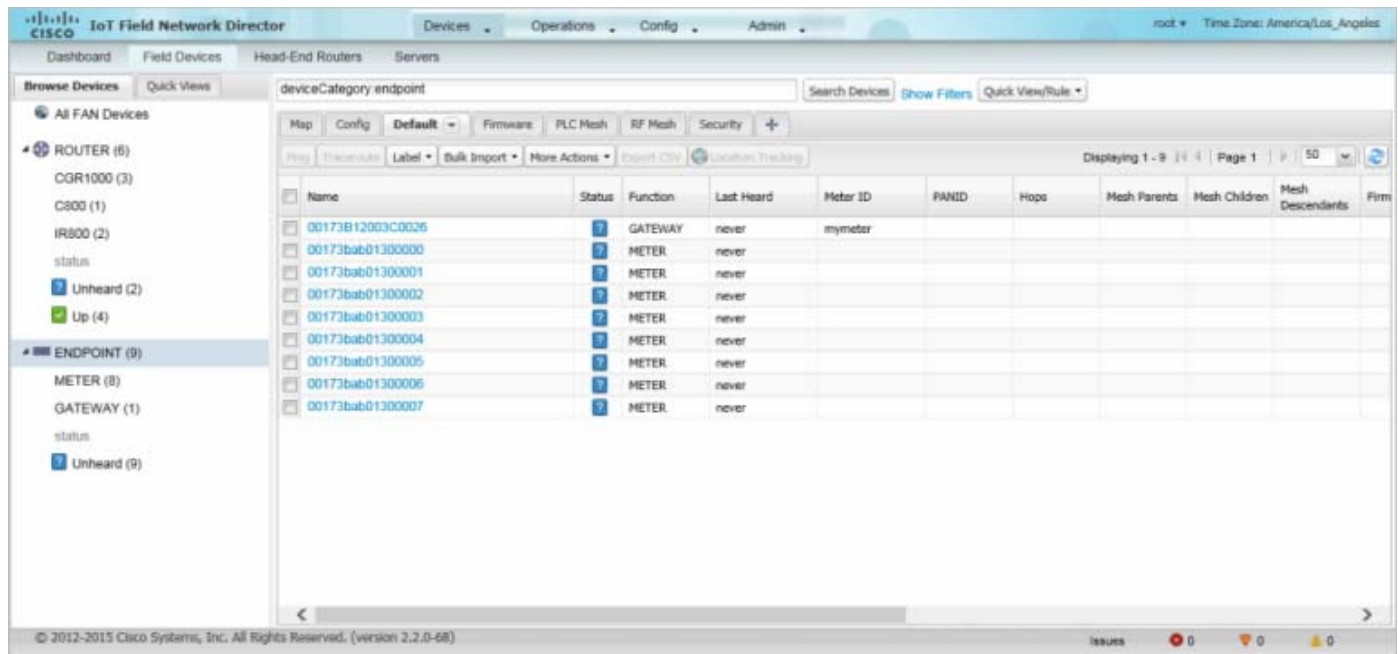
Using Filters to Control the Display of Devices

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 5](#), 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 5 Built-in Filter to Search for MEs



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 Name field of the Save Quick View dialog box, enter the name for the Quick View filter.
4. Click **Save**.

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.
name:00173*	Finds all FARs 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:

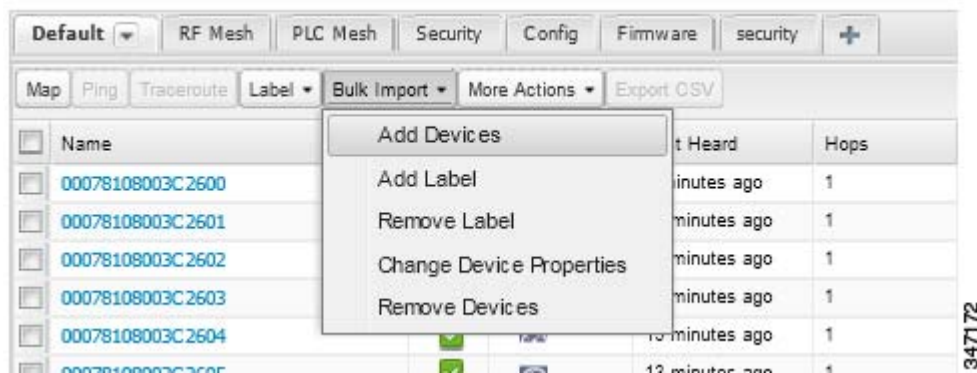
- [Adding Devices in Bulk](#)
- [Removing Devices in Bulk](#)
- [Changing Device Properties in Bulk](#)
- [Adding Labels in Bulk](#)
- [Removing Labels in Bulk](#)

Adding Devices in Bulk

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

To add devices in bulk:

1. On any device page, from the Bulk Import drop-down menu, choose **Add Devices**.



2. Click **Browse** to locate the CSV file containing the device information to import, and then click **Open**.

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

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

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

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

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 FARs to IoT FND

Typically, when adding FARs 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 FAR 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 237](#).

Table 6 describes the FAR properties defined in the R record used in this example:

Table 6 FAR Import Fields

Field	Description
PID	The product ID, as supplied by Cisco. This is not printed on the product.
SN	The FAR serial number. Note: IoT FND forms the FAR EID by combining the PID and SN.
ESN	A serial number assigned by your Cisco partner to the WPAN mesh card inside the FAR. This field is not used by IoT FND.
wifiSsid	This information is configured on the FAR 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 FARs to HERs

After you determine the FAR-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 FAR record in the Notice-of-Shipment XML file.
- Creating a CSV file specifying the mapping of FARs to HERs.

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

To map a FAR to an HER, add the tunnelHerEid and ipsecTunnelDestAddr1 HER properties to the FAR 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 FAR-to-HER Mappings to a CSV File

To map FARs to HERs using a CSV file, add a line for every FAR-to-HER mapping. The line must specify the EID of the FAR, 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 FARs, 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 Import** > **Remove Devices**.



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

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.

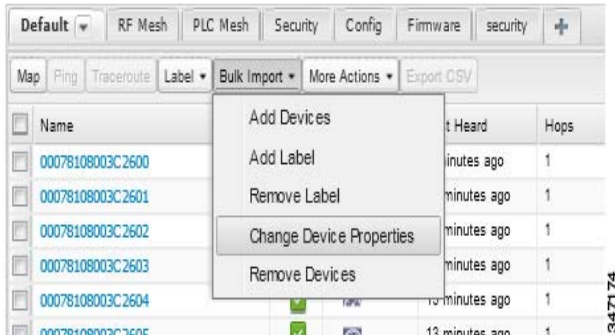
Changing Device Properties in Bulk

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 Import > 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.

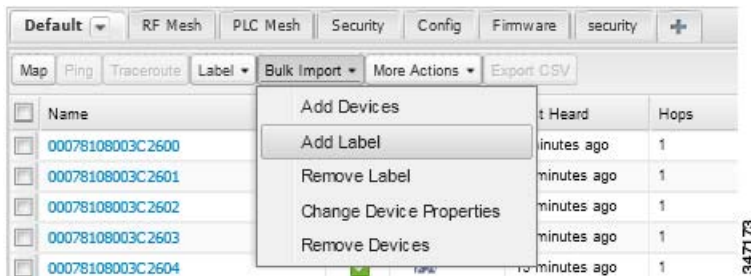
Adding Labels in Bulk

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 Import > 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.

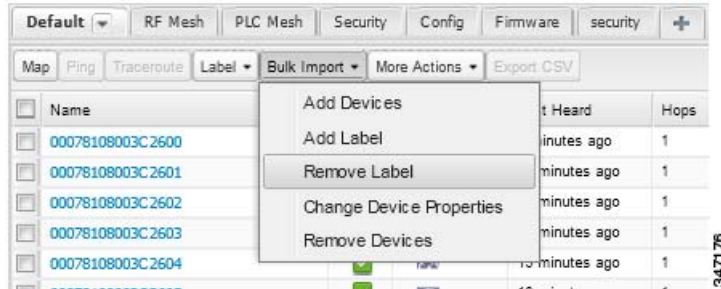
5. Click **Close** when done.

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 Import > 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 FAR 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	<p>The syntax of the rule.</p> <p>For example, IoT FND executes this rule when a device battery 0 level drops below 50%:</p> <pre>battery0Level<50</pre>
Rule Actions	<p>The actions performed by the rule. For example:</p> <pre>Log Event With: CA-Registered , Add Label: CA-Registered</pre> <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 [Adding a Rule](#).

Adding 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. Enter the syntax of the rule.

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

6. 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.
 - **Event Name**—Enter the event name to assign to the event (see [Searching By Event Name, page 327](#)).

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 2012 22:32:41.964 +0000: %CGMS-7-UNSPECIFIED:
%[ch=EventProducer][sev=DEBUG][tid=com.esperitech.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,
eventId=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 **Save**.

Activating Rules

IoT FND does not apply rules if they are not activated.

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 FARs](#)
- [Pushing Configurations to Endpoints](#)

Configuring Device Group Settings

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

- [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 **Devices > Field Devices** page left tree as follows:

Group Name	Description
default-act	By default, all Itron OpenWay RIVA Electric devices (METER) 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 (METER) 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 (ROOT) 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-cgmesh	By default, all cgmesh endpoints (METER) are members of this group.
default-cgr1000	By default, all CGRs (ROUTER) are members of this group.
default-ir800	By default, all IR800s (ROUTER) 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.

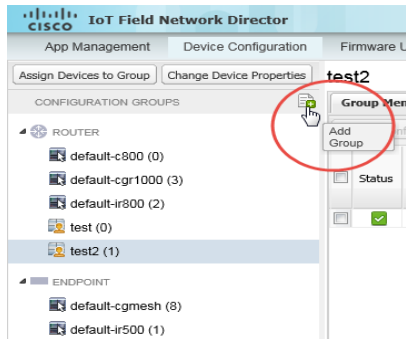
- [Creating ROUTER Groups](#)
- [Creating ENDPOINT Groups](#)

Creating ROUTER Groups

Note: CGRs, IR800s, and ISR800s can coexist on a network; however, you must create custom templates that includes all router types.

To create a ROUTER configuration group:

1. Choose **Config > Device Configuration**.
2. Select the default group: **default-cgr1000** **default-ir800**, or **default-c800**
3. Click the **Add Group** button.



4. Enter the name of the group.

The device category is selected 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 **OK** button.

5. Click **Add**.

The new group entry appears in the ROUTERS 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-cgmesh**, **default-act**, **default-cam**)
3. Click the **Add Group** (📁) button.
4. Enter a name for the group.

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 ENDPOINT list (left pane).

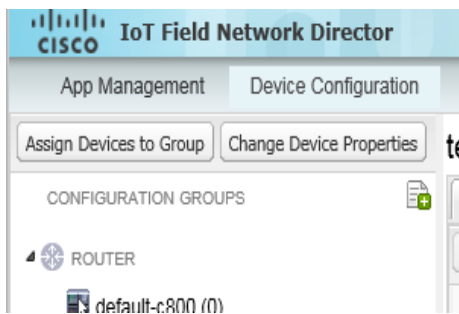
- To change the name of a group, see [Renaming a Device Configuration Group](#).
- To remove a group, see [Deleting Device Groups](#).

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 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. Check the check boxes of the devices to move.
4. Click **Change Configuration Group**.

Group Members				
Edit Configuration Template Push Configuration Group Properties				
Change Configuration Group				
1 Items selected (Max 1000) Clear Selection				
<input type="checkbox"/>	Status	Name	IP Address	Last Heard
<input type="checkbox"/>	✓	CGR1120/K9+JAF1548AMBB	2001:420:7bf:6e8:0:0:0:9	2013-02-2...
<input checked="" type="checkbox"/>	✓	CGR1240/K9+JSJ1538000Q	2001:420:7bf:6e8:0:0:0:3	2013-02-2...

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

Moving Devices to Another Configuration Group in Bulk

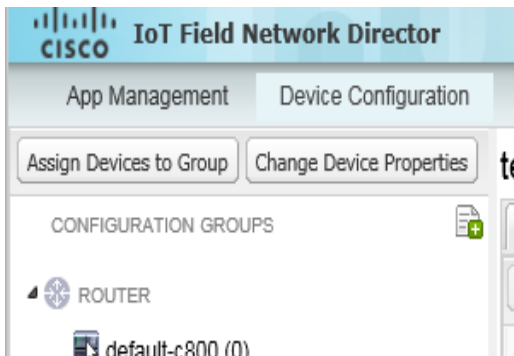
To move a large number of devices from one group to another, you can import a CSV file containing the list of the devices to move.

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:

- Choose **Config > Device Configuration**.
- Click **Assign Devices to Group**.



- Click **Browse** to locate the CSV file containing the list of devices to move, and then click **Open**.
- From the Group drop-down menu, choose the target group for the devices.
- Click **Change Group**.
- Click **OK**.

Listing Devices in a Configuration Group

To list the devices in a configuration group:

- Choose **Config > Device Configuration**.
- 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.

Configuring Periodic Inventory Notification and Mark-Down Time

You can change the periodic inventory notification interval for a configuration group of FARs without affecting the logic that IoT FND uses to mark those FARs as **Down**. However, for this to happen, you must enable the periodic configuration notification frequency for the FAR 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>

```

CG-IOS CGRs

CG-OS CGRs

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 an 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 **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**.

4. In the **Mark Routers Down After** field, enter the number of seconds after which IoT FND marks the FARs 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.

5. Click **Save Changes**.
6. Ensure that the periodic-configuration notification frequency in the configuration template is less than the value you entered the **Mark Routers Down After** field:
 - a. Click **Edit Configuration Template**.
 - b. 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>
```

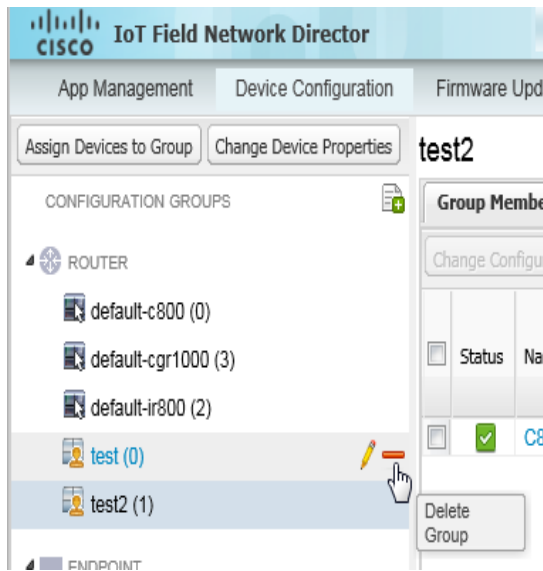
Note: The ability to control the periodic inventory notification interval and the periodic-configuration notification frequency applies to CGR image version 3.2.

Renaming a Device Configuration Group

To rename a device configuration group:

1. Choose **Config > Device Configuration**.
2. Select a group from the list of configuration groups (left pane).
3. Click the **Edit Group** icon.

The Edit Group button displays as a pencil icon when you hover over the name of the group in the list.



4. 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**.

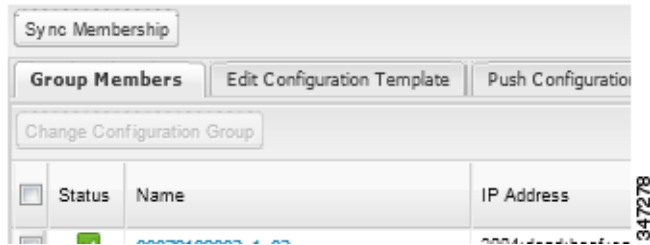
Synchronizing Endpoint Membership

MEs maintain information about the IoT FND group to which they belong. If the group information changes, the ME becomes out of sync. For example, if you rename an ME 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 MEs remain in sync, use the Sync Membership button to push the group information to group members.

To send group information to MEs:

1. Choose **Config > Device Configuration**.
2. Select an **ENDPOINT** group (left pane).
3. Check the check boxes of the members in the group to sync.

4. Click **Sync Membership**.



5. When prompted to synchronize membership for the group, click **Yes**.

6. Click **OK**.

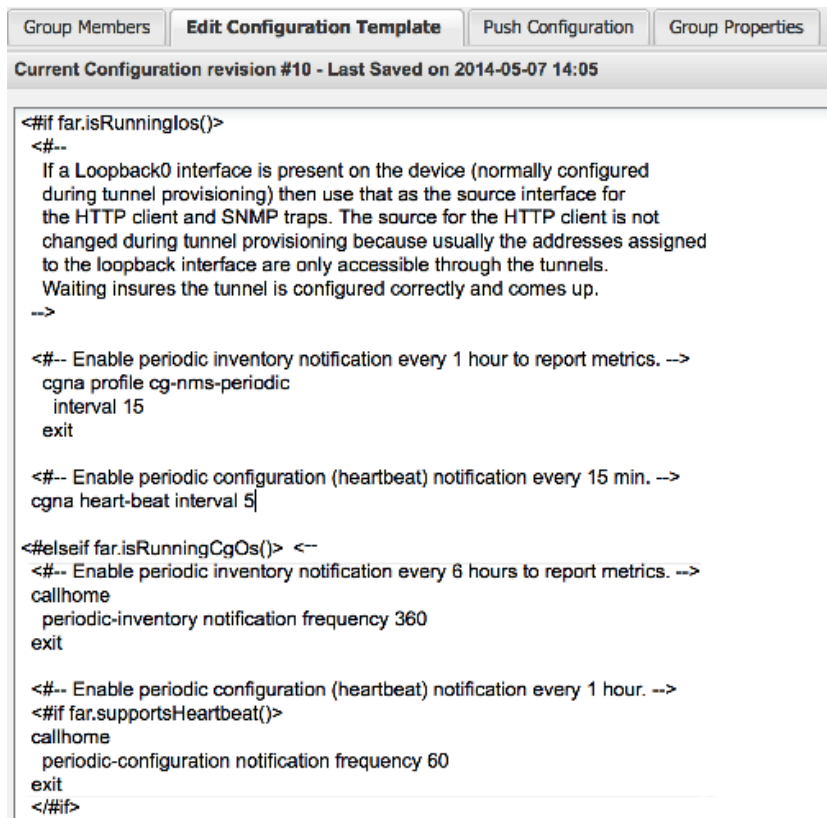
Devices sync for the first time after they register with IoT FND.

Editing the ROUTER Configuration Template

IoT FND lets you configure FARs in bulk using a configuration template. When a FAR 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**.



347219

4. Edit the template.

The template is expressed in FreeMarker syntax. For more information about FreeMarker, see [Tunnel Provisioning Template 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**.

default-c800

Group Members
Edit Configuration Template
Edit AP Configuration Template
Push Configuration
Group Properties

Current Configuration revision #1 - Last Saved on 2015-07-21 19:31

<#-- Default Access point Configuration -->

4. Edit the template.

The template is expressed in FreeMarker syntax. For more information about FreeMarker, see [Tunnel Provisioning Template Syntax](#).

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

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 \(Cisco IOS\)](#).

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)
-->
<#-- cгна geo-fence interval 10 -->
<#-- cгна 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 [Adding 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**.

Sync Membership

Group Members
Edit Configuration Template
Push Configuration

Current Configuration revision #12 - Last Saved on 2014-04-01 18:10

Report Interval (seconds): 907
(For metrics: InterfaceMetrics, GroupInfo, FirmwareImageInfo, Uptime, RawTCPForwarderStatus, RawTCPForwarder)

BBU Settings: Enable

Enable Ethernet: ☒

Map-T Settings

DefaultMapping IPv6 Prefix: 2199:0:0:0:0:0:0:0:0
IPv6 Prefix Length: 64
IPv4 Prefix: 2.2.6.0
IPv4 Prefix Length: 24
EA Bits Length: 8

Serial Interface 0 Settings (DCE)

Media Type: RS232
Baud rate: 19200
Data Bits: 8
Parity: None
Stop Bit: 1
Flow Control: None

TCP Raw Socket Sessions

TCP Idle Time Out	Connect Time Out	Peer IP Address	Peer Port	Local Port	Packet Length
20100	0	2.2.6.10	5000	5001	0

Serial Interface 1 Settings (DTE)

Media Type: Disable
Baud rate: 115200
Data Bits: 8
Parity: None
Stop Bit: 1
Flow Control: None

TCP Raw Socket Sessions

TCP Idle Time Out	Connect Time Out	Peer IP Address	Peer Port	Local Port	Packet Length
0	0	127.0.0.1	0	0	0

Save Changes

391265

4. Edit the template.

For example, in the **Report Interval** field, you can enter the number of seconds between data updates. By default, MEs 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 – Designate the device as the client/server.
- TCP idle timeout (min) – Set the time to maintain an idle connection
- Local port – Set the port number of the device.
- Peer port – Set the port number of the client/server connected to the device.
- Peer IP address – Set the IP address to the host connected to the device.
- Connect timeout – Set 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 FARs

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

To push the configuration to FARs:

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.

The screenshot shows the 'Push Configuration' tab in a management interface. It includes a 'Push Router Configuration' dropdown and a 'Start' button. Below this, configuration details are listed: Pushing Config Version (10), Pushed Data (Config Push with template revision 10), Start Time (2015-10-26 04:17), Completed Devices (0/2), Status (Stopped), Finish Time (2015-10-26 04:20), and Error Devices (2/2). A 'Device Status' section contains a table with columns: Name, Push Status, IP Address, Error Message, and Error Details. The table shows two devices with an 'ERROR' status and the message 'Operation was canceled before this element was processed'.

Name	Push Status	IP Address	Error Message	Error Details
CGR1240/K9+JAF1616AQCS	ERROR	66.66.0.134	Operation was canceled before this element was processed	
CGR1240/K9+JAF1715BJDN	ERROR	10.197.73.200	Operation was canceled before this element was processed	

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. 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 appear:

- 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.

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

Push SD Card Password ▼ Start

Pushing Config Version: 10 **Status:** Stopped
Pushed Data: Config Push with template revision 10
Start Time: 2015-10-26 04:17 **Finish Time:** 2015-10-26 04:20
Completed Devices: 0/2 **Error Devices:** 2/2

Device Status

Displaying 1 - 2 | Page 1 | 50

Name	Push Status ▲	IP Address	Error Message	Error Details
CGR1240/K9+JAF1616AQCS	ERROR	66.66.0.134	Operation was canceled before this element was processed	
CGR1240/K9+JAF1715BJDN	ERROR	10.197.73.200	Operation was canceled before this element was processed	

4. In the **Select Operation** drop-down menu, choose **Push SD Card Password**.

5. Click **Start**.

6. Select **SD Card protection > Enable**.

SD Card Password Configuration

SD Card protection: ☒ Disable ☐ Enable

Push SD Card Password Cancel

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	Number of nodes within the group. In the example above, there are a total of 51 nodes within the group, which are split across three different subnets.
Total in Subnet	Number of nodes with the subnet. In the example above, there are 19 nodes in the subnet.
Config Synced	Shows how many nodes within a Pan ID are in the process or have finished a configuration push out of the total nodes in that Pan.

PanId	Subnet Prefix	Nodes in Group (Total in Subnet)	Config Synced
0	200a:0:0:0:0:0:0:0	11 (19)	11 / 11
1	200b:0:0:0:0:0:0:0	20 (19)	20 / 20
2	200c:0:0:0:0:0:0:0	20 (19)	20 / 20

4. In the **Select Operation** drop-down menu, choose **Push Endpoint Configuration**.

5. 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 appear:

- 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.

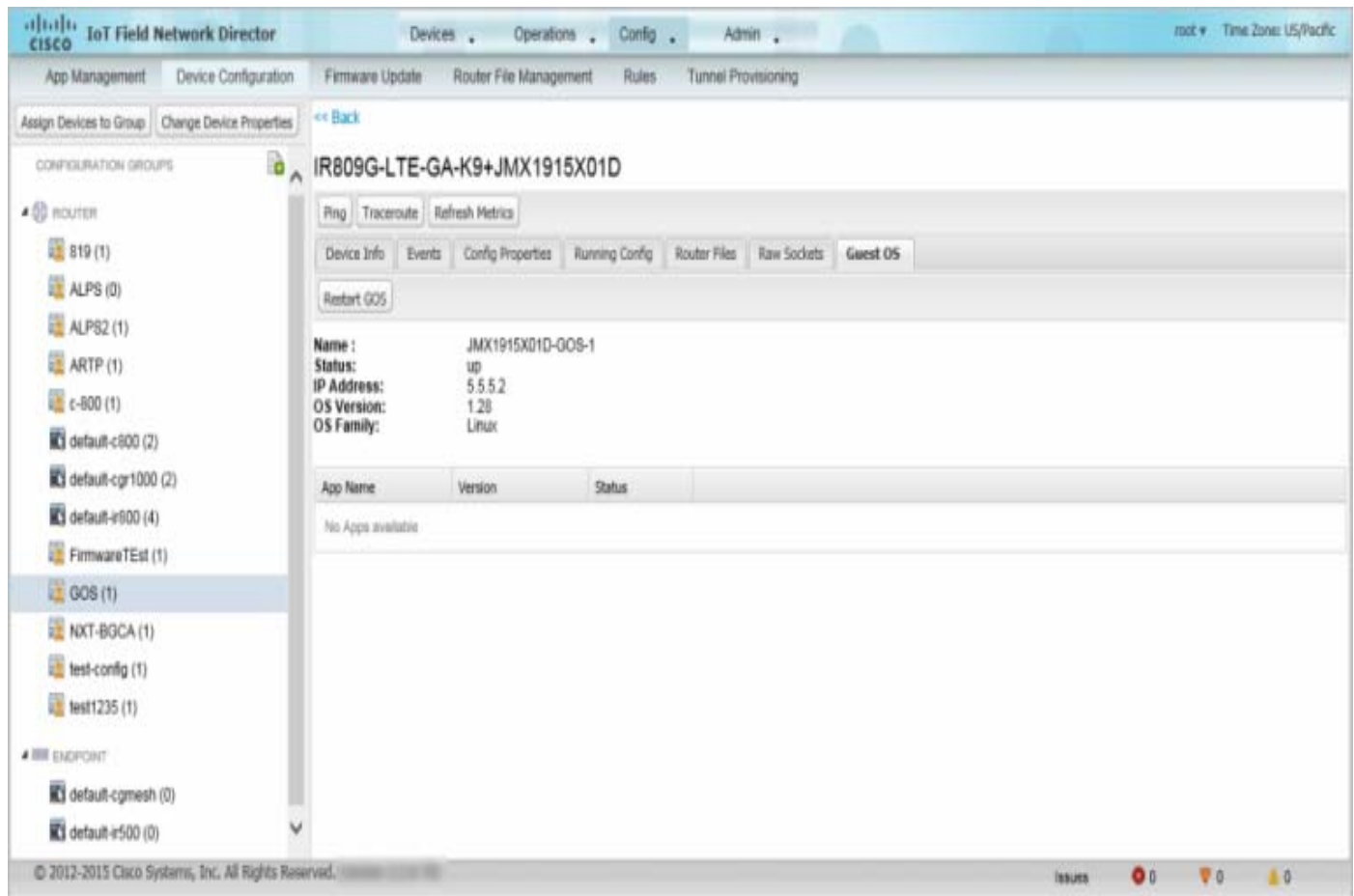
Managing a Guest OS

Cisco IOS CGRs 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. IoT FND supports the following role-based features on the GOS:

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

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

You manage and monitor a GOS on the **Config > Device Configuration** page, on the **Guest OS** tab.

Figure 6 Config > Device Configuration Page – Guest OS Tab Restart GOS Button

This section includes the following topics:

- [Installing a GOS](#)
- [Managing GOS Applications](#)
- [Restarting a Guest OS](#)

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 [“FAR Firmware Updates”](#) section on page -259). 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 IoT FND detects a non-Cisco OS is installed on the VM, the firmware bundle will not upload and the Cisco reference GOS will not install.

Managing GOS Applications

Applications (apps) run on the VM instance, but are not included in the Cisco IOS firmware bundle. You distribute GOS apps as standard `app-<appname>-ver-<version>.zip` files, and use the **Config > App Management** page to upload, install, start and stop, and uninstall GOS apps. The IoT FND internal backup and restore mechanism preserves existing apps during upgrades.

Note: For IoT FND GOS communications such as application uploads to the GOS using ssh, the `gosPassword` must be the CGR properties file. You upload the properties file in a CSV/XML upload. Without the `gosPassword` property, IoT FND cannot upload apps to a GOS.

Users with the GOS Application Management role enabled can upload, install, and deploy apps on Cisco IOS CGRs within your network.

Figure 7 Config > Apps Management Page—Last Job Status

The screenshot shows the Cisco IoT Field Network Director interface. The left sidebar lists various firmware and configuration groups. The main panel is titled 'Activity Status' and shows details for a specific job. The job summary indicates it was completed successfully on 2015-07-23 14:06. Below this, a table lists the devices involved in the activity.

Device Name	GOS Host Name	GOS Type	App Name	App Version	Start Time	Last Status Time	Activity	Activity Status
IR809G-LTE-GA-K9+JMX1915X01D	JMX1915X01D-GOS-1	Linux	sensorbot	7.5	2015-07-23 14:06	2015-07-23 14:06	Delete Remote Package	REMOTE_APP_PAC

Managing GOS App Activities

You can manage app activities (jobs) on the Config > App Management **Activity Status** tab. The top pane (above the device list) displays job-related info for the last activity performed, which includes:

- The start and stop time of the last activity.
- The app name.
- The status of the activity.
- The number of devices with successful results and the number of devices with errored results.

Table 8 lists fields that display in the device list on the Activity Status tab.

Table 8 Activity Status Tab

Field	Description
Device Name	Name of the selected device.
GOS Host Name	Name of the GOS host.
App Name	Name of the app.
App Version	Version assigned to the app.
Start Time	The start for the selected activity.
Last Status Time	The last status update time.
Activity	The selected activity: Upload, Set to Run, Install, Start, Stop, Uninstall, and Delete Remote Package.
Activity Status	The status of the selected activity.
Progress	How much of the activity completed.
Message	Notes generated by the activity.
Error Details	Details on errors encountered during the activity.

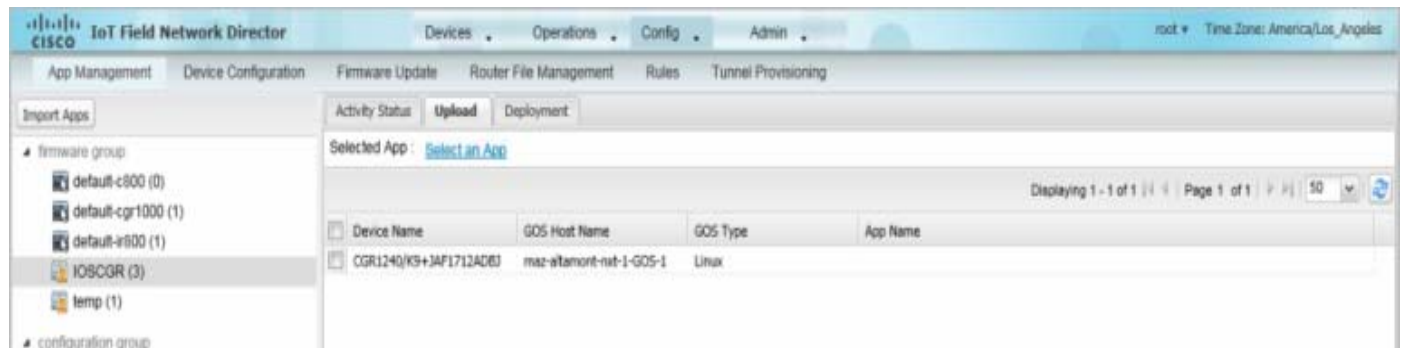
On the **Activity Status** tab, you can also:

- Click the **Cancel Current Activity** button to cancel any activity. Any activity in progress can be canceled.
- Click the **Refresh Status** button to update activity status.

Uploading GOS Apps

After GOS apps are imported to IoT FND, you can upload them for deployment on the GOS on Cisco IOS CGRs and IR800s, using the **Config > Apps Management** page **Upload** tab (Figure 8). Apps are OS specific. If the GOS is Linux, any apps you upload must run on Linux.

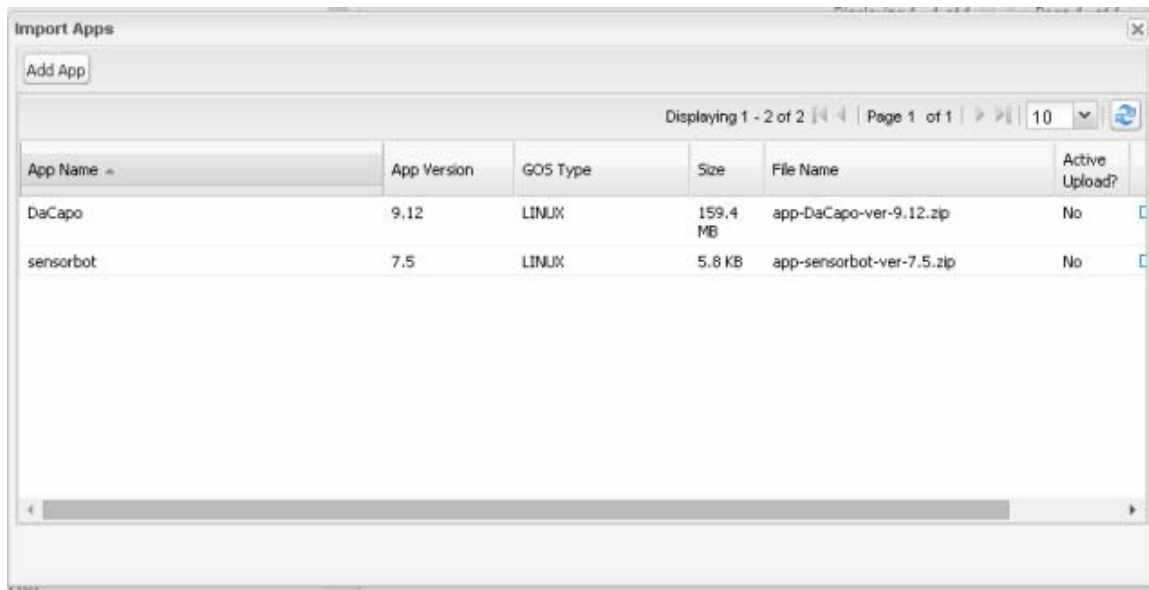
Figure 8 Upload Tab



To upload apps to IoT FND to deploy on Cisco IOS CGRs and IR800s, on the **Config > Apps Management** page:

1. Select a firmware or configuration group in the left pane.
2. Click the **Upload** tab.
3. Click **Select an App** or click the **Import Apps** button in the left pane.

The Import Apps dialog box displays apps already uploaded to the NMS server.



4. In the Import Apps dialog box, click **Add App**.

5. In the Add App dialog box, click **Browse** to navigate to the directory containing your app.

Note: Apps must be in the standard `<appname>-<version>.zip` file format.

6. In the Open dialog box, select the app file, and click **Open**.

7. Click **Add File**.

Note: Only one app may be uploaded at a time.

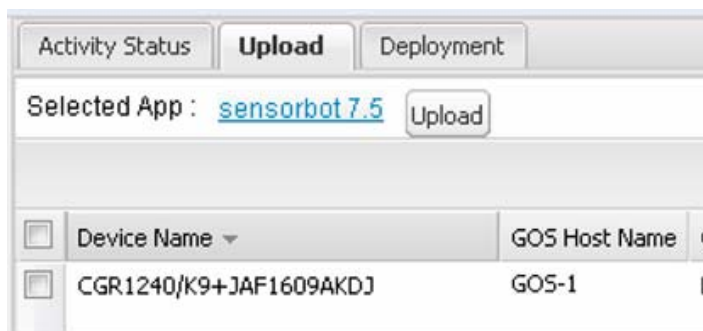
The app file uploads to the NMS server and displays in the App Name list.

8. In the Add App dialog box, click the desired app to upload to CGRs, click **Add to Upload**, and click **OK**.

The app filename displays in the App Name list.

9. In the App Name list, select the desired app to upload.

The app filename displays on the Upload tab as a link in the Selected App field, which is sensorbot 7.5 in the following example.



10. Click the **Upload** button to upload the file to IoT FND.

The activity status (UPLOAD_OP_COMPLETE or UPLOAD_OP_WAITING) displays on the Upload tab.

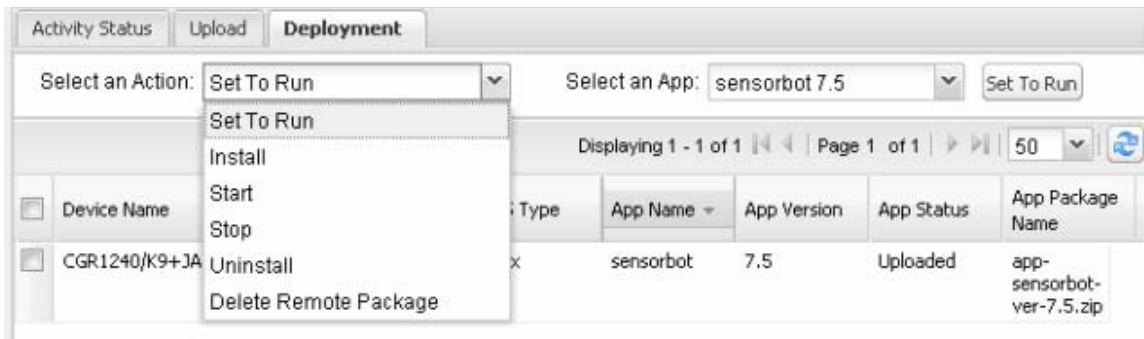
Deploying GOS Apps

The **Config > App Management Deployment** tab allows you to perform the following activities on selected CGRs and IR800s:

- Set to Run – A combination of install and start operations.
- Install – Installs the remote package and extracts the app.
- Start and Stop – Starts or stops the app.
- Uninstall – Uninstalls the app.
- Delete Remote Package – Deletes the previous upload package from the repository.

To deploy GOS apps on selected CGRs:

1. On the **Config > Apps Management** page, select a firmware or configuration group in the left pane.
2. Click the **Deployment** tab.
3. In the **Select an Action** drop-down menu, choose the desired action to perform on the selected group.



The action button at the right reflects your selected action (that is, if you select Install as the action, the action button label is “Install.”)

4. In the **Select an App** drop-down menu, choose an app or select all apps.
5. Click the action button.

The activity begins. You can monitor activity progress on the Activity Status tab.

Deleting GOS Apps

To delete an app from the NMS server, on the **Config > Apps Management** page:

1. Select a firmware or configuration group in the left pane.
2. Click the **Upload** tab.
3. Click **Select an App** or click the **Import Apps** button in the left pane.

The Import Apps dialog box displays apps already uploaded to the NMS server.

4. In the **App Name** list, scroll to the right and click the **Delete** link in the row with the app to delete from the NMS server.



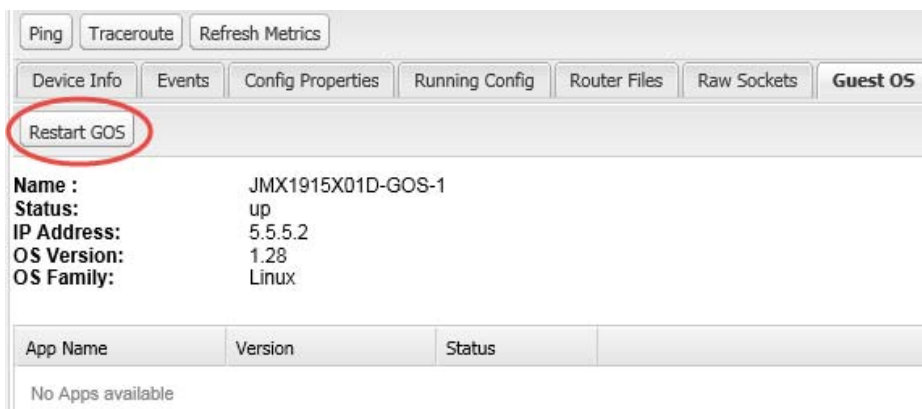
5. Click **OK** in the confirmation dialog box.

Restarting a Guest OS

To restart a GOS, on the **Config > Device Configuration** page:

1. In the **CONFIGURATION GROUPS** pane, select the device with the GOS to restart.
2. Click the **Guest OS** tab.
3. Click the Restart button (Figure 9).

Figure 9 Config > Device Configuration Page – Guest OS Tab Restart Button



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 > Router File Management** page to transfer and execute dual backhaul and Embedded Event Manager (EEM) scripts on the FAR. 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](#).

File Types and Attributes

Two types of EEM scripts are used on the FAR: an embedded applet, and Tool Command Language (TCL) scripts that execute on the FAR individually. You can upload and run new EEM TCL scripts on the FAR without doing a firmware upgrade. EEM files upload to the *eem* directory in FAR 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 FAR OS versions currently supported by IoT FND.

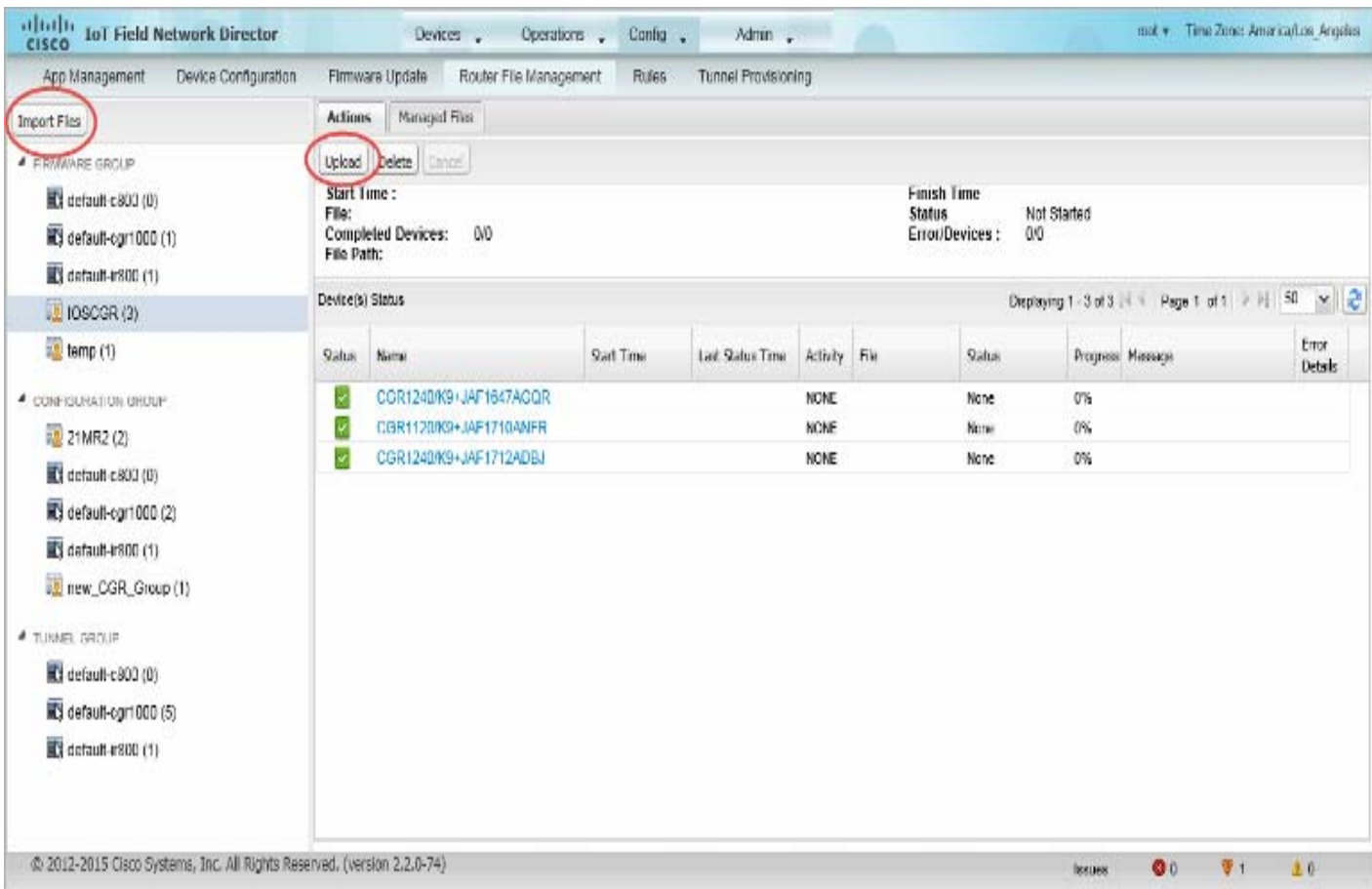
You can also transfer other file types to the FAR for better file management capability. You must first import the files to IoT FND to upload files to the FAR. IoT FND processes the file and stores it in the IoT FND database with the following attributes:

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

Adding a File to IoT FND

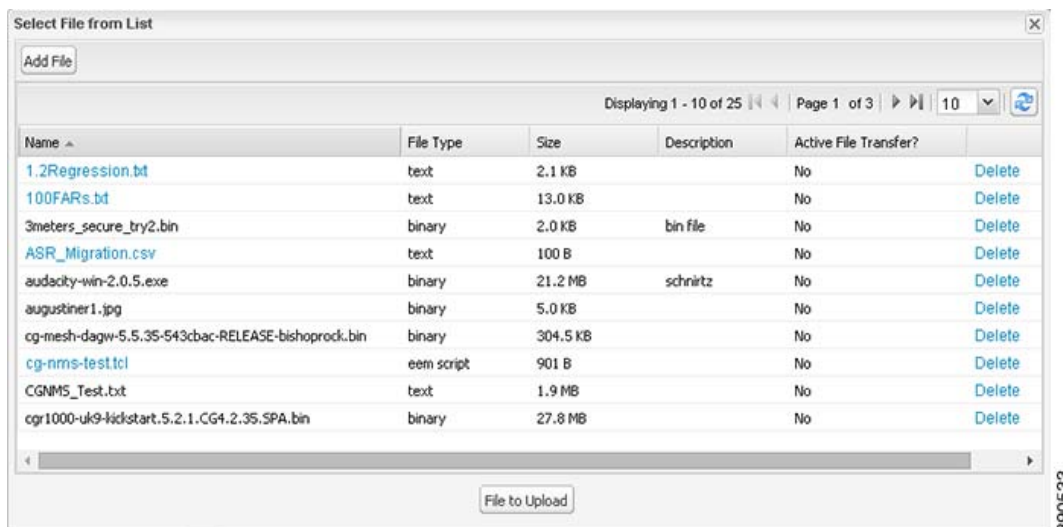
To add a file to IoT FND:

1. On the **Config > Router File Management** page, click **Import Files** or **Upload** to open the Select File from List dialog box.



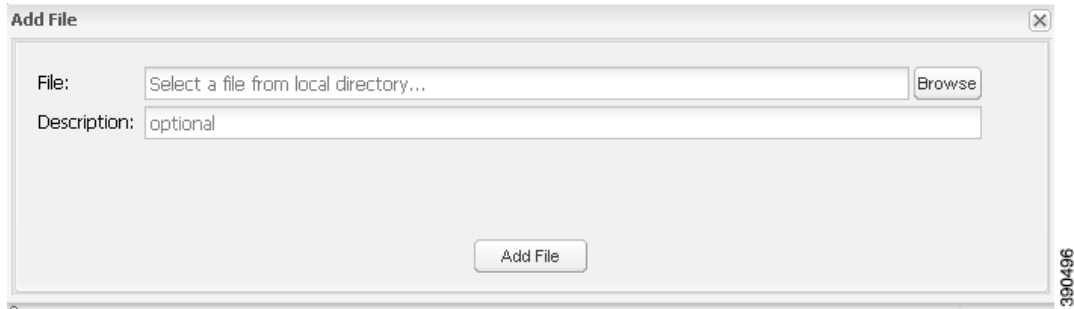
2. Click **Add File** and browse to the file location.

Note: The maximum import file size is 200 MB.



Note: In the **Select File from List** dialog box, you can also delete imported files from the IoT FND database if the file is not in an active file transfer. This only removes the file from the IoT FND database, not from any FARs that contain the file. Click the Name hyperlink to view uploaded text files (file size must be less than 100KB).

3. (Optional) Type a description for the file.



4. Click **Add File**.

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

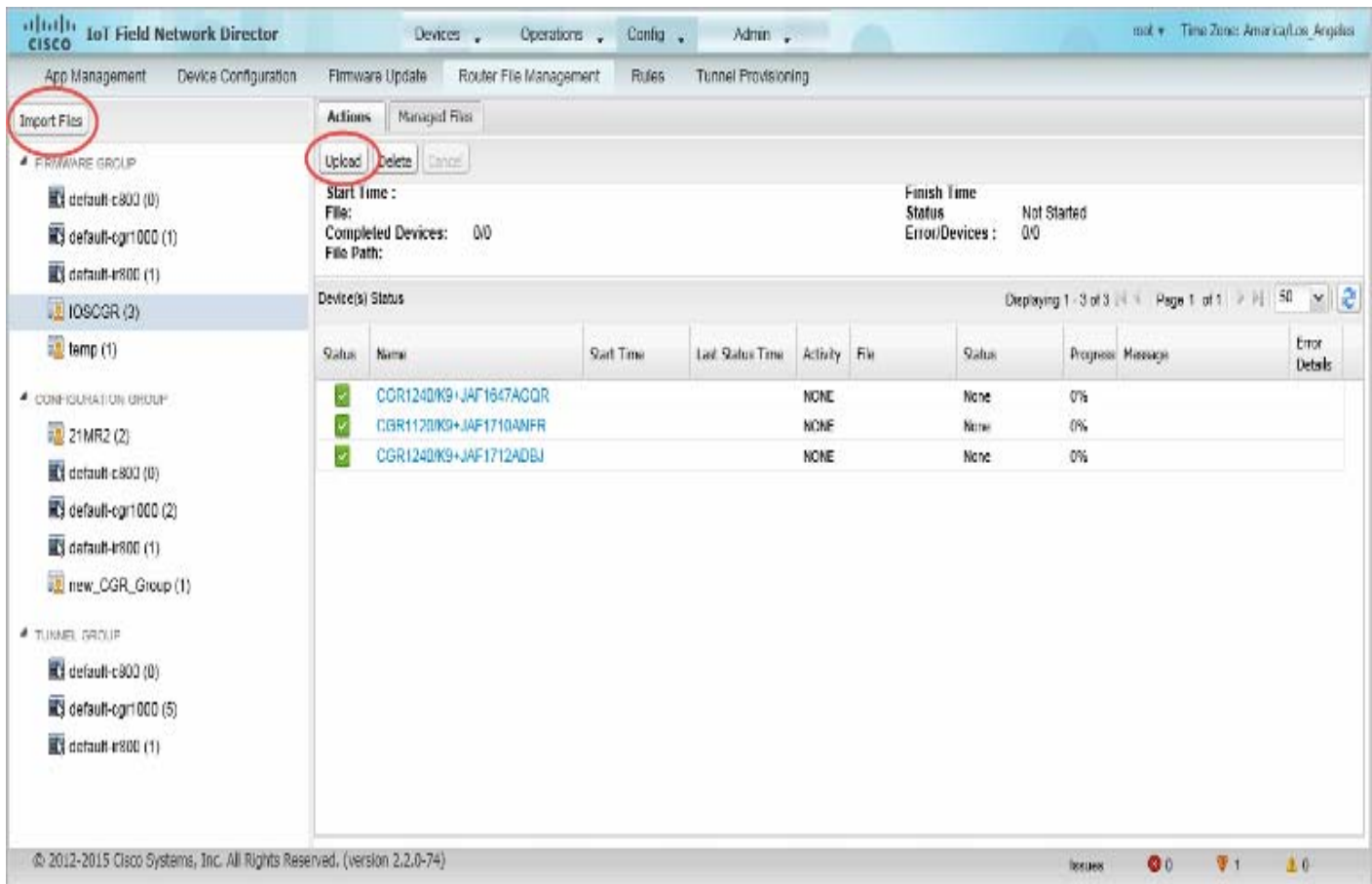
5. Repeat steps 2 through 4 to add another file, or see [Transferring Files](#) to upload the file to the selected device or group, or close the Select File From List dialog box.

Transferring Files

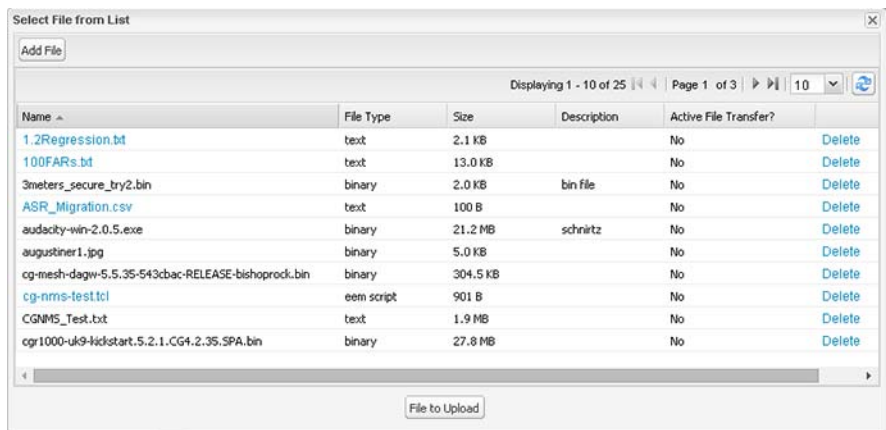
You can transfer files from the NMS database to any firmware, configuration or tunnel provisioning group, or to individual FARs. The maximum import file size is 200 MB.

To perform a file transfer:

1. On the **Config > Router File Management** page, select the group to transfer the file to in the **Browse Devices** 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 FARs in the selected group.

4. Click **File to Upload**.

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

Upload File to Routers

File to upload: 123 [Change File](#)

File Path: /managed/files

Override: ☐

Displaying 1 - 5 of 5 | Page 1 of 1 | 10

5 items selected (Max 1000) [Clear Selection](#)

<input checked="" type="checkbox"/>	Name	Start Time	Finish Time	Activity	File	Status	Progress
<input checked="" type="checkbox"/>	CGR1240/K9+J5J200204	2013-12-04 14:52	2013-12-04 14:53	UPLOAD	cgr1000-uk9-kickstart.5.2.1.CG4.2.27-5.2.1.CG3.3.SPA.bin	UPLOAD_COM...	100%
<input checked="" type="checkbox"/>	CGR1240/K9+J5J200203	2013-12-04 12:12	2013-12-04 12:12	UPLOAD	cgr1000-uk9-kickstart.5.2.1.CG4.2.27.5...	ERROR	100%
<input checked="" type="checkbox"/>	CGR1240/K9+JAF172SAKGF	2013-12-06 15:03	2013-12-06 15:03	UPLOAD	MANIFEST	UPLOAD_COM...	100%

[Upload](#)

390532

5. Check the check boxes of the FARs 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 FARs in the selected group or select only a subset of the FARs in the group. You can also select another group and file to perform a separate file transfer or deletion simultaneously.

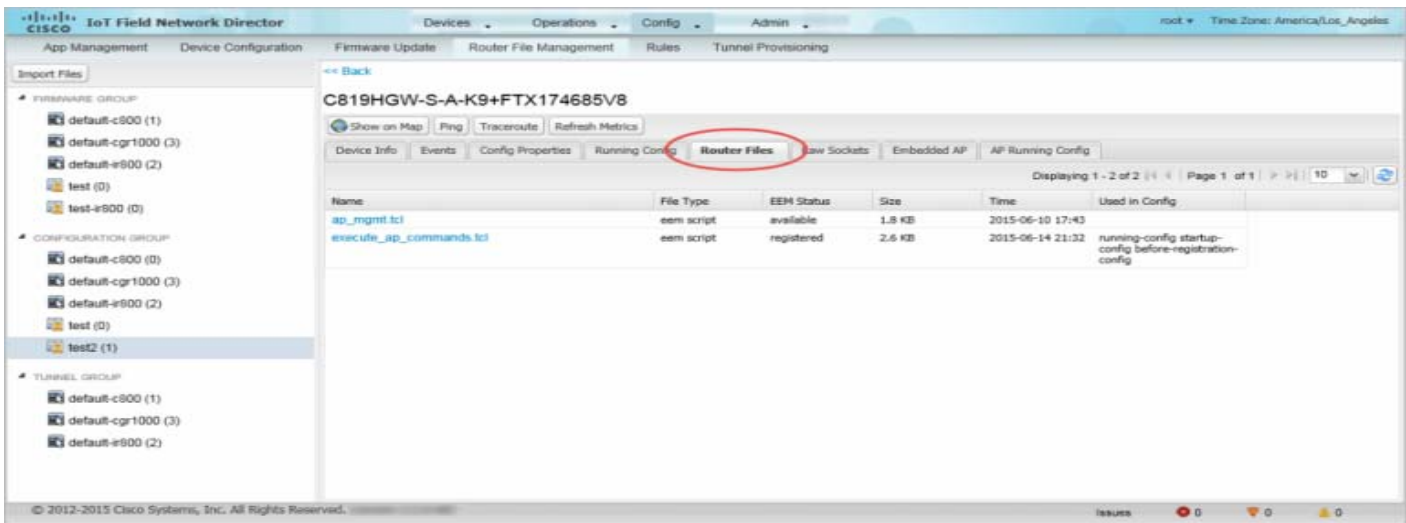
All files transferred from IoT FND reside on the FAR in flash:/managed/files/ for Cisco IOS CGRs, and bootflash:/managed/files/ for CG-OS CGRs.

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.

Viewing Files

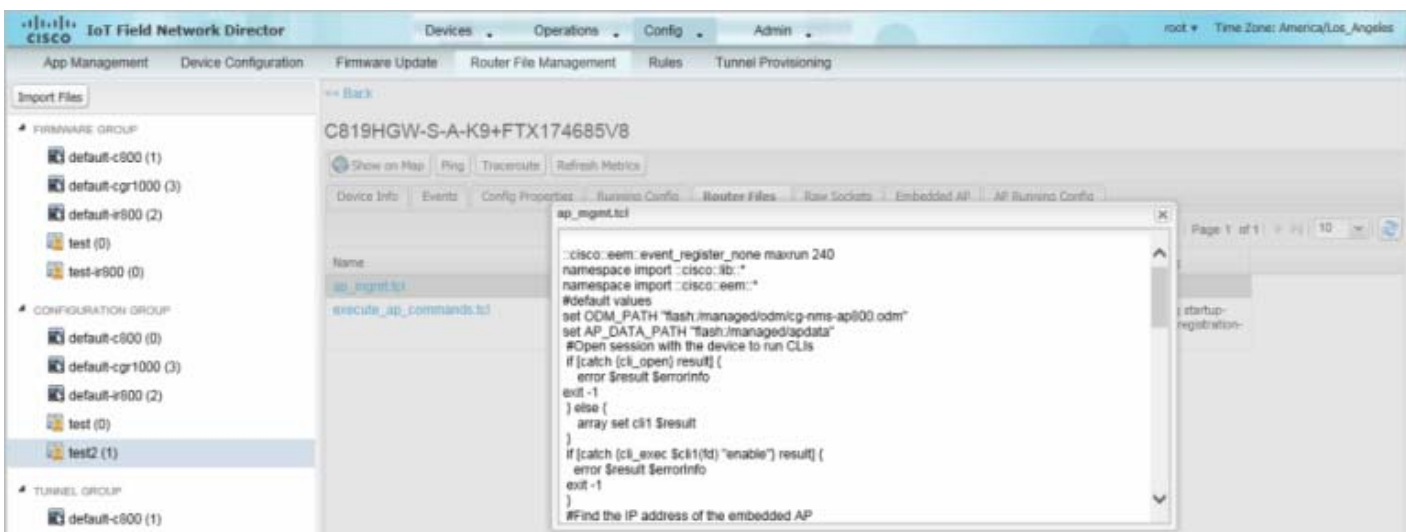
To view imported text file content:

1. Click the EID link to display the Device Info pane.
2. Click the **Router Files** tab.



3. Click the file name link to view the content in a new window.

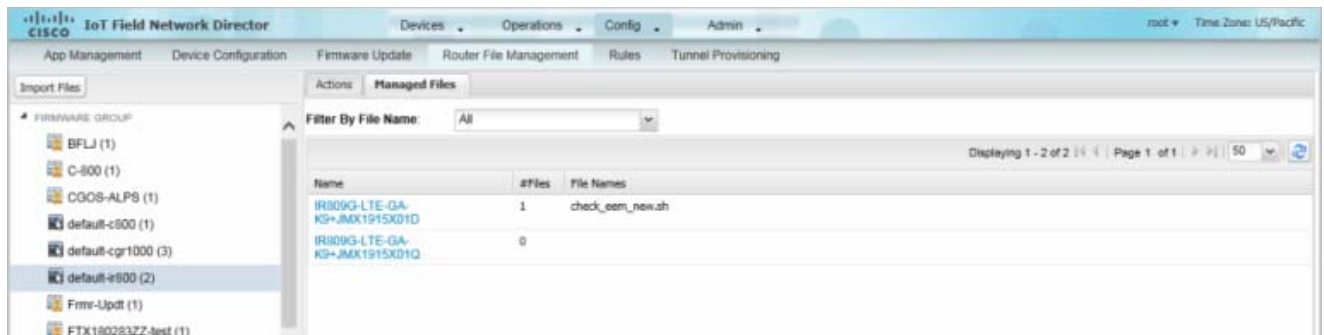
Note: IoT FND only displays files saved as plain text that are under 100 KB are viewable. You cannot view larger text files or binary files of any size. Those file types do not have a hyperlink.



Monitoring Files

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

Figure 10 Managed Files Tab



The following information is included in this list:

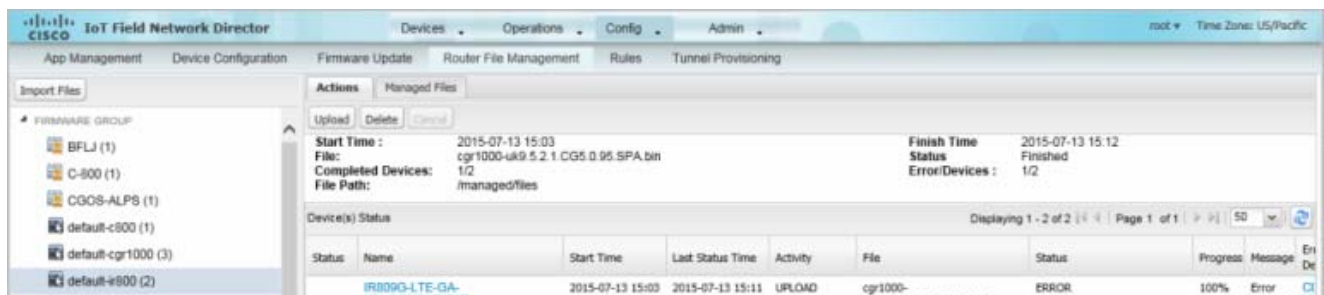
- EID link to the Device Info page
- Number of files stored on the device
- Uploaded file names

You can use the **Filter By File Name** drop-down menu to only view devices that contain a particular file. Select **All** 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 > Router File Management** page, click the **Actions** tab to view the status of the last file transfer or last file deleted for FARs in the selected group. You can click the Cancel button to terminate any active file operation.

Figure 11 Actions Tab



The Actions tab lists the following attributes:

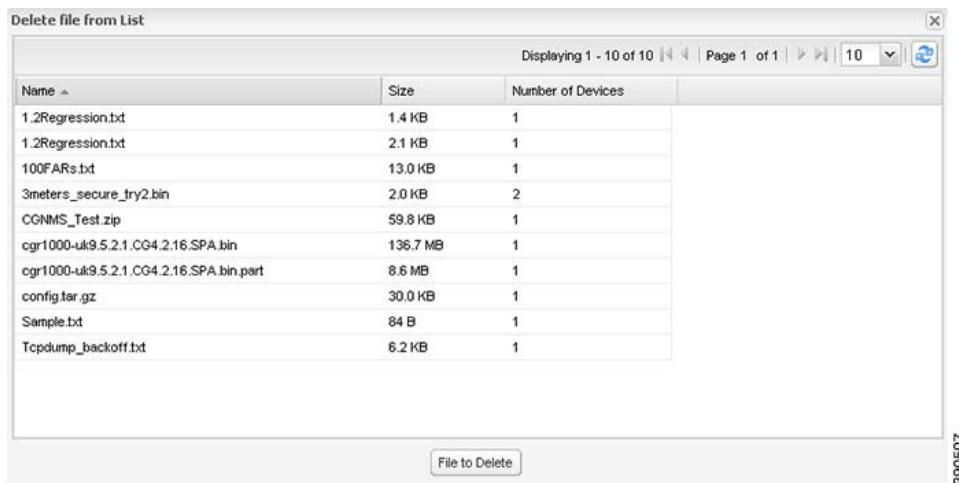
- Start date and time of the last transfer
- End date and time of the last transfer
- File name
- Status of the process: UNKNOWN, AWAITING_DELETE, DELETE_IN_PROGRESS, DELETE_COMPLETE, CANCELLED, NOTSTARTED, UPLOAD_IN_PROGRESS, UPLOAD_COMPLETE, STOPPING, STOPPED
- Number of devices with upload complete and total number of target devices
- Number of errors and errored device count
- File path

- EID link to Device Info page
- Activity performed: UPLOAD, DELETE, NONE
- Progress percentage
- Messages regarding any issues discovered during the process
- Error details

Deleting Files

To delete files from FARs:

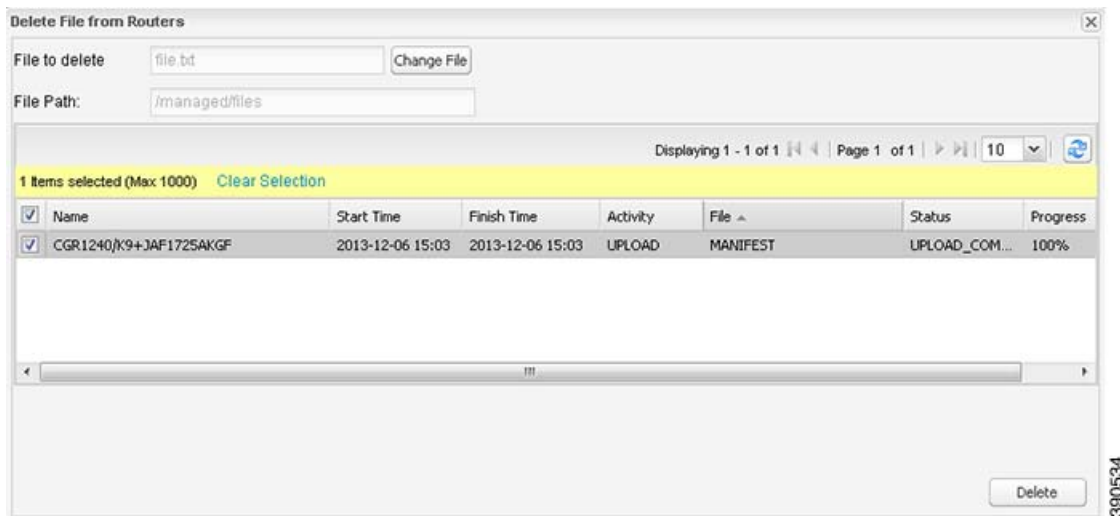
1. On the **Config > Router File Management** page, select the group to transfer the file to in the **Browse Devices** pane.
2. On the **Actions** tab, click **Delete**.
3. In the **Delete file from List** dialog, select a file to delete.



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

4. Click **File to Delete**.

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



5. Check the check boxes of the FARs from which you want to delete the file.

- You can click Change File to select a different file to delete from the selected FARs.
- You can select multiple FARs.
- Only one file can be deleted at a time.

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 processes before they complete, the currently running file deletion process completes and all waiting file deletion processes are canceled.

Managing Work Orders

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

Note: The Work Orders feature works with Release 3.0 or later of IoT-DM. 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: If you are using CGDM Release 3.1 and later, you must enable SSLv3 for IoT-DM–IoT FND connection authentication:

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
```

Viewing Work Orders

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

Work Order Number	Work Order Name	Role	Device Type	FAR Name/EID	Technician User Name	Time Zone	Start Date	End Date	Last Update	Status
WZTWIMNB	CGOS1	admin	CGR1000	CGR1120/K9+3AP1741BAFR	bahamas	Coordinated Universal Time	2015-05-22 00:00:00	2015-11-06 00:00:00	2015-05-23 01:13:58.0	Assigned
UGAVCWDZ	Workorder4	token	CGR1000	CGR1240/K9+3AP1712ADB3	bahamas	Coordinated Universal Time	2015-04-20 00:00:00	2015-02-06 00:00:00	2015-04-20 23:51:37.0	In Service
BKHAWSYG	Workorder 2	token	CGR1000	CGR1240/K9+3AP1712ADB3	bahamas	Coordinated Universal Time	2015-04-20 00:00:00	2015-06-08 00:00:00	2015-04-20 21:48:33.0	In Service

Table 9 lists fields that display on the Work Orders page.

Table 9 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.
FAR Name	EID of the FAR associated with the work order.
Technician User Name	User name of the assigned technician.
Time Zone	The time zone where the FAR is located—not the user's time zone. This value is deployment dependent, and can match the user's time zone.
Start Date	Project start and end date allotted to the field technician.
End Date	
Last Update	Time of last work order status update.
Status	Work order status. Valid status values are: New, Assigned, InService, Completed, Incomplete, or Expired.

Searching Work Orders

To refine your search, use the following syntax in the Search Work Order field (**Operations > Work Orders**):

Parameter	Description
workOrderNumber	Unique identifier of the work order.
role	(CG-OS only) Role of the user assigned to the work order. Valid roles are: tech, admin, or viewer.
technicianUserName	User name of the technician assigned to the work order.
workOrderStatus	Status of the work order. Valid status labels are: New, Assigned, InService, Completed, Incomplete, or Expired.
eid	EID of the FAR associated with the work order.

For example, to search for completed work orders that have a user with an admin role assigned to them, use this syntax:

role:admin workOrderStatus:Completed

To search work orders in IoT FND:

1. Choose **Operations > Work Orders**.
2. In the Search Work Order field, enter the search syntax and click **Search Work Orders**.

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

Before creating work orders, you must create user accounts 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 then click **Save**.
2. Create the user account:
 - a. Choose **Admin > Access Management > Users**, and then click **Add**.
 - b. Configure the user name, password, and time zone information.
 - c. Check the check boxes for **Monitor Only** and the Device Manager User role you created in Step 1.
 - d. Click **Save**.

Creating Work Orders

If you need a technician to inspect a deployed FAR (CGR 1120 or CGR 1240) or DA Gateway (IR509) in the field, create a work order. A work order includes the WiFi credentials required for the technician to connect to the router.

BEFORE YOU BEGIN

- Your user account must have the Work Order Management permissions enabled.

- 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. (See [Creating User Accounts for Device Manager \(IoT-DM\) Users](#))

Note: You can only create work orders for CGRs and IR509 devices.

DETAILED STEPS

To create a work order for Router (CGR1000) or Endpoint (IR509):

1. Choose **Operations > Work Orders**.

Work Order Number	Work Order Name	Rule	Device Type	FAR Name/EID	Technician User Name	Time Zone	Start Date	End Date	Last Update	Status
W2TWIMNB	CGOS1	admin	CGR1000	CGR1120/K9+JAF17H1BAFR	bahamas	Coordinated Universal Time	2015-05-22 00:00:00	2015-11-06 00:00:00	2015-05-23 01:13:58.0	Assigned
UQAVCWDZ	Workorder4	token	CGR1000	CGR1240/K9+JAF1712ADB3	bahamas	Coordinated Universal Time	2015-04-20 00:00:00	2016-02-06 00:00:00	2015-04-20 23:51:37.0	In Service
BKHAWSYG	Workorder 2	token	CGR1000	CGR1240/K9+JAF1712ADB3	bahamas	Coordinated Universal Time	2015-04-20 00:00:00	2015-08-08 00:00:00	2015-04-20 21:46:22.0	In Service

2. Click **Add Work Order**.

Work Order:

Work Order Name:

Field Device Names/EIDs:

Enter comma-separated values

Device Type: ☒ Router ☐ End Point

CGR OS Version: ☐ CG-OS ☒ IOS

Device Username:

Technician User Name:

Status:

Start Date:

End Date:

Device Time Zone:

3. In the **Work Order Name** field, enter the name of the work order.
4. In the **Field Device Names/EIDs** field, enter a comma-separated list of FAR names or EIDs.
For every FAR in the list, IoT FND creates a separate work order.
5. **Device Type** (Router or Endpoint) and **CGR OS** version (CG-OS or IOS) auto-populate.
6. 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.
7. 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**.

8. 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.

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

10. Click **Save**.

11. Click **OK**.

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

Downloading Work Orders

To download the work orders created by IoT FND, field technicians use Cisco IoT-DM, a Windows-based application that field technicians use 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](#).

Editing Work Orders

To edit work order details:

1. Choose **Operations > Work Orders**.
2. Select the work order to edit, and then click **Edit Work Order**.

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

3. Click **Save**.

Deleting Work Orders

To delete work orders:

1. Choose **Operations > Work Orders**.
2. Check the check box of the work orders to delete.
3. Click **Delete Work Order**.
4. Click **Yes**.

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 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 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](#)
- [Mesh Device Health](#)
- [Mesh Link Keys](#)
- [Mesh Link Settings](#)
- [Mesh Link Metrics](#)
- [NAT44 Metrics](#)
- [PLC Mesh Info](#)
- [Raw Sockets Metrics and Sessions](#)
- [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 FARs.

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 support 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 Metrics

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.
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.
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. Possible values are: <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. The LED states on the cellular interface and corresponding RSSI values are: <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.
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.
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.
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 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, 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).
BVI1	–	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.
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

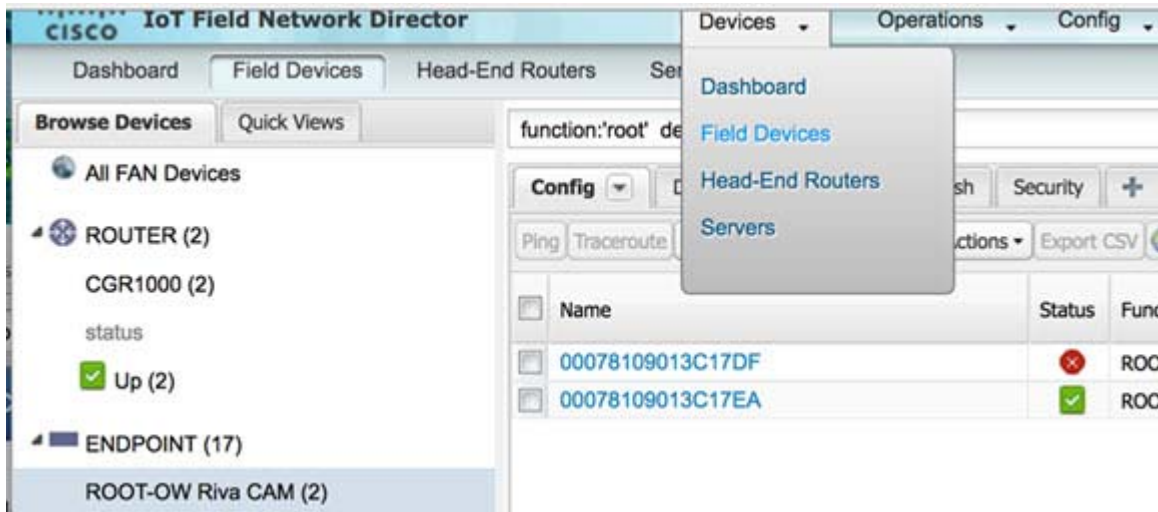
Table 20 describes the fields in the Tunnel 2 Config area of the **Head-End Routers > Config Properties** page.

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: Devices > Field Devices > ENDPOINT > ROOT-OW Riva CAM > Name (Select product link in Config Panel).

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 is communicated with 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.
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 FAR.
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.
Mesh 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.

Mesh Device Health

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

Table 23 Mesh Device Health Fields

Field	Key	Description
Uptime	uptime	The amount of time, in seconds, that the element has been running since last boot.

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.

Mesh Link Settings

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

Table 25 Mesh Link Settings Fields

Field	Key	Description
Firmware Version	meshFirmwareVersion	The ME firmware version.
Mesh Interface Active	meshActive	The status of the ME.
Mesh SSID	meshSsid	The ME network ID.
PANID	meshPanid	The subnet PAN ID.
Transmit RF Power	meshTxPower	The ME transmission power (dBm).
Security Mode	meshSecMode	The ME 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>
RPL DIO Min	meshRplDioMin	An unsigned integer used to configure the Imin of the DODAG Information Object (DIO) Trickle timer.

Table 25 Mesh Link Settings Fields (continued)

Field	Key	Description
RPL DIO Double	meshRplDioDbl	An unsigned integer used to configure the I _{max} of the DIO Trickle timer.
RPL DODAG Lifetime	meshRplDodagLifetime	An unsigned integer used to configure the default lifetime (in minutes) for all downward routes 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.

Mesh Link Metrics

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

Table 26 Mesh Link Metrics Fields

Field	Key	Description
Meter ID	meterId	The ME meter ID.
PANID	meshPanid	The ME PANID.
Mesh Endpoints	meshEndpointCount	Number of MEs.
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.
Mesh Route RPL Hops	meshHops	The number of hops that the element is from the root of its RPL routing tree.
Mesh Route RPL Link Cost	linkCost	The RPL cost value for the link between the element and its uplink neighbor.
Mesh 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 in 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, used in conjunction with RSSI, combine to determine viable channels.
Mesh Absolute Phase of Power	—	Mesh absolute phase of power is basically 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.

Table 29 Raw Sockets Metrics and Sessions View (continued)

Field	Key	Description
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 area of the Device Info page.

Table 30 Router Battery Device View

Field	Key	Configurable?	Description
Battery 0 Charge	battery0Charge	No	The percentage of charge remaining in battery 0.
Battery 0 Level (%)	battery0Level	No	The percentage of charge remaining in battery 0.
Battery 0 Remaining Time	battery0Runtime	No	How long battery 0 has been up and running since its installation or its last reset.
Battery 0 State	battery0State	No	The current battery 0 state of the device.
Battery 1 Level (%)	battery1Level	No	The percentage of charge remaining in battery 1.
Battery 1 Remaining Time	battery1Runtime	No	How long battery 1 has been up and running since its installation or its last reset.
Battery 1 State	battery1State	No	The current battery 0 state of the device.
Battery 2 Level (%)	battery2Level	No	The percentage of charge remaining in battery 2.
Battery 2 Remaining Time	battery2Runtime	No	How long battery 2 has been up and running since its installation or its last reset.
Battery 2 State	battery2State	No	The current battery 0 state of the device.
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 FAR connects with through secure tunnels.
Common Name of Certificate Issuer		No	Displays the name of the certificate issuer.
NBMA NHS IPv4 Address		Yes	Displays the Non-Broadcast Multiple Access (NBMA) IPv4 address.
NBMA 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 FAR communicates to the RTU.
Protocol Type	protocol	No	Identifies the Protocol Translation type.
Messages Sent	—	No	The number of messages sent by the FAR.
Messages Received	—	No	The number of messages received by the FAR.
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 FAR.
Link Errors	—	No	Displays the number of link errors generated by the FAR.
Address Errors	—	No	Displays the number of address errors generated by the FAR.
Local IP	—	No	Displays the local IP address of the FAR.
Local Port	—	No	Displays the local port of the FAR.
Remote IP	—	No	Displays the remote IP address of the FAR.
Data Socket	—	No	Displays the Raw Socket server configured for the FAR.

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 FAR.
Pre-Shared Key	type6PasswordMasterKey	No	The key used to encrypt other pre-shared keys stored on the FAR.

WiMAX Config

Table 41 describes the fields in the WiMAX Config area of the Device Info page.

Table 41 WiMAX Config Fields

Field	Key	Description
PkmUsername	PkmUsername	
PkmPassword	PkmPassword	

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.

