

Manage Devices

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

- Overview, on page 2
- Guided Tours, on page 5
- Enabling Google Snap to Roads, on page 6
- Managing Routers, on page 6
- Managing Endpoints, on page 13
- Managing Itron Bridge Meters, on page 17
- LDevID: Auto-Renewal of Certs and Saving Configuration, on page 20
- Support Expired SUDI Certificate, on page 21
- Configuring Enrollment over Secure Transport, on page 23
- Configuring FND Registration Authority (RA), on page 24
- Managing the Cisco Industrial Compute IC3000 Gateway, on page 29
- Managing the Cisco Wireless Gateway for LoRaWAN, on page 32
- Managing Cisco IR510 WPAN gateways, on page 35
- Wi-SUN 1.0 Support, on page 42
- Managing Head-End Routers, on page 44
- Cisco Catalyst IR1100 Expansion Modules in Cisco IoT FND, on page 44
- Itron CAM Module, on page 45
- Lorawan Gateway Module, on page 46
- Managing Servers, on page 48
- Common Device Operations, on page 48
- Configuring Rules, on page 72
- Configuring Devices, on page 76
- Synchronizing Endpoint Membership, on page 87
- Editing the ROUTER Configuration Template, on page 88
- Editing the ENDPOINT Configuration Template, on page 91
- Pushing Configurations to Routers, on page 93
- Pushing Configurations to Endpoints, on page 95
- Certificate Re-Enrollment for ITRON30 and IR500, on page 97
- New Events for IR500, on page 99
- Audit Trail for Re-enrollment for Gateway-IR500 Endpoints, on page 100
- Monitoring a Guest OS, on page 100
- Application Management Support in IoT FND, on page 102

• PIMs in Cisco IoT FND, on page 109
• Managing Files, on page 113
• Hardware Security Module, on page 120
• Demo and Bandwidth Operation Modes, on page 123
• Bandwidth Optimization Mode Configuration, on page 125
• Device Properties, on page 127

Overview

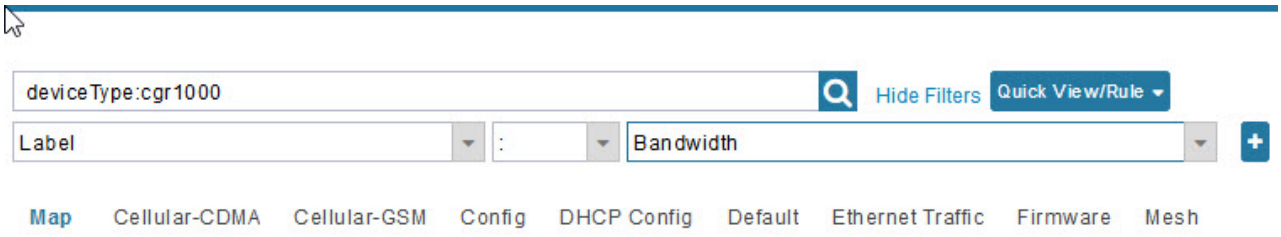
Use the following IoT FND pages to monitor, add and remove devices, and perform other device management tasks that do not include device configuration.

Procedure

Select **DEVICES** > **FIELD DEVICES**.

In the Browse Devices panel of the Devices menu options as shown below, search for Field Devices such as Routers (CGR1000, C800, IR800, SBR (C5921), IR1100 Pluggable and Expansion Modules (IR-1100-SP), Endpoints (meters and IR500 gateways), and IoT Gateways (such as the LoRaWAN gateway and IC3000).

Note
In some textual displays of the IoT FND, routers may display as “FAR” rather than the router model (cgr1000, etc).



Note
You can view PID and descriptive properties for the IR1100 pluggable and expansion modules in the IoT FND UI at the Cellular Link Settings page; however, you must refer to the NB API for properties and metrics for the pluggable and expansion interfaces, specifically the getMetricHistory () and getDeviceDetails ().

Pluggable Module Info

PID P-LTEA-LA

Details :

Name	Description	PID	SN
Modem on Cellular0/1/0	Sierra Wireless EM7430	EM7430	355813070197162

Expansion Module Info

PID IRM-1100-SPMI

Details :

Name	Description	PID	SN
Expansion module 2 - mSATA Module	Snowfinch mSATA Module	IR1100-SSD-100G	FOC2330032N
subslot 0/0 transceiver 5	100BASE FX-GE	GLC-FE-100FX-RGD	FNS232904HG
module subslot 0/3	P-LTE-GB Module	P-LTE-GB	FOC23100UG2
Modem on Cellular0/3/0	Sierra Wireless WP7607	WP7607	351732090142640

Cellular Link Settings

	Modem1	Modem2
Network Type	LTE	LTE
Network Name	IND airtel	IND airtel
IMSI	404450985151422	404450985143858
Roaming Status	Home	Home
Serial Number	LR827779180210	VN834472230810
Firmware Version	SWI9X30C_02.24.05.06	SWI9X07Y_02.13.02.00
Connection Type	LTE	LTE
Cellular Modem Active	true	true
Cellular Module Temperature	43.0 Celsius	39.0 Celsius
System Identification Number	unknown	unknown
Network Identification Number	unknown	unknown
Mobile Directory Number	unknown	unknown
Serving Cell Tower Longitude	unknown	unknown
Serving Cell Tower Latitude	unknown	unknown
Preferred Roaming List Version	unknown	unknown

- To work with Head-End Routers (ASR1000, ISR3900, ISR4000) use the **DEVICES** > **Head-End Routers** page.
- To work with IoT FND NMS and database servers, use the **DEVICES** > **Servers** page.

- To view assets associated with the Cisco Wireless Gateway for LoRaWAN (IXM-LPWA-900), use the **DEVICES** > **Assets** page.

Note
Refer to the Managing Firmware Upgrades chapter for more information on firmware updates for Routers and Gateways.

Guided Tours



Note The Guided Tour feature must be enabled by the first-time FND root user that logs into the FND system before you can use the feature.

Procedure

Step 1 At first login, as a root user, click Dashboard. A No Devices or Dashlets panel appears, which displays the following options: ADD LICENSE, ADD DEVICES, ADD DASHLET and GUIDED TOUR.

Step 2 Click GUIDED TOUR.

Note
You may need to add a license or create a dummy device to enable the Guided Tour.

Step 3 At the root user menu (upper-right corner) that appears, select Guided Tour. This opens a Guided Tour Settings window that lists all available Guided Tours:

- Add Devices
- Device Configuration
- Device Configuration Group Management
- Tunnel Group Management
- Tunnel Provisioning
- Provisioning Settings
- Firmware Update
- Zero Touch Provisioning Setup Guided Tour

Step 4 After you select one of the Guided Tours, you will be redirected to the Sign In pane. That configuration page and windows appear to step you through the configuration steps and let you Add or Update Values as necessary.

Note

When you select the Zero Touch Provisioning option list in step 3 above, a Zero Touch Provisioning setup guided tour window appears that lists all the prerequisites for the device on-boarding: (Provisioning Settings, Group Management, Manage Configuration: Bootstrap Template, Tunnel Provisioning, Device Configuration, Add Devices).

Enabling Google Snap to Roads

When navigating with GPS, sometimes the trace or coordinates do not always match up to the road or path traveled by a vehicle.

When you enable the Snap to Roads feature in IoT FND, it eliminates the wrong latitude and longitude coordinates collected along a route and replaces it with a set of corresponding data with points that snap to the most likely roads and similar road names that the vehicle has traveled along.

The Google Snap to Roads feature is a premium service, and to work with the feature you must enable the Google Map API Key within IoT FND user interface.

Managing Routers

You manage routers on the Field Devices page (**DEVICES** > **Field Devices**). Initially, the page displays devices in the Default view.

Working with Router Views

The router or routers you select determine which tabs display.

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

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, on page 49 .

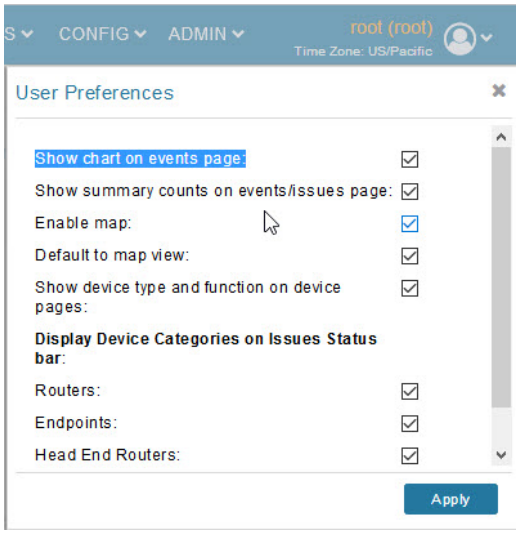
For information about the device properties that display in each view, see Device Properties, on page 127 .

For information about common actions performed in these views (for example, adding labels and changing device properties), see Common Device Operations, on page 48 .

Viewing Routers in Map View

At the top, upper-right-hand corner of the screen, select root or user name, and click Preferences option. To view the routers in Map view, select the **Enable map** checkbox.

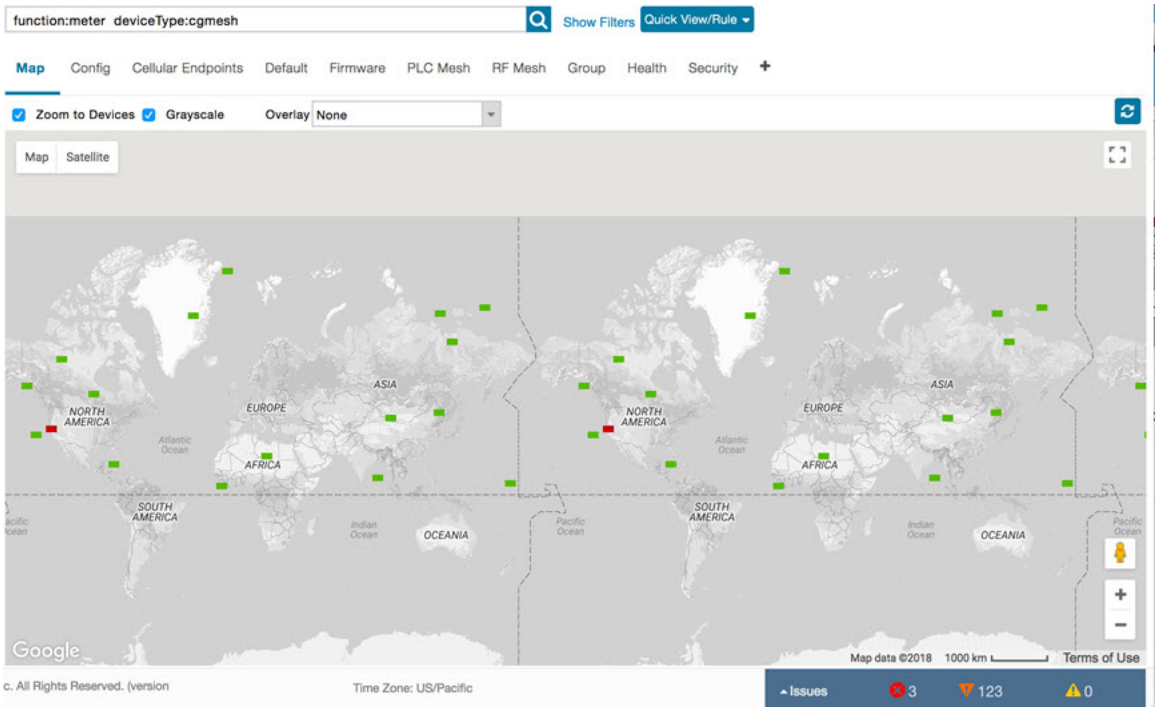
Figure 1: Setting User Preferences for User Interface Display



Note The additional options (not seen in the Figure 1: Setting User Preferences for User Interface Display, on page 7) are found as selectable options on the User Preferences page (Servers, Show PAN ID in Hexadecimal).

To view the routers in the Map view, navigate to DEVICES > FIELD DEVICES, choose the router and click Map.

Figure 2: Map View



Note You can view any RPL tree by clicking the device in Map view, and closing the information pop-up window.

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

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

Migrating Router Operating Systems

You can migrate CGR operating systems from CG-OS to Cisco IOS on the **CONFIG** > **Firmware Update** page, using the procedure in the section, "Performing CG-OS to Cisco IOS Migration" section in the Firmware Management chapter of this book.

Refreshing the Router Mesh Key

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

Note Refreshing the router mesh key can result in mesh endpoints being unable to communicate with the router for a period of time until the mesh endpoints reregister with the router, which happens automatically.

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

Procedure

Step 1 Check the check boxes of the routers to refresh.

Step 2 Choose **More** > **Actions** > **Refresh Router Mesh Key** from the drop-down menu.

Step 3 Click **Yes** to continue.

Device File Management for Routers

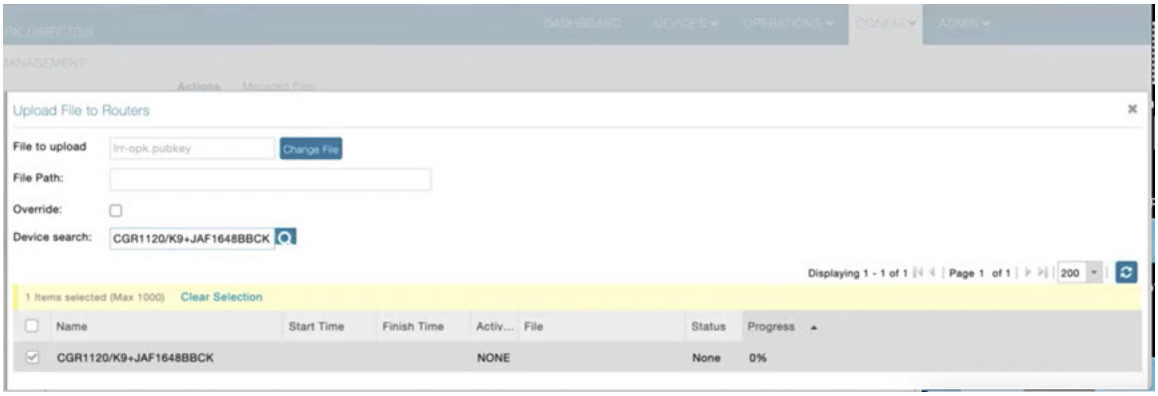
When you want to upload router device files to be managed by IoT FND, go to **CONFIG** > **DEVICE FILE MANAGEMENT** within the application. At that page, select **Actions** > **Upload** to get to the Upload File to Routers page. This page provides you the ability to:

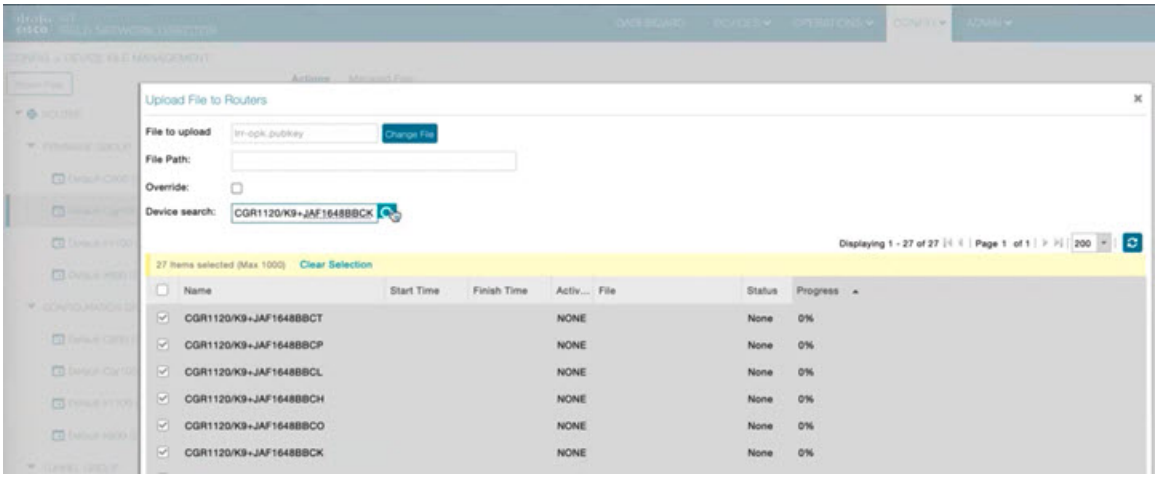
- Search for a router device file by its name such as CGR1120/K9+JAF1648BBCK to upload.
- Search by an abbreviated Device file string such as CGR120/K9+JAF or BBCK to display a range of routers available to upload.

The number of router files available to upload (based on your search criteria) displays and all listed routers are selected (checked boxes) by default. You can define the number of routers that display, by using the

drop-down menu on that page. Options are 10 (default), 50, 100 and 200. You can remove the check mark next to any router, that you do not want to upload.

After you have finalized the list to upload, click **Upload**.





Managing Embedded Access Points on Cisco C800 and Cisco IR829 ISRs

IoT Field Network Director allows you to manage the following embedded access point (AP) attributes on C800 (IR819) and IR829 ISRs. The embedded Access Points on the C800 and IR829 routers are identified as AP800 in the FND user interface.

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

You can perform and manage the following aspects for AP800s in FND:

- 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 IR829 ISR features matrix is here.

Setting AP800 Firmware Upgrade Support During Zero Touch Deployment (ZTD)

You must define a specific firmware image to use during ZTD.

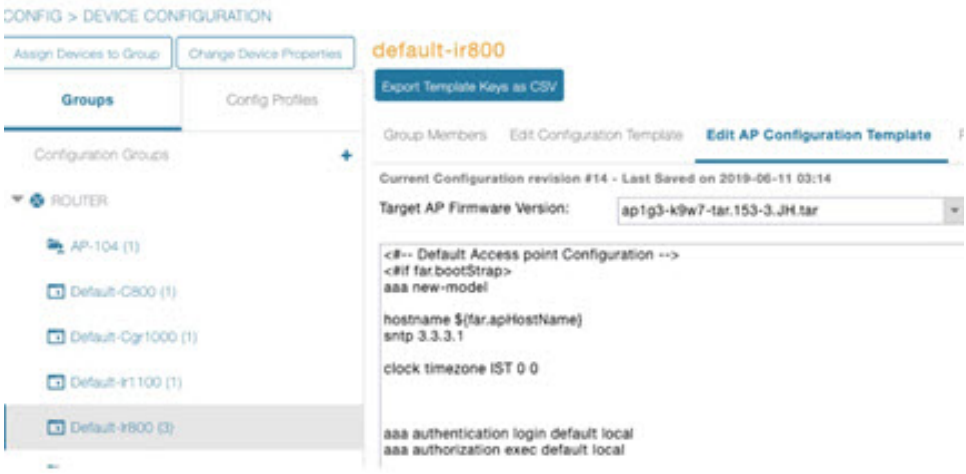
You can only define a unified image (k9w8 - factory shipped) for update via ZTD

Defining the Unified Mode Option

Note Setting the AP to the unified mode, requires that the following configuration be pushed by IoT FND to the router (IR800), from the router config template, after that management of the AP is done from the Cisco Wireless LAN Controller (WLC) and not from IoT FND:

Procedure

Step 1 At the **CONFIG** > **DEVICE CONFIGURATION** page, select Default-ir800 from the Groups panel and select the Edit AP Configuration Template tab.



Step 2 To perform an Unified Upgrade, enter the following configuration in the Edit AP Configuration Template window (right-pane):

```
ip dhcp pool embedded-ap-pool
network <router_ip> 255.255.255.0
dns-server <dns_ip>
default-router <router_ip>
```

```
option 43 hex f104.0a0a.0a0f (single WLC IP address(10.10.10.15)
in hex
format)
ip address <router_ip> 255.255.255.0
!
service-module wlan-ap 0 bootimage unified
```

Step 3 Click the Disk icon at the bottom of the panel to save the configuration.

Step 4 At the Router Device Details page, when you select the Embedded AP tab, the pane displays “Unified access points are not managed.” because they are being managed by the Cisco Wireless LAN Controller and not IoT FND.

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 (right pane). For example, to display all operational routers, click the **Up** group under ROUTERS in the Browse Devices pane. Click a filter to insert the corresponding search string in the Search Devices field. For example, clicking the **Up** group under ROUTERS inserts the search string **status:up** in the Search Devices field.

Displaying Router Configuration Groups

Use the Browse Devices pane to display routers that belong to one of the groups (such as CGR1000) listed under ROUTER.

Procedure

Step 1 Navigate to the **DEVICES** > **Field Devices** page.

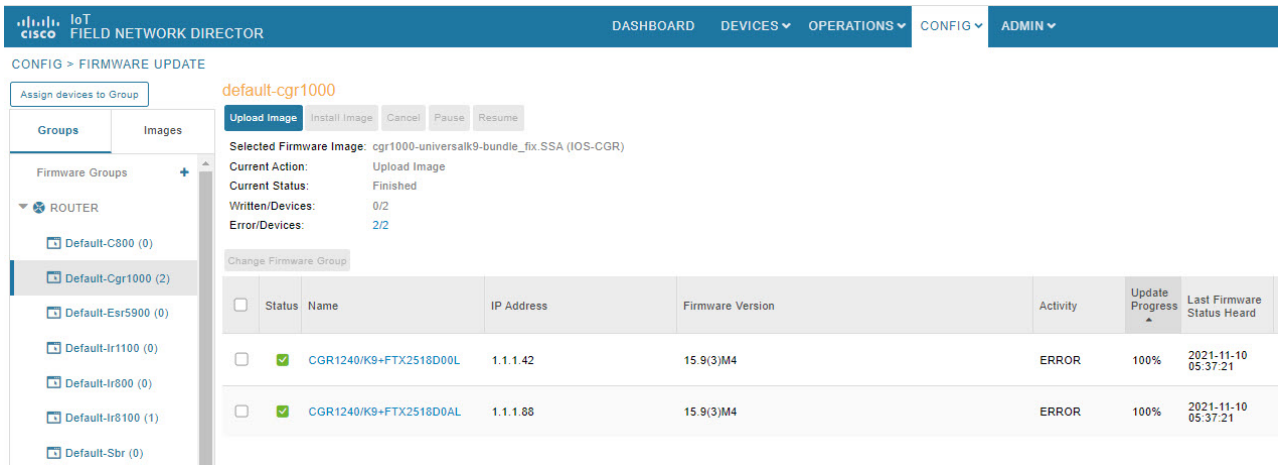
Step 2 From the **Browse Devices** pane, select the desired group listed under ROUTER to display the associated routers.

Displaying Router Firmware Groups

Procedure

Step 1 Navigate to **CONFIG** > **Firmware Update**.

Step 2 From the left pane, select the **Groups** tab and choose one of the ROUTER Groups (such as Default-c800, Default-cgr1000, Default-esr5900, Default-ir1100, Default-ir800 or Default-sbr).



The firmware image available for the router displays under the **Name** field in the right-pane. In the case of the Default-ir800, it includes both the IR809 and IR829, so there are two different firmware images listed.

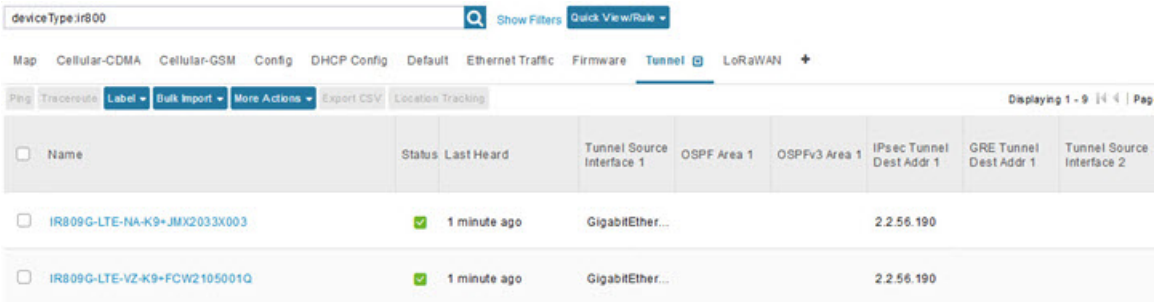
Displaying Router Tunnel Groups

A router tunnel group is used to organize and manage router devices within the network infrastructure.

Router Tunnel Group Display Methods

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

Figure 3: Browse Devices Pane



Replace Routers In Cisco IoT FND

Before proceeding with a Return Material Authorization (RMA) for any device integrated with Cisco IoT FND that you want to replace, use the following steps:

1. Perform a backup of the configuration from the router that you want to replace.
2. Install the new router in the same location as the router that you want to replace.
3. Before connecting the new device to the network, restore the configuration from the backup device.

4. Verify if the new router that you are adding as a replacement is functioning as expected while it is connected to the network.



Note For more details on how to add new FAR devices and routers, see Managing Devices.

Managing Endpoints

To manage endpoints, view the **DEVICES** > **Field Devices** page. By default, the page displays the endpoints in List view.

Viewing Endpoints in Default View

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

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



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

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

For information on how to customize endpoint views, see Customizing Device Views, on page 49.

For information about the device properties displayed in each view, see Device Properties, on page 127.

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, on page 48.

Viewing Mesh Endpoints in Map View

To view mesh endpoints in Map view:

Procedure

Step 1 Select Enable map in <*user*>> **Preferences**.

Step 2 Click the **Map** tab.

Blocking Mesh Devices to Prevent Unauthorized Access

If you suspect unauthorized access attempts to a mesh device (mesh endpoint, IR500), you can block it from accessing IoT FND.



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

To block a mesh endpoint device, in Default view (**DEVICES** > **Field Devices** > **ENDPOINTS**).

Procedure

Step 1 Check the check boxes of the mesh devices to refresh.

Step 2 Choose **More Actions** > **Block Mesh Device** from the drop-down menu.

Note
If your mesh endpoints are running Cisco Resilient Mesh Release 6.1 software or greater, FND will automatically invoke the Blacklist for endpoints (cg-mesh, IR509, IR510, IR529, IR530) that you suspect are not valid endpoints with the WPAN. You do not need to select **More Actions** > **Block Mesh Device**. Additionally, the mesh endpoint will show a 'blocked' status.

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

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

Displaying Mesh Endpoint Configuration Groups

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

Displaying Mesh Endpoint Firmware Groups

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

Troubleshooting On-Demand Statistics for Endpoints

You can generate any of the following predefined system reports within IoT FND to help troubleshoot issues with an endpoint such as GATEWAY-IR500, EXTENDER-IR500, METER-CGMESH, or any third-party METERS. A **Troubleshoot** page is displayed for each supported endpoint.

Report	Description
All TLVs	Generates a report from the list of available TLV identifiers in the device.

Report	Description
Connectivity	Generates a device connectivity report with the following parameters: • WPAN Status • PPP Link Stats • Neighbor 802.15.4g
General	Generates a report with the following general parameters associated to the device: • Device ID • Current Time • Uptime • IEEE 802.1x Status • IEEE 802.1x Settings • Firmware Image Information
Registration	Generates a report with the following registration parameters: • Network Management System Redirect Request • Report Subscribe • Connected Grid Management System Settings • Connected Grid Management System Status • Connected Grid Management System Notification • Connected Grid Management System Stats • Signature Certificate • Signature Settings

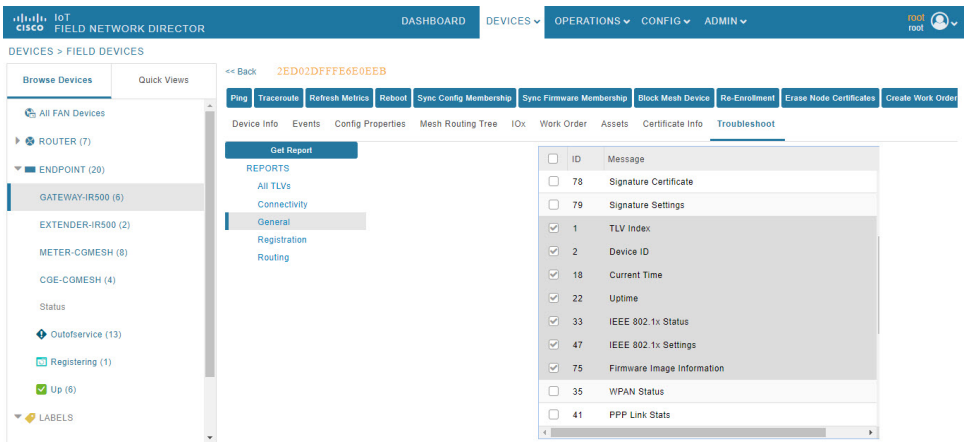
Report	Description
Routing	Generates a report with the following routing parameters: • IP Address • RPL Settings • IEEE 802.11i Status • DHCPv6 Client Status • IEEE 802.15.4 Beacon Stats • Stored Information • Fast Synchronization Status • RPL Stats

To generate a troubleshooting report for endpoints:

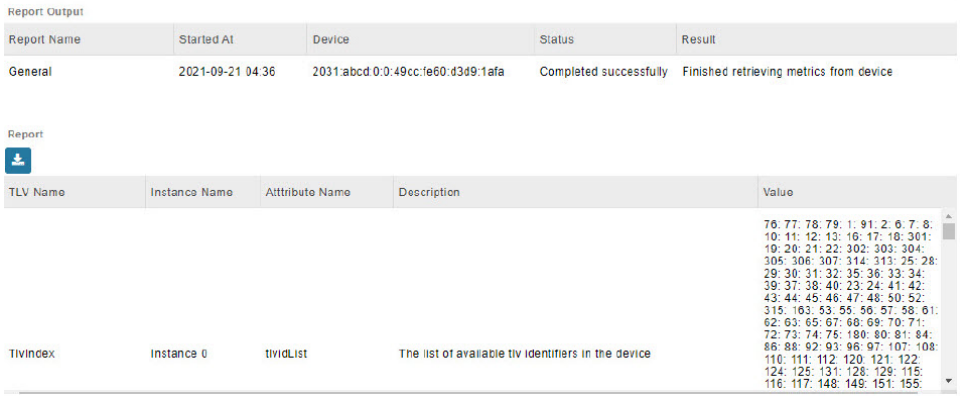
1. Choose **DEVICES** > **Field Devices** > **Browse Devices tab** > **ENDPOINT** .
2. Click the device on the right pane to view the device information.
3. On the Device Info page, click the **Troubleshoot** tab.
4. Under the **Get Report** section of the **Troubleshoot** page, select the report type. The troubleshooting report types available are All TLVs, Connectivity, General, Register, and Routing.

Note Based on the report type selected, the check boxes are auto-selected on the Troubleshoot page; indicating that the report displayed is only for the selected parameters.

5. Click **Get Report**. A report appears on the **Report Output** page.



6. Click the **Report** icon to export the report in CSV format. The following figure displays a troubleshooting report generated for General report type.


Report Output

Report Name	Started At	Device	Status	Result
General	2021-09-21 04:36	2031:abcd:0:0:49cc:fe60:d3d9:1afa	Completed successfully	Finished retrieving metrics from device

Report

TLV Name	Instance Name	Attribute Name	Description	Value
TlvIndex	Instance 0	tlvIdList	The list of available tlv identifiers in the device	76: 77: 78: 79: 1: 91: 2: 6: 7: 8: 10: 11: 12: 13: 16: 17: 18: 301: 19: 20: 21: 22: 302: 303: 304: 305: 306: 307: 314: 313: 25: 28: 29: 30: 31: 32: 35: 36: 33: 34: 39: 37: 38: 40: 23: 24: 41: 42: 43: 44: 45: 46: 47: 48: 50: 52: 315: 163: 53: 55: 56: 57: 58: 61: 62: 63: 65: 67: 68: 69: 70: 71: 72: 73: 74: 75: 180: 80: 81: 84: 86: 88: 92: 93: 96: 97: 107: 108: 110: 111: 112: 120: 121: 122: 124: 125: 131: 128: 129: 115: 116: 117: 148: 149: 151: 155:

Managing Itron Bridge Meters

An Endpoint Operator can manage Itron Bridge Meters such as ITRON30 as a cg-mesh device type (METER-CGMESH) using IoT-FND. This meter type was previously run in RFLAN mode.

Note Only Root and Endpoint Operators (RBAC) can see and perform the endpoint operations and scheduling for the Channel Notch feature.

To manage an Itron Bridge Meter in cg-mesh mode, an Endpoint Operator (RBAC) must convert the RFLAN meter to a cg-mesh device type and upgrade all cg-mesh firmware to cg-mesh 5.6.x.

After successful registration, the channel notch settings (in the bootstrap config.bin) must be pushed to all modes by the Endpoint Operator as soon as possible to be compliant with local regulations.

There are two new properties associated with this feature:

- channelNotchSettingEnd
- To appear in the IoT FND user interface. Pages supported are **CONFIG** > **CHANNEL NOTCH SETTINGS** and **CONFIG** > **CHANNEL NOTCH CONFIG**.
- channelNotchMaxAttempts = 20 (The maximum attempts to try to send the configuration and schedule information to all the endpoints).

After successful registration, the channel notch settings (in the bootstrap config.bin file) must be pushed to all nodes by the Endpoint Operator.

There are two new properties for this feature:

- channelNotchMaxAttempts = 20. This property defines the maximum attempts allowed to send the configuration and schedule information to all the endpoints.
- channelNotchSettingEnabled = true. This property allows you to enable the channel notch feature.

You can define up to four pairs of Notch Range Start and End Channels on the Channel Notch Settings page. These channel ranges must have increasing channel numbers for each range and cannot have any overlapping ranges. The ranges are blacklist ranges which are used to prohibit nodes from using the ranges of channels.

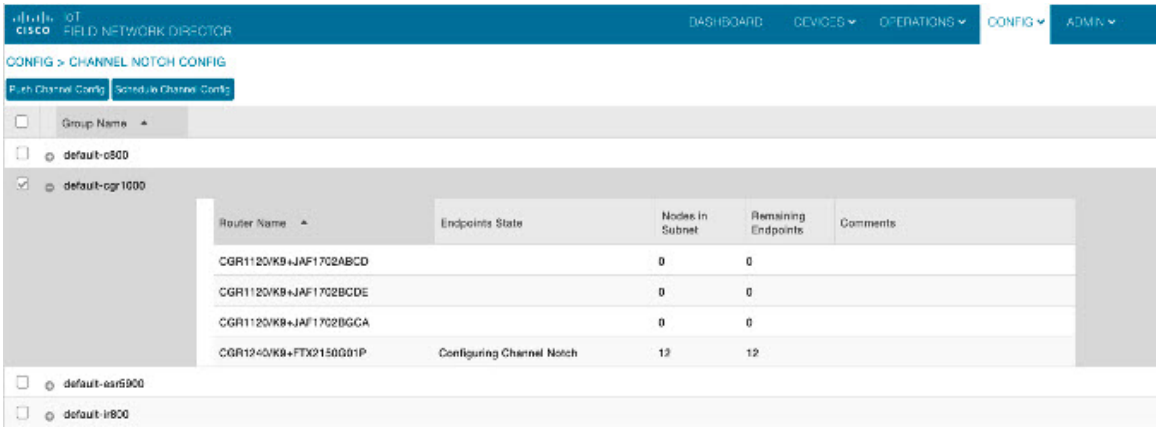
The **CONFIG** > **CHANNEL NOTCH CONFIG** page displays a list of the Config groups along with the details of group members and endpoints of each subnet. To initiate a Config push of current channel settings to the endpoints for all routers in the selected router config groups, you can press the Push Channel Config button. As the process of the channel config push progresses, the associated router config groups nested tables show the updated, remaining endpoint count and endpoint state of all endpoints.

The endpoints respond with a TLV 366 with the appropriate values to the channel notch config push, TLV 365.

Two additional properties are available:

- channelNotchMaxAttempts = 20: This setting defines the maximum attempts that the software will attempt to send the config and schedule information to all of the endpoints.
- allowNewNotchSettings=true: This setting allows notch settings to be changed at will and defines those setting that will be used in the config push.

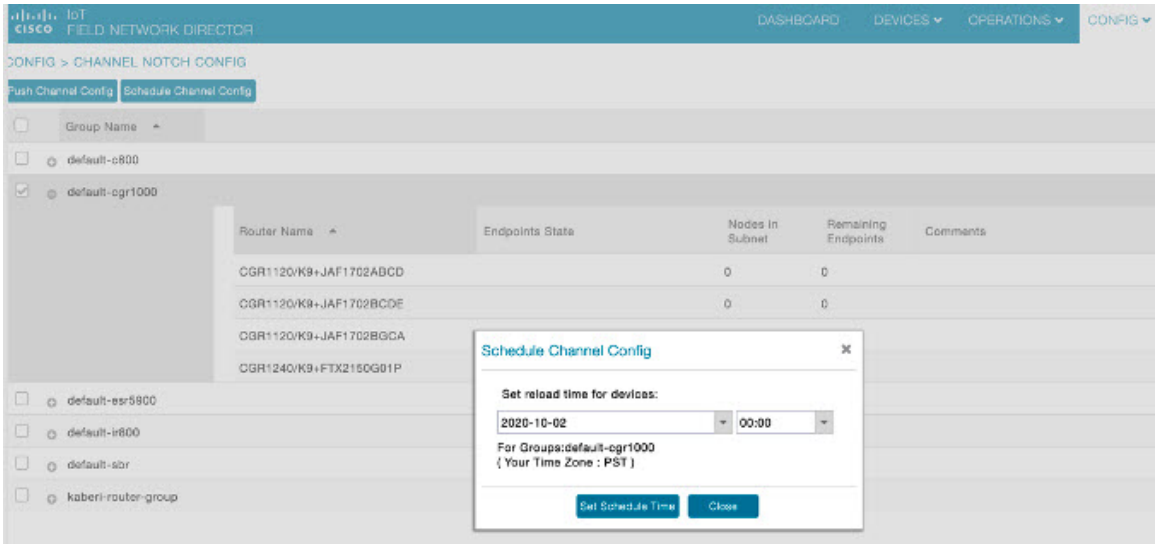


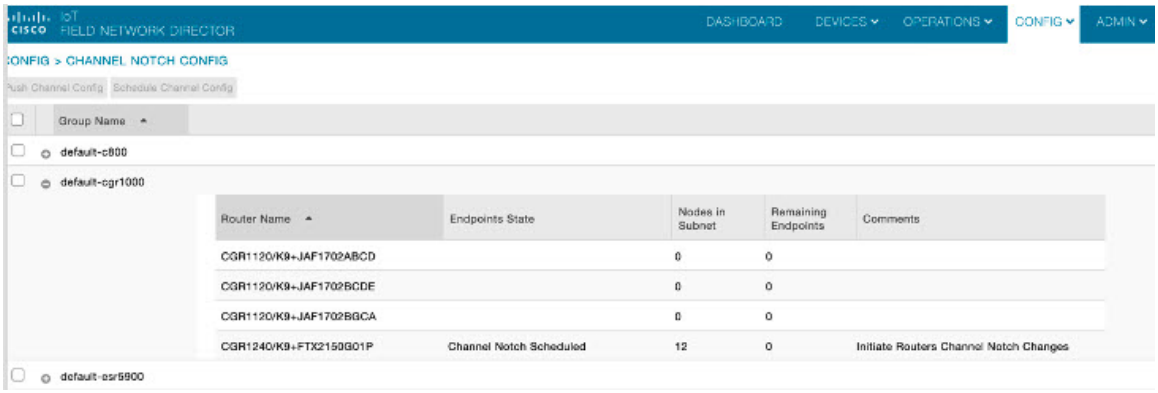


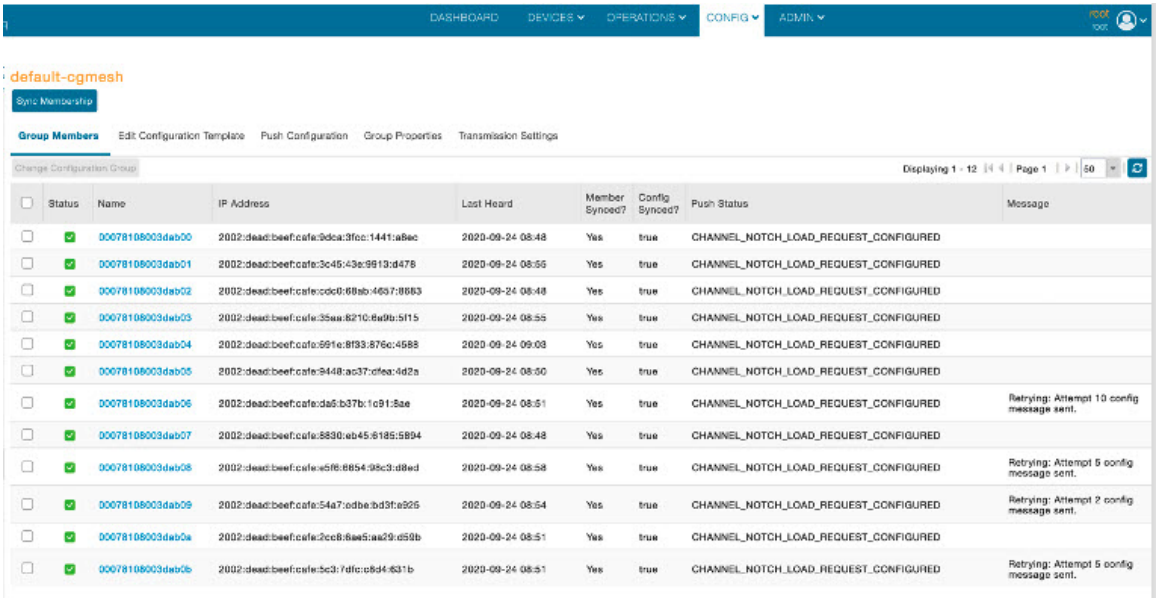
Note Before you can schedule activation of a Channel Notch Config, the router config groups must have successfully received their channel notch configuration. Note: Before you can schedule activation of a Channel Notch Config, the router config groups must have successfully received their channel notch configuration.

When you select the Schedule Channel Notch Config button, a pop up panel appears for you to set a reload time (day and time) that the Channel Notch Config will be activated.

Additionally, at the same time of the Channel Notch activation, you must also change the Channel Notch Config of the corresponding routers through Config Push.








```
[root@iot-fnd-oracle bin]# ./csmp-request -r [2002:dead:beef:cafe:9dca:3fcc:1441:a8ec] 365 366 367 20
2020-09-24 09:09:52,148:INFO:main:CoapClient: CoAP Client's traffic class set to 72
[365/NotchUpdReq]: {"notchrangenum": 1,"notchlist": [{"startChnl": 38,"stopChnl": 39}]}
[366/NotchUpdResp]: {"errcode": 7}
[367/NotchUpdLoadReq]: {"loadtime": 4293908595}
[20/WPANSettings]: {"ifIndex": 2,"panid": 5577,"bcastSlotsize": 125000,"bcastPeriod": 500000,"neighborProbeRate": 300,"SSID": "\x46\x4e\x44\x3
1","notchList": [{"startChnl": 20,"stopChnl": 25}],"dwell": {"window": 20000,"maxdwell": 400}}
[root@iot-fnd-oracle bin]#
```

To enable PAN-wide nodes to use the new Channel Notch at the same time, the node employs the following three mechanisms at the same time to guarantee that the new configuration is enabled:

- Supports scheduling of time that the new Channel Notch Settings should take effect by using TLV 367. Note that the new Channel Notch Settings are stored in the platform flash. When the scheduled time arrives, the setting is copied to the device flash and then the node is rebooted to load the new config. If the node attempts to reboot before the scheduled time, the node will continue to wait until the scheduled time.
- CGR sends an async beacon which includes the excluded channel range (ECR) through the new Channel Hopping Schedule.
- When the nodes have been offline for five days, nodes will immediately enable the new Channel Notch Settings.

After endpoints have completed the initial enrollment and joined the mesh network, the endpoints may need to re-enroll the Utility IDevID and/or the LDEVID due to certificate expiration or proactive refresh of the certificates. FND 4.7 supports on-demand and auto re-enrollment. This action is seen in the Device Configuration page for a group of devices and on the Device Detail page for a single device.

LDevID: Auto-Renewal of Certs and Saving Configuration

Auto-enroll command is pushed along with `LDevID-update` and `autorenewal_update` TCL scripts on all the Field Area Routers that are managed by IoT FND. This ensures that all the managed FAR devices have the latest certificates for both new (Greenfield) and existing (Brownfield) deployments.

Note This feature is not supported on IC3000 or IXM devices.

Note By default, the certificate is renewed when it reaches the lifetime of 90% or you can use the following property to set the required percentage as per your requirement.

```
ldevid-auto-enroll-limit=<%>
```

LDevID Certificate Renewal for FND Releases, 4.7.1 and 4.7.2

By default, the auto-renewal and update of LDevID certs feature is enabled.

The `ldevid-update` and `autorenewal_update.tcl` scripts update the following files with new certs and event manager configs:

- `before-tunnel-config`
- `before-registration-config`
- `before-tunnel-config.bak`
- `before-registration-config.bak`

Ensure that the following commands are in the running-configuration file for successful certificate renewal:

Deployment Type	Commands	Action
New Deployment	• `ip ssh version` • `cgna gzip`	Specify the commands in the **bootstrap** template.
Existing Deployment		Check if the commands are available in the router (running-config).

Support Expired SUDI Certificate

Note In IoT FND 4.7.x, this feature is enabled in the software. Therefore, FND 4.7.x supports expired SUDI certificates.

During the initial Simple Certificate Enrollment Protocol (SCEP) process, the Cisco SUDI certificate is used for authentication with the Registration Authority (RA) to acquire the Local Device Identifier (LDevID) certificate from the customer's Public Key Infrastructure (PKI). Once the LDevID is enrolled, it is used for communicating with the IoT Field Network Director (IoT FND) and the Cisco SUDI certificate is no longer required unless one of these actions occurs:

- Factory reset

- Return Material Authorization (RMA)
- Router configuration is rolled back to express-setup-config

A previously enrolled device will see no impact for an expired Cisco SUDI certificate since the LDevID is used for ongoing communications. LDevID certificates have limited lifetimes and can be renewed or re-acquired using Cisco SUDI as credentials.

However, if a device with an expired Cisco SUDI certificate that was not previously enrolled or a previously enrolled device that was reinitialized and is added to a system using FND, authentication during SCEP enrollment fails unless FND skips the expiry check while validating the SUDI certificate as part of incoming request.

The Cisco Secure Unique Device Identifier (SUDI) certificate feature is supported on the following Cisco Field Area Routers (FARs) in which the SUDI is burned into the device:

C819, CGR1120, CGR1240, IR807, IR809, IR829, IXM, and IR1101.

The SUDI for the systems listed above expires on either Date of Manufacture plus 20 years or on May 14, 2029 (2029-05-14), whichever date is earlier.

In addition, the Certificate Expiry check is skipped at the security module, if the request comes from any flow such as Zero Touch Deployment (ZTD) or WSMA communications if it is a SUDI certificate.

Example Display

```
SUDI Certificate:

Certificate
Status: Available
Certificate Serial Number (hex): 01CDAFB1
Certificate Usage: General Purpose

Issuer:
cn=ACT2 SUDI CA
o=Cisco

Subject:
Name: CGR1240
Serial Number: PID:CGR1240/K9 SN:FTX2133G01Z
cn=CGR1240
ou=ACT-2 Lite SUDI
o=Cisco
serialNumber=PID:CGR1240/K9 SN:FTX2133G01Z
Validity Date:
start date: 03:19:56 UTC Aug 17 2017
end date: 03:19:56 UTC Aug 17 2027
Associated Trustpoints: CISCO_IDEVID_SUDI

CA Certificate
Status: Available
Certificate Serial Number (hex): 61096E7D00000000000C
Certificate Usage: Signature
Issuer:

cn=Cisco Root CA 2048
o=Cisco Systems

Subject:
cn=ACT2 SUDI CA
o=Cisco

CRL Distribution Points:
```

```
http://www.cisco.com/security/pki/crl/crca2048.crl

Validity Date:

start date: 17:56:57 UTC Jun 30 2011
end date: 20:25:42 UTC May 14 2029

Associated Trustpoints: CISCO_IDEVID_SUDI
```

Configuring Enrollment over Secure Transport

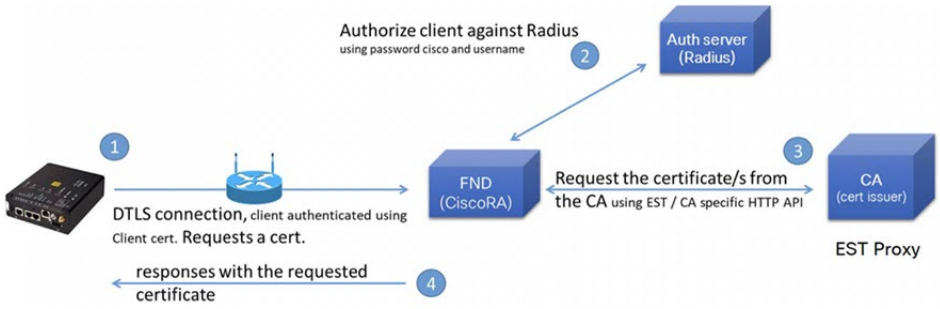
This section provides an overview of the components and configurations involved in integrating Enrollment over Secure Transport (EST) certificate enrollment for clients over the secure transport layer within the network. EST is based on public-private key exchange. This feature is supported on Itron meters, L+G meters, IR510, and IR530.

Table 1: EST Support

CR-Mesh Release	Platform	EST Support
6.2.34 MR onwards	IR530, IR510	Enrollment and re-enrollment
	ITRON30	Re-enrollment
6.3.20 onwards	IR510, IR530, ITRON30	Enrollment and re-enrollment

EST Overview

The EST service is located between a Certification Authority (CA) and a client. EST uses Hypertext Transfer Protocol (HTTP) to provide an authenticated and authorized channel for Simple Public Key Infrastructure (PKI) Requests and Responses.



EST also operates with the following protocols and authentication methods:

- Constrained Application Protocol (COAP) web transfer protocol for use with constrained nodes and constrained networks such as low-power, lossy networks.
- TLS/SSL Handshake between Registration Authority (RA) and CA.
- Datagram Transport Layer Security (DTLS) protocol is the preferred method for securing CoAP messages when the Nodes do not have any IPv6 (IP) addresses configured. DTLS uses UDP. It is based on Transport Layer Security (TLS).

- Trust Anchor is explicitly configured on the client or server for use during EST TLS authentication.

Configuring FND Registration Authority (RA)

Follow these steps to configure the FND Registration Authority:

Procedure

Step 1 Install FND-RA rpm.

Step 2 Upon successful installation, configure FND-RA as shown in the example below:

```
[root@iot-fnd-ra fnd-ra]# cd /opt/fnd-ra/bin
python3.9 ra_setup.pyc
Do you want to change the Authentication server[y/n]? y

What Authentication server are you using?
1) Microsoft Certificate Services Auth
2) RADIUS
Enter 1 or 2

Authentication Server: 2

Host Name or IP address of the RADIUS server [10.29.36.224]:
Port Number of the RADIUS server (MIN=1, MAX=65535) [1812]:
Number of retries allowed for authentication requests (MIN=1, MAX=30) [5]:
RADIUS timeout in seconds (MIN = 1, MAX = 30) [5]:
Do you want to set the RADIUS realm [y/n]: n

Do you want to change the CA server[y/n]? y

What CA server are you using?
1) Microsoft CA
2) EST Proxy
Enter 1 or 2

CA Server: 2

Host Name or IP address of the EST CA [] 10.29.36.232
Port number of the EST CA (MIN=1, MAX=65535) [6789]:
EST CA proxy user ID[estuser]: <causer>
Timeout for the EST CA (MIN=1, MAX=60) [10]: 10
Do you want to set the Injected Path Segment [y/n]: n

Do you want to change the CA/Auth server credentials [y/n]? y

Enter CA/Auth credentials

Path and file name of the private key file: /home/certs/server-key.pem
Password to use with EST Proxy: password
RADIUS shared secret: <radius password>

Do you want to change RA server settings[y/n]? y

Host Name or IP Address for the RA to listen on[]: 10.29.36.243
Path to the identity certificate of RA []: /home/certs/server-cert.pem
Path and file name to the trusted certificate store for the RA[]:
[/home/certs/est_trust_certificate.pem
```

```
Path and file name to the CACerts response file[]:
/home/certs/multicacerts.crt
RA log level (debug/info/warn/error) [debug]: debug
Transport protocol (http/coap) [coap]: coap
What is the DTLS handshake timeout (MIN=2, MAX=60) [5]:5
What is the DTLS MTU size (MIN=256, MAX=1152) [1152]:1152

Do you want to change the FND server details[y/n]? y

FND IP address or host name [2100::5]: 10.29.36.235
FND Username [root]: root
Allow self signed certificate for fnd (y/n) [y]: y
FND password : <FND UI password for root user>

Please find your selections below:

Host Name or IP address of the RADIUS server : 10.29.36.224
Port Number of the RADIUS server (MIN=1, MAX=65535) : 1812
Number of retries allowed for authentication requests (MIN=1, MAX=30) : 5
RADIUS timeout in seconds (MIN = 1, MAX = 30) : 5
Do you want to enable Enhanced Certificate Auth CSR Checking (on/off) :
off
Certificate attribute to be used in the local PKI domain? : commonName
Name for manufacturer 1 : cisco
Certificate attribute to be used in this manufacturer's local PKI domain :
serialNumber
Path of the trust store for manufacturer 1 : /opt/fnd-ra/conf/sudica.pem
Host Name or IP address of the EST CA : 10.29.36.232
Port number of the EST CA (MIN=1, MAX=65535) : 6789
EST CA proxy user ID : estuser
Timeout for the EST CA (MIN=1, MAX=60) : 10
Host Name or IP Address for the RA to listen on : 10.29.36.243
Path to the identity certificate of RA : /home/certs/server-cert.pem
Path and file name to the trusted certificate store for the RA:
/home/certs/est_trust_certificate.pem
Path and file name to the CACerts response file :
/home/certs/multicacerts.crt
RA log level (debug/info/warn/error) : debug
Transport protocol (http/coap) : coap
What is the DTLS handshake timeout (MIN=2, MAX=60) : 5
What is the DTLS MTU size (MIN=256, MAX=1152) : 1152
FND IP address or host name : 10.29.36.235
FND Username : root
Allow self signed certificate for fnd (y/n) y
Do you confirm the selections[y/n]? : y

3. Start the RA.
[root@iot-fnd-ra fnd-ra]# service fnd-ra start

4. Verify the status of RA service.
[root@iot-fnd-ra fnd-ra]# service fnd-ra status

5. Error logs
#cat /opt/fnd-ra/logs/error.log

6. RA start stop restart status:
#service fnd-ra start|stop|status|restart

7. Verify the Configuration:
#cat /opt/fnd-ra/conf/nginx.con
```

DTLS Relay Configuration and Watchdog Cisco-RA Monitoring in FND

Set the DTLS relay configuration and Watchdog Cisco-RA monitoring in FND.

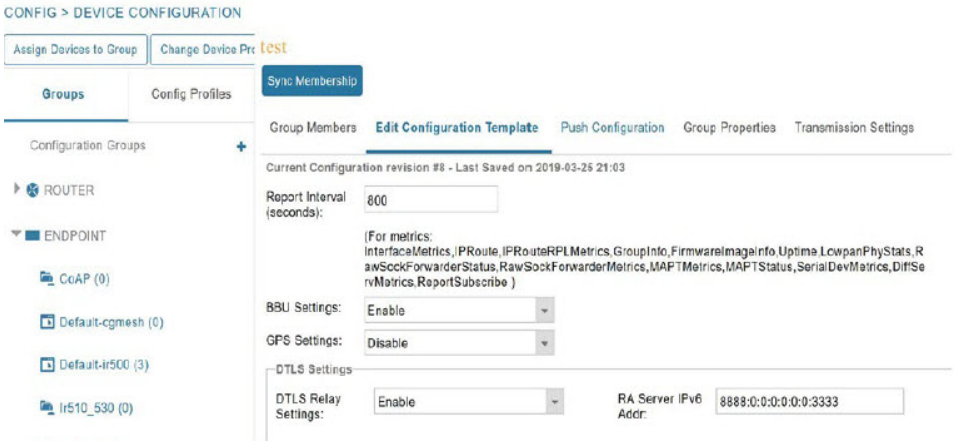
Note Supported from version 4.5.0.122 onwards.

Procedure

Step 1 Choose **CONFIG** > **Device Configuration** > **Groups** > **ENDPOINT** > **Default-IR500** > **Edit Configuration Template**.

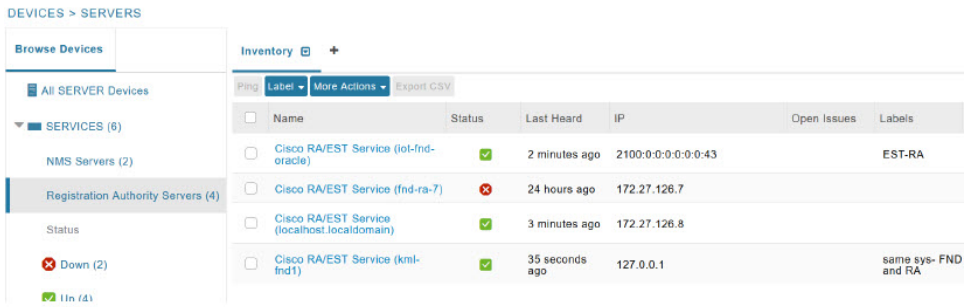
Step 2 Select **Enable** from the **DTLS Relay Settings** drop-down list.

Step 3 Enter the **RA Server IPv6 Address**. Push configuration to the first (then subsequent) hop nodes, which have already joined CGR and registered with FND.



Step 4 Watchdog Cisco-RA monitoring from FND 4.5.x: Choose **DEVICES** > **Servers** > **Registration Authority Servers**.

The IP address corresponding to each of the RA server is picked from FND-RA:nginx.conf input.



Step 5 Cisco RA/EST-CA and RADIUS IPv4 Address Authentication: Choose **DEVICES** > **Servers** > **SERVICES** > **Registration Authority Servers**.

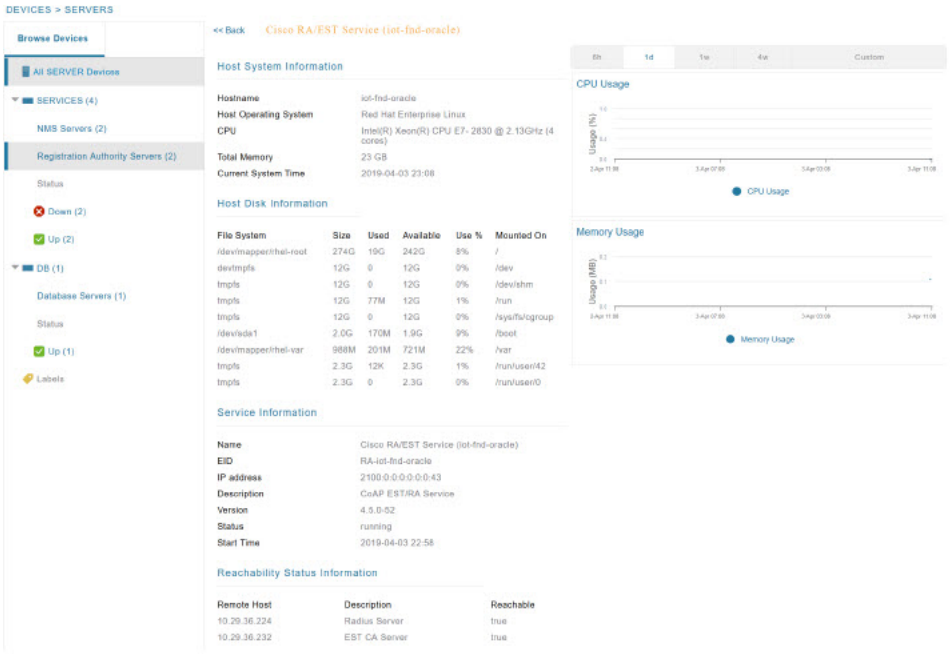


Figure 4: Events for FND-RA Service

Severity	Name	Time	Event Name	Message
	Cisco RA/EST Service (iot-fnd-oracle)	2019-04-03 22:58:44:690	Up	Service is up.

Figure 5: Periodic Audit Trail for the FND-RA

ADMIN > SYSTEM MANAGEMENT > AUDIT TRAIL

Clear Filter

Date/Time	Domain	User Name	IP	Operation	Status	Details
2019-05-17 06:10:05	root	root	10.29.36.243	NBAPI user login	Success	N/A
2019-05-17 06:06:25	root	nbapi	172.27.126.8	NBAPI user login	Success	N/A

FND Server Logs for Cisco RA/FND-RA Connectivity with FND

The following example shows the server.log for incorrect password:

```
tail -f /opt/cgms/server/cgms/log/server.log | grep 10.29.36.243

6844: localhost: Apr 03 2019 22:48:36.589 +0000: %IOTFND-6-UNSPECIFIED: %
[ch=CustomLoginModule][sev=INFO][tid=http-/0.0.0.0:443-7][rip=10.29.36.243]
[rp=10051]: userName :[root]

6845: localhost: Apr 03 2019 22:48:36.625 +0000: %IOTFND-3-UNSPECIFIED: %
[ch=AAAUtils][sev=ERROR][tid=http-/0.0.0.0:443-7][rip=10.29.36.243]
[rp=10051]: Passwords do not match for local user 'root'

6846: localhost: Apr 03 2019 22:48:36.635 +0000: %IOTFND-3-UNSPECIFIED: %
[ch=CustomLoginModule][sev=ERROR][tid=http-/0.0.0.0:443-7]
```

```
[rip=10.29.36.243][rp=10051]: Local Northbound API user 'root' failed
authentication.
```

This example shows the server.log when the RA registration is successful:

```
tail -f /opt/cgms/server/cgms/log/server.log | grep 10.29.36.243

7105: localhost: Apr 03 2019 22:58:44.582 +0000: %IOTFND-6-UNSPECIFIED: %
[ch=CustomLoginModule][sev=INFO][tid=http-/0.0.0.0:443-6][rip=10.29.36.243]
[rp=10057]: userName :[root]

7106: localhost: Apr 03 2019 22:58:44.610 +0000: %IOTFND-6-UNSPECIFIED: %
[ch=CustomLoginModule][sev=INFO][tid=http-/0.0.0.0:443-6][rip=10.29.36.243]
[rp=10057]: Local Northbound API user 'root', IP '10.29.36.243'
successfully authenticated. Passwords matched.

6916: kml-fnd1: Apr 15 2019 17:53:44.680 +0000: %IOTFND-6-UNSPECIFIED: %
[ch=SessionListener][sev=INFO][tid=http-/0.0.0.0:443-7]: Session timeout:
1800 secs.

6917: kml-fnd1: Apr 15 2019 17:53:44.681 +0000: %IOTFND-6-UNSPECIFIED: %
[ch=BaseApiWebService][sev=INFO][tid=http-/0.0.0.0:443-7]: Checking
permission for user : root

6918: kml-fnd1: Apr 15 2019 17:53:44.712 +0000: %IOTFND-6-UNSPECIFIED: %
[ch=ServiceServer][sev=INFO][tid=http-/0.0.0.0:443-7]: Received service
notification request from service [RAiot-fnd-ra]
```

This example shows the server.log when the RA registration is unsuccessful because the user does not have NBAPI orchestration permission:

```
907: kml-fnd1: Apr 15 2019 17:53:07.492 +0000: %IOTFND-6-UNSPECIFIED: %
[ch=CustomLoginModule][sev=INFO][tid=http-/0.0.0.0:443-7][rip=172.27.126.8]
[rp=42167]: userName :[kaberi]

6908: kml-fnd1: Apr 15 2019 17:53:07.520 +0000: %IOTFND-6-UNSPECIFIED: %
[ch=CustomLoginModule][sev=INFO][tid=http-/0.0.0.0:443-7][rip=172.27.126.8]
[rp=42167]: Local Northbound API user 'kaberi', IP '172.27.126.8'
successfully authenticated. Passwords matched.

6909: kml-fnd1: Apr 15 2019 17:53:07.526 +0000: %IOTFND-6-UNSPECIFIED: %
[ch=SessionListener][sev=INFO][tid=http-/0.0.0.0:443-7]: Session timeout:
1800 secs.

6910: kml-fnd1: Apr 15 2019 17:53:07.527 +0000: %IOTFND-6-UNSPECIFIED: %
[ch=BaseApiWebService][sev=INFO][tid=http-/0.0.0.0:443-7]: Checking
permission for user : kaberi

6911: kml-fnd1: Apr 15 2019 17:53:07.546 +0000: %IOTFND-3-UNSPECIFIED: %
[ch=CustomPermissionResolver][sev=ERROR][tid=http-/0.0.0.0:443-7]:
Northbound API user 'kaberi' is NOT allowed to perform action
'nbapi-orchestrationService'.
```

Cisco RA Events on FND

The following RA events are supported from IoT FND version 4.5.0.122 onwards:

- Enroll request/response/failure — Generated during initial enrollment and re-enrollment of node with CA server. Failure occurs when the CA server(./runserver.sh is not running) is not up or port is blocked.

- Auth success/failure — Generated during the dot1x authentication of node with the RADIUS server. Failure occurs when the Radius server IP is wrong in the FND-RA script(nginx.conf), dot1x entries are either wrong or not present.
- CACert Request/Response — Generated during the CA cert re-enrollment.
- Device Unknown Event — RA Events generated by a node which is not recognized/registered on FND.
- SSL Event — Generated when there is an SSL protocol error.

Managing the Cisco Industrial Compute IC3000 Gateway

Before you can manage the IC3000 with the IoT FND you must review the details in Unboxing, Installing and Connecting to the IC3000 topic of the Cisco IC3000 Industrial Compute Gateway Deployment Guide.



Important Before you can manage the IC3000 Gateway using IoT FND 4.3 and greater, you must first Deploy Pre-built IOx Applications via the App tab within IoT FND.

For more information, refer to the Use Case Example within the Cisco IC3000 Industrial Compute Gateway Deployment Guide.

- Installing a Prebuilt Applications via Local Manager

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

Overview

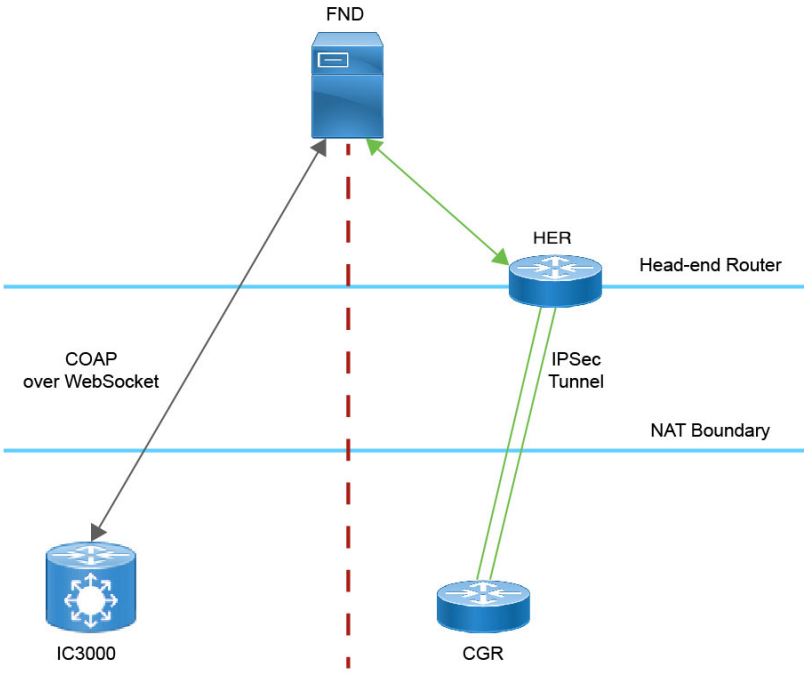
IC3000 supports edge computing and communicates with IoT FND through the IOx application, Cisco Fog Director which is accessible via IOT FND.

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

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

Using the WebSocket protocol allows the client and server to talk to each other as well as operate independently of each other as shown in the image below. The client does not need to make a request to connect to the server (see left side of network diagram).

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

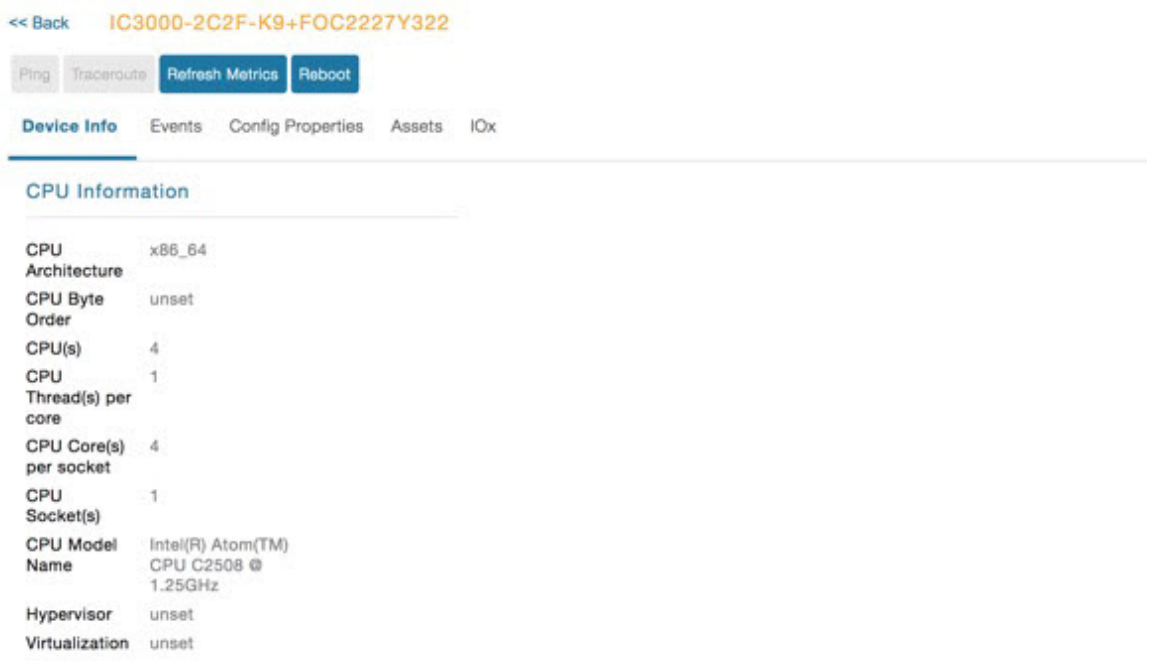


You can perform the following actions for an IC3000 device type on demand:

- Refresh Metrics
- Reboot

Device Category: GATEWAY (in Browse Devices pane). To view the IC3000 Gateway details:

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



For details on the IC3000 Devices, refer to the Cisco IC3000 Industrial Compute Gateway Deployment Guide.

Editing the IC3000 Gateway Configuration Template

To edit the IC3000 gateway configuration template:

Procedure

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

Step 2 Under CONFIGURATION GROUPS (left pane), select the **GATEWAY group** with the template to edit.

Step 3 Click **Edit Configuration Template**.

Step 4 Edit the configuration and use the Push Configuration tab to push the new configuration to the active or registered device.

Step 5 Click **Save Changes**.

NTP Configuration

To push the NTP configuration via FND,

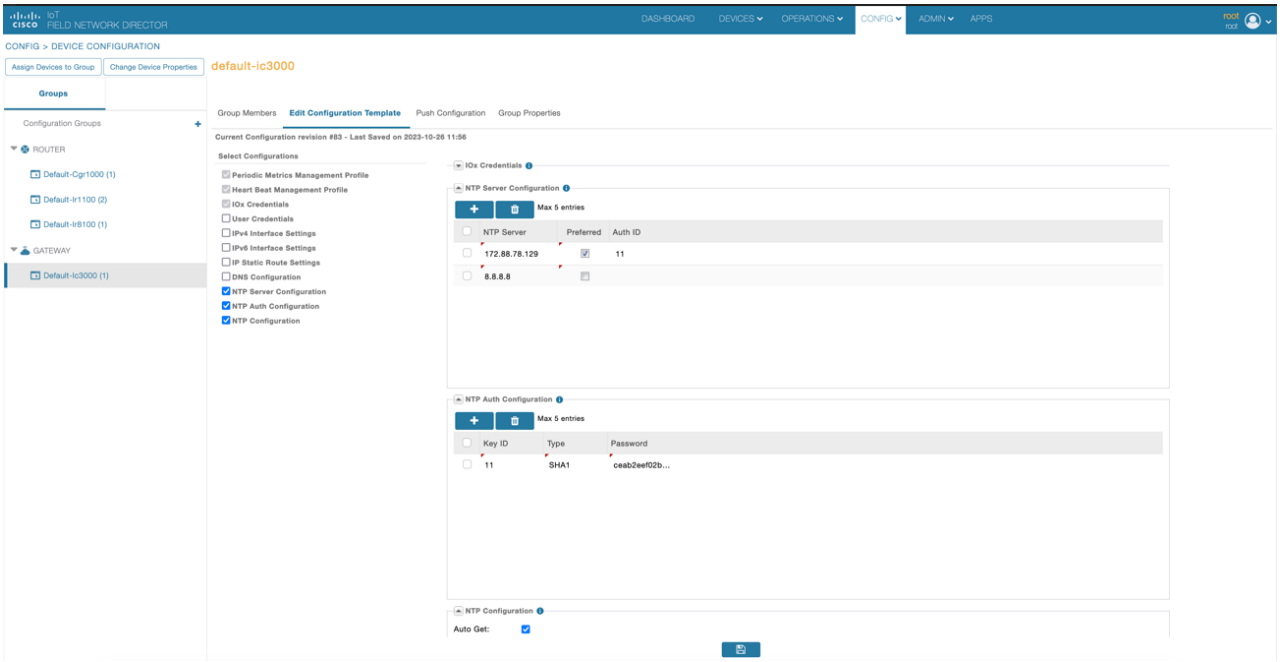
Procedure

Step 1 Choose **CONFIG** > **Device Configuration**

Step 2 Under CONFIGURATION GROUPS (left pane), select the **GATEWAY group** with the template to edit.

Step 3 Click **Edit Configuration Template**.

Step 4 Select both **NTP Configuration** and **NTP Server Configuration** checkboxes. If NTP server is configured with authentication, select **NTP Auth Configuration** checkbox.



Note
The Auto Get checkbox under **NTP Configuration** deletes the NTP configuration that is manually pushed to the device from IoT FND. Hence, **NTP Configuration** should be configured along with **NTP Server Configuration** and **NTP Auth Configuration**.

Step 5 Enter values for all the fields under **NTP Server Configuration** and **NTP Auth Configuration** with the appropriate parameters.

Step 6 Click **Save Changes**.

Managing the Cisco Wireless Gateway for LoRaWAN

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

The two Cisco Wireless Gateway for LoRaWAN products are:

- A virtual interface (IXM-LPWA-800-16-K9) of the Cisco 809 and 829 Industrial Integrated Service Routers (IR809, IR829) to provide LoRa radio access with the IR809 and IR829 providing an IP backhaul (Gigabit Ethernet, Fiber, 4G/LTE, and Wi-Fi). In this case, LoRaWAN has an Operating Mode of IOS Interface and displays the Hosting Device ID for the IR800 system to which it connects (See Cisco Catalyst IR1100 Expansion Modules in Cisco IoT FND, on page 44).

- A standalone unit (IXM-LPWA-900-16-K9) using its own built-in Fast Ethernet backhaul to access LAN switches, routers, Wi-Fi AP or other IP interfaces. When functioning as a standalone gateway, LoRaWAN has an Operating Mode of Standalone.

Device Category: GATEWAY (in Browse Devices pane). To view the LoRaWAN Gateway:

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



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

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

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


<< Back
IXM-LPWA-900-16-K9+FOC21028RJ4
Show on Map
Ping
Traceroute
Refresh Metrics
Restart Radio
Device Info
Events
Config Properties
Running Config
Assets
Inventory
Name IXM-LPWA-900-16-K9+FOC21028RJ4
EID IXM-LPWA-900-16-K9+FOC21028RJ4
Domain root
Device Category IOTGATEWAY
Device Type LORAWAN
Status up
IP Address 20.20.4.127
Operating Mode Standalone
IPv6 Address unknown
First Heard 2017-10-16 19:14
Last Heard 2018-01-21 10:35
Last Property Heard 2017-10-16 19:16
Last Metric Heard 2018-01-21 10:35
Last Reboot Time unknown
Model Number IXM-LPWA-900-16-K9
Serial Number FOC21028RJ4
Firmware Version 2.0.20
Agent Version N-A
Boot Loader Version 20160830_cisco
Gateway Health
Uptime 1d 22hr 37min
Door Status closed
Modem Temperature 37.0 Celsius
Load Average 1min 0.54 5min 0.23 15min 0.17
System LED unknown
FPGA Information
FPGA Version 61
HAL Version 5.1.0
SPI Speed speed set to 2000000
LoRaWAN Chip 1 Type SX1301
LoRaWAN Chip 1 Version 103
LoRaWAN Chip 1 ID 1
LoRaWAN Chip 2 Type SX1301
LoRaWAN Chip 2 Version 103
LoRaWAN Chip 2 ID 1
FPGA Version Check OK
Packet Forwarder Information
Packet Forwarder Status Running
Packet Forwarder Firmware Installed
Packet Forwarder Version 1.6.11
Packet Forwarder Public Key Installed
Packet Forwarder Id 6596c3e0
Gateway Properties
Location 10.6, 10.0
GPS Info Time unknown
RF Chip ID LSB = 0x2876f90f MSB = 0x00f14212
Tx Power Calibration <NA,NA,NA,54,35,108,99,91,82,74,66,56,47,38,29,20-NA,NA,NA,51,32,106,97,89,80,72,64,55,46,37,28,19>
Antenna 1 RSSI Offset(dBm) -205.00
6h
1d
1w
4w
Custom
Load Average
% Utilization
Load Average
Modem Temperature
Degree Celsius
Modem Temperature

Managing Cisco IR510 WPAN gateways

Cisco IR500 Industrial Router formerly known as Cisco 500 Series Wireless Personal Area Network (WPAN) industrial routers, provides unlicensed 902-928MHz, ISM-band IEEE 802.15.4g/e/v WPAN communications to diverse Cisco Internet of Things (IoT) applications such as smart grid, Distribution Automation (DA), and Supervisory Control and Data Acquisition (SCADA).

As the next generation of the DA gateway, IR510 provides higher throughput, distributed intelligence, GPS, and enhanced security. unlicensed 915-MHz industrial, scientific, and medical band WPAN communications.

Note

- Cisco IR510 industrial router is identified and managed as an ENDPOINT in Cisco IoT FND: **DEVICES** > **FIELD DEVICES** > **ENDPOINT** > **GATEWAY**.
- When you update the existing installed software base for Cisco IR510 and IR530 industrial routers, Cisco IoT FND uploads only the new software updates, rather than the full image, by using `bsdiff` and `bspatch` files.

Profile instances

Cisco IoT FND implements profile based configuration for Cisco IR510 routers. This allows you to define a specific profile instance (as part of configuration), that you can assign to multiple Cisco IR500 routers configuration groups. See Table 6. Pre-defined Profiles for IR510, for the list of supported profile types.

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



To create a new profile:

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

To delete a profile:

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

2. Select the Profile name (excluding Default-Profile) that you want to delete. Click on the trash icon to remove the Profile.
3. In the pop up window that appears, click Yes to confirm deletion.

To rename a profile:

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

To clone a profile:

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

Table 2: Pre-defined Profiles for IR510

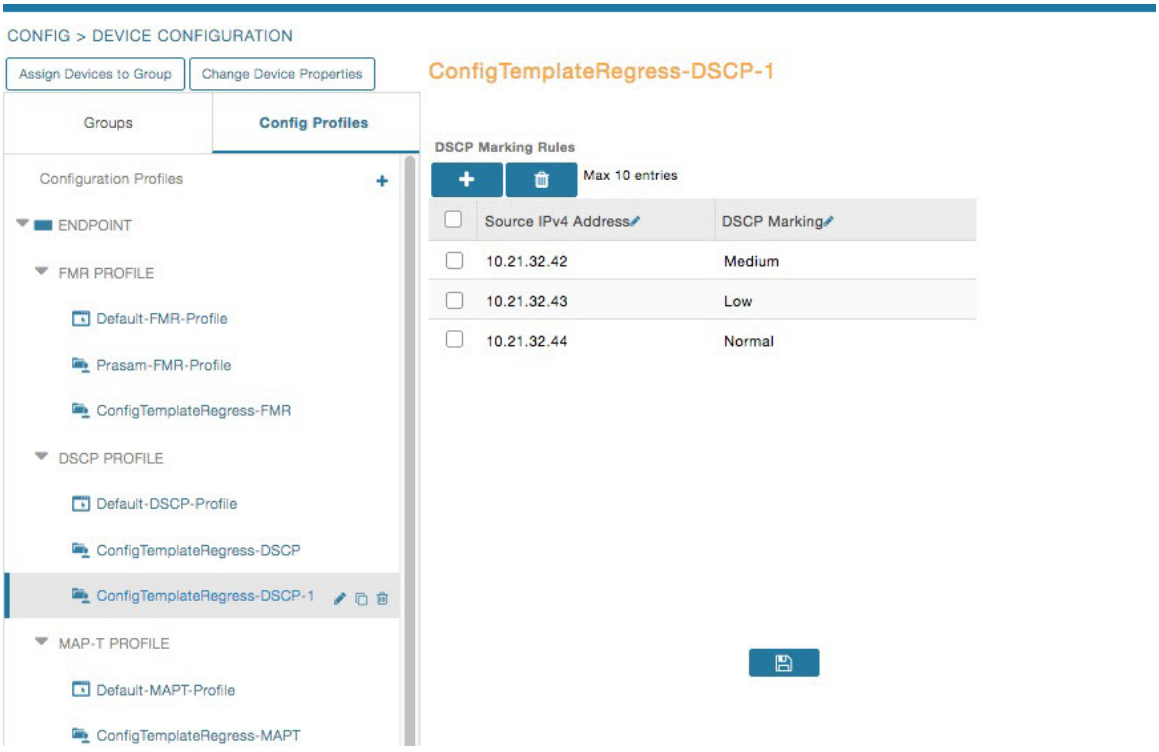
Profile Name	Description	Properties Configurable in CSV File
Forward Mapping Rule (FMR) Profile **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **FMR PROFILE** Interface configuration **CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template** Select the FMR profile from the drop-down menu	Processes IPv4 traffic between MAP nodes that are in two different MAP domains. Each FMR rule has IPv4 Prefix, IPv4 Prefix Length and EA Bits Length. You can define up to 10 FMR Profiles. FMR settings are pushed to the device as a part of MAP-T Settings during configuration push.	Forward Mapping Rule IPv6 Prefix: fmrIPv6Prefix0 to fmrIPv6Prefix9 Forward Mapping Rule IPv6 Prefix Length: fmrIPv6PrefixLen0 to fmrIPv6PrefixLen9

Profile Name	Description	Properties Configurable in CSV File
DSCP profile **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **DSCP PROFILE** Interface configuration **CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template** Select the DSCP profile from the drop-down menu	Sets the DSCP marking for the Ethernet QoS configuration. DSCP marking has eight (8) marking options to choose. - User Controlled - Default Queue (Best Effort) - Normal Queue: Low drop probability (AF11) - Normal Queue: Medium drop probability (AF12) - Normal Queue: High drop probability (AF13) - Medium Queue: Low drop probability (AF21) - Medium Queue: Medium drop probability (AF22) - Medium Queue: High drop probability (AF23) You can specify a maximum of 10 IPv4 addresses and associated DSCP markings.	NA
MAP-T Profile **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **MAP-T PROFILE** Interface configuration **CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template** Configures Basic Mapping Rule (BMR) and Default Mapping Rule (DMR) settings for IR509/IR510	Configures endUser properties.	endUserIPv6PrefixbmrIPv6PrefixLen

Profile Name	Description	Properties Configurable in CSV File
Serial Port Profile (DCE and DTE) **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **SERIAL PROFILE** Interface configuration **CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template** Select the Serial Port profile (DTE) and/or Serial Port profile (DCE) from the drop-down menu	You can use different serial port profiles for DCE and DTE serial port settings). You can configure the following settings on the serial interface: • Port affinity • Media Type • Data Bits • Parity • Flow Control • DSCP Marking • Baud rate • Stop Bit **Note** You can also configure Raw Socket Sessions settings at the this page.	NA
DHCP Client Profile **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **DHCP CLIENT PROFILE** Interface configuration **CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template** Select the DSCP Client profile from the drop-down menu	The DHCPv4 server allocates an address to each client according to a static binding between a client-id and an IPv4 address. FND configures this static binding supports up to 10 client mappings. The DHCP Client ID binding profile configuration associates a client ID to an IPv4 Host address. The Client-id of each Client is expected to be unique within a single IR510. Any string can be used as client-id (for example, client-id=”iox”) can be mapped to a binding address in the pool.	NA

Profile Name	Description	Properties Configurable in CSV File
DHCP Server Profile **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **DHCP SERVER PROFILE** Interface configuration **CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template** Select the DSCP Server profile from the drop-down menu	Information that the DHCPV4 Server returns as part of DHCP Options in the response, can be configured in the DHCP server profile configuration includes: 1. Lease Time 2. DNS server list	NA
NAT44 Profile **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **NAT 44 PROFILE** Interface configuration **CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template** Select the NAT44 profile from the drop-down menu	You can use one of the following methods to configure the NAT44 properties for the IR500 device: - CSV import method - NAT44 profile instance within FND user interface You configure three fields for NAT44: Internal Address, Internal Port and External Port You can configure up to fifteen NAT 44 Static Map entries **Note** Before you push the configuration, be sure to: 1. Enable Ethernet on the configuration group to which the device belongs (select check box) 2. Save Configuration Group	NA

Profile Name	Description	Properties Configurable in CSV File
Access Control List (ACL) Profile **CONFIG > DEVICE CONFIGURATION > Config Profiles tab > ACL PROFILE** Interface configuration **CONFIG > DEVICE CONFIGURATION > GROUPS tab > Default-ir500 > Edit Configuration Template** Select the ACL Profile from the drop-down menu.	Perform packet filtering to control which packets move through the network for increased security. You can define up to 20 ACL Profiles. Each defined ACL has one associated Access Control Entry (ACE) for a maximum of 20 ACEs. The check process goes through ACL from 1 to 20. There is an implicit deny for all ACL at the end of 20 ACL unless configured differently. To configure the interface for the Default-IR500, with Groups tab selected: In the right-pane, choose Edit Configuration Template tab and select the Enable Interface ACL check box.	NA

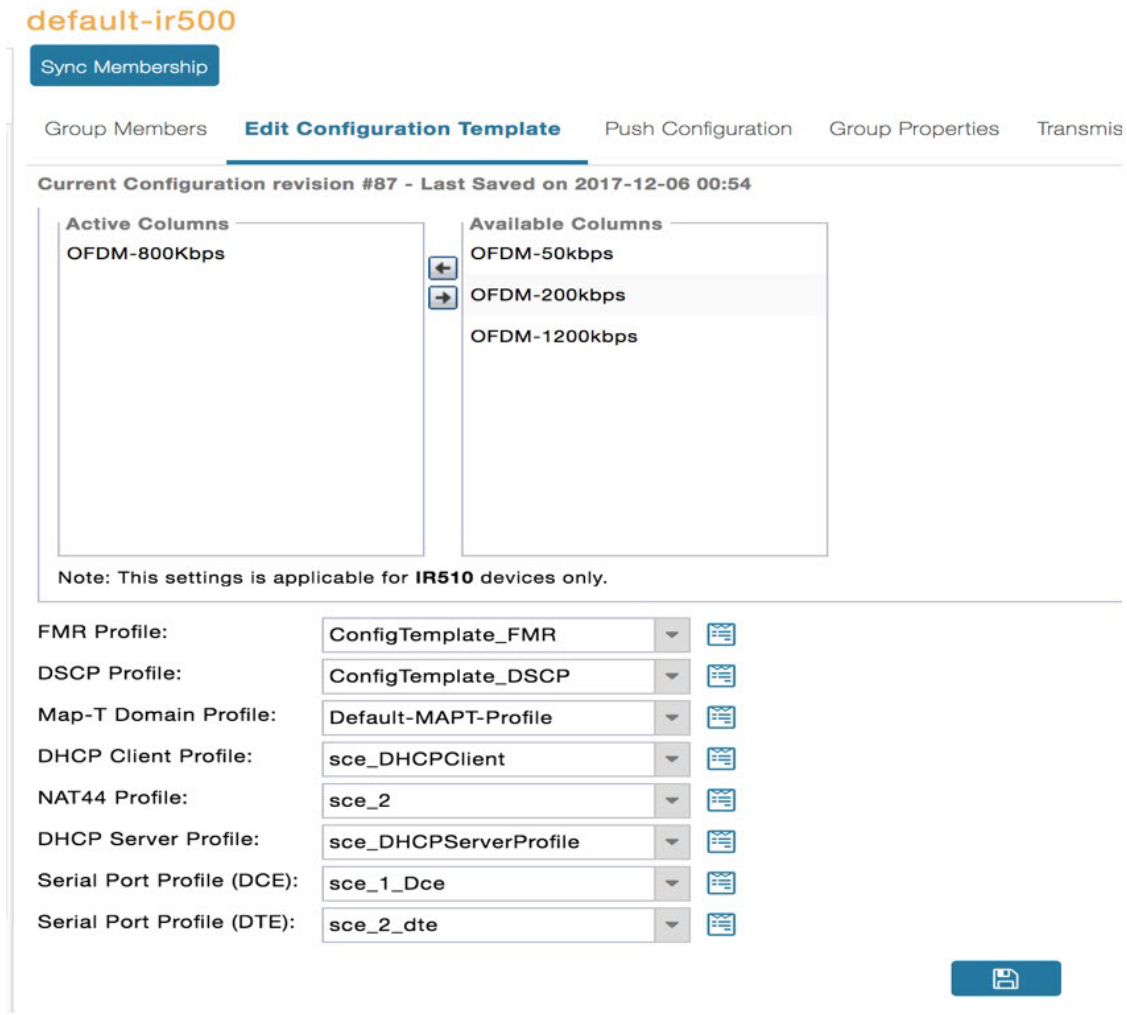


Configuration Notes:

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

Configuration Profile for a Group

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



Wi-SUN 1.0 Support

You can define and review the supported actions for Wi-SUN 1.0 on the Cisco IR509 and IR510 WPAN gateways and the Cisco IR529 and IR530 Resilient Mesh Range Extenders along with WPAN OFDM module installed within a CGR 1000 platform, by using the **CONFIG** > **DEVICE CONFIGURATION** and **DEVICES** > **FIELD DEVICES** > **ENDPOINTS** pages.

Summary of features and actions supported:

- A search parameter, Mesh Protocol, allows you to filter based on Wi-SUN or Pre-Wi-SUN mode. (**DEVICES** > **FIELD DEVICES** > **Browse Devices tab** > **function: gateway deviceType:ir500**).
- Registration and Configuration Push Validation Notifications (Success or Failure) sent for Cisco IR500 devices and other resilient mesh endpoints.
- A Block Mesh Device option under the More Actions menu, allows you to block and blacklist resilient mesh endpoints (Cisco IR509, IR510, IR529, and IR530) that you suspect are not valid endpoints within the WPAN.

- DSCP Markings Rule: Allows configuration of low, medium, and high precedence with a combination of 4 classes to provide 8 assignable options for DSCP Marking Profiles including default user-controlled options. (Previously, only three markings were supported). This feature is applicable to Cisco IR510 only.

Note

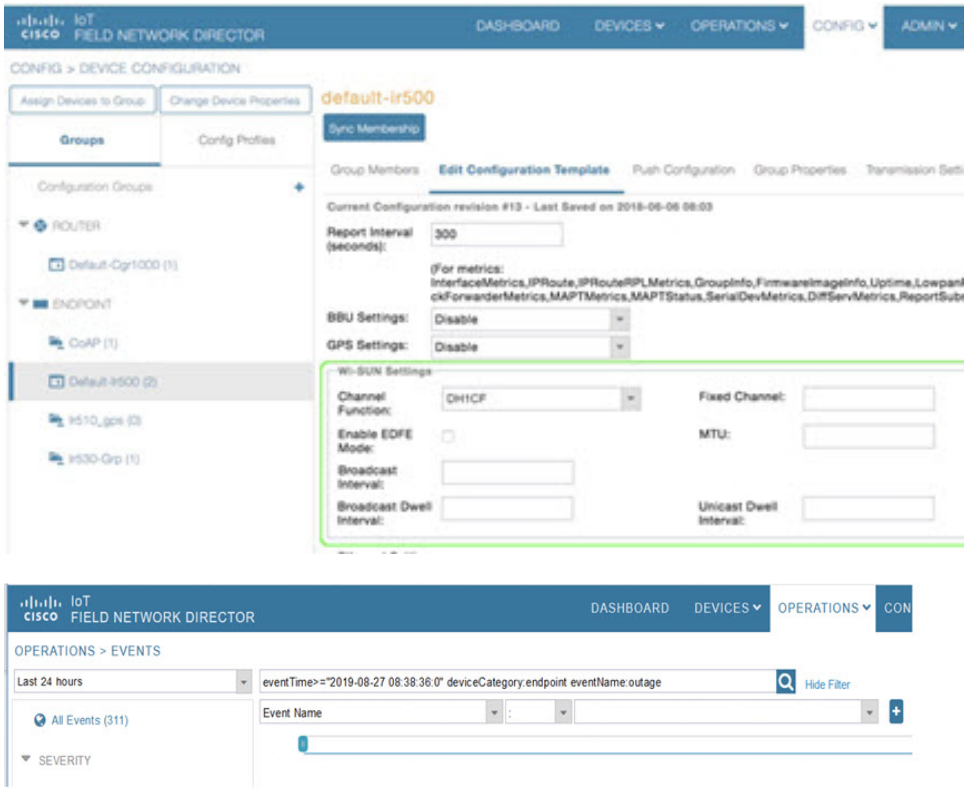
- In Mesh Software 6.3, only the Wi-SUN 1.0 protocol is supported for all mesh endpoints. It displays Wi-SUN 1.0 from the mesh 6.3 firmware onward under the Mesh Protocol heading on the **DEVICES** > **FIELD DEVICES** > **ENDPOINT** > **Inventory** page.

  The Wi-SUN settings have been removed from the Cisco IR500 Config Group template: **CONFIG** > **DEVICE CONFIGURATION** > **Default-ir500** > **Edit Configuration Template** in Cisco IoT FND 4.7.

- When using Mesh Software 6.2, for a Cisco IR510 running Wi-SUN mode 1.0, the Power Outage (PON) and Restore (PRN) messages will be sent as regular CSMP (Layer 2 to CSMP messages) / CoAP18 messages to port 61628. There is no change to the events generated by the new PON and PRN messages. Your router must be running 15.9(3)M1or greater for this capability.

  When using Mesh Software 6.1, the Wi-SUN protocol is supported for all Cisco IR500 platforms. The mesh protocol setting between CG-Mesh and Wi-SUN 1.0 can only be set in the bootstrap configuration.

- For Mesh Software 6.1, mesh endpoints send the PON and PRN messages to Cisco IoT FND port 61625 as UDP messages. There are no changes in the events that are generated by the new PON and PRN CSMP messages.

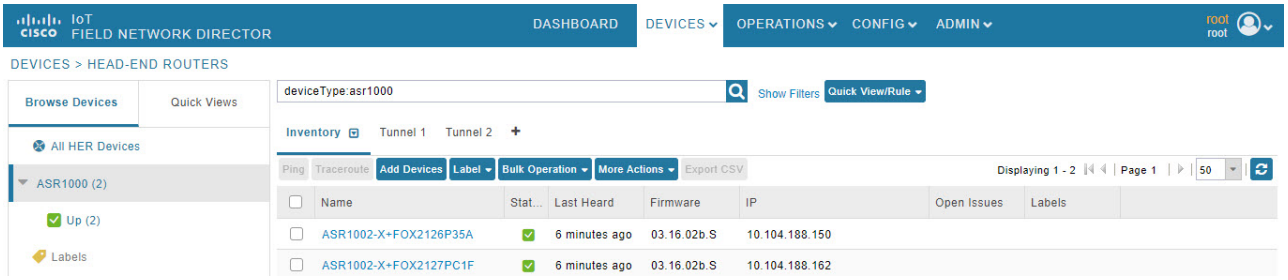


Managing Head-End Routers

To manage Head-End Routers (HERs), open the Head-End Routers page by choosing **Devices** > **Head-End Routers**. 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.



For information on how to customize HER views, see Customizing Device Views, on page 49

For information about the device properties displayed in each view, see Device Properties, on page 127.

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, on page 48

Cisco Catalyst IR1100 Expansion Modules in Cisco IoT FND

Expansion modules adds functionality by adding new interfaces or features when you insert them into supported routers or gateways. You can manage and monitor these modules through Cisco IoT FND to adapt your network infrastructure to changing requirements.

Table 3: Feature history

Feature name	Release information	Description
Cisco IR1100 expansion module	Cisco IoT FND Release 4.7	Adds support for Cisco IR1100 Expansion Module, allowing you to manage and configure the module using Cisco IoT FND on Cisco Catalyst IR1100.

Install Cisco IRM-1100-4S8I expansion module

This task describes how to install the Cisco IRM-1100. The Expansion Module attaches to the Cisco Catalyst IR1101 Base using 4 mating screws, and is connected through a mating connector. The Expansion Module is grounded and powered through the connection to the IR1101.

Before you begin

- Unpack the box and verify that all items listed on the invoice were shipped with the Cisco IRM-1100-4S8I expansion module.

  The following items are shipped with your Expansion Module:

  - 4 mating screws to connect the IRM-1100 to the IR1101

- Cisco IR1100 must run Cisco IOS XE Release 17.18.01a and later releases.
- Hard swap is not supported for the Cisco IRM-1100-4S8I expansion module on Cisco IoT FND. You need to restart your Cisco IR1100 device and register the device once again with Cisco IoT FND. For more information see, Register IR1100 with Cisco IoT FND.
- You don't need to re-register your device if it was already registered before the reboot.
- The expansion module info is automatically displayed in Cisco IoT FND during periodic metrics updates.
- You can configure the expansion module using Cisco IoT FND including the interfaces ports and SFPs.
- The IRM-1100-4S8I works only only on the top side of Cisco IR1101.

Procedure

Follow the instructions in the Cisco Catalyst IR1101 Rugged Series Router Software Configuration Guide to configure the expansion module.

Itron CAM Module

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

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

Procedure

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

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

```
manage-actd=true
```

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

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

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

a) Choose **CONFIG** > **FIRMWARE UPDATE** > **Images** tab.
b) Select CGR-Default profile from under the Groups panel and click the **Upload Image** button.
c) Click + to open the Upload Image panel.
d) Select the type ACTD-CGR and select the appropriate Image from the drop-down menu such app-actd-ver-x.y.z.tar. In the confirmation box, click **Upload Image**.
e) Click Yes to confirm upload.

Feature Name	Release Information	Description
IR8100 with CAM Module Support	IoT FND 4.10	Itron CAM is the hardware module inserted into IR8100. The integration only applies to IR8100 routers.

Lorawan Gateway Module

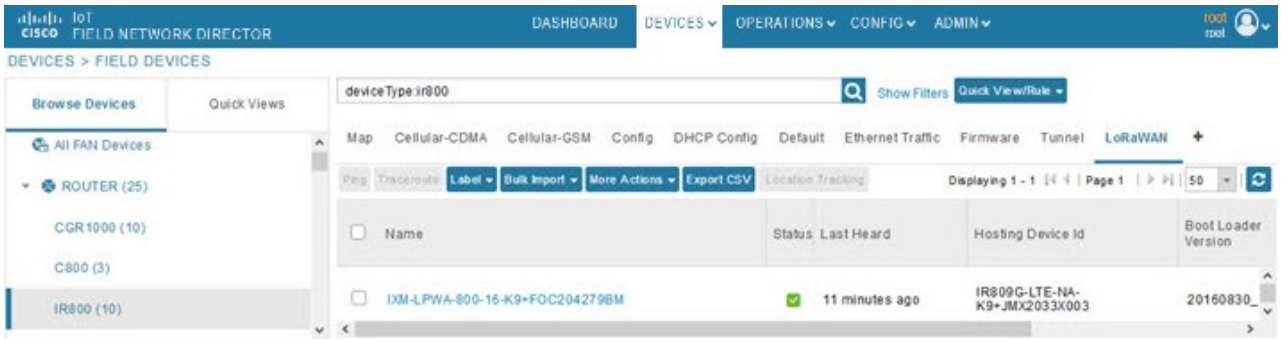
Procedure

Step 1 LoRaWAN (IXM-LPWA-800) interface to IR800 router.

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

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

Step 2 To view LoRaWAN modules in a Device List, choose an IR800 router in the **Browse Devices** list and select the **LoRaWAN** tab.



Step 3 To reboot the modem on the LoRaWAN module:

a) Click the relevant IXM-LORA link under the Name column to display the information seen below:



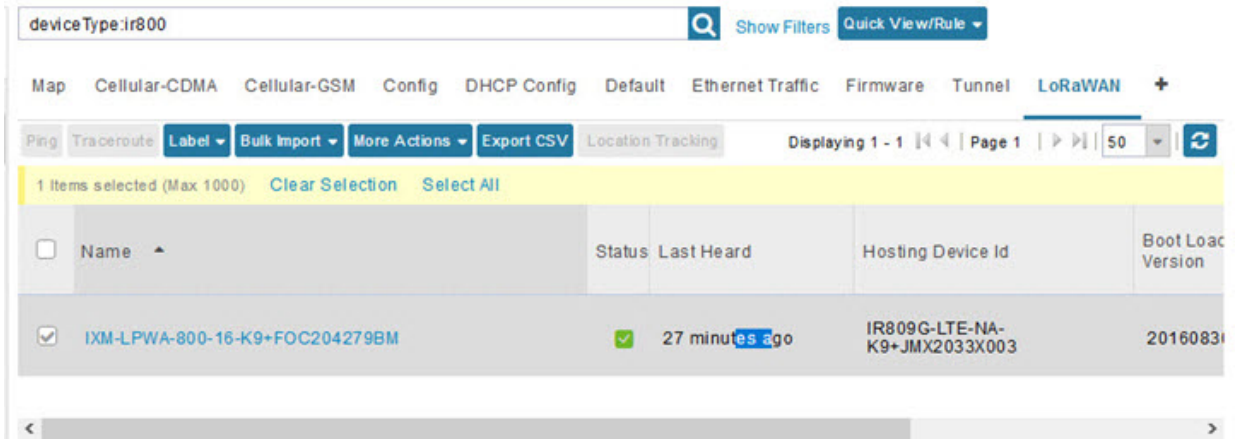
b) Click **Reboot Modem**. When the reboot completes, the date and time display in the Last Reboot Time field in the Device Info pane for the LoRaWAN module. You can only process one modem reboot at a time.

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

Step 4 To remove a LoRaWAN module from the IR800 router inventory:

a) In the **Browse Devices** pane, select the IR800, which has the LoRAWAN module that needs to be disabled and removed from inventory.

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



c) At the More Actions drop-down list, select **Remove Devices**.

Step 5 To create a user-defined LoRaWAN (IXM) Tunnel, choose **CONFIG** > **Tunnel Provisioning**.

a) In the left-pane, under GATEWAY, select the LoRaWAN system for which you want to configure a tunnel.

b) Select the **Gateway Tunnel Addition** tab.

c) In the **Add Group** window that appears, enter a Name for the LoRaWAN (IXM) Tunnel and select Gateway as the Device Category.

d) Click **Add**.

The new tunnel appears under the GATEWAY heading in the left-pane.

Managing Servers

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

To add additional views, see Customizing Device Views, on page 49.

For more information about the device properties displayed in each view, see Device Properties, on page 127.

For information about the common actions in this view, see Common Device Operations, on page 48 .

Managing NMS and Database Servers

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

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

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



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

Managing Application Management Servers

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

Common Device Operations

This section describes how to use IoT FND to manage and view information about devices.

Tracking Assets

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

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

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

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

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

  Example of Asset content in CSV file:

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



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

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

Guidelines for Adding or Associating an Asset with a Device:

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

Selecting Devices

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

Customizing Device Views

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

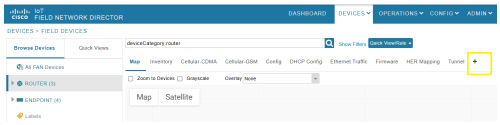
- Add and delete tabs
- Specify the properties to display in the columns for each view (see Device Properties by Category, on page 128 for available properties)
- Change the order of columns

Adding Device Views

To add the device views, navigate to **DEVICES** > **FIELD DEVICES** > **ROUTER**.

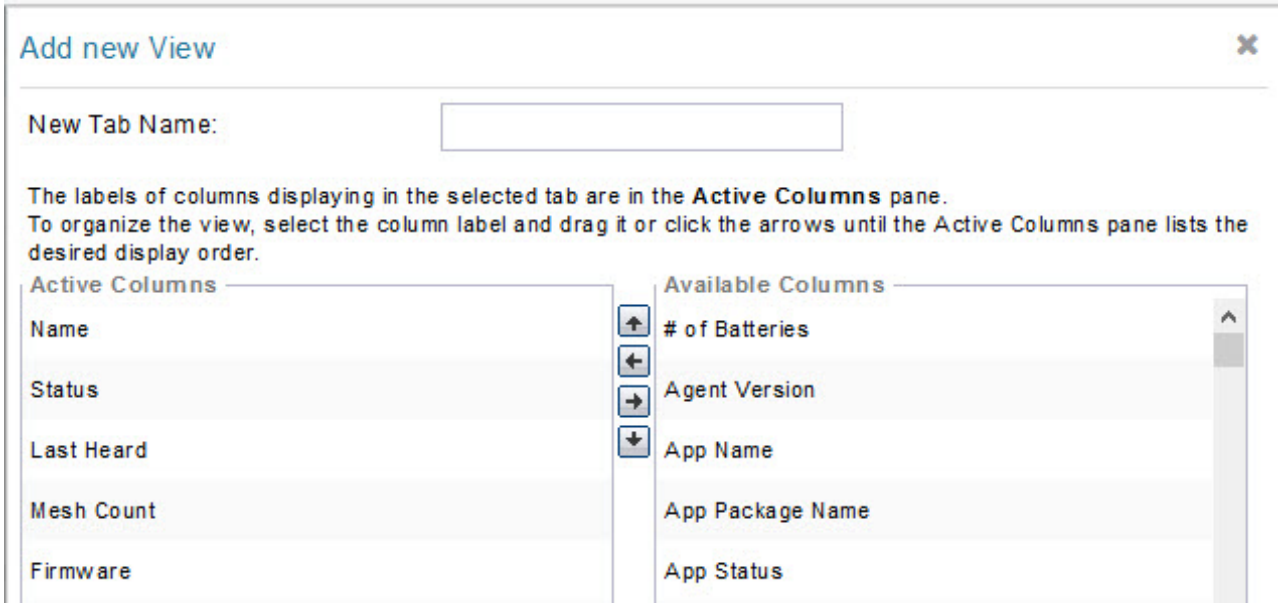
Procedure

Step 1 Click the + icon at the end of the tabs list in the **Field Devices** page.



Once you click the + icon it will display the **Add new View** dialog box.

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



Step 3 Select the properties from the **Available Columns** list and click the left-arrow button, or drag them into the **Active Columns** list to add them.

Table 4: Active and Available Columns

Column Labels Event	Description
Changing the order of column labels.	Use up and down arrow buttons or drag the properties to the desired position to change the column order.
Deleting column labels.	Click the right arrow button or drag properties out of the **Active Columns** list to remove them.
Shifting multiple column labels.	Hold the Shift key to select multiple column labels and move them to either list.

Step 4 Click **Save View**.

Editing Device Views

To edit or delete the device views, navigate to **DEVICES** > **FIELD DEVICES** > **ROUTER**.

Procedure

Step 1 Select the device type in the **Browse Devices** tab.

Step 2 Click the **Inventory** field appearing in the right pane.

There is default drop-down arrow appearing next to the **Inventory** field.

Step 3 Click this default drop-down arrow next to the **Inventory** field. This will open the **Edit/Delete View** dialog box.

Step 4 In the **Edit/Delete View** dialog box:

a) Select the properties from the **Active Columns** list and click the right-arrow button or drag them out to remove from the **Active Columns**.

b) Select the properties from the **Available Columns** to add those properties into the **Active Columns** list and click the left-arrow button, or drag them into the **Active Columns** list.

c) Select the properties from the **Available Columns** list and click the left-arrow button, or drag them into the **Active Columns** list to add them.

d) Use the up and down-arrow buttons or drag the **Active Columns** to change the order.

e) Click the **X** icon to close this view without saving changes.

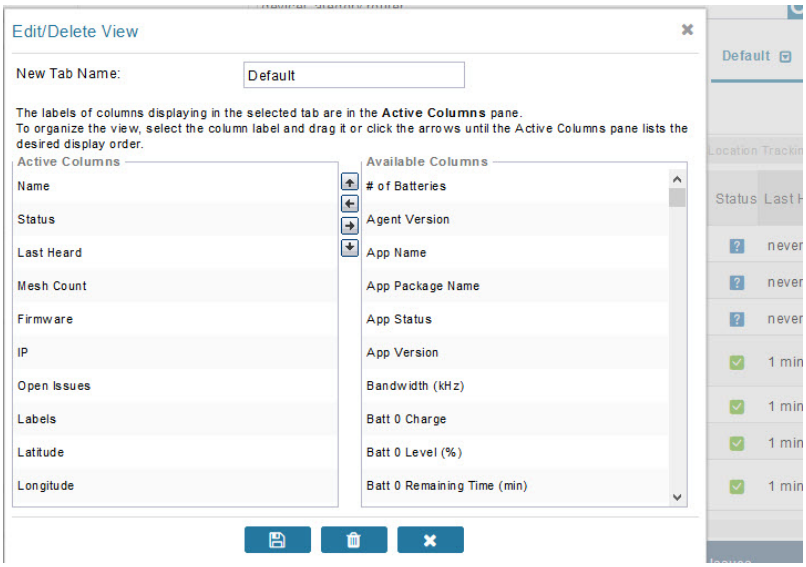
Step 5 Click the disk icon to save the view.

Deleting a Device View

Procedure

Step 1 Select a device type under the **Browse Devices** pane, and click the Default drop-down arrow to open the **Edit/Delete View** dialog box.

Step 2 Click the trash icon to delete the custom view.



Viewing Devices in Map View

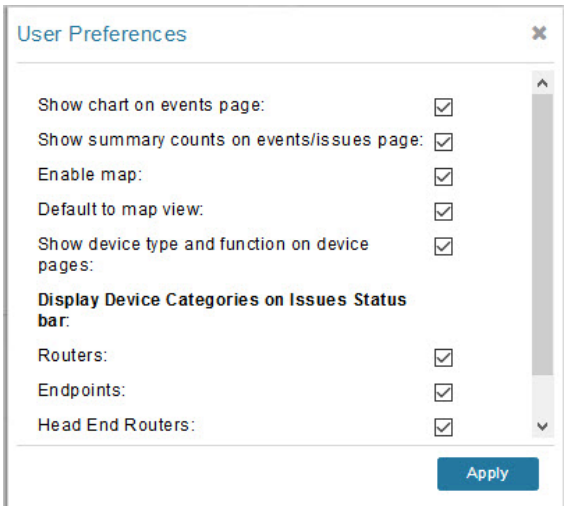
IoT FND provides a map view for visualizing device information based on geographic location. In Map view, IoT FND displays a Geographic Information System (GIS) map and uses GIS Map services to show device icons on the map based on the latitude and longitude information of the device. When this information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

To view devices in Map view:

Procedure

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

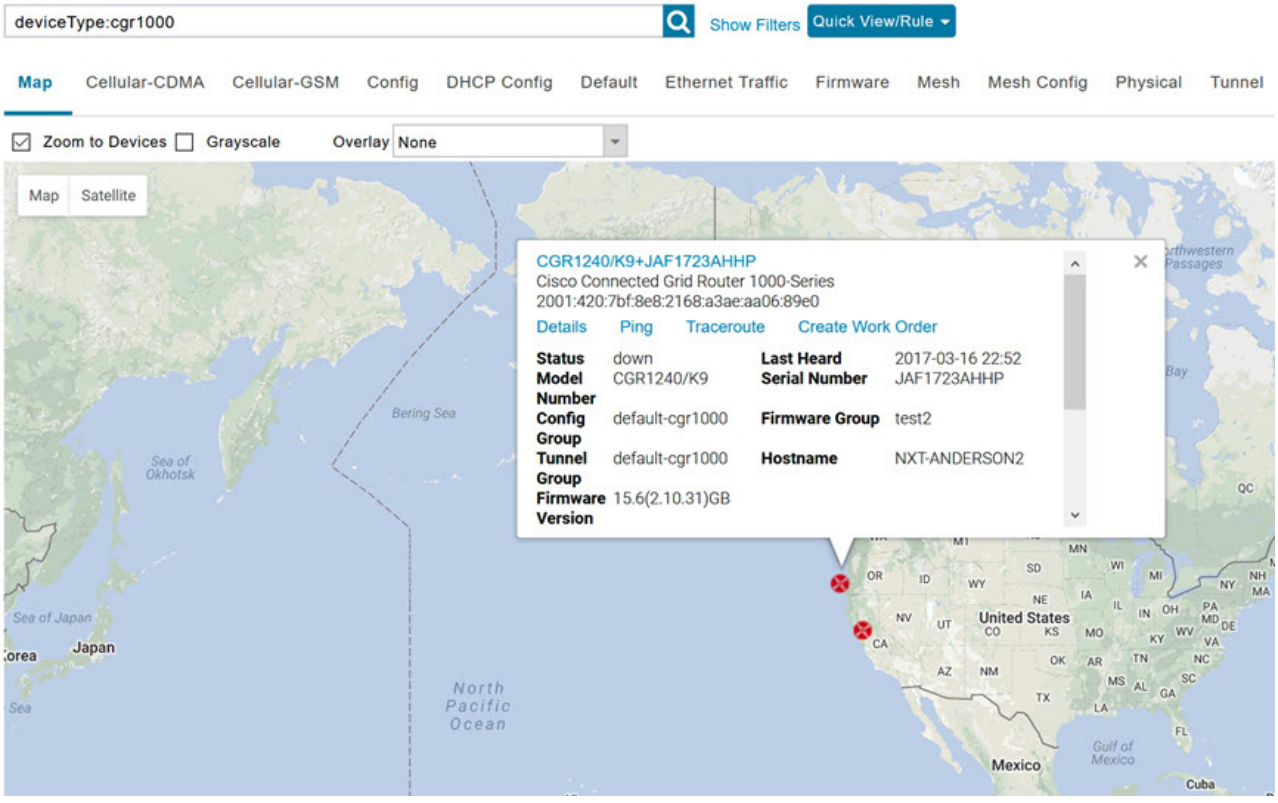
Step 2 Select the **Enable map** check box, and click **Apply**.



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

Step 4 Click the **Map** tab.

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



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

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

To display a subset of all devices, click one of the filters listed in the Browse Devices pane.
IoT FND changes the map region based on your selection and displays the devices found by the filter. For example, you can use the **Routers > Up** filter to display all routers that are up and running. You can also use saved custom filters in the Quick View pane (left pane) to filter the device view. For information about creating custom filters, see Create or Edit Quick View Filters, on page 65.
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.

Step 5 Close the Device popup window to view the RPL tree associated with the device. See Configure RPL tree polling in the Managing System Settings chapter.

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.

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

Configuring Map Settings

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

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

To configure map settings:

Procedure

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

Step 2 Click the **Map** tab.

• To automatically zoom to devices, check the **Zoom to Devices** check box.
• To display the map in grayscale, check the **Grayscale** check box.
Using the Overlay drop-down menu: • For Routers you can overlay: None, All, or Associated Endpoints on the map. • For Endpoints you can overlay: None, All, All Associated Routers, All Modulations, Active Link Type.

To set the map location to open to a certain area, display the area of the map to display by default, and then click **Quick View/Rule**(top of page).

Step 3 Click **OK** .

Changing the Sorting Order of Devices

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

Exporting Device Information

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

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

Procedure

Step 1 Select the devices to export by checking their corresponding check boxes.

Step 2 Click **Export CSV**.

Step 3 Click **Yes** in the confirmation dialog box.

What to do next

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:

Procedure

Step 1 Check the check boxes of the devices to ping.

Note
If the status of a device is Unheard, a ping gets no response.

Step 2 Click **Ping** button in heading above List view entries.

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

Step 3 To close ping display, click X icon.

Tracing Routes to Devices

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



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

To trace routes to selected devices, in List view:

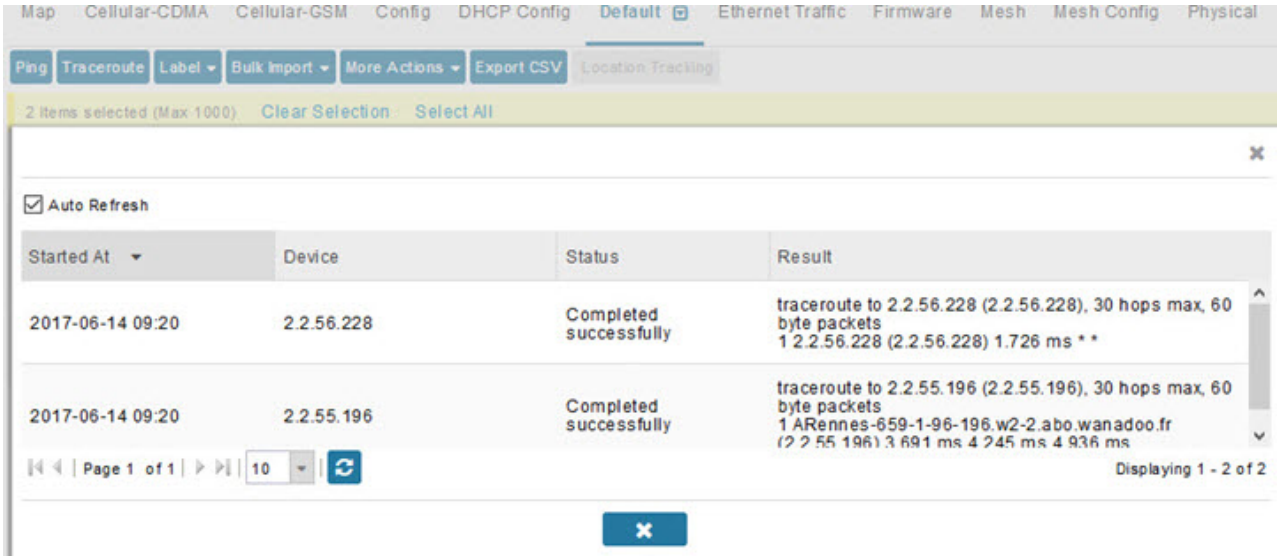
Procedure

Step 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.

Step 2 Click **Traceroute**.

A window displays with the route-tracing results.



Expand the Result column to view complete route information.

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

Step 3 Click X to close the window.

Managing Device Labels

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

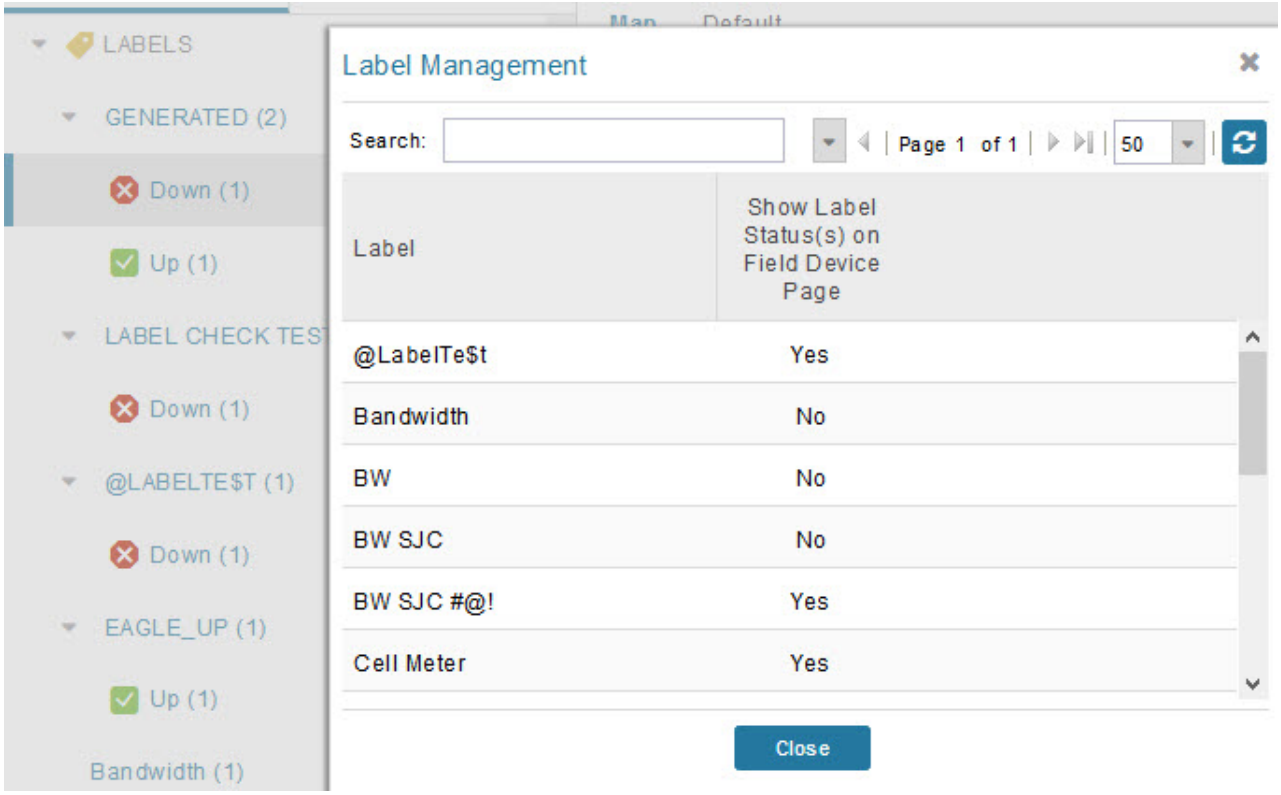
Managing Labels

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

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

Procedure

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



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

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

Step 3 Click **Close**.

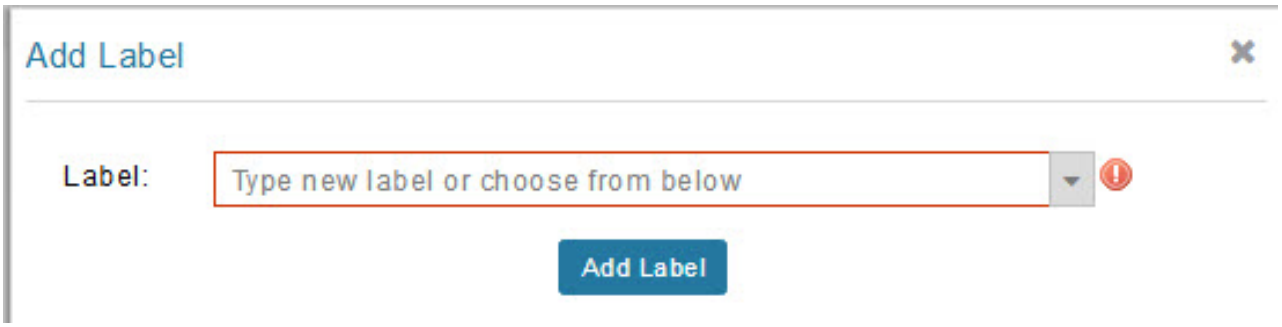
Adding Labels

To add labels to selected devices, in List view:

Procedure

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

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



Step 2 Enter the name of the label or choose an existing label from the drop-down list.

Step 3 Click **Add Label**.

Tip
You can add multiple labels to one device.

Step 4 Click **OK**.

What to do next

To add labels in bulk, see Adding Labels in Bulk, on page 71.

Removing Labels

To remove labels from selected devices, in List view:

Procedure

Step 1 Check the check boxes of the devices from which to remove the label.

Step 2 Choose **Label** > **Remove Label**.

Step 3 Click **OK**.

To remove labels in bulk, see Removing Labels in Bulk, on page 72.

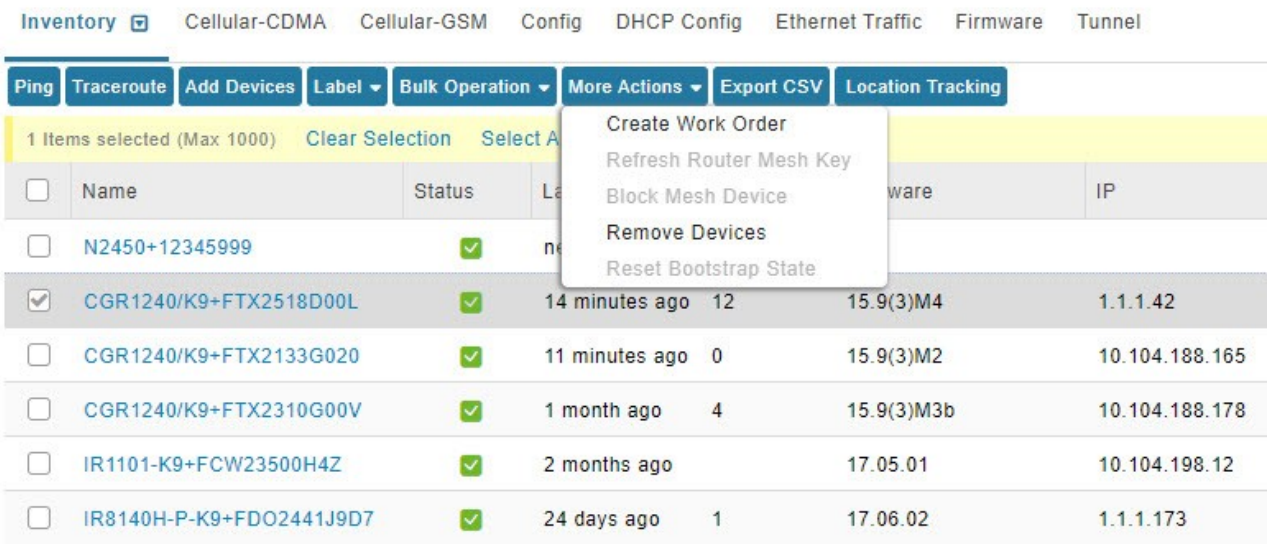
Removing Devices

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

To remove devices, in List view:

Procedure

Step 1 Check the check boxes of the devices to remove.



Step 2 Choose **More Actions** > **Remove Devices**.

Step 3 Click **Yes**.

Displaying Detailed Device Information

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

Detailed Device Information Displayed

- Server Information, on page 60
- Head-end Router, Router, and Endpoint Information, on page 61

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

Server Information

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

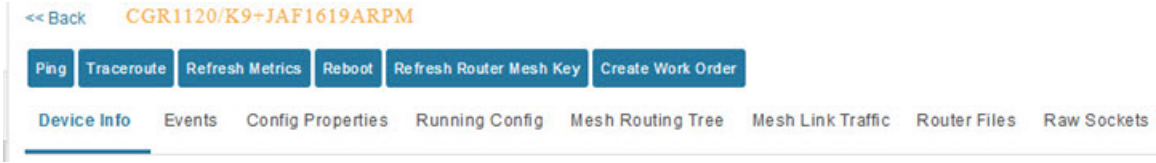
Table 5: NMS Server Pane Areas

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

Head-end Router, Router, and Endpoint Information

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

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



Information Category	Description
Device Info (all)	Displays detailed device information (see Device Properties, on page 127). For routers and endpoints, IoT FND also displays charts (see Viewing Device Charts in the Monitoring chapter of this guide.
Events (all)	Displays information about events associated with the device.
Config Properties (routers, endpoints: meter-cgmesh, gateway-IR500, meter-cellular)	Displays the configurable properties of a device (see Device Properties, on page 127). 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, on page 80.
Running Config (routers)	Displays the running configuration on the device.
Routing Tree (CGR1000, endpoints: gateway-IR500, meter-cgmesh, meter-OW Riva)	Displays the routing tree. For routers, the pane displays all the possible routers from the endpoints to the router. For endpoints, the Routing Tree pane displays the mesh route to the router.
Link Traffic (routers)	Displays the type of link traffic over time in bits per second.
Router Files (routers)	Lists files uploaded to the .../managed/files/ directory.
Raw Sockets (routers)	Lists metrics and session data for the TCP Raw Sockets (see table in the Raw Sockets Metrics and Sessions).
Embedded AP (IR829 only)	Lists inventory (configuration) details and metrics for the attached access point.
AP Running Config (C800 and IR8829 only)	Lists the running configuration file for the attached access point.

Actions You Can Perform from the Detailed Device Information Page



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

Action	Description
Show on Map (C800, endpoints)	Displays a popup window with a map location of the device. This is the equivalent of entering **eid:***Device_EID* in the search field in Map View.
Ping	Sends a ping to the device to determine its network connectivity. See Pinging Devices, on page 55.
Traceroute	Traces the route to the device. See Tracing Routes to Devices, on page 56.
Refresh Metrics (Head-end routers and routers only)	Instructs the device to send metrics to IoT FND. **Note** IoT FND assigns historical values for metrics for each device. To access historical metric values, use the GetMetricHistory North Bound API call.
Reboot	Enables a reboot of the modem on LoRaWAN.
Sync Config Membership (Mesh endpoints only)	Synchronizes the configuration membership for this device. See Synchronizing Endpoint Membership, on page 87.
Sync Firmware Membership (Mesh endpoints only)	Click **Firmware Membership**to synchronize the firmware membership for this device, and then click **Yes** to complete the process.
Block Mesh Device (Mesh endpoints only)	Blocks the mesh endpoint device. **Caution** This is a disruptive operation. **Note** You cannot use Block Mesh Device with the Itron OpenWay RIVA CAM module or the Itron OpenWay RIVA Electric devices and Itron OpenWay RIVA G-W (Gas-Water) devices.
Erase Node Certificates	Removes Node certificates.
Create Work Order (Routers and DA Gateway only)	Creates a work order. See Demo and Bandwidth Operation Modes, on page 123.

Device Filters

Filters in IoT FND are tools that allow users to control which devices are displayed in Map View and List view, making it easier to manage large numbers of devices.

- IoT FND supports up to 10 million devices.
- Filters help users locate and display devices efficiently.
- Filters are available 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 **Inventory** 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. The top-level Endpoints label is selected, which inserts the following built-in filter in the Search Devices field: deviceType:cgmesh firmwareGroup:default-cgmesh.

Add a Filter

Before you begin

- Ensure that you have understood the function of the filter operators before using them.
- If using date fields, ensure that you have the dates formatted as yyyy-MM-dd HH:mm:ss:SSS.

To add a filter to the **Search** field, follow these steps:

Procedure

Step 1 If the **Add Filter** fields are not present under the **Search** field, click **Show Filters**.

Step 2 In the drop-down menu that displays **Label** as the default entry, choose a filter.

These filters apply to all device information categories. For more details about categories, see Working with Router Views, on page 6.

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

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 set the date range for the filter. This table lists the operators you can use to create filters.

Table 6: Filter Operators

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

Step 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.

Step 5 Click the Add (+) button to add the filter to the existing filter syntax in the **Search** field.

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.

Step 6 (Optional) Repeat the process to continue adding filters.

Table 7: Filter Examples

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

What to do next

Create quick view filters using the filter criteria that you added, for easy and quick filtering of devices. See Create or Edit Quick View Filters, on page 65.

Create or Edit Quick View Filters

Use the quick view filter to display devices that match your search criteria in the **Quick View** pane. You can create, edit, or manage quick view filters to control which devices appear on the **Devices** page.

Before you begin

- Before creating a quick view filter, filter devices by your chosen criteria. For details on filtering devices, refer to Filter Devices.
- You can create quick view filters for devices in **Devices** > **Field Devices** and **Devices** > **Head-End Routers** pages.

Procedure

Step 1 On the **Field Devices** or **Head-End Routers** page, click **Show Filters**, select your criteria, and start a search.

Step 2 When you see the filtered results, click the **Quick View/Rule** drop-down menu and select **Create Quick View**.

Step 3 In the **Create Quick View** modal, review your search query, enter a filter name, and click the disk icon to save the quick view filter.

Your new quick view filter appears in the **Quick Views** tab.

Step 4 To edit a quick view filter, select the filter in the **Quick Views** tab and click the **Quick View/Rule** drop-down menu.

Step 5 Select **Edit Quick View**. In the **Update Quick View** modal, make your changes and save.

To remove a quick view filter that you no longer need, click the delete icon.

Performing Bulk Import Actions

In IoT FND, you can perform the bulk import device actions.

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

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

To add devices in bulk:

Procedure

Step 1 On any Device page (such as **DEVICES** > **FIELD DEVICES**), choose **Add Devices** .

Step 2 In the Add Devices window, click **Browse** to locate the CSV file containing the device information to import, and then click **Add** .

Note
IoT FND will allow to select only CSV or XML files from the system and the file with other extension will be in disabled state.

IoT FND will not allow you to upload file names with special characters such as &,<,>,",',`,\,/,=,{,},[,],(,),%, and ;.

For more information about adding gateways, see Adding an IC3000 Gateway, on page 67

For more information about adding HERs, see Adding HERs to IoT FND, on page 67

For more information about adding routers, see Adding Routers to IoT FND, on page 68

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

Step 3 Click **Add** .

Step 4 Click **Close** .

Adding an IC3000 Gateway

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

```
eid,deviceType,lat,lng,IOxUserName,IOxUserPassword
IC3000+FOC2219Y47Z,ic3000,10,10,system,
r6Bx/jSWuFi2vs9U1Zh21NSILakPJNwS1CY/jQBYYRcxSH8qLpgUtOn7nqywr/
vOkVPYbNPAFXj4Pbag6m1spjZLR6oc1PkT9eF6108frFXy+
eI2FFaUZlSCKTdjSqfur5EwEu1E5u54ckMi1e07X8INZuNdFNFU7ZgElt3es8yrpR3i/
EgDOdSb5dqw0u3lOeVrEtPY0xBHraYgPv+dBh3XtW4i2Kv/sveiTBPx2FiNRvuLWil7Qm+
D7bl1Fh4ZJCivapy7EYZirwHHAVJlQh6bWYrGAccNPkY+KqIZDCyX/
Ck5psmgzyAHKmj8Dq7K0nBsnq2+b2VKReEhsj9+Fw==
```

Adding HERs to IoT FND

Configuring HERs Before Adding them to IoT FND

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

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

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

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

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

Adding HERs

To add HERs, create a CSV file that consists of a header line followed by one or more lines, each representing an HER.

The below table describes the fields to include in the CSV file.



Note For device configuration field descriptions, see Device Properties, on page 127

Table 8: 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, *HER_PID +HER_SN*).
deviceType	The device type must be asr1000 or isr3900.
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.

Adding Routers to IoT FND

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

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

Note For a list of all Device Properties that you can configure using the XML configuration template go to Device Properties, on page 127.

The Router Import Fields table describes the router properties defined in the <R> record used in this example:

Table 9: Router Import Fields

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

Mapping Routers to HERs

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

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

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

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

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

For example:

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

Adding Router-to-HER Mappings to a CSV File

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

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

Removing Devices in Bulk

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

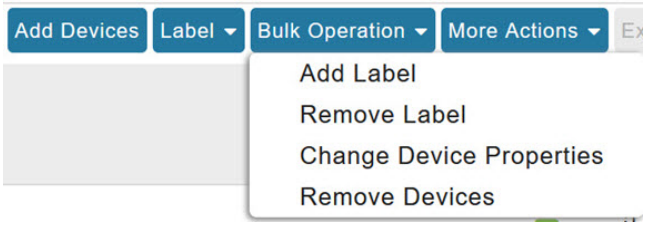
Caution When you remove routers, IoT FND returns all the leased IP addresses associated with these devices to CNR and removes the corresponding tunnels from the HERs.

To remove devices in bulk:

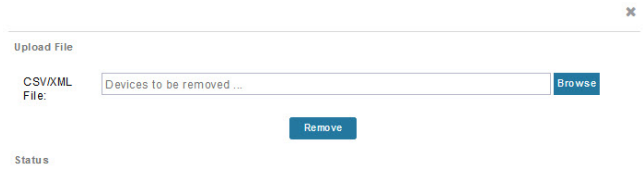
Procedure

Step 1 Choose **Devices** > *Device Type*.

Step 2 Choose **Bulk Operation** > **Remove Devices**.



Step 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
```

Step 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.

Step 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:

Procedure

Step 1 On any device page, choose **Bulk Operation** > **Change Device Properties**.

Step 2 Click **Browse** to locate the CSV containing the list of devices and corresponding properties to configure, and then click **Open**

Step 3 Click **Change**.

Step 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:

Procedure

Step 1 On any device page, choose **Bulk Operation** > **Add Label**.

Step 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
```

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

Step 4 Click **Add Label**.

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

Step 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:

Procedure

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

What to do next

From the drop-down list, choose the label to remove.

Configuring Rules

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

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

When working with rules, you can do the following:

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

Viewing and Editing Rules

To view rules:

Procedure

Step 1 Choose **CONFIG > Rules**.

IoT FND displays the list of rules stored in its database. The Rule field describes the fields displayed in the list.

Field	Description
Name	The name of the rule.
Active?	Whether the rule is active. Rules are not applied until you activate them.
Rule definition	The syntax of the rule. Some examples are listed below. • IoT FND executes this rule when a device battery 0 level drops below 50%: `battery0Level<50` • `deviceType:cgmesh eventName:up` • `deviceType:ir500 eventName:outage`
Rule Actions	The actions performed by the rule. For example: `Log Event With: CA-Registered, Add Label: CA-Registered` In this example, the actions: • 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.

Step 2 To edit a rule, click its name.

For information on how to edit rules, see Creating a Rule, on page 73

Creating a Rule

To add a rule:

Procedure

Step 1 Choose **CONFIG** > **Rules**.

Step 2 Click **Add**.

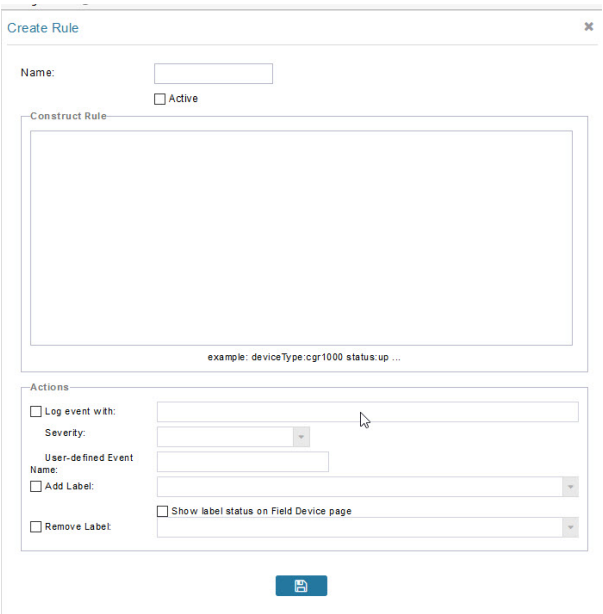
Step 3 Enter a name for the rule.

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.

Step 4 To activate the rule, check the **Active** check box.

Step 5 In the Construct Rule panel, enter the syntax of the rule.

Use the same syntax used for creating filters. See Search Syntax.



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

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

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

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

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

Add Label — Enter the name of a new label or choose one from the **Add Label** drop-down menu.

Show label status on Field Devices page — Shows the status of the device that triggered this rule in the LABELS section of the Browse Devices pane.

Remove Label — Choose the label to remove from the **Remove Label** drop-down menu.

Step 7 Click the disk icon to **Save changes**.

Activating Rules

IoT FND only applies rules that you activate.

To activate a rule:

Procedure

Step 1 Choose **CONFIG** > **Rules**.

Step 2 Check the check boxes of the rules to activate.

Step 3 Click **Activate**.

Step 4 Click **Yes** to activate the rule.

Step 5 Click **OK**.

Deactivating Rules

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

To deactivate rules:

Procedure

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

Deleting Rules

To delete rules:

Procedure

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

Configuring Devices

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

- Configuring Device Group Settings, on page 77
- Editing the ROUTER Configuration Template, on page 88
- Editing the ENDPOINT Configuration Template, on page 91
- Pushing Configurations to Routers, on page 93
- Pushing Configurations to Endpoints, on page 95

Configuring Device Group Settings

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

Creating Device Groups

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

Group Name	Description
Default-act	By default, all Itron OpenWay RIVA Electric devices (ENDPOINT) are members of this group. • Individual RIVA electric devices listed under the Group heading display as OW Riva CENTRON.
Default-bact	By default, all Itron OpenWay RIVA G-W (Gas-Water) devices (ENDPOINT) are members of this group. • Individual RIVA water meters listed under the Group heading display as OW Riva G-W. • Individual RIVA gas meters listed under the Group heading display as OW Riva G-W.
Default-cam	By default, all Itron OpenWay RIVA CAM modules (ENDPOINT) are members of this group. • Individual RIVA CAM modules listed under the CAM heading display as OW Riva CAM.
Default-c800	By default, all C800s, and ISRs (ROUTER) are members of this group.
Default-ir800	By default, all IR807s, IR809s, and IR829s (ROUTER) are members of this group.
Default-cgmesh	By default, all crmesh endpoints (ENDPOINT) are members of this group.
Default-cgr1000	By default, all CGRs (ROUTER) are members of this group.
Default-sbr	By default, all ESRs (ROUTER) are members of this group. This product is also identified as C5921.
Default-ir500	By default, all IR500s (ENDPOINT) are members of this group.
Default-lorawan	By default all LoRaWAN Gateways (IOT GATEWAY) are members of this group.
Default-ir1100	By default, all IR1100 (ROUTER) are members of this group.
Default-ir8100	By default, all IR8100 (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.

- Creating ROUTER Groups, on page 78
- Creating Endpoint Groups, on page 79

Creating ROUTER Groups

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

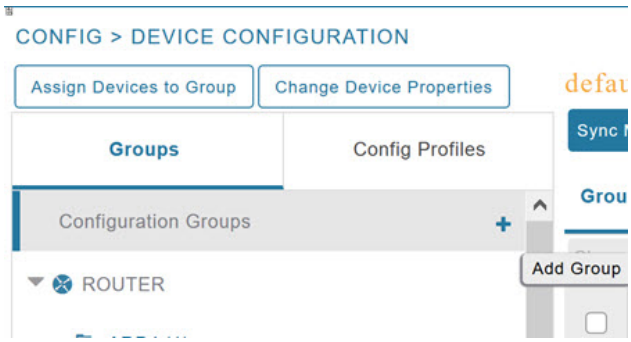
To create a router configuration group:

Procedure

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

Step 2 Select the default configuration group: **Default-cgr1000**, **Default-ir800**, **Default-c800**, or **Default-sbr**.

Step 3 With the Groups tab selected (top, left pane of page), click the + icon (under the heading) to open the **Add Group** entry panel.



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

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

Step 5 Click **Add**.

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

What to do next

- To change the name of a group, see Renaming a Device Configuration Group, on page 83
- To remove a group, see Deleting Device Groups, on page 84

Creating Endpoint Groups

To create an endpoint configuration group:

Procedure

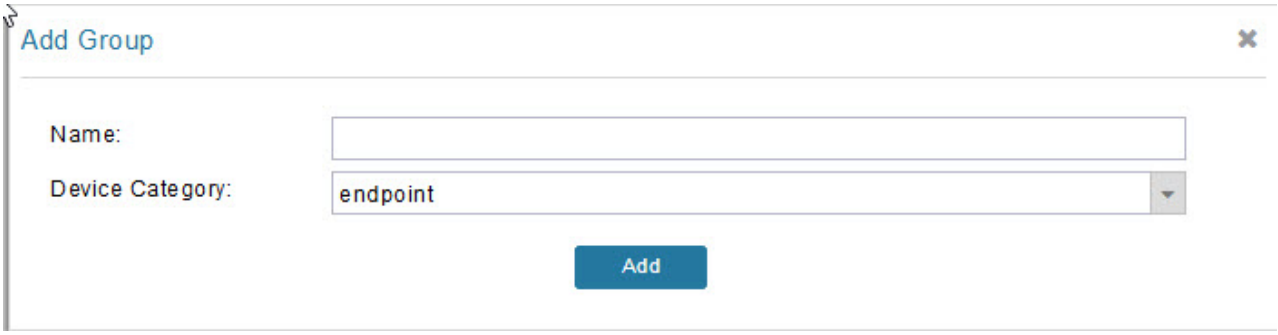
Step 1 Choose **CONFIG** > **Device Configuration**.

Step 2 Select the default group (Default-act, Default-bact, Default-cam, Default-cgmesh, Default-ir500).

Step 3 With the Groups tab selected (top, left panel of page), click the + icon (under the heading) to open the **Add Group** entry panel.

Note
The device category (such as endpoint or router) auto-populates.

Step 4 Enter a name for the group. The device category (endpoint, gateway, or router) auto-populates.



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

Step 5 Click **Add**.

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

What to do next

- To change the name of a group, see Renaming a Device Configuration Group, on page 83

- To remove a group, see Deleting Device Groups, on page 84

Changing Device Configuration Properties

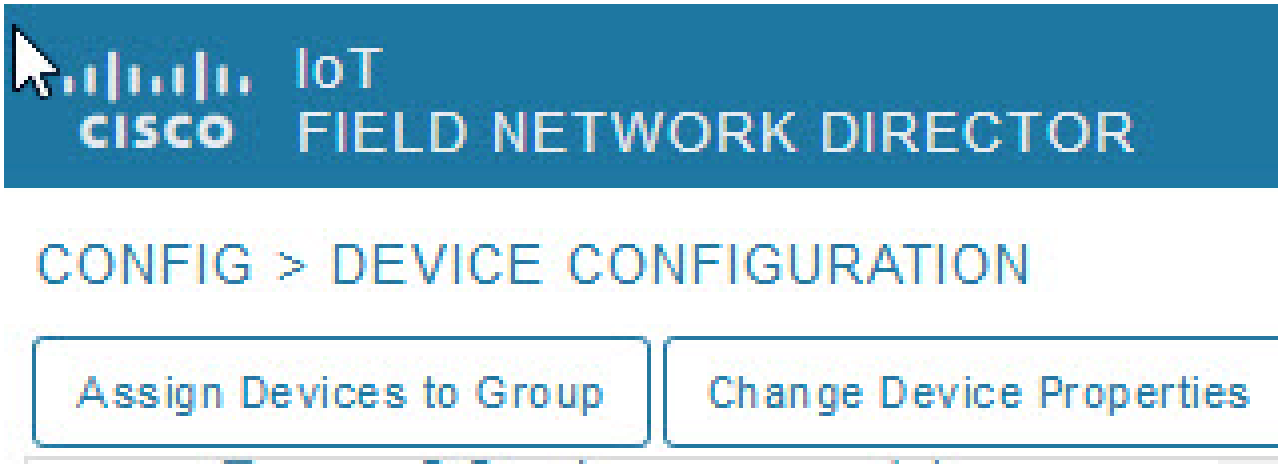
You can change the configurable properties of devices by uploading a Device Properties CSV file with modified values for the devices.

To change device configuration properties:

Procedure

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

Step 2 Click **Change Device Properties**.



Step 3 Click **Browse** and select the Device Properties CSV or XML file to upload

Step 4 Click **Change**.

Step 5 Click **Close** when done.

For a list of configurable device properties in IoT FND, see Device Properties, on page 127.

Configuring Periodic Inventory Notification and Mark-Down Time

This section explains how to configure the periodic inventory timer and heartbeat notification in the **Edit Configuration Template** tab, and mark the device downtime in the **Group Properties** tab for a specific router or endpoint configuration group.

- Configuring Periodic Inventory Timer
- Configuring Heartbeat Notification
- Configuring the Mark-Down Timer

Configuring Periodic Inventory Timer

To configure the periodic inventory timer for a ROUTER configuration group:

Procedure

Step 1 Click **CONFIG** > **DEVICE CONFIGURATION**.

Step 2 Select a ROUTER configuration group from the left pane.

Step 3 Click **Edit Configuration Template** to configure the periodic inventory notification interval in the template. The default periodic inventory notification interval is 360 minutes.

```
<#-- Enable periodic inventory notification every 6 hours to report metrics. -->
callhome
  periodic-inventory notification frequency 360
exit
```

For example, to enable periodic inventory notification to report metrics every 60 minutes, add the following lines to the template:

```
<#-- Enable periodic inventory notification every 1 hour to report metrics. -->
periodic-inventory notification frequency 60
exit
```

Step 4 Click the disk icon to save the changes.

Configuring Heartbeat Notification

To configure the heartbeat notification for a ROUTER configuration group:

Procedure

Step 1 Click **CONFIG** > **DEVICE CONFIGURATION**.

Step 2 Select a ROUTER configuration group from the left pane.

Step 3 Click **Edit Configuration Template** to configure the heartbeat notification interval in the template. The default notification interval is 60 minutes.

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

For example, if you want to enable the heartbeat notification for every 120 minutes, then add the following lines to the template:

```
<#-- Enable periodic configuration (heartbeat) notification every 2 hours.
periodic-configuration notification frequency 120
```

Step 4 Click the disk icon to save the changes.

Configuring Mark-Down Timer

The **Group Properties** page allows you to set the mark-down timer value for a default or user-defined configuration group of a router, endpoint, or gateway. The mark-down timer value that you set must be greater than the heartbeat value defined in the Edit Configuration Template.

Based on the heartbeat value received from the device every few minutes, IoT FND updates the last heard value of the device in the Device Info page (**DEVICES** > **Field Devices** > **ROUTER**).

If the last heard value is greater than the device mark-down value, then IoT FND marks the device state as *Down* in the IoT FND GUI. However, before marking the device *Down*, IoT FND must check the status of the tunnel interface that is associated with the device. If the tunnel interface is *Down* as well, then IoT FND marks the device state as *Down*. If the tunnel interface state is Up, then IoT FND must wait until the tunnel interface state goes *Down* as well before marking the device as *Down* in the IoT FND GUI.

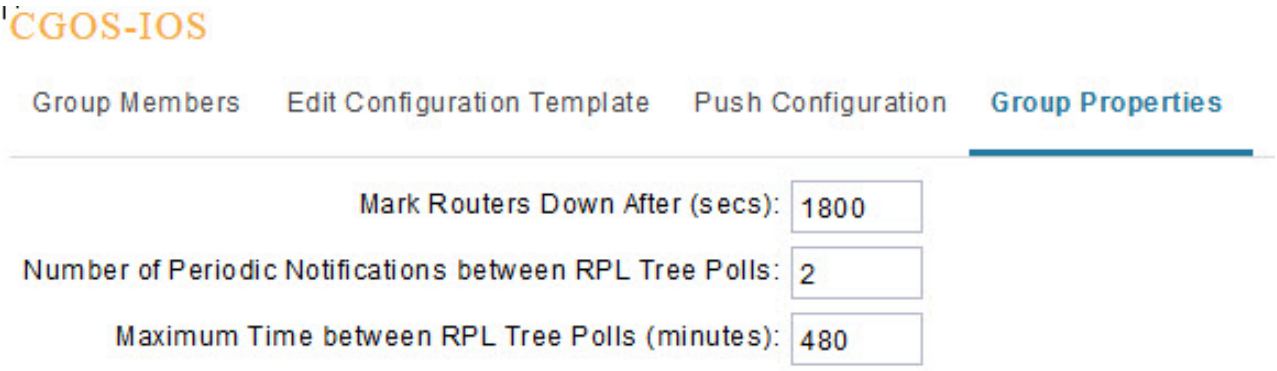
To configure the mark-down timer for a ROUTER configuration group:

Procedure

Step 1 Click **CONFIG** > **DEVICE CONFIGURATION**.

Step 2 Select a ROUTER configuration group from the left pane.

Step 3 Click **Group Properties**.



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

Step 4 In the **Mark Routers Down After** field, enter the number of seconds after which the IoT FND marks the device *Down* if it does not receive the heartbeat value from the device during the specified heartbeat time interval.

Note
Ensure that the periodic configuration notification frequency in the configuration template is less than the value you entered in the **Mark Routers Down After** field. We recommend 1:3 ratio of heartbeat interval to mark-down timer. For more information on configuring the heartbeat interval, refer to Configuring Heartbeat Notification , on page 81.

Step 5 Click the disk icon to **save changes**.

Renaming a Device Configuration Group

To rename a device configuration group:

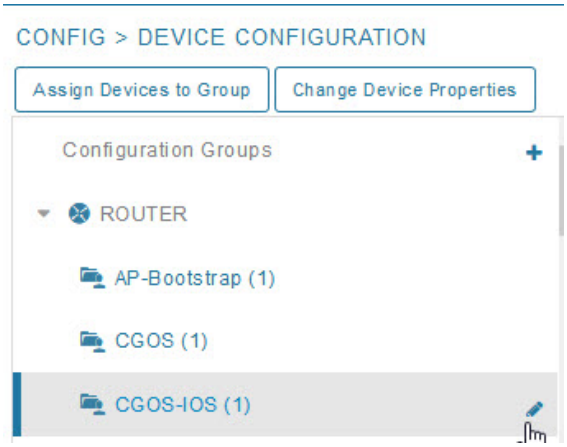
Procedure

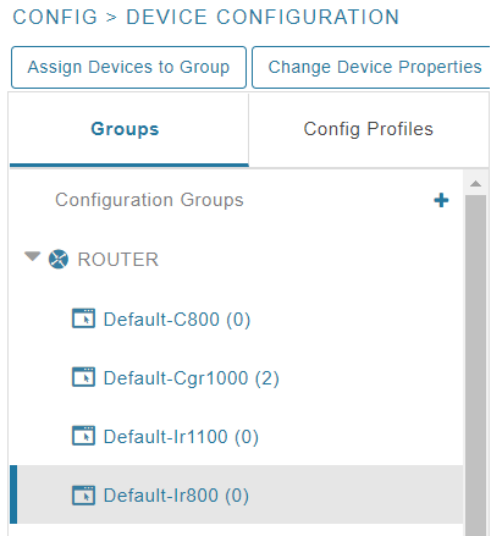
Step 1 Choose **CONFIG** > **Device Configuration**.

Step 2 Select a group from the list of configuration groups (left pane).

Step 3 Hover over the name of the group in the list. A pencil icon appears.

Step 4 Click the pencil icon to open the **Edit Group** panel.





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

Note

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

Deleting Device Groups



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

To delete a configuration group:

Procedure

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

Step 2 Select a group from the list of configuration groups (left pane)

Step 3 Ensure that the group is empty.

Step 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.

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

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

To move devices to another configuration group:

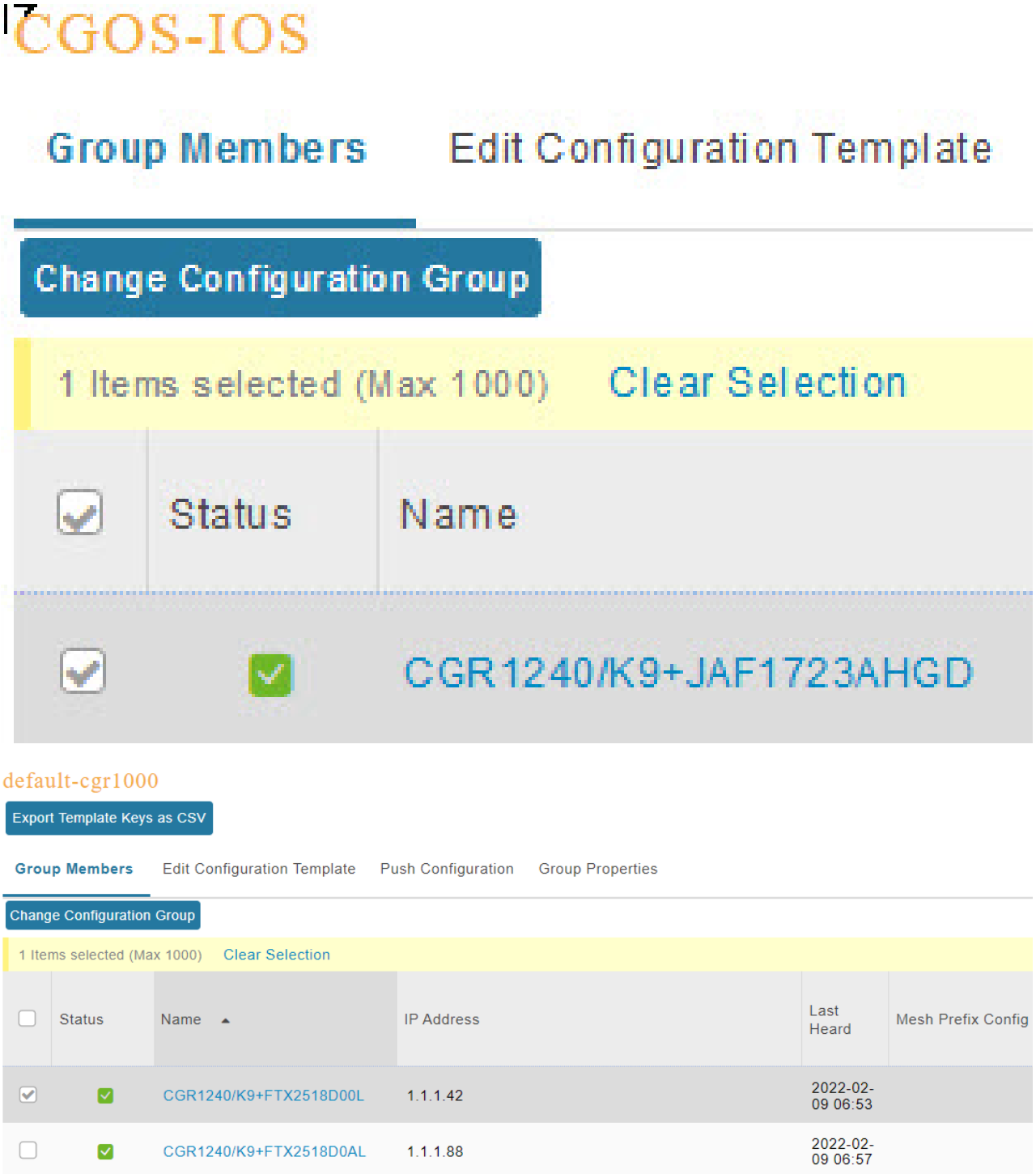
Procedure

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

Step 2 Select a group from the list of configuration groups (left pane).

Step 3 Select the check box of the devices to move.

Step 4 Click **Change Configuration Group**.



Step 5 From the drop-down menu in the dialog box, choose the target group for the devices.

Step 6 Click **Change Config Group**.

Step 7 Click **OK**.

Moving Devices to Another Configuration Group in Bulk

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

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

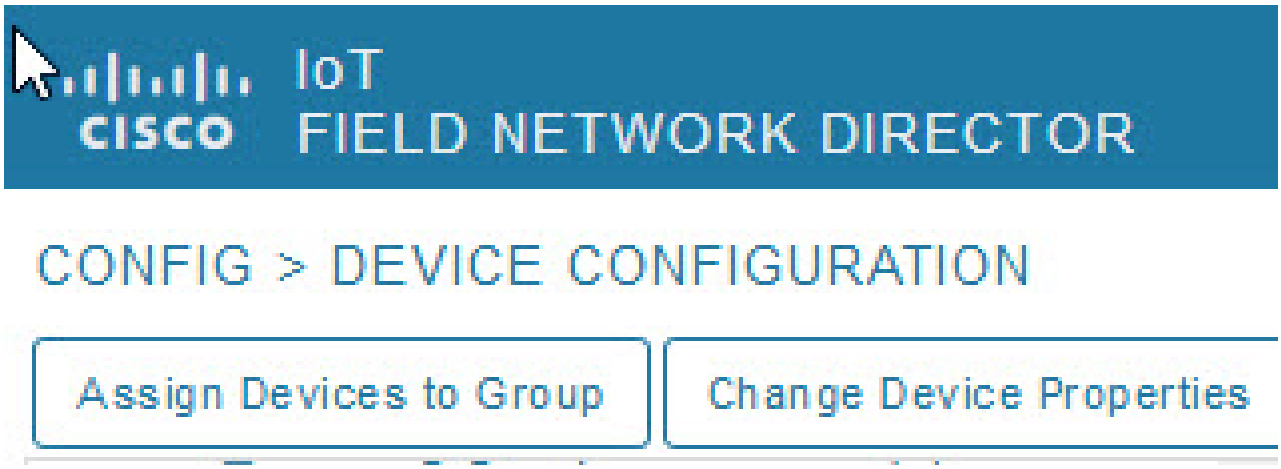
```
eid
CGR1120/k9+JS1
CGR1120/k9+JS2
CGR1120/k9+JS3
```

To move devices to another configuration group in bulk:

Procedure

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

Step 2 Click **Assign Devices to Group**.



Step 3 Click **Browse** to locate the CSV or XML file containing the list of devices to move, and then click **Open**.

Step 4 From the Group drop-down menu, choose the target group for the devices.

Step 5 Click **Assign to Group**.

Step 6 Click **OK**.

Listing Devices in a Configuration Group

To list the devices in a configuration group:

Procedure

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

Step 2 Select a group from the list of configuration groups (left pane).

Step 3 To get more information about a device in the list, click its EID (for example: CGR1240/K9+JAF1723AHGD)

Synchronizing Endpoint Membership

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

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

To send group information to endpoints:

Procedure

Step 1 Choose **CONFIG** > **Device Configuration**

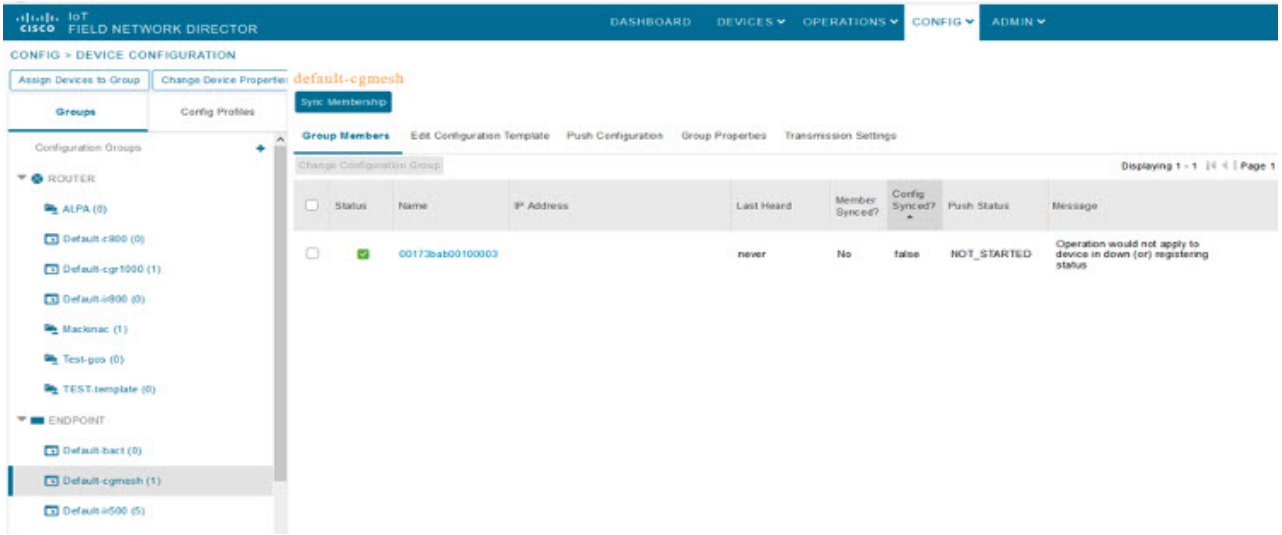
Step 2 Select an ENDPOINT group (left pane) such as Default-cgmesh.

Step 3 Select the Group Members tab (right pane), click on the name of an endpoint. (Note: The Group Members tab is a new addition to this page).

Step 4 Click **Sync Config Membership button on the page that appears**.

Step 5 When prompted, click Yes to confirm synchronization.

Step 6 Click **OK**.



Editing the ROUTER Configuration Template

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

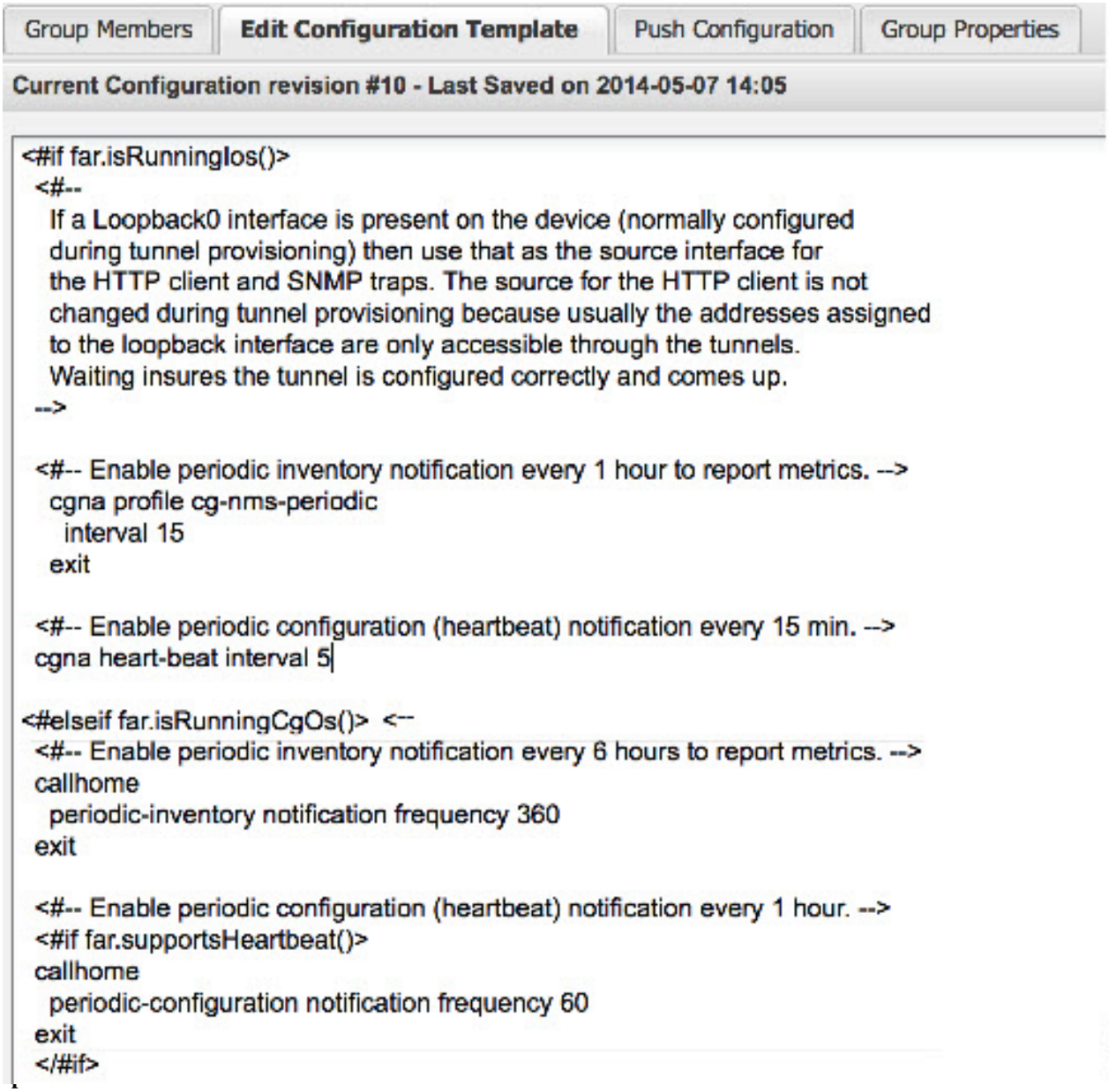
To edit a ROUTER group configuration template:

Procedure

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

Step 2 Under CONFIGURATION GROUPS (left pane), select the group with the template to edit.

Step 3 Click **Edit Configuration**



Step 4 Edit the template.

The template is expressed in FreeMarker syntax

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

Step 5 Click **Save Changes**.

What to do next

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

Editing the AP Configuration Template

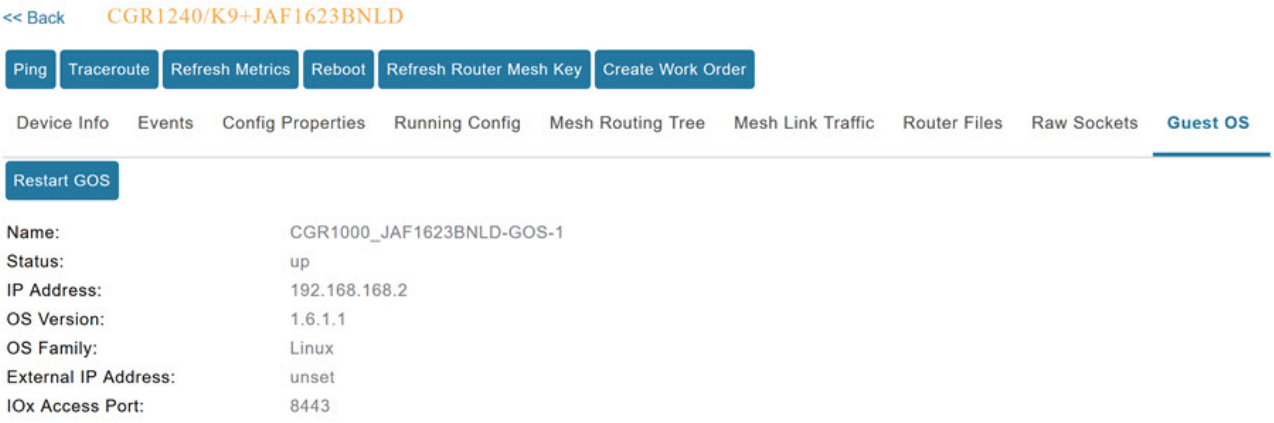
To edit an AP group configuration template:

Procedure

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

Step 2 Under CONFIGURATION GROUPS (left pane), select the C800 device group with embedded AP devices with the template to edit.

Step 3 Click **Edit AP Configuration Template**.



Step 4 Edit the template.

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

AP TEMPLATE EXAMPLE

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

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

.

Step 5 Click **Save Changes**.

What to do next



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

Editing the ENDPOINT Configuration Template

To edit an ENDPOINT configuration template:

Procedure

Step 1 Choose **CONFIG** > **Device Configuration**

Step 2 Under CONFIGURATION GROUPS (left pane), select the **ENDPOINT group** with the template to edit

Step 3 Click **Edit Configuration Template**.

Step 4 Edit the template.

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

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

• **Report Interval**: The number of seconds between data updates.
• **BBU Settings**: Enable this option to configure BBU Settings for range extenders with a battery backup unit.
• **Enable Ethernet**: Check this check box to enable Ethernet for selected devices or configure NAT 44 settings on selected DA Gateway devices.
Note For NAT 44 configuration, you must specify values for all three fields in a CSV file. The default values are 127.0.0.1, 0, 0, respectively. You do not need to configure any other settings for a particular map index. If these settings are invalid for that map index, they are ignored during a configuration push.
• **MAP-T Settings**: The IPv6 and IPv4 settings for the device.

Note For Cisco IOS CGRs, MAP-T rules are set by indicating the MAP-T IPv6 basic mapping rule (BMR), IPv4 BMR, and IPv6 default mapping rule (DMR). On Cisco IR509 devices, the MAP-T IPv6 is an IPv6 prefix that integrates the MAP-T BMR IPv6 rules, IPv4 suffix value, and length being based on the BMR EA length value.
• **Serial Interface 0 (DCE)Settings**: The data communications equipment (DCE) communication settings for the selected device.
Note There can be only one session per serial interface. You must configure the following parameters for all TCP Raw Socket sessions (for each virtual line and serial port) for the selected DA Gateway device(s):
• Initiator – Designates the device as the client/server
• TCP idle timeout (min) – Sets the time to maintain an idle connection.
• Local port – Sets the port number of the device
• Peer port – Sets the port number of the client/server connected to the device.
• Peer IP address – Sets the IP address of the host connected to the device.
• Connect timeout – Sets the TCP client connect timeout for Initiator DA Gateway devices.
• Packet length – Sets the maximum length of serial data to convert into the TCP packet.
• Packet timer (ms) – Sets the time interval between each TCP packet creation.
• – Special Character – Sets the delimiter for TCP packet creation.
• **Serial Interface 1 (DTE) Settings**: The data terminal equipment (DTE) communication settings for the selected device.
Note The IPv6 prefix must valid. Maximum prefix lengths are:
• IPv6: 0–128
• IPv4: 0–32

Step 5 Click **Save Changes**.

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

.

Pushing Configurations to Routers

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

To push the configuration to routers:

Procedure

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

Step 2 Select the group or subset of a group to push the configuration to the **Configuration Groups** pane.

Step 3 Click the **Push Configuration** tab to display that window.

Step 4 In the **Select Operation** drop-down list, choose **Push ROUTER Configuration**.

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

Step 5 In the Select Operation drop-down list, choose **Push ENDPOINT Configuration** .

Step 6 Click **Start**.

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

In the Status column, one of these values appears:

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

What to do next



Note 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

Procedure

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

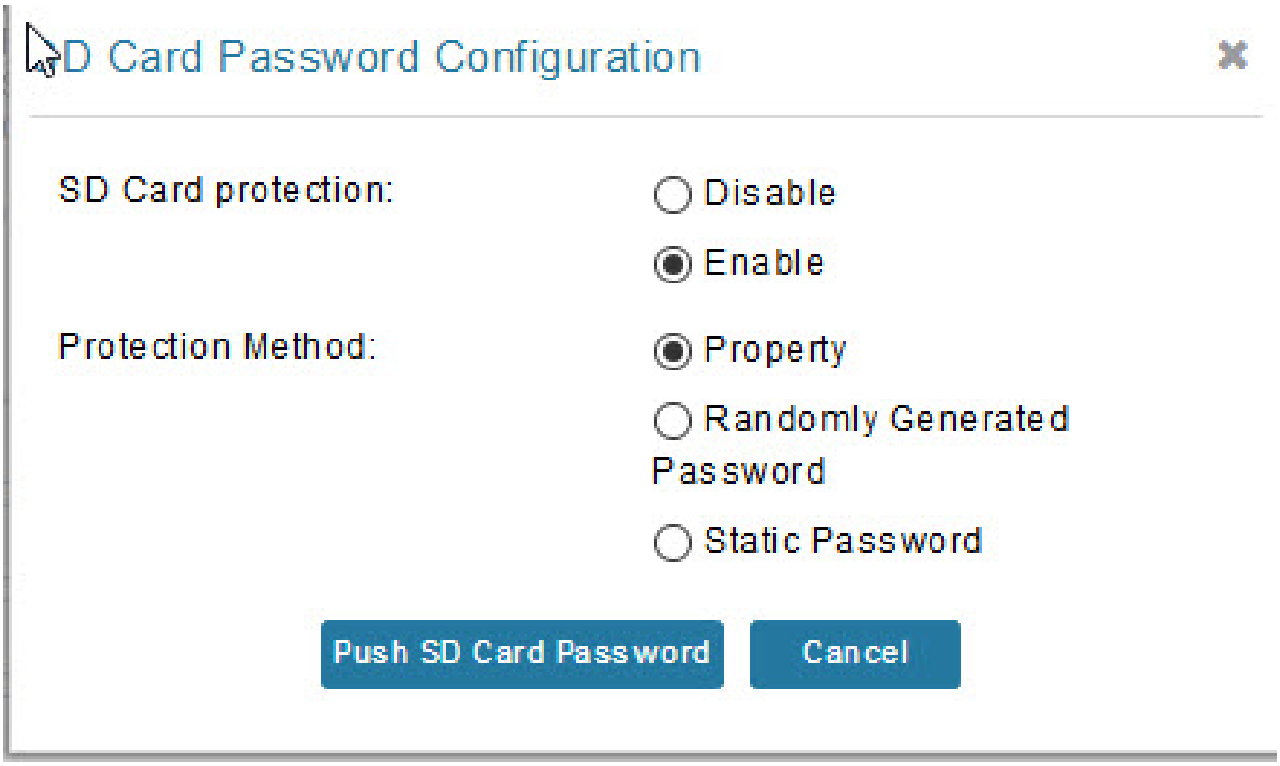
Step 2 Select the CGR group or CGRs to push the configuration to in the Configuration Groups pane

Step 3 Select the **Push Configuration** tab.

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

Step 5 Click **Start**. Click **Yes** to confirm action or No to stop action.

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



Step 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.

Step 8 Click **Push SD Card Password**.

Pushing Configurations to Endpoints

To push configuration to mesh endpoints:

Procedure

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

Step 2 Select the group or subset of a group to push the configuration to the ENDPOINT list.

Step 3 Click the **Push Configuration** tab.

Note
The **Push Configuration** tab supports a subnet view for crmesh endpoints that summarizes:

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

Step 4 In the **Select Operation** drop-down list, choose **Push ENDPOINT Configuration**.

Step 5 Click **Start**. Confirm action by clicking the **Yes** button or stop the action by clicking the **No** button.

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

In the Status column, one of these values appears:

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

What to do next

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

Certificate Re-Enrollment for ITRON30 and IR500

After endpoints have completed initial enrollment and joined the mesh network, the endpoints may must re-enroll the Utility IDevID and/or the LDevID due to certificate expiration or proactive refresh of the certificates. You can select the appropriate certificate and the supported device types from the following:

Supported Devices:

- IR510 and IR530 (Added in FND 4.7)
- ITRON30 (Added in FND 4.7)

Certificates:

- Get NMS Cert and NPS/AAA Cert
- LDevID Certificate
- IDevID Certificate

The message is sent as a unicast. (Multicast is not supported).

Re-enrollment can be triggered on demand or automatically based on the predefined policy. You can review the status of re-enrollment of a device on the Device Details page for a single device or the Device Configuration page for a group of devices by selecting the **Push Configuration** tab.

Beginning with IoT FND Release 4.7, Certificate Re-enrollment is supported for ITRON30 and IR500 devices:

- Devices page — Figure 6: DEVICES > FIELD DEVICES > Endpoint Re-Enrollment (1 of 2), on page 97
- Device Configuration page — Figure 8: CONFIG > DEVICE CONFIGURATION > Endpoint Certificate Re-enrollment, on page 98
- DTLS Relay Settings — Figure 9: Support for DTLS Relay Settings and Cert Auto-Renew Settings for ITRON30 and IR500 Devices, on page 99
- Additionally, Certificate Information is provided for IR500s — Figure 10: Certificate Information for IR500, on page 99

Figure 6: DEVICES > FIELD DEVICES > Endpoint Re-Enrollment (1 of 2)

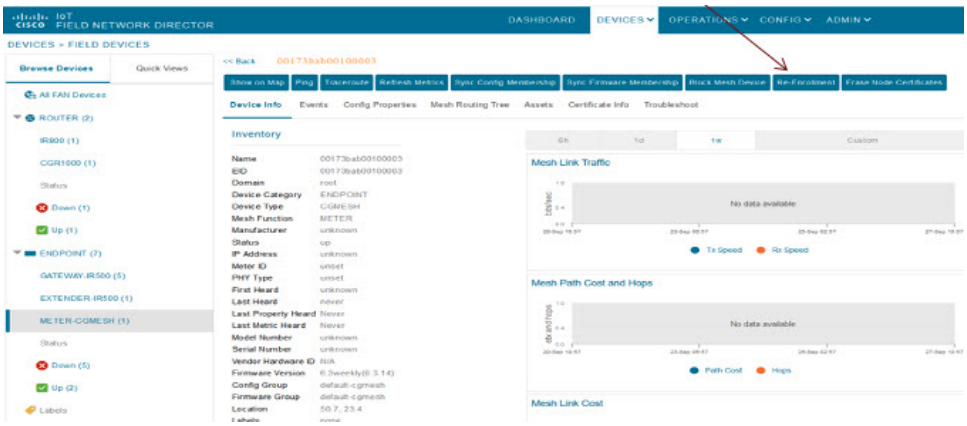


Figure 7: DEVICES > FIELD DEVICES > Endpoint Re-Enrollment (2 of 2)

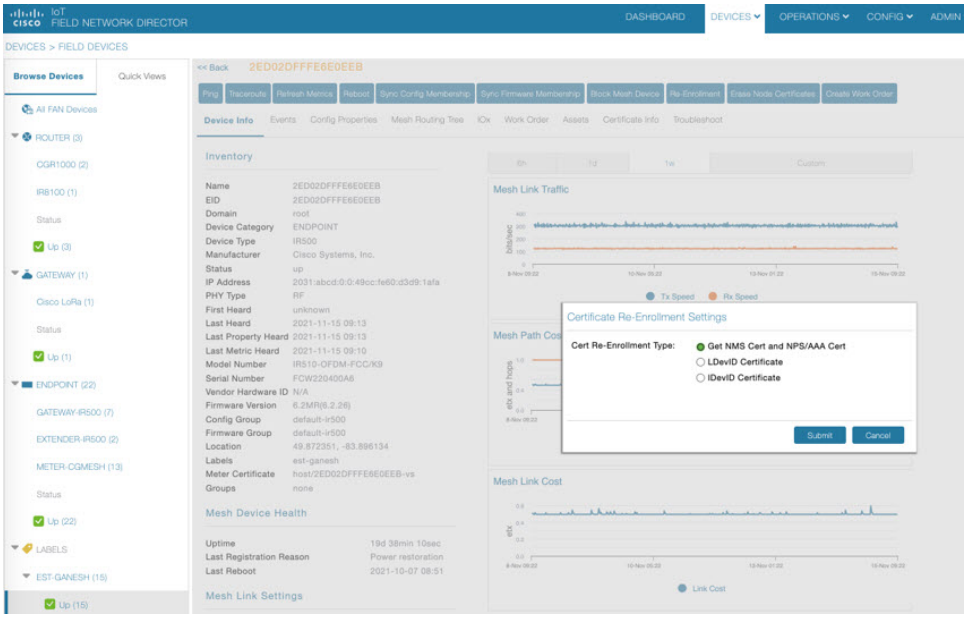


Figure 8: CONFIG > DEVICE CONFIGURATION > Endpoint Certificate Re-enrollment

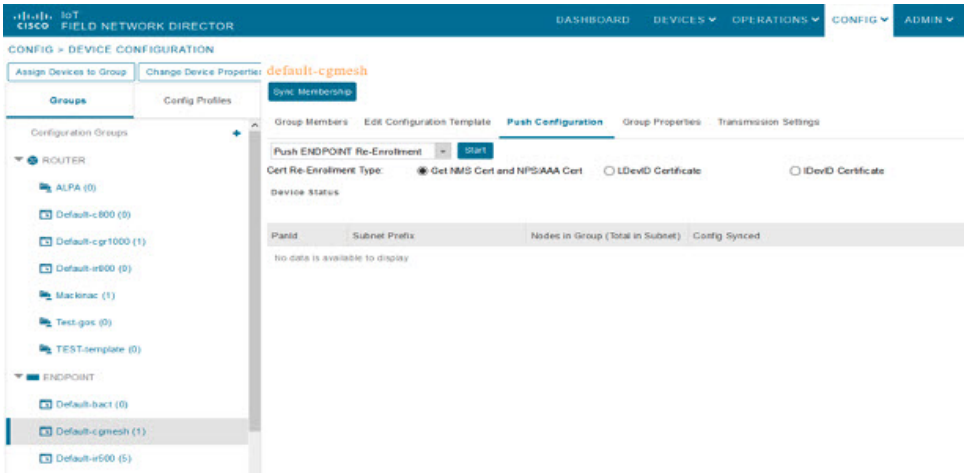
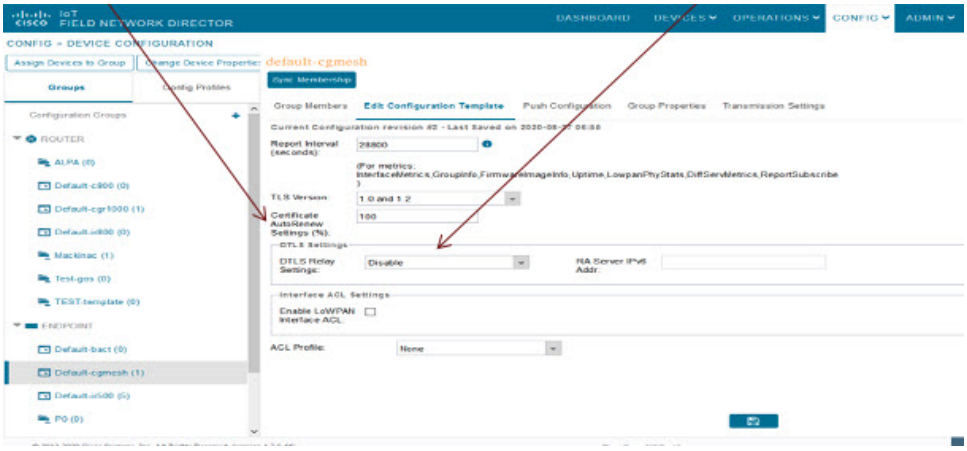
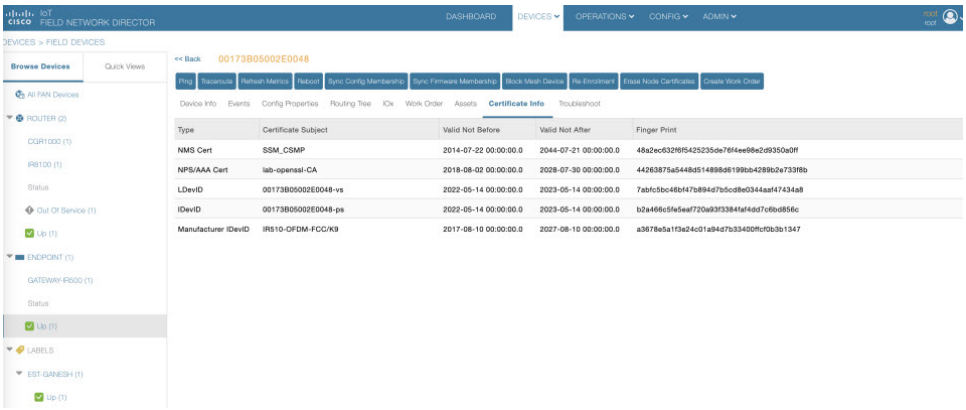


Figure 9: Support for DTLS Relay Settings and Cert Auto-Renew Settings for ITRON30 and IR500 Devices



Use the TLS version drop-down list on the Edit Configuration Template page above, to assign the appropriate TLS version. Options are: 1.2, 1.0 and 1.2 or N/A.

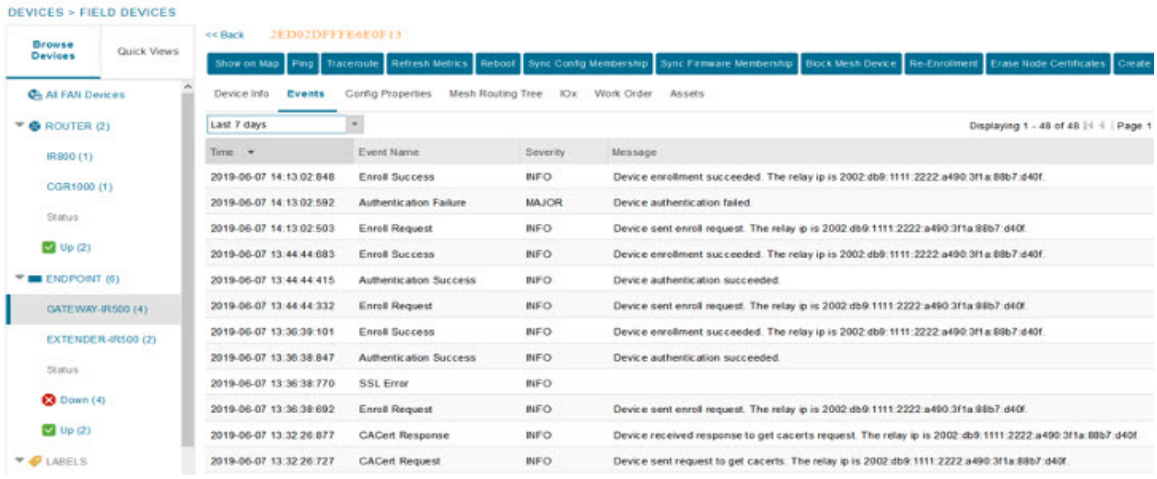
Figure 10: Certificate Information for IR500



New Events for IR500

Additional events are added for IR500 and they display on the **DEVICE** > **FIELD DEVICES** > **ENDPOINT** page.

Figure 11: New Events for IR500



Audit Trail for Re-enrollment for Gateway-IR500 Endpoints

Listed below is the new operation tracked and the items reported for Re-enrollment on the **ADMIN** > **SYSTEM MANAGEMENT** > **AUDIT TRAIL:**

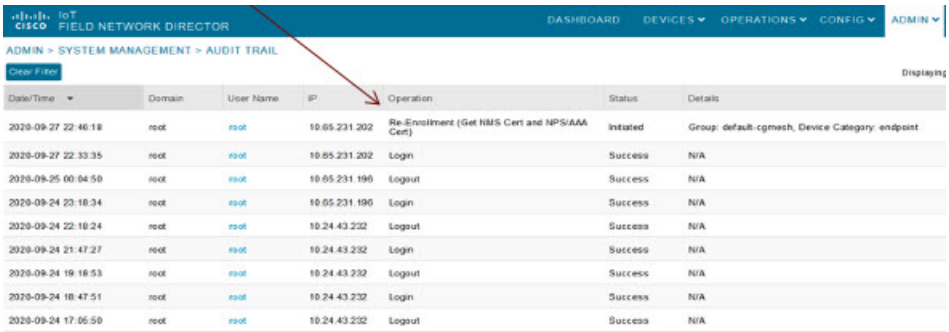
Operation: Re-enrollment (Get NMS Cert and NPS/AAA Cert)

Status: Initiated

Details: Group default-cg-mesh

Device category: endpoint

Figure 12: Audit Trail for Re-enrollment



Monitoring a Guest OS

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

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

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

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

Installing a GOS

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

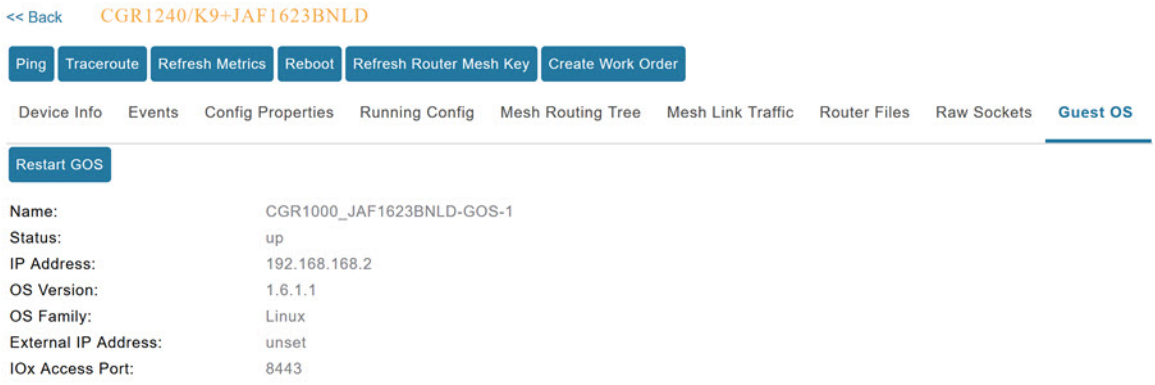
After any Cisco IOS install or upgrade, when IoT FND discovers a GOS, it checks if the initial communications setup is complete before it performs the required setup. The CGR must have a DHCP pool and Gigabit Ethernet 0/1 interface configured to provide an IP address and act as the gateway for the Guest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

Note If the router is configured with Guest-OS CLI during the router's registration with FND, FND detects that Guest-OS is running and populates a new Guest OS tab on the Device Info page for that particular router. From that page, you can trigger a Guest-OS restart. After the Guest-OS is restarted, a pop-up with the status of the operation is seen on the UI and messages are logged in the server.log file.

Restarting a GOS

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

Figure 13: DEVICES Field Devices Information Page Showing Guest OS tab and Restart GOS Button



This section includes the following topics:

• Pushing GOS Configurations, on page 102

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.

Application Management Support in IoT FND

Prerequisites

- The configuration required for the application hosting are:
  - Enabling IOx
  - Configuring a VirtualPortGroup to a Layer 3 Data Port
- FND and FD Integrated OVA with FD version v1.18.1 and above.

Registering IR1100 Devices with IoT FND through CSV

To register the device:

Procedure

Step 1 Prepare the CSV and add the IOx device to IoT FND. The CSV format is in the following format:

eid,name,status,lastHeard,meshEndpointCount,
runningFirmwareversion,ip,openIssues,labels,lat,lng

IR1101-K9+FCW23500H4Z,IR1101-K9+FCW23500H4Z,up,Jul 12 2022 8:21:46 AM UTC,17.05.01,10.104.198.12,49.933798, 65.696298

Step 2 In IoT FND UI, navigate to **Devices** > **Field Devices** > **Add Devices**.

Step 3 Specify the location of your CSV file and click **Add**.

Once the device is registered in IoT FND, the App tab in the Field Devices page is enabled.

Starting the IOx Service in Device Details Page

In the device details page:

Procedure

Step 1 Navigate to IOx tab check whether IOx is started.

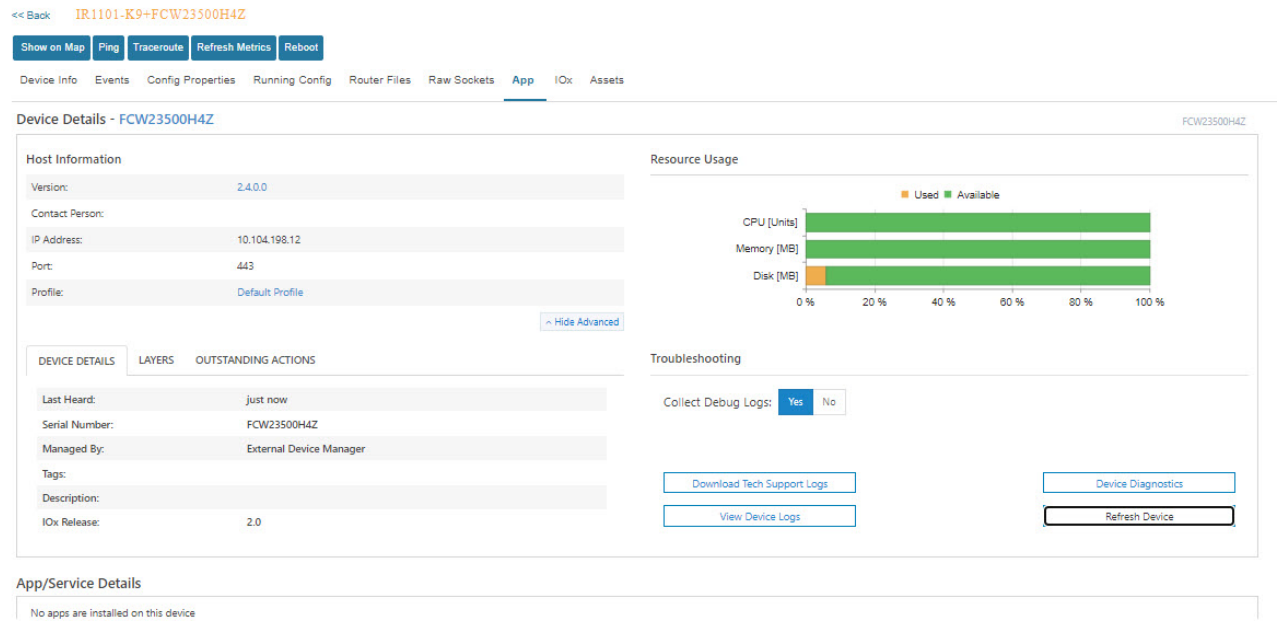
Step 2 Click **Start IOx** button if the service has not started.



Step 3 Click **Yes** in the confirmation dialog box.

Step 4 Navigate to App tab and click **Show Advanced**.

Note
Click **Refresh Device** in the Troubleshooting section, if the registered device is not populating the resource usage information in App Tab. The host information and device details are fetched from the device to IoT FND.



Note

If the last heard state of the device is Just now, then it confirms that the device is properly registered and started with IOx service.

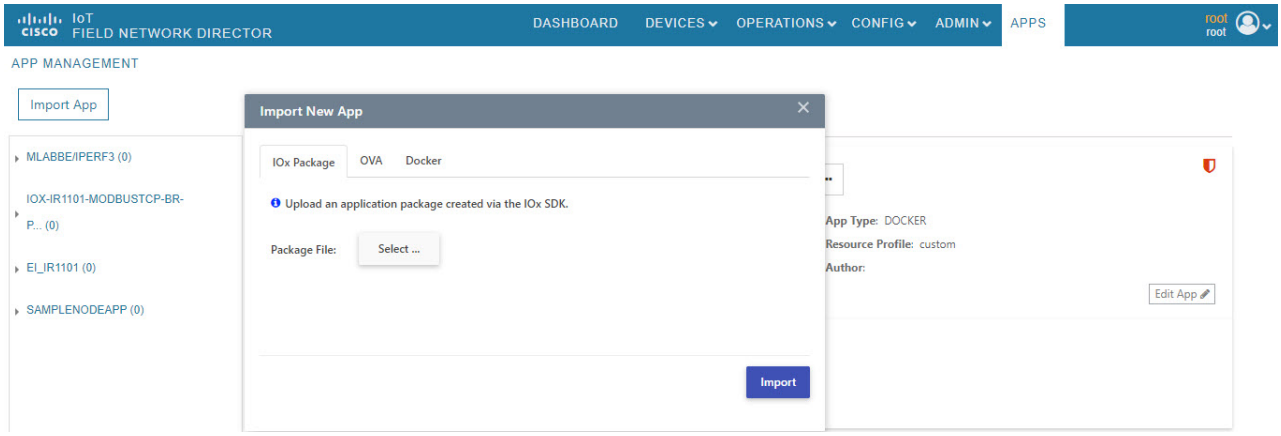
Importing the Application in APPS Main Menu

If the device is refreshed successfully through FD and properly discovered by IoT FND, navigate to APPS main menu and install the application to the IOx node in the router.

Procedure

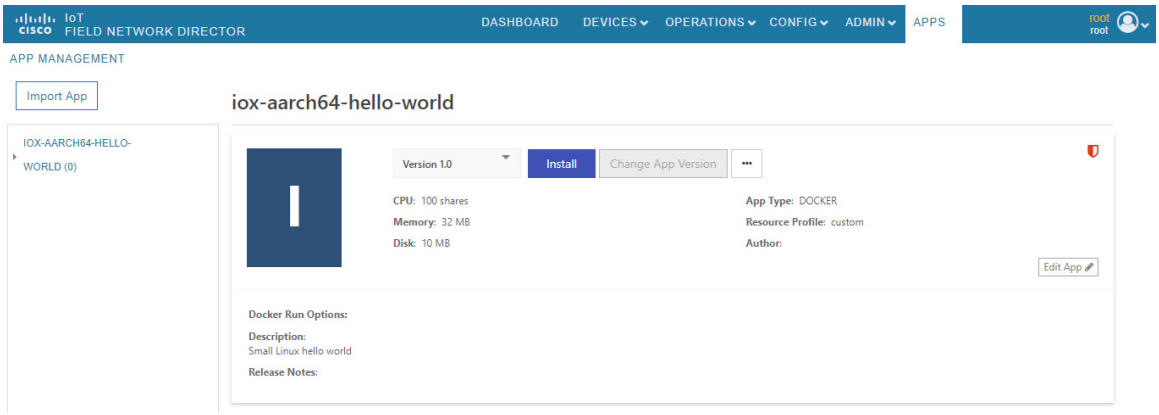
Step 1 Click **Import App**.

Step 2 Select the package from the local drive and click **Import**. The application is imported and listed in the left pane.



Installing the Application

Once the import is complete, select the application which you want to install and click **Install**.



Note If you install the application without configuring the interface or enabling the IOx, you will get the following error "No networks have been configured on this device" and the application installation will fail.

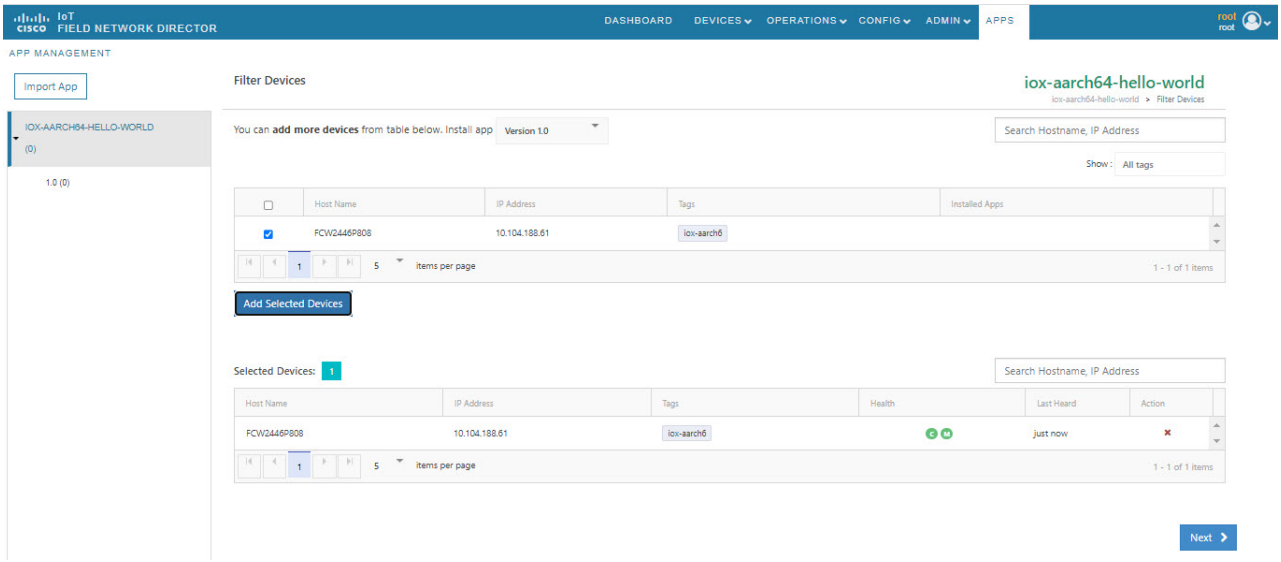
Procedure

Step 1 Select the device in which the application must be installed.

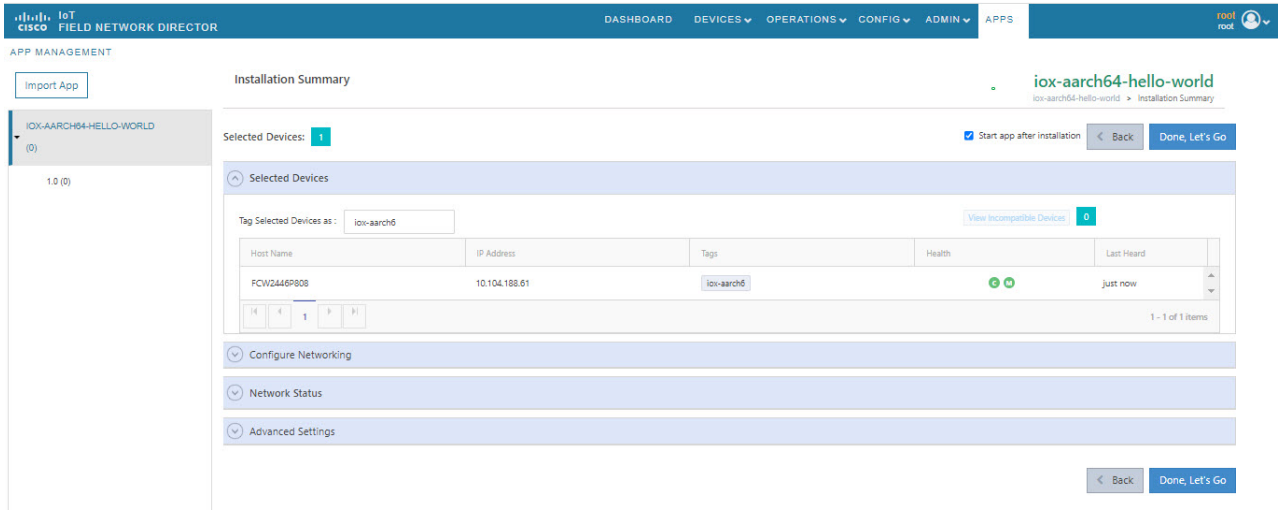
Step 2 Click **Add Selected Devices**. The device is added to the Selected Devices section where the Last Heard status of the device can be seen.

Note
As the device is recently registered, the status of the device is shown as just now.

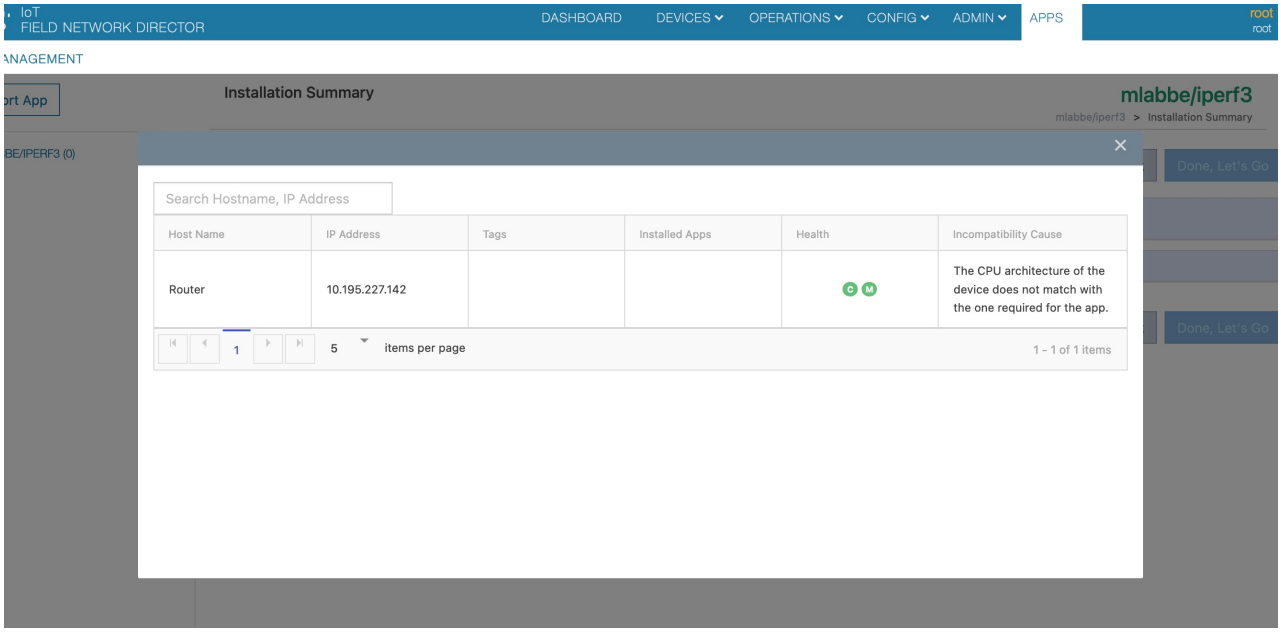
Step 3 Click **Next**.



Step 4 Check the Installation Summary where the device details are given in five different tabs and click **Done, Let's Go** .

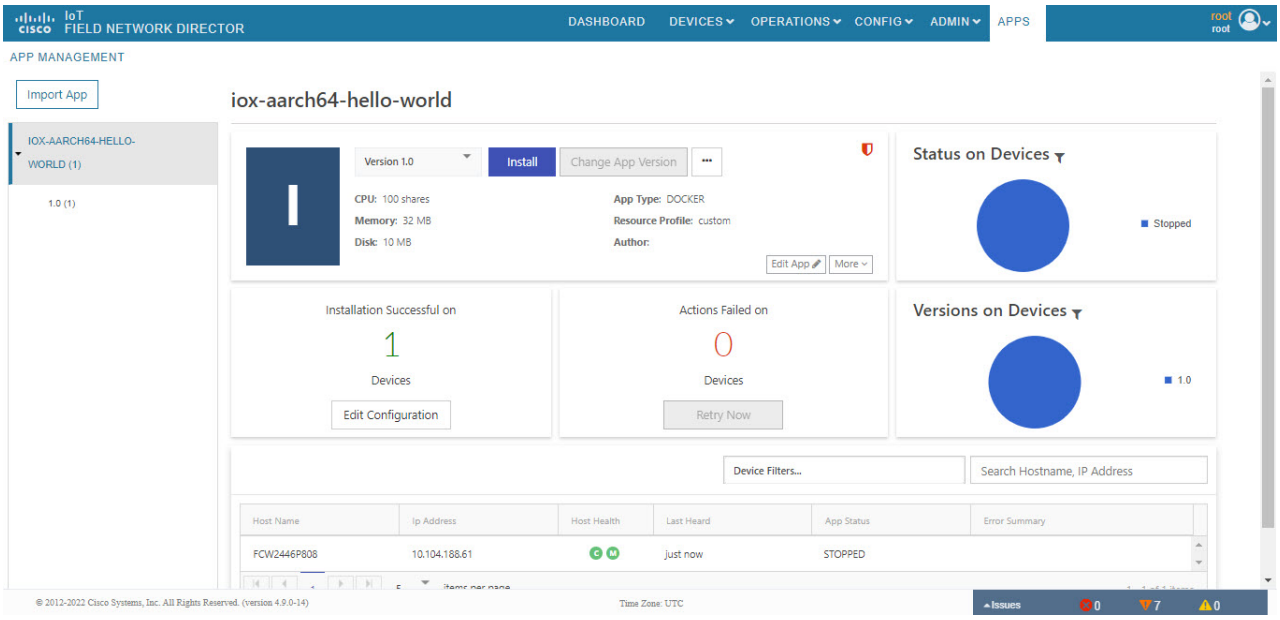


Note
If you install incompatible application, then you will get the following CPU architecture error.



Step 5 Click **Done, Let's Go**. The application is activated for the device and the installation process is started.

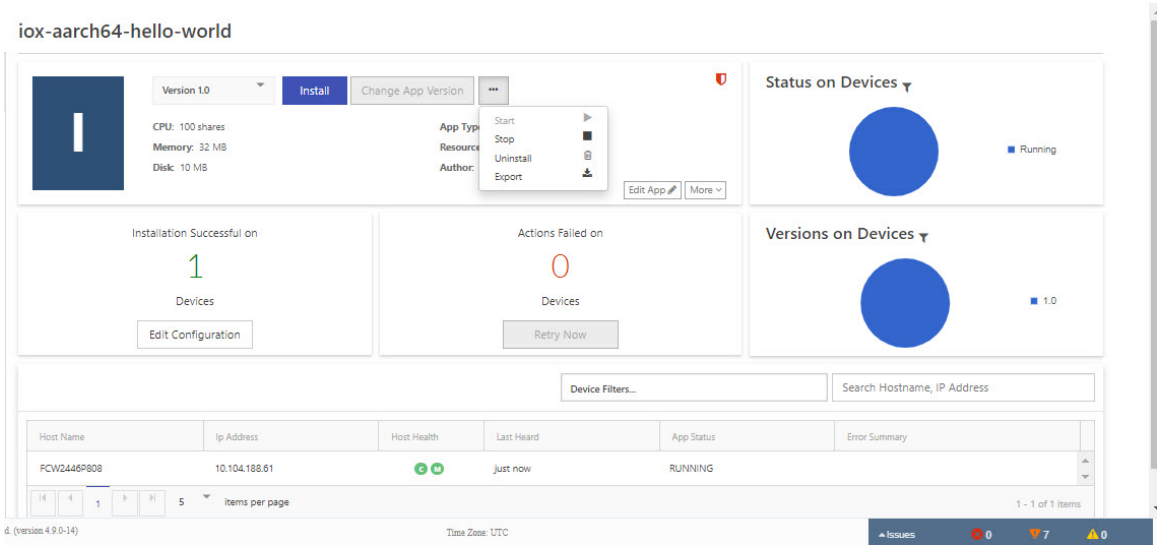
"Installation Successful on device" message appears once installation is complete. The device that is capable of IOx is discovered automatically and the Host Name, Ip Address are properly populated in IoT FND.



Managing the Application

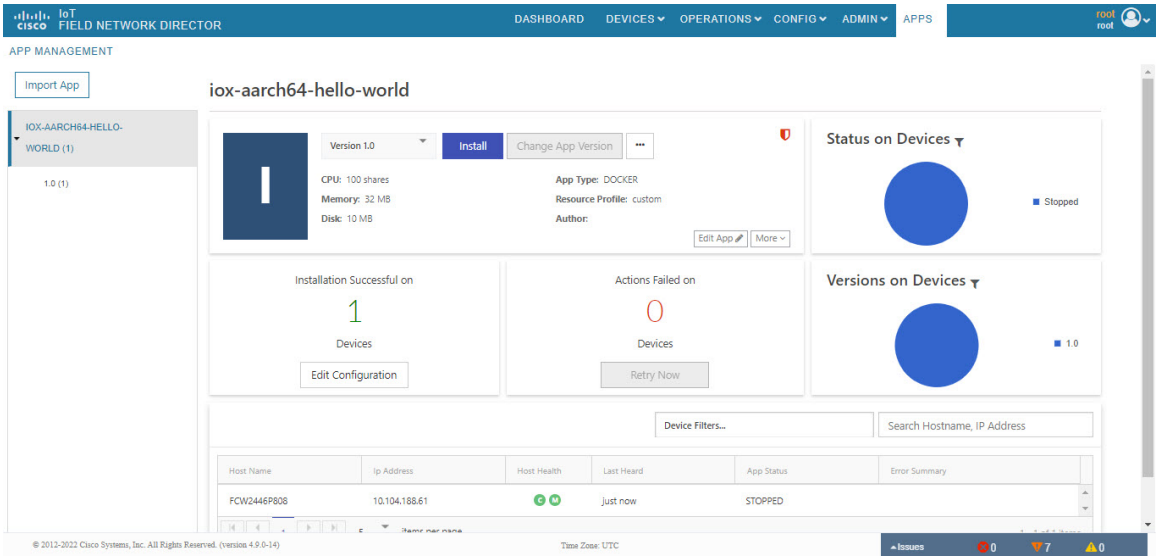
This section describes how to start, stop, and uninstall the application from the APPS menu.

Go to APPS menu and click the application. As the application is just installed and started, the other options are listed. Click … icon to use them.

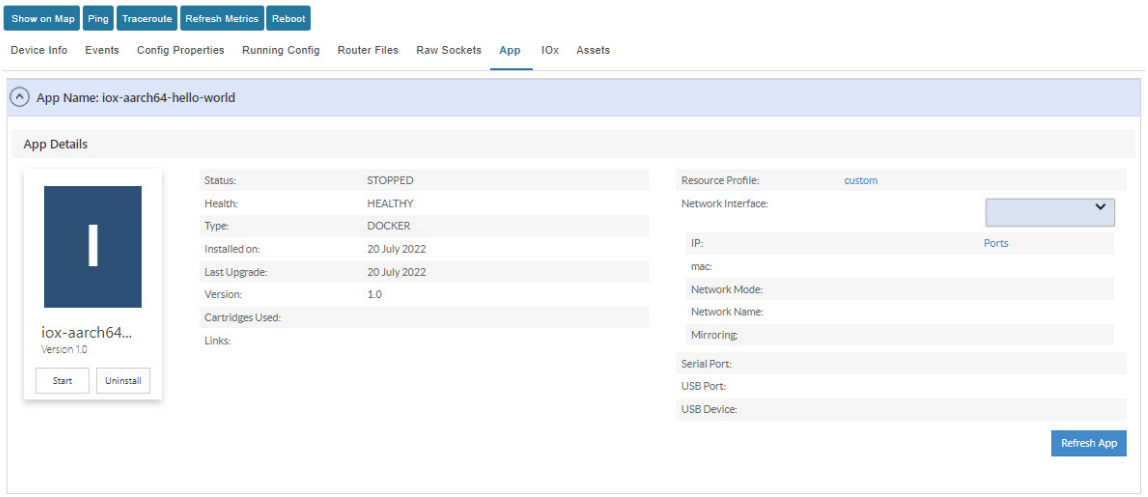


Stopping the Application

In the APPS menu, select the application and choose Stop from the drop-down list. Follow the same procedure as for installing the application and click **Done, Let's Go**. The following screen "Stopping iox-aarch64-hello-world succeeded on 1 device(s)." appears in the App management page.



Note Navigate to App tab in the Device Details page to check the status of the application under App/Service Details section. The status is shown as STOPPED.



You can either start or uninstall the application from this page or from the APPS main menu. If you click **Uninstall**, the operation is complete and the following message is displayed "Successfully performed undeploy action on iox-aarch64-hello-world app."

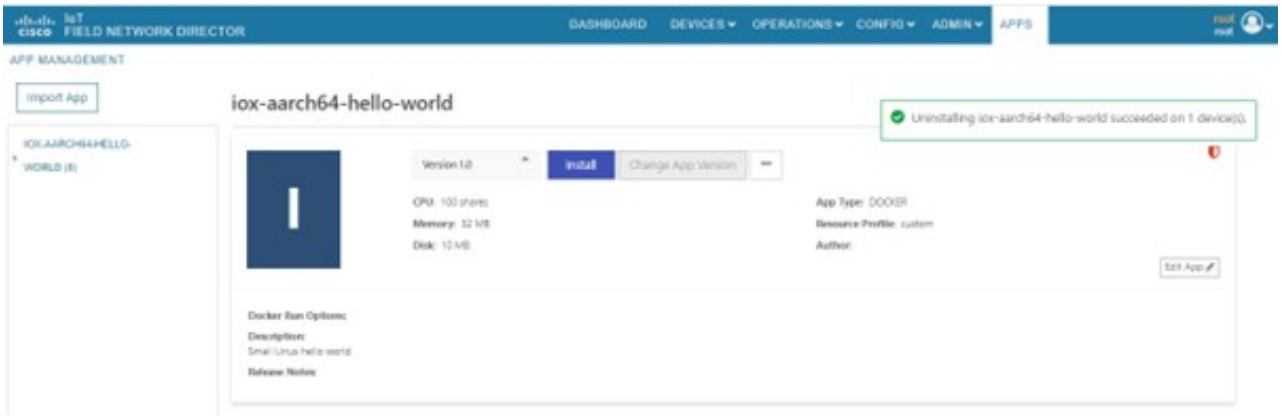
Uninstalling the Application

Go to APPS menu, click the application and choose Uninstall from the drop-down list.

Procedure

Step 1 In the Uninstall App page, select the device and click **Add Selected Devices**.

Step 2 Click **Done, Lets go**. The uninstallation is successful.



Exporting the Application

When you want to export the application and save it in the local drive, you can use this method. Go to APPS menu, click the application and choose Export from the drop-down list. The application gets downloaded.

PIMs in Cisco IoT FND

Pluggable Interface Modules (PIMs) are pluggable modular components that can be easily installed or removed on any router platform. They are used for configuring and upgrading network devices and provide flexibility for adding different interfaces.

Table 10: Feature History

Release Information	Feature Name	Description
Cisco IoT FND 4.11	P-LTEA7-NA (EM7411), P-LTEA7-EAL (EM7421), and P-LTEA7-JP (EM7431) PIMs support for Catalyst IR1100 routers	Adds support for Cat7 LTE PIMs for North America, Rest of World, and Japan, supporting multiple slots and modems.

Release Information	Feature Name	Description
Cisco IoT FND Release 4.10	P-LTE-450 PIM support for Cisco Catalyst IR1100 routers	Adds support for P-LTE-450 Mhz or PIM, which is a third-party LTE module that supports private networks and operates at a 450 MHz frequency.

PIMs

PIM Name	PID	Devices Supported	Minimum Supported Cisco IoT FND Release	Cisco IoT FND Supported Device Version	Description
P-LTE-450 MHz PIM	P-LTE-450	Cisco Catalyst IR1100	Cisco IoT FND Release 4.10	Cisco IOS XE Release 17.9.3 and later releases	Third-party LTE module (Cisco/Intelliport) for private LTE networks in the 450 MHz band; supports multi-PDN and multiple APNs per SIM; base or compute slot only. For more details, see Cisco Catalyst IR1100 Rugged Series Router
LTE Cat7 PIM (North America)	P-LTEA7-NA (EM7411)	Cisco Catalyst IR1101	Cisco IoT FND Release 4.11	Cisco IOS XE Release 17.13.1 and later releases	LTE Cat7 cellular pluggable module for North America; supports dual modem configuration; can be inserted in base, expansion module, or compute module slots. For more details, see Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide
LTE Cat7 PIM (Rest of World)	P-LTEA7-EAL (EM7421)	Cisco Catalyst IR1101	Cisco IoT FND Release 4.11	Cisco IOS XE Release 17.13.1 and later releases	LTE Cat7 cellular pluggable module for regions outside North America and Japan; supports dual modem configuration; insertable in multiple slots. For more details, see Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide

PIM Name	PID	Devices Supported	Minimum Supported Cisco IoT FND Release	Cisco IoT FND Supported Device Version	Description
LTE Cat7 PIM (Japan)	P-LTEA7-JP (EM7431)	Cisco Catalyst IR1101	Cisco IoT FND Release 4.11	Cisco IOS XE Release 17.13.1 and later releases	LTE Cat7 cellular pluggable module for Japan region; supports dual modem configuration; can be inserted in base, expansion module, or compute module slots. For more details, see Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide

PIM cellular connectivity

Each PIM installed in the Cisco IoT routers provides additional cellular connectivity options, allowing the routers to connect to cellular networks for WAN access. Here are the supported cellular interfaces:

Router Model	PIM Slot(s)	Supported Cellular Interfaces	Notes
Cisco Catalyst IR1101	Slot 1	Cellular 0/1/0 and Cellular 0/1/1	Gigabit Ethernet interface as first supported interface, followed by Cellular interfaces. Both LTE PIM and 5G PIM are recognized with Gigabit Ethernet and Cellular interfaces. **Note** Slot 1 is used for base pluggable module.
Cisco Catalyst IR1101	Slot 3, Slot 4	Cellular 0/3/0 and Cellular 0/3/1, Cellular 0/4/0 and Cellular 0/4/1	Only LTE PIMs are recognized with Gigabit Ethernet and Cellular interfaces for dual SIM or dual radio. **Note** Slot 3 or 4 depends on the LTE module inserted in the expansion module or compute module.

Router Model	PIM Slot(s)	Supported Cellular Interfaces	Notes
Cisco Catalyst IR8100	Slot 2, Slot 3	Cellular 0/2/0, Cellular 0/2/1, Cellular 0/3/0 and Cellular 0/3/1	Both LTE PIM and 5G PIMs are recognized, with two logical interfaces (e.g., for dual SIM or dual radio).
Cisco Catalyst IR1800	Slot 4	Cellular0/4/0 and Cellular0/4/1	Both LTE PIM and 5G PIMs are recognized, two logical interfaces (e.g., for dual SIM or dual radio).
Cisco Catalyst IR1800	Slot 5	Cellular0/5/0 and Cellular0/5/1	Both LTE PIM and 5G PIMs are recognized, with two logical interfaces (e.g., for dual SIM or dual radio).

Monitor PIMs in field devices page

Use this task to view these PIM details in the **Device Info** page:

- **Cellular Link Settings**,
- **Cellular Link Info**,
- **Cellular Link Metrics**,
- **Pluggable Module Info**.

Before you begin

Note

- The **Network Interface** table in the **Device Info** page display the GigabitEthernet interfaces. When P-LTE-450 Mhz module is connected to base module it uses the GigabitEthernet 0/1/0 interface, when connected to compute module it uses GigabitEthernet 0/4/0 interface.
- P-LTE-450 can be connected in the base slot or in the expansion CM slot, and it always appears in Modem2 . The APNs have 3,4, and 5 as interface numbers.
- Cisco IoT FND detects the module inserted in router during registration of the router.

Procedure

Step 1 Choose **DEVICES** > **Field Devices** > **Browse Devices** > **Router**.

Step 2 Click router in the list of routers.

You will see the PIM details appearing in the **Device Info** page.

Note

- See NB API guide, for more information about the properties and metrics used for pluggable and expansion interfaces. Also, see getMetricHistory and getDeviceDetails for more details.

What to do next

See *View Metrics in the Cellular Link Traffic and RSSI Charts*.

View cellular link traffic and cellular RSSI chart metrics

Use this task to view these details of PIM metrics and charts from the **Device Info** page:

- **Cellular Link Traffic**,
- **Cellular RSSI**.

Procedure

Step 1 Choose **DEVICES** > **Field Devices** > **Browse Devices** > **Router**.

Step 2 Click router in the list of routers.

You will see the cellular details and charts appearing in the **Device Info** page.

Managing Files

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

- File Types and Attributes, on page 114
- Adding a Router Device File to IoT FND, on page 114
- Transferring Files, on page 116
- Viewing Files, on page 117
- Monitoring Files, on page 117
- Monitoring Actions, on page 118
- Deleting Files, on page 118

Note File management is role-dependent and may not be available to all users. See Managing Roles and Permissions in the Managing User Access chapter.

File Types and Attributes

Two types of EEM scripts are used on the router: an embedded applet, and Tool Command Language (TCL) scripts that execute on the router individually. You can upload and run new EEM TCL scripts on the router without doing a firmware upgrade. EEM files upload to the *eem* directory in router flash memory. These scripts display in the **Import File** page File Type column as *eem script* . You must edit the configuration template file to activate the EEM TCL scripts (see Editing the ROUTER Configuration Template, on page 88). This feature works with all router OS versions currently supported by IoT FND.

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

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

Adding a Router Device File to IoT FND

When you want to upload router device files to be managed by IoT FND, go to **CONFIG** > **DEVICE FILE MANAGEMENT** within the application.

At that page, select **Actions** > **Upload** to get to the Upload File to Routers page (Figure 14: Search for a Specific CGR Device File Name and Upload to FND Router Page, on page 115). This page provides you the ability to search for a specific device by its name such as CGR1120/K9+JAF1648BBCT or you can search by an abbreviated string such as CGR1120/K9+JAF that will display a list of all routers that share that string (Figure 15: Upload Multiple CGR Files Within a Given String Search Range to the FND Router Page, on page 115).

Additionally, you can enter the File Path to the router in the File Path field on the page.

The searches yield the number of routers available to upload (based on your search criteria) for management by IoT-FND and displays on the Upload File to Routers page.

You can define how many devices display on the screen by selecting a value from the drop-down menu at the far-right of the screen. Options are 10 (default), 50, 100 and 200. You can remove the check mark next to any individual router file that you do not want to upload.

After you finalize the list you want to upload, click Upload File.

Figure 14: Search for a Specific CGR Device File Name and Upload to FND Router Page

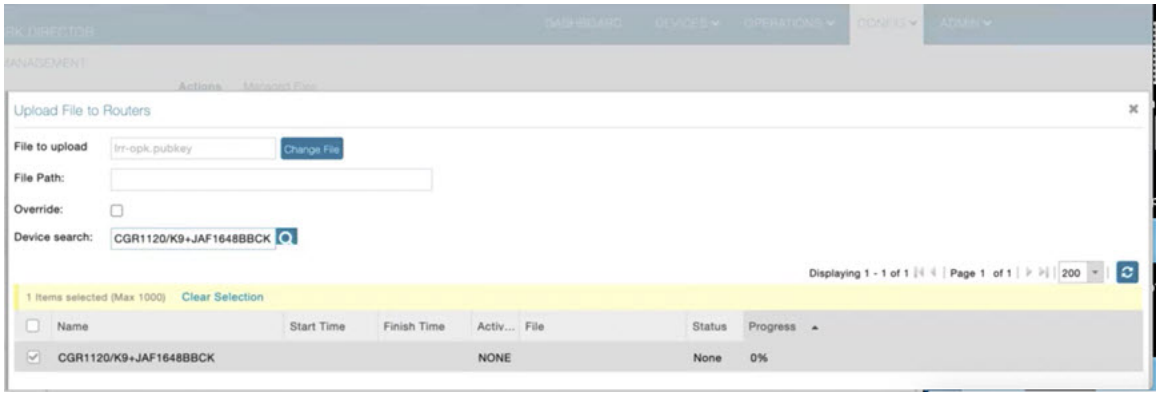
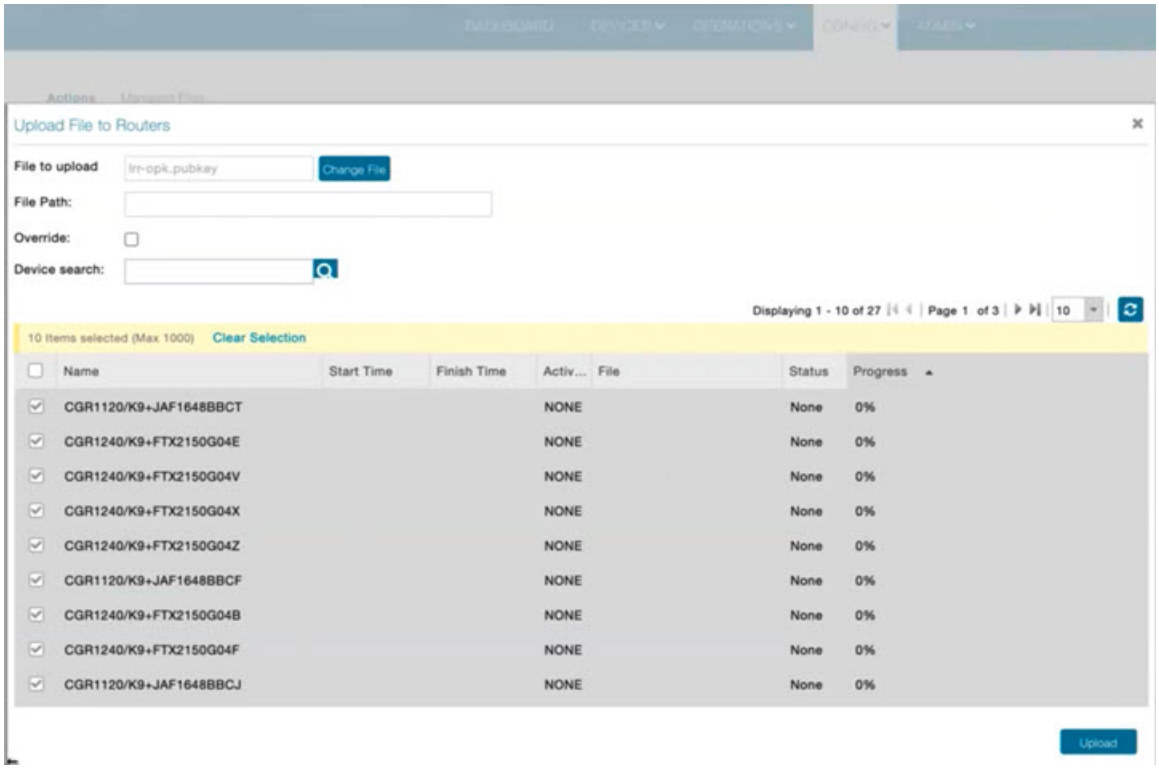


Figure 15: Upload Multiple CGR Files Within a Given String Search Range to the FND Router Page



Deleting a File from IoT FND

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

To delete a file from IoT FND:

Procedure

Step 1 On the **CONFIG** > **Device File Management** page, select a file from the List dialog box (far-left panel).

Step 2 At the **Actions** tab, click **Delete**.

Step 3 At the **Delete from List** panel, select a file and click **Delete File**.

Transferring Files

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

To perform a file transfer:

Procedure

Step 1 On the **CONFIG** > **Device File Management** page, select the group to transfer the file from the **Browse Devices** left pane.

Step 2 Click **Import Files** or **Upload** on the **Actions** tab. The **Select File from List** dialog box displays.

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

Step 4 Click **Upload File**.

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

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

Step 6 Click **Upload**.

What to do next

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

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

All files that are transferred from IoT FND reside on the router in `flash:/managed/files/` for Cisco IOS CGRs.

and bootflash:/managed/files/ for CG-OS CGRs.

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

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

- File Operation: upload
- Start Date/Time of the last transfer

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

Viewing Files

To view imported text file content:

Procedure

Step 1 Select **CONFIG** > **Device File Management**.

Step 2 Click the EID link (such as CGR1240/K9+JAF1626BLDK) listed under the Name column to display the Device Info pane.

Step 3 Click the **Router Files** tab.

Step 4 Click the filename link to view the content in a new window.

What to do next

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

Monitoring Files

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

The following information is included in this list:

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

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

Monitoring Actions

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

The Actions tab lists the following attributes:

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

Deleting Files

To delete files from routers:

Procedure

Step 1 On the **CONFIG** > **Device File Management** page, within the **Browse Devices** pane, select the file that you want to delete.

Step 2 On the **Actions** tab, click **Delete**.

Step 3 In the **Delete file from List** dialog, select a file to delete.

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

Step 4 Click **Delete File**.

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

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

• You can click Change File to select a different file to delete from the selected routers.
• You can select multiple routers.
• Only one file can be deleted at a time.
• You can click Clear Selection and (x) close the windows to stop deletion.

Step 6 Click **Delete**.

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

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

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

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

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

- Error Details

Hardware Security Module

IoT FND accesses the HSM (Hardware Security Module) server using the HSM Client.

In order for IoT FND to access the HSM Server, the HSM Client corresponding to the HSM Server version must be installed on the Linux server where the IoT FND application server is installed.

IoT FND is integrated with the HSM Client by using the HSM client API. The HSM client assigns a slot number to the HSM Server and also to the HA Group. On HSM Client 5.4 or earlier, the slot numbering started from one (1). However, in HSM Client 6.x and later, the slot numbering starts from zero (0).



Note IoT FND gets the slot value dynamically from the HSM Client API. Sometimes during an upgrade from 5.4 to 7.3, the slot ID change is not dynamically populated. (CSCvz38606)



Note HSM Client 5.4 uses slot ID 1 (one). However, HSM Client 6.x and onward, slot ID 0 (zero) is used by the HSM client. The IoT FND application gets the value of the slot ID dynamically from the HSM client. The slot ID change will be communicated to the FND server by the HSM Client API upon restart of the IoT FND application. However, in some cases, the HSM client fails to send the correct value of the slot to the FND application server.

In such cases, where the FND Application Server has a value of 1 for the slot ID, but the HSM Client is using slot 0, and the HSM Client API is not giving the correct value dynamically, we can set the slot ID manually to one (1) in the HSM Client configuration file -/etc/Chrystoki.conf with the below:

```
Presentation = {OneBaseSlotID=1;}
```

Verification of FND and HSM Integration After FND and HSM Upgrade

If HSM is deployed with a FND application for storing the CSMP keys and certificates; then, after a FND upgrade or after a HSM client upgrade, the following checks can be made to ensure that HSM integration is working.

To verify FND and HSM Integration after an FND and HSM upgrade, do the following:

Procedure

Step 1 Go to **Admin** > **Certificates** in the FND GUI. Check to see if the CSMP certificate is present. If the CSMP certificate is missing, then follow the steps listed in the common errors table for “HSM 5.x certificate will not load.”

Note
If it is a High Availability (HA) setup for the FND server, then follow the step above for both FND servers.

Step 2 Enter **cat/opt/cgms/server/cgms/log/server.log | grep HSM**
cat/opt/cgms/server/cgms/log/server.log | grep HSM

Retrieved public key:

3059301306072a8648ce3d020106082a8648ce3d03010703420004d914167514ec0a110f3170eef74

2a000572cea6f0285a3074db87e43da398ab016e40ca4be5b888c26c4fe91106cbf685a04b0f61d599

826bdbcff25cf065d24

Note
If it is a High Availability (HA) setup for the FND server, then follow the step above for both FND servers.

Step 3 Check the connectivity of HSM client and HSM server is good. Check if NTLS is established on port 1792 and check if the HSM client is able to retrieve the HSM partition number and HSM partition name of the HSM partition from the HSM server. Use the./vtl verify and ccfg listservers command in the lunacm utility as below:

```
[root@fndblr17 ~]# cd /usr/safenet/lunaclient/bin
[root@fndblr17 bin]#
[root@fndblr17 bin]#./vtl verify
vtl (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.
The following Luna SA Slots/Partitions were found:
Slot Serial # Label
==== ================ =====
- 1358678309716 TEST2
TEST2 is partition name
1358678309716 is the serial number assigned to partition TEST2
[root@fndblr17 bin]#./lunacm
lunacm (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.
Available HSMs:
Slot Id -> 0
Label -> TEST2
Serial Number -> 1358678309716
Model -> LunaSA 7.4.0
Firmware Version -> 7.4.2
Configuration -> Luna User Partition With SO (PED) Key Export With Cloning Mode
Slot Description -> Net Token Slot
Slot Id -> 4
HSM Label -> TEST2HAGroup1
HSM Serial Number -> 11358678309716
HSM Model -> LunaVirtual
HSM Firmware Version -> 7.4.2
HSM Configuration -> Luna Virtual HSM (PED) Key Export With Cloning Mode
HSM Status -> N/A - HA Group
Current Slot Id: 0
lunacm:>ccfg listservers
Server ID Server Channel HTL Required
_____________________________________________________________
1 172.27.126.15 NTLS no
Command Result : No Error
lunacm:>exit
[root@fndblr17 bin]#
```

Step 4 Check if the cmu list command is able to retrieve the label of the key and CSMP certificate. This will ask for password. The password is same as the HSM partition. In case of HA, it will be the password of the HSM HAGroup.

```
[root@fndblr17 bin]# cd /usr/safenet/lunaclient/bin
[root@fndblr17 bin]#./cmu list
Certificate Management Utility (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights
reserved.
Please enter password for token in slot 0 : *******
handle=2000001 label=NMS_SOUTHBOUND_KEY
handle=2000002 label=NMS_SOUTHBOUND_KEY--cert0
```

```
You have new mail in /var/spool/mail/root
[root@fndblr17 bin]#
```

Step 5 If steps 3 and 4 are successful, it means that the HSM client and HSM communication is good. However, sometimes, there will be an issue with the HSM client API and FND. In such cases, try enabling CK logs as noted below. CK logs are a diagnostic utility of the HSM client. CK logs are resource intensive, so, enable them only when required and disable them after use.

When cklog is enabled, then, the log file will be created in /tmp directory.

This file will generate logs related to FND server access to HSM.

Sometimes it is possible that the HSM client to HSM server is up. However, the FND server is not able to connect to HSM client. In such cases, it will help to find the communication logs between the FND server and also the HSM server.

To enable cklogs:

- Go to directory: **/usr/safenet/lunaclient/bin**, then run the command, **./vtl cklogsupport enable.**

```
[root@fndserver ~]#cd /usr/safenet/lunaclient/bin
[root@fndserver bin]# pwd
/usr/safenet/lunaclient/bin
[root@fndserver bin]#./vtl cklogsupport enable
vtl (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.
Chrystoki2 LibUNIX = /usr/safenet/lunaclient/lib/libCryptoki2.so
Chrystoki2 LibUNIX64 = /usr/safenet/lunaclient/lib/libCryptoki2_64.so
Cklog not enabled (entry is Null)
Enabling cklog
[root@fndserver bin]#
```

- The location of the cklog file generated is **/tmp/cklog.txt**.

```
[root@fndserver bin]# cd /tmp
[root@fndserver tmp]# ls | grep cklog.txt
cklog.txt
[root@fndserver tmp]#
```

Note
HSM does not recommend cklogs to be enabled all the time. Please enable it for troubleshooting and then disable it after use.

To disable:

[root@fndserver bin]#./vtl cklogsupport disable

The Linux server will stop logging the FND communications to and from HSM server when **cklog** is disabled. The log file, **/tmp/cklog.txt** itself is not deleted. When it is enabled again, then, the new logs will be appended to the old logs. If this is not desirable, then after disabling, the cklogs can be renamed if the file is needed or deleted if it is no longer needed.

For example, **cklog.txt** is renamed as **cklog_old_<date>.txt**

```
[root@fndserver ~]# cd /tmp
[root@fndserver tmp]# ls -al | grep cklog.txt
-rw-r--r--. 1 root root 12643866 Oct 11 00:17 cklog.txt
[root@fndserver tmp]#
[root@fndserver tmp]# mv cklog.txt cklog_old_11oct21.txt
You have new mail in /var/spool/mail/root
[root@fndserver tmp]# ls -al | grep cklog.txt
[root@fndserver tmp]#
[root@fndserver tmp]# ls -al | grep old
```

```
-rw-r--r--. 1 root root 12646086 Oct 11 00:20 cklog_old_11oct21.txt
[root@fndserver tmp]#
```

Demo and Bandwidth Operation Modes

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

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

Table 11: Communication Method Given FND Operation Mode

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

FND Configuration Changes

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

Procedure

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

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

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

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

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

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

Router Configuration Changes

In order to manage routers in Demo mode:

Procedure

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

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

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

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

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

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

Configuring Demo Mode in User Interface

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

To setup Demo Mode for FND and router communications:

Procedure

Step 1 Choose **ADMIN** > **SYSTEM MANAGEMENT** > **Provisioning Settings**.

Step 2 In the Provisioning Process panel, enter the IoT FND URL in the following format: http:// <ip address:9121> in both the IoT FND URL and Periodic Metrics URL.

What to do next

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

Bandwidth Optimization Mode Configuration

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

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

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

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

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

Configuring Bandwidth Optimization Mode in User Interface



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

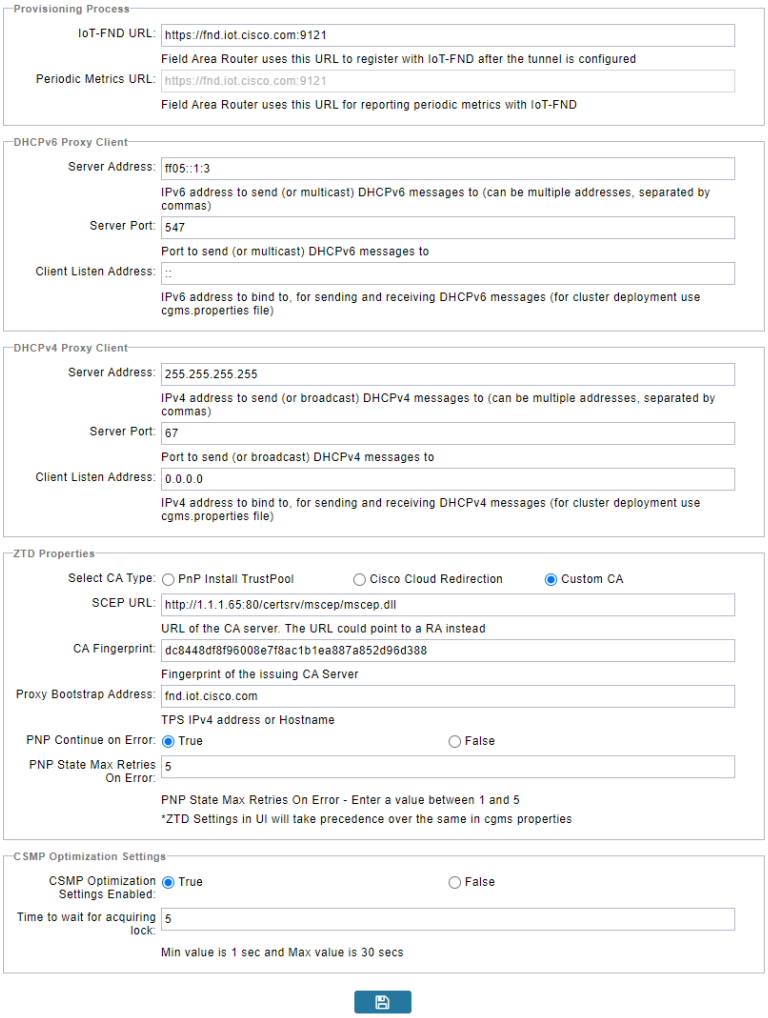
To setup Bandwidth Optimization Mode for FND and router communications:

Procedure

Step 1 Choose **ADMIN** > **SYSTEM MANAGEMENT** > **Provisioning Settings**

Step 2 In the Provisioning Process panel:

- Enter your IoT FND URL in the following format: “https:// FND IP/HostName:9121" in the IoT FND URL field. FAR uses this URL to communicate with IoT FND after the tunnel is configured.
- Enter the following URL in the Periodic Metrics URL field: http:// <ip address:9124>FAR uses this URL to report periodic metrics and notifications with IoT FND.



Device Properties

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

Types of Device Properties

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.

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

Cellular Link Metrics for CGRs

Cellular Link Metrics for CGRs describes the fields in the Cellular Link Metrics area of the Device Info view.

Table 12: Cellular Link Metrics for CGRs

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: • 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.

Field	Key	Description
Cell Connect Time	cellConnectTime	Length of time that the current call lasted. This field only applies only to CDMA.
Cellular RSRP	cellularRsrp	Reference Signal Received Power is the average power of resource elements that carry cell specific reference signals over the entire bandwidth.
Cellular RSRQ	cellularRsrq	Indicates the quality of the received reference signal.

Cellular Link Settings

Cellular Link Settings Fields lists the fields in the Cellular Link area of the Device Detail page for all Cellular interfaces.



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

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

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

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

Additionally, the 4G LTE dual-active radio module does not support or display all fields summarized in Cellular Link Settings Fields

Table 13: 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	N/A	Yes	Defines the service provider name, for example, AT&T or Verizon.
Cell ID	cellularID	No	Displays the cell ID for the cellular interface. This value must exist to activate the interface.

Field	Key	Configurable	Description
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: • Packet switched • Circuit switched • LTE
Location Area Code	locationAreaCode	No	Displays the Location Area Code (LAC) given by the base station.
Routing Area Code	routingAreaCode	No	Displays the routing area code given by the base station.
APN	cellularAPN	No	Displays the Access Point Name (APN) of the AP to which the cellular interface connects.
Cellular Modem Firmware Version	cellularModemFirmwareVersion	No	Displays the version of the modem firmware on the Cellular module installed within the CGR.
Connection Type	connectionType	No	Displays the connection type as: • 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: • 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.

Field	Key	Configurable	Description
Cellular Module Temperature	cellularModemTemp	—	Displays the modem temperature.
ICCID	cellularICCID	—	The Integrated Circuit Card Identification Number is a unique 18-22 digit code that includes a SIM card's country, home network, and identification number.

DA Gateway Properties

DA Gateway Metrics Area Fields describe the fields in the DA Gateway area of the Device Info view.

Table 14: DA Gateway Metrics Area Fields

Field	Key	Description
SSID	N/A	The mesh SSID.
PANID	N/A	The subnet PAN ID.
Transmit Power	N/A	The mesh transmit power.
Security Mode	N/A	Mesh Security mode: • 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: • 0 = Robo • 1 = DBPSK • 2 = DQPSK • 3 = D8PSK
Mesh Tone Map Reverse Modulation	N/A	Mesh tone map reverse modulation: • 0 = Robo • 1 = DBPSK • 2 = DQPSK • 3 = D8PSK
Mesh Device Type	N/A	The primary function of the mesh device (for example, meter, range extender, or DA gateway).
Manufacturer of the Mesh Devices	N/A	Manufacturer of the mesh device as reported by the device.

Field	Key	Description
Basic Mapping Rule End User IPv6 Prefix	N/A	End-user IPv6 address for basic rule mapping for the device.
Basic Mapping Rule End User IPv6 Prefix Length	N/A	Specified prefix length for the end-user IPv6 address.
Map-T IPv6 Address	N/A	IPv6 address for MAP-T settings.
Map-T IPv4 Address	N/A	IPv4 address for MAP-T settings.
Map-T PSID	N/A	MAP-T PSID.
Active Link Type	N/A	Link type of the physical link over which device communicates with other devices including IoT FND.

Device Health

The Device Health Fields describes the fields in the Device Health area of the Device Info view.

Table 15: Device Health Fields

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

Embedded Access Point (AP) Credentials

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

Table 16: Embedded Access Point Credentials Fields

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

Embedded AP Properties

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

Table 17: Embedded AP Properties

Field	Key	Description
Inventory	NA	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.

Field	Key	Description
Wi-Fi Clients	N/A	Provides client MAC address, SSID, IPv4 address, IPv6 address, device type, state, name, and parent.
Dot11Radio 0 Traffic	N/A	Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps), and Rx speed (bps).
Dot11Radio 1 Traffic	N/A	Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps,) and Rx speed (bps).
Tunnel3	N/A	Provides admin status (up/down), operational status (up/down), Tx speed (bps), Tx drops (bps), and Rx speed (bps).
BVI1	N/A	Provides admin status (up/down), operational status (up/down), IP address, physical address, Tx speed (bps), Tx drops (bps) and Rx speed (bps).
GigabitEthernet0	N/A	Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps), and Rx speed (bps).

Ethernet Link Metrics

Ethernet Link Metrics Area Fields describes the fields in the Ethernet link traffic area of the Device Info view.

Table 18: 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.

IOx Node Properties

IoX Node Properties Fields describe the fields in the Iox Node Properties area of the Config Properties page.

Table 19: IOx Node Properties Fields

Field	Key	Description
DHCPv4 Link for IOX Node Gateway	dhcpV4IOxLink	The DHCPv4 gateway address
IOx Node Gateway IPv4 Address	ioxGwyV4Address	The IPv4 gateway address
IOx Node IPv4 Subnet mask	ioxV4Subnetmask	The IPv4 subnet mask address
IOx Node Gateway IPv6 Address	ioxGwyV6Address	The IPv6 gateway address
IOx Node IPv6 Subnet Prefix Length	ioxV6PrefixLength	The IPv6 subnet prefix length

Field	Key	Description
Preferred IOx Node interface on the platform	ioxInterface	The interface on the platform
IOx Node External IP Address	ioxIpAddress	The external IP address
IOx Access Port	ioxAccessPort	The access port

Head-End Routers Netconf Config

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

Table 20: 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

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

Table 21: 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

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

Table 22: 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.

Field	Key	Configurable	Description
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

The table describes the fields in the Inventory area of the Device Info page for CGR1000.

Table 23: Inventory Fields

Field	Key	Configurable	Description
Config Group	configGroup	Yes	Name of the configuration group to which the device belongs.
Device Category	deviceCategory	No	Category of the device.
Device Type	deviceType	No	Device type that determines other fields, the way the device communicates, and the way it appears in IoT FND.
Domain Name	domainName	Yes	Domain name configured for this device.
EID	eid	No	Primary element ID of the device, which is used as the primary unique key for device queries.
Firmware Group	firmwareGroup	Yes	Name of the firmware group to which the device belongs.
Firmware Version	runningFirmwareVersion	No	Firmware version running on the device.
Hardware Version	vid	No	Hardware version of the device.
Hypervisor Version	hypervisor	No	(Cisco IOS CGRs running Guest OS only) The version of the Hypervisor.
Hostname	hostname	No	Hostname of the device.
IP Address	ip	Yes	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 an XML or CSV file.
Last Heard	lastHeard	No	Last date and time the device contacted IoT FND.
Last Metric Heard	N/A	No	Time of last polling (periodic notification).
Last Property Heard	N/A	No	The time of last property update for the router.
Last RPL Tree Update	N/A	No	The time of last Routing Protocol for Low power and Lossy Networks (RPL) tree poll update (periodic notification).

Field	Key	Configurable	Description
Location	N/A	No	Latitude and longitude of the device.
Manufacturer	N/A	No	Manufacturer of the endpoint device.
Function	crmesh	No	Function of the mesh device. Valid values are Range Extender and Meter.
Meter Certificate	meterCert	No	Global or unique certificate reported by the meter.
Meter ID	meterId	No	Meter ID of the mesh endpoint (ME).
Model Number	pid	No	Product ID of the device.
Name	name	Yes	Unique name assigned to the device.
SD Card Password Lock	N/A	Yes	(CGRs only) State of the SD card password lock (on/off).
Serial Number	sn	No	Serial number of the device.
Status	status	No	Status of the device.
Tunnel Group	tunnelGroup	Yes	Name of the tunnel group to which the device belongs.

Link Metrics

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

Table 24: Link Metrics Fields

Field	Key	Description
Active Link Type	activeLinkType	Determines the most recent active RF or PLC link of a meter.
Meter ID	meterId	Meter ID of the device.
PANID	meshPanid	PAN ID of the endpoint.
Mesh Endpoints	meshEndpointCount	Number of RMEs.
Mesh Link Transmit Speed	meshTxSpeed	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	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	N/A	Number of data packets dropped in the uplink.
Route RPL Hops	meshHops	Number of hops that the element is from the root of its RPL routing tree.
Route RPL Link Cost	linkCost	RPL cost value for the link between the element and its uplink neighbor.
Route RPL Path Cost	pathCost	RPL path cost value between the element and the root of the routing tree.

Field	Key	Description
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)

Link Settings

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

Table 25: Link Settings Fields

Field	Key	Description
Firmware Version	meshFirmwareVersion	The Cisco Resilient Mesh Endpoint (RME) firmware version.
Mesh Interface Active	meshActive	The status of the RME.
Mesh SSID	meshSsid	The RME network ID.
PANID	meshPanid	The subnet PAN ID.
Transmit RF Power	meshTxPower	The RME transmission power (dBm).
Security Mode	meshSecMode	The RME security mode.
Transmit PLC TX Level	tx_level dBuV	The PLC level for Itron OpenWay RIVA CAM module and Itron OpenWay RIVA Electric devices (dBuV) where u = micro
RPL DIO Min	meshRplDioMin	An unsigned integer used to configure the Imin of the DODAG Information Object (DIO) Trickle timer.
RPL DIO Double	meshRplDioDbl	An unsigned integer used to configure the Imax of the DIO Trickle timer.
RPL DODAG Lifetime	meshRplDodagLifetime	An unsigned integer used to configure the default lifetime (in minutes) for all downward routes that display as Directed Acyclic Graphs (DAGs).
RPL Version Incr. Time	meshRplVersionIncrementTime	An unsigned integer used to specify the duration (in minutes) between incrementing the RPL version.

Mesh Link Config

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

Table 26: 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.

Mesh Link Keys

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

Table 27: 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.

NAT44 Metrics

NAT44 Metrics Fields describes the fields in the NAT44 area of the Device Info page.

Table 28: 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

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

Table 29: PLC Mesh Info Fields

Field	Key	Description
Mesh Tone Map Forward Modulation	toneMapForwardModulation	Mesh tone map forward modulation: • 0 = Robo • 1 = DBPSK • 2 = DQPSK • 3 = D8PSK
Mesh Tone Map Forward Map	toneMapForward	Indicates the number of usable subcarriers in the channel, shown as a binary octet (for example, 0011 1111). Ones indicate viable channels. The more ones on the map, the higher the channel capacity.
Mesh Tone Map Reverse Modulation	toneMapRevModulation	Mesh tone map reverse modulation: • 0 = Robo • 1 = DBPSK • 2 = DQPSK • 3 = D8PSK
Mesh Tone Map Reverse Map	toneMapReverse	Indicates the number of usable subcarriers in the channel, shown as a binary octet (for example, 0011 1111). Ones indicate viable channels. The more ones in the map, the higher the channel capacity. The reverse map information and RSSI combine to determine viable channels.
Mesh Absolute Phase of Power	N/A	Mesh absolute phase of power is the relative position of current and voltage waveforms for a PLC node.
LMAC Version	N/A	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.

PLC Mesh Info

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

Table 30: PLC Mesh Info Fields

Field	Key	Description
Mesh Tone Map Forward Modulation	toneMapForwardModulation	Mesh tone map forward modulation: • 0 = Robo • 1 = DBPSK • 2 = DQPSK • 3 = D8PSK

Field	Key	Description
Mesh Tone Map Forward Map	toneMapForward	Indicates the number of usable subcarriers in the channel, shown as a binary octet (for example, 0011 1111). Ones indicate viable channels. The more ones on the map, the higher the channel capacity.
Mesh Tone Map Reverse Modulation	toneMapRevModulation	Mesh tone map reverse modulation: • 0 = Robo • 1 = DBPSK • 2 = DQPSK • 3 = D8PSK
Mesh Tone Map Reverse Map	toneMapReverse	Indicates the number of usable subcarriers in the channel, shown as a binary octet (for example, 0011 1111). Ones indicate viable channels. The more ones in the map, the higher the channel capacity. The reverse map information and RSSI combine to determine viable channels.
Mesh Absolute Phase of Power	N/A	Mesh absolute phase of power is the relative position of current and voltage waveforms for a PLC node.
LMAC Version	N/A	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

Raw Sockets Metrics and Sessions View describes the fields in the TCP Raw Sockets area of the **Field Devices** > **Config Properties** page.

Table 31: 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	N/A	The name of the serial interface configured for Raw Socket encapsulation.
TTY	N/A	The asynchronous serial line on the router associated with the serial interface.
VRF Name	N/A	Virtual Routing and Forwarding instance name.

Field	Key	Description
Socket	N/A	The number identifying one of 32 connections.
Socket Mode	N/A	Client or server. The mode in which the asynchronous line interface is set up.
Local IP Address	N/A	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	N/A	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	N/A	The destination IP address of the remote TCP Raw Socket server.
Dest. Port	N/A	Destination port number to use for the connection to the remote server.
Up Time	N/A	The length of time that the connection has been up.
Idle Time	N/A	The length of time that no packets were sent.
Time Out	N/A	The currently configured session idle timeout, in minutes.

Router Battery

The Router Battery Device View describes the fields in the Router Battery (Battery Backup Unit or BBU) area of the **Device Info** page.

Table 32: Router Battery Device View

Field	Key	Configurable	Description
Battery 0 Charge	battery0Charge	No	Shows the battery voltage of BBU 0.
Battery 0 Level (%)	battery0Level	No	Displays the percentage of charge remaining in BBU 0 as a percentage of 100.
Battery 0 Remaining Time	battery0Runtime	No	How many hours remain before the BBU 0 needs to be recharged.
Battery 0 State	battery0State	No	How long BBU 0 has been up and running since its installation or its last reset.
Battery 1 Level (%)	battery1Level	No	Displays the percentage of charge remaining in BBU 1 as a percentage of 100.
Battery 1 Remaining Time	battery1Runtime	No	How many hours remain before BBU 1 needs to be recharged.
Battery 1 State	battery1State	No	How long BBU 1 has been up and running since its installation or its last reset.
Battery 2 Level (%)	battery2Level	No	Displays the percentage of charge remaining in BBU 2 as a percentage of 100.
Battery 2 Remaining Time	battery2Runtime	No	How many hours remain before BBU 2 needs to be recharged.

Field	Key	Configurable	Description
Battery 2 State	battery2State	No	How long BBU 2 has been up and running since its installation or its last reset.
Battery Total Remaining Time	batteryRuntime	No	The total aggregate charge time remaining for all batteries.
Number of BBU	numBBU	No	The number of battery backup units (BBUs) installed in the router. The router can accept up to three BBUs (battery 0, battery 1, battery 2).
Power Source	powerSource	No	The router power source: AC or BBU.

Router Config

Router Config Device View describes the fields in the Router Config area of the **Field Devices** > **Config Properties** page.

Table 33: 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

Router Credentials Fields describes the fields in the Router Credentials area of the **Field Devices** > **Config Properties** page.

Table 34: Router Credentials Fields

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

Router DHCP Proxy Config

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

Table 35: 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

Router Health Device View describes the Router Health fields in the Device Info view.

Table 36: 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: • "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 1 Config

Router Tunnel 1 Config Device View 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.

Field	Key	Configurable	Description
OSPFv3 Area 1	ospfV3Area1	Yes	Defines OSPFv3 Area 1 in which the router (running IPv6) is a member.
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 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

Router Tunnel 2 Config Device View 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	tunnelSrcInterface2	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.

Router Tunnel Config

Router Tunnel Config Device View describes the fields in the Router Tunnel Config area of the **Field Devices** > **Config Properties** page.

Table 39: Router Tunnel Config Device View

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

Field	Key	Configurable	Description
NMBA NHS IPv6 Address	N/A	Yes	Displays the NBMA IPv6 address.
Use FlexVPN Tunnels	N/A	Yes	Displays the FlexVPN tunnel setting.

SCADA Metrics

SCADA Metrics View describes the fields on the SCADA tab of the Device Info page.

Table 40: SCADA Metrics View

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

WiFi Interface Config

WiFi Interface Config Fields describe the fields in the WiFi Interface Config area of the **Field Devices** > **Config Properties** page.

Table 41: WiFi Interface Config Fields

Field	Key	Configurable	Description
SSID	wifiSsid	No	The service set identifier (SSID) assigned to the WiFi interface on the router.

Field	Key	Configurable	Description
Pre-Shared Key	type6PasswordMasterKey	No	The key used to encrypt other pre-shared keys stored on the router.

WiMAX Config

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



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

Table 42: WiMAX Config Fields

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

WiMAX Link Metrics

WiMAX Link Health Fields describe the fields in the WiMAX Link Health area of the Device Info page.

Table 43: 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

WiMAX Link Settings Fields describe the fields in the WiMAX Link Settings area of the Device Info page.

Table 44: 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.

Field	Key	Description
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.