

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
- Setting Preferences for the User Interface, on page 6
- Cisco IoT FND Username and Password Validation, on page 7
- Password Rotation for Router Admin, on page 10
- Managing Routers, on page 17
- Managing Endpoints, on page 34
- Managing MMB GEN 2 Devices, on page 39
- Managing Out-of-Service Devices, on page 45
- Managing Itron Bridge Meters, on page 54
- Landis+Gyr devices, on page 57
- LDevID: Auto-Renewal of Certs and Saving Configuration, on page 59
- Support Expired SUDI Certificate, on page 60
- Configuring Enrollment over Secure Transport, on page 61
- Configuring FND Registration Authority (RA), on page 62
- Managing the Cisco Industrial Compute IC3000 Gateway, on page 68
- Managing the Cisco Wireless Gateway for LoRaWAN, on page 71
- Managing Head-End Routers, on page 74
- Cisco Catalyst IR1100 Expansion Modules in Cisco IoT FND, on page 74
- Itron CAM Module, on page 76
- Lorawan Gateway Module, on page 77
- Routing Path, on page 79
- Managing Servers, on page 80
- Common Device Operations, on page 80
- Configuring Rules, on page 107
- Configuring Devices, on page 111
- Synchronizing Endpoint Membership, on page 121
- Edit the ROUTER configuration template, on page 122
- Cisco IoT FND WPAN, on page 125
- Editing the ENDPOINT Configuration Template, on page 150
- Device-level configuration push, on page 152
- Push configurations to routers, on page 159

- Pushing Configurations to Endpoints, on page 162
- Certificate Re-Enrollment for ITRON30 and IR500, on page 163
- New Events for IR500, on page 166
- Audit Trail for Re-enrollment for Gateway-IR500 Endpoints, on page 166
- Monitoring a Guest OS, on page 167
- Application Management Support in IoT FND, on page 168
- PIMs in Cisco IoT FND, on page 176
- Managing Files, on page 181
- Improved Audit Trail, on page 187
- Hardware Security Module, on page 188
- Demo and Bandwidth Operation Modes, on page 191
- Bandwidth Optimization Mode Configuration, on page 194
- Device Properties, on page 195

Overview

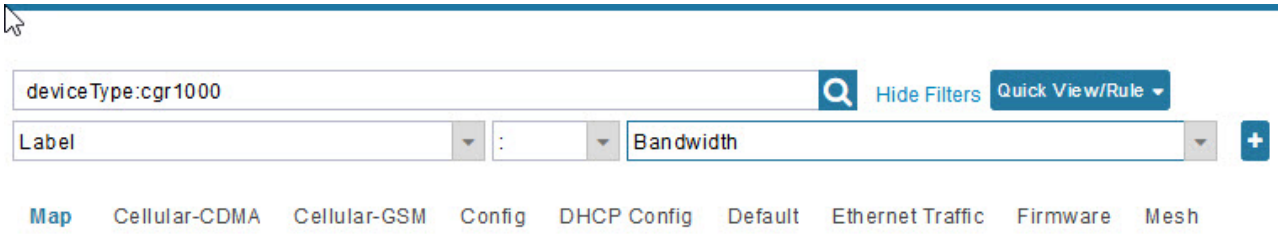
Use the following IoT FND pages to monitor, add and remove devices, and perform other device management tasks that do not include device configuration.

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, IR800, 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, C8000) 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).

Setting Preferences for the User Interface

You can define the preference settings to customize the user interface. The Preferences option is located in the right upper-top corner of the UI.

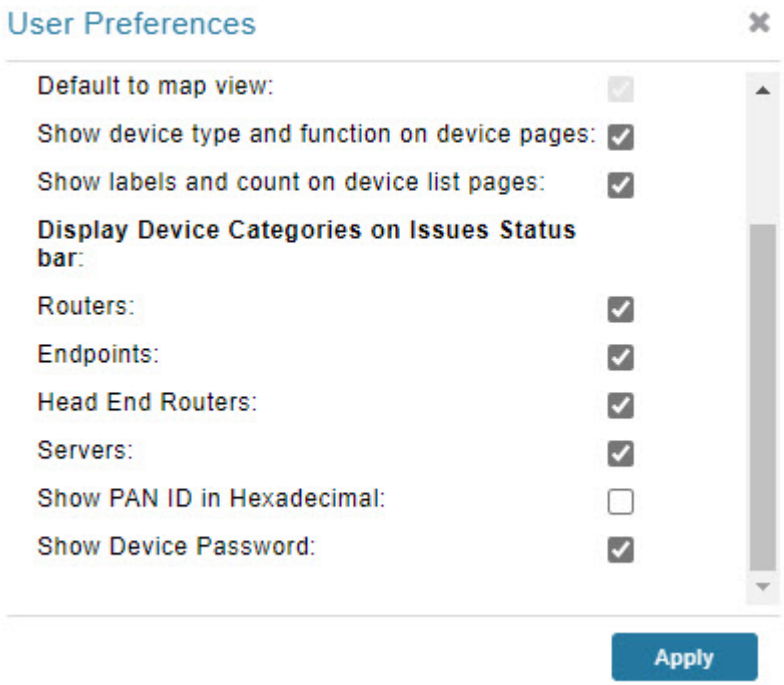


Table 1: User Preference Settings

Options	Description
Show chart on events page	Displays the device events in chart for the current day. To view the chart, go to the OPERATIONS > Events page.
Show summary counts on events/issues page	Displays the summary of the device events and issues, based on the severity level, in the left pane. To view events, go to OPERATIONS > Events page. To view issues, go to OPERATIONS > Issues page.
Enable map	Displays the Map tab in the DEVICES > Field Devices and the OPERATIONS > Issues pages.

Options	Description
Default to map view	Sets the Map tab as the default view in the DEVICES > Field Devices and the OPERATIONS > Issues pages. **Note** To use this option, you must check the Enable Map check box.
Show device type and function on device pages	Displays the device types in the left pane and device function tabs in the right pane of the Device Listing page.
Show labels and counts on device list pages	Displays the device status and count for each device type in the left pane of the Device Listing page.
Display Device Categories on Issues Status bar	The Issues Status bar located in the right-lower end of the user interface displays the device issues for all the device categories. However, you have the option to select the device category as per the requirement. • Routers • Endpoints • Head End Routers • Servers
Show Device Password	The Show Device Password option is available only for the root users and the user with permission "Manage Device Credentials". For other users, this option is not available. By default, this option is not selected. Check the Show Device Password check box and click **Apply** to view the device credentials under Config Properties tab in the Device Details page.
Show PAN ID in hexadecimal	Displays the PAN ID in hexadecimal in the Device Listing page.

Cisco IoT FND Username and Password Validation

Table 2: Feature History

Feature Name	Release Information	Description
Username and Password Validation	Cisco IoT FND Release 5.0	Cisco IoT FND includes username and password validation check for CSV file input.

Information about Cisco IoT FND Username and Password Validation

Starting from Cisco IoT FND Release 5.0, all usernames and passwords that are entered through a device CSV file have to undergo a validation check, before getting saved in the Cisco IoT FND database. This is to ensure that any input which is coming from the automation tools through North Bound API (NBAPI), meets the permitted security standard.

Benefits of Cisco IoT FND Validation for Usernames and Passwords

Cisco IoT FND username and password validation helps in deciphering the admin passwords based on which proper error message can be generated. It also ensures that all username and password credentials are secure and meet necessary standards for the communication between Cisco IoT FND and routers along with other devices.

Validation Criteria for Admin Passwords

Admin passwords:

- Must include characters from at least three of the following four categories: uppercase letters, lowercase letters, numbers, and special characters (excluding '?' and '\').
- Must not contain three consecutive identical characters.
- Must not match the username or the reversed username.
- Permitted characters are: a-z, A-Z, 0-9, and special characters !"#$%&'()*+,-./:;<=>@[]^_`{|}~.

Validation Criteria for Usernames or Passwords

Permitted characters are: a-z, A-Z, 0-9, and special characters !"#$%&'()*+,-./:;<=>@[]^_`{|}~.

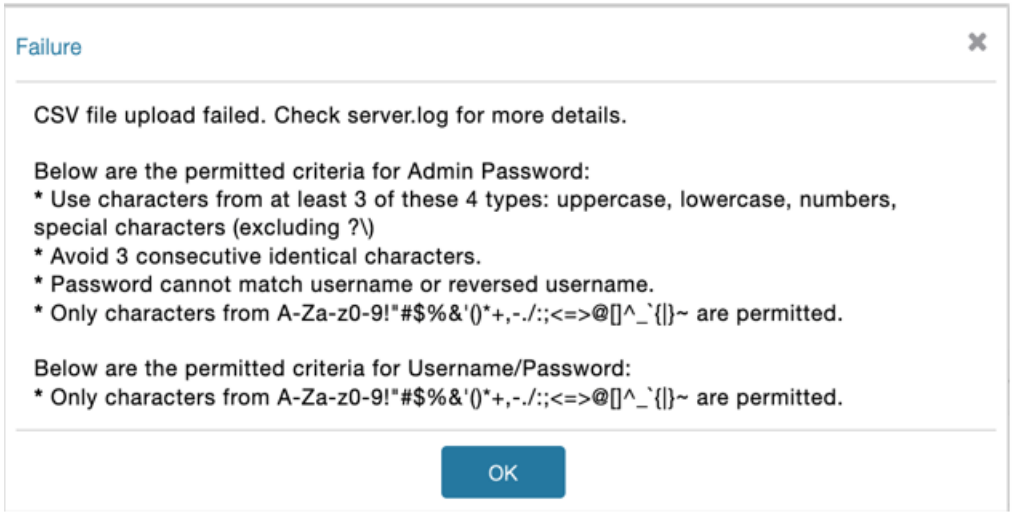
Cisco IoT FND UI CSV File Operations

The device CSV file upload will fail for these instances, as they are not in the required format.

- adminUsername=Admin1
- adminPassword=Admin1
- cgrusername1=test1_®
- wimaxpkmusername=pkm1_®
- wimaxpkmpassword=pkm1@123?



Note A UI failure pop-up message is displayed for such instances.



Server log example:

```
10424: fnd-hsm-ora: Dec 15 2024 18:20:11.873 +0000: %IOTFND-3-UNSPECIFIED:
%[ch=FileUploadJsonAction][sev=ERROR][tid=default task-1]: Failed to upload csv file as
following entries are invalid and do not match the minimum criteria:
[EID:IR807G-LTE-GA-K9+DUMMY-1, 'wimaxpkmusername' should contain following permitted
characters: A-Za-z0-9!"#$%&'()*+,-./:;<=>@[]^_`{|}~ ; 'adminPassword' field has following
errors: 'adminPassword' should not contain 'adminUsername' or reverse of the 'adminUsername'
 field value ; 'cgrusername1' should contain following permitted characters:
A-Za-z0-9!"#$%&'()*+,-./:;<=>@[]^_`{|}~ ; 'wimaxpkmpassword' should contain following
permitted characters: A-Za-z0-9!"#$%&'()*+,-./:;<=>@[]^_`{|}~]
```

Cisco IoT FND NBAPI CSV File Operations

The device CSV file upload through NBAPI will fail for these instances as they are not in the required format.

- adminUsername=Admin1
- adminPassword=Admin1
- cgrusername1=test1_®
- wimaxpkmusername=pkm1_®
- wimaxpkmpassword=pkm1@123?

SOAP UI, fault string example:

```
<faultstring>CSV file upload failed. Few or all entries are invalid and does not match the
 minimum criteria. Please check server.log for more details.</faultstring>
```

Server log example:

```
10462: fnd-hsm-ora: Dec 15 2024 18:24:07.291 +0000: %IOTFND-3-UNSPECIFIED:
%[ch=NBAPICsvFileValidator][sev=ERROR][tid=default task-1][rip=173.38.209.10][rp=22211]:
Failed to upload csv file as following entries are invalid and do not match the minimum
criteria: [EID:IR807G-LTE-GA-K9+DUMMY-1, 'wimaxpkmusername' should contain following permitted
 characters: A-Za-z0-9!"#$%&'()*+,-./:;<=>@[]^_`{|}~ ; 'adminPassword' field has following
 errors: 'adminPassword' should not contain 'adminUsername' or reverse of the 'adminUsername'
 field value ; 'cgrusername1' should contain following permitted characters:
A-Za-z0-9!"#$%&'()*+,-./:;<=>@[]^_`{|}~ ; 'wimaxpkmpassword' should contain following
```

```
permitted characters: A-Za-z0-9!"#$%&'()*+,-./:;<=>@[]^_`{|}~]
```

Password Rotation for Router Admin

Table 3: Feature History

Feature Name	Release Information	Description
Admin Password Rotation	Cisco IoT FND Release 5.0	The Cisco IoT FND tools package includes a new script `rotate_admin_password.sh` with CSV input file. This script enables the seamless rotation of administrator passwords across Cisco IoT FND devices, supporting both Cisco IOS and Cisco IOS XE device types.

Cisco IoT FND supports admin password rotation for routers to prevent unauthorized network access. This password rotation process involves running a script (`rotate_admin_password.sh`) either manually or schedule using a CronJob. The script is available with the cgms tools package in the Cisco IoT FND bundle OVA/rpm as `/opt/cgms-tools/bin/rotate_admin_password.sh`. It is compatible with all Cisco IOS or IOS-XE device types.

Run the `rotate_admin_password.sh` script along with the CSV file.

```
$ ./rotate_admin_password.sh <csv-file>
```

Here are some examples:

Success case:

```
[root@iot-fnd log]# cat rotate_admin_password_status_1750360977943.csv
"EID","MESSAGE","STATUS"
"IR1831-K9+FCW2729Y2QL",
"Successfully updated the admin password.
The new password is <rotated password>","SUCCESS"
```

Failure case:

```
[root@iot-fnd-oracle log]# cat rotate_admin_password_status_1749039357401.csv
"EID","MESSAGE","STATUS"
"IR1101-K9+FCW2708YA7X","'adminPassword' length must be greater than or equal to 3,
'adminPassword' must contain at least 3 out of 4 types: uppercase, lowercase, numbers,
permitted special characters !""#$%&'()*+,-./:;<=>@[]^_`{|}~","FAILURE"
```

Note The `<csv-file>` is the path to the CSV file containing the list of EIDs, and admin passwords.

The password rotation can be either specific to a router or at the HER level, as defined in the CSV file:

- For the router-specific rotation, specify the router EID and the password in the CSV file. The password can be plaintext, secret, or system generated.

- For the HER level rotation, specify the HER in the CSV file and the password is system-generated. The password is rotated for all the devices that tunnel with the HER specified in the CSV file.

The cgms tools package is installed on either Cisco FND Oracle Bare Metal or Postgres Virtual Machine. However, you can also install the cgms tools package on a separate VM (It is not necessary to have FND installed in this VM). For information on installing cgms tools on a separate VM, Installing CGMS Tools RPM on a Separate VM.

Update passwords on multiple routers

You can update passwords on up to 20 routers in parallel using Cisco IoT FND. You can customize the default value of 20 based on your deployment needs.

Here are the instructions to customize the number of parallel password updates:

1. Locate the configuration file located in the path

   `/opt/cgms-tools/conf/rotate-admin-password.properties`
2. Edit the configuration file `rotate-admin-password.properties` using a text editor of your choice
3. Look for the attribute `rotate_admin_pwd_thread_count=20`
4. Change the value `20` to the desired number of threads based on your requirements. For example:

   `rotate_admin_pwd_thread_count=50`

Supported Platforms

- Cisco IOS Device Types: CGR1000 and IR800
- Cisco IOS-XE Device Types: IR8100, IR1800, and IR1100

Prerequisites

Complete the following prerequisites before executing the `rotate_admin_password` script.

- Setting Password Preferences, on page 12 in the `command.txt` file and the device configuration.
- Define parameters in the CSV File.
- Ensure that routers are in `Up` state.
- No active operation such as config push, firmware upgrade should be running in FND.
- Based on the deployment type (Oracle or Postgres), copy the following files to the `cgms-tools` package.
  - **Oracle Bare Metal Deployment**

Filename	Copy From	Copy To
.fnd_psk_enc	/opt/cgms/server/cgms/conf/.fnd_psk_enc	/opt/cgms-tools/conf
fnd_psk.keystore	/opt/cgms/server/cgms/conf/fnd_psk.keystore	/opt/cgms-tools/conf
jdbc.properties	/opt/cgms/tools/conf/jdbc.properties	/opt/cgms-tools/conf/jdbc.properties

Filename	Copy From	Copy To
cgms_keystore	/opt/cgms/server/cgms/conf/cgms_keystore	/opt/cgms-tools/conf
cgms.properties	/opt/cgms/server/cgms/conf/cgms.properties	/opt/cgms-tools/conf

- **Postgres Virtual Machine Deployment**

Copy From	Copy To
docker cp fnd-container:/opt/cgms/server/cgms/conf/.fnd_psk_enc /opt/cgms-tools/conf	/opt/cgms-tools/conf
docker cp fnd-container:/opt/cgms/server/cgms/conf/fnd_psk.keystore	/opt/cgms-tools/conf
docker cp fnd-container:/opt/cgms/tools/conf/jdbc.properties	/opt/cgms-tools/conf/jdbc.properties
docker cp fnd-container:/opt/cgms/server/cgms/conf/cgms_keystore	/opt/cgms-tools/conf
docker cp fnd-container:/opt/cgms/server/cgms/conf/cgms.properties	/opt/cgms-tools/conf

Setting Password Preferences

For a successful admin password rotation, the password preference that is specified in the `command.txt` (located at: `/opt/cgms-tools/conf`) and the device configuration must be in sync. If there is a mismatch, the admin password rotation script that is pushed from FND fails. For example, if the password configured in the device is "plaintext", then the input is "password" in the `command.txt` file.

- **Router password configuration**: The router is configured with either plaintext or secret password.
- **Command.txt file**: The `command.txt` file has two commands, namely "password" and "secret" as shown below. Based on the password configured in the device (plaintext or secret), provide the command (password or secret) in the `command.txt` file.

```
username {username} privilege 15 password {password}
username {username} privilege 15 secret {password}
```

The table lists the allowed password combination for a successful admin password rotation.

Device Configuration	Command.txt
Plaintext	Password (plaintext)
Encrypted	Secret

Attention The admin password rotation fails if there is a password preference mismatch in the `command.txt` and the router configuration. For example, if the router is configured with plaintext and the `command.txt` is enabled for secret, then the password rotation fails. The table lists the password preference combination that is not supported.

Device Configuration	Command.txt
Plaintext	Secret
Secret	Plaintext

What to do next

Define the parameters in the CSV File, on page 13.

CSV File

The `rotate_admin_password` script is executed based on the information you provide in the CSV file, which contains the device EID and the password.

- **EID**: The EID can either be router-specific (EID) or HER-specific (HER EID).
  - If you provide the HER EID, the admin password is rotated for all the routers that are associated with the HER.

    Here's a sample CSV file for a HER device:

    ```
    HEREID,ADMINPASSWORD
    CSR1000V+9J04F38WNBP
    ```

  - If you provide the router-specific EID, the admin password is rotated for that specific router.
- **Password**: Cisco IoT FND provides the following options for the password field in the CSV file:
  - Plaintext Password, on page 14
  - Encrypted Password, on page 14
  - Blank, on page 14

Note
- Regardless of your password preference (plaintext, encrypted, or blank) specified in the CSV file:
  - The admin password is encrypted in the Cisco IoT FND logs, which is decrypted using the signature tool.
  - The admin password appears either in plaintext or secret format depending on the password preference set in the `command.txt` file and the device configuration. For more information, see Setting Password Preferences, on page 12.
- To see the password in the Cisco IoT FND, navigate to **DEVICES** > **FIELD DEVICES** > **Config Properties Tab** > **Router Credentials**.

Plaintext Password

In the CSV file, provide a password that is a combination of uppercase (A-Z), lowercase (a-z), numbers (0-9), and special character (!@#$%^&*.).

Sample CSV file for routers:

```
EID,ADMINPASSWORD
IR1101-K9+FCW2226006G,cisco123!
IR1101-K9+FCW2226004G,Cisco123
IR8140H-P-K9+FDO2J46Z,pdsL$123
```

Encrypted Password

If you want to encrypt the admin password, use the signature tool.

Sample CSV file for routers:

In the following example, the plaintext password is encrypted using the signature tool.

```
[root@iot-tps bin]# cat Single_Device_encrypted.csv
EID,ADMINPASSWORD
IR1831-K9+FCW2729Y2QV,VAXKhqI03xomp40f9xdyhIqYl4hh+6pztOAsRGwhrFUjD0xp+
F7zrIJUWOHpBiGC7yVIsqZyb70AEPuLVuZXGFLU/gQ9wpDSkoBNLVyxBYkSABD5vBG5Z2OS
TtaSva3xjnR9kGnw2P30nXSxEB2PNYHjpi8NVQLEiAz8JwVWLePt2xs6v+kXmsKYFrxZE6e2
Q5Mi9z+FW5COSiDLpt1//aLHIQIzR3QHgsiCi0RG/dVxvBn4Ra6NdYBqAsl17GVcFyvkSJhNs
KyeW0bPvuDpAAgRiga2i3rlJ5m0im/eT513aQWJXjHOotJmU/6sZ4jDzWQKop96modyEYuzrvNQrg==
```

Blank

If the admin password field is blank in the CSV file, the password is autogenerated.

Sample CSV file for routers:

```
EID,ADMINPASSWORD
IR1101-K9+FCW2226005G
```

Sample CSV file for HERs:

```
HEREID,ADMINPASSWORD
CSR1000V+9J04F38WNBP
```

Manual Router Admin Password Rotation

To rotate the admin password manually:

Before you begin

Completing the Prerequisites, on page 11 is a must.

Procedure

Step 1 Run the script to change the password for the router admin.

```
$ ./rotate_admin_password.sh <csv-file>
```

The CSV file contains the list of EIDs and admin passwords. For more information, see CSV File, on page 13.

Step 2 On successful execution of the script, disconnect and reconnect to the router with the new password.

a) If the password update is successful, the database is updated with the new password and the Tcl script updates the password in the `before-tunnel-config`, `before-registration-config`, and `express-setup-config`.
b) If the password update fails, refer to the log for more information.

   You can see the log for more information on the success or failure status, which is available at: `/opt/cgms-tools/log/rotate-router-admin-password.log`.

c) For consolidated success and failure logs on specific devices, you can view them in .csv file.

   For example, rotate_admin_password_status_123.csv

What to do next

Upon successful script execution, verify if the operations such as refresh metrics, config push, firmware upgrade are working fine in FND.

Schedule Admin Password Rotation with CronJob

You can automate the script (`rotate_admin_password`) execution by scheduling at particular time and day of a month. We recommend scheduling the cron job during the monthly maintenance window to avoid conflicts with the active operations in FND. For example, schedule the script to run at 12:00 AM on the first day of every month.

The script automation is supported for the following deployments:

- Schedule for Oracle Bare Metal Deployment, on page 15
- Schedule for Postgres VM Deployment, on page 16

Note For a successful password rotation, it is recommended to allow a 24-hour gap between each script execution.

Schedule for Oracle Bare Metal Deployment

To schedule admin password rotation for Oracle BM deployment:

Before you begin

Prerequisites, on page 11

Procedure

Oracle Bare Metal Deployment: Run the script to schedule for the password rotation.

```
$ cd /etc
$ crontab -e
```

```
#Add below line in crontab. Save the file
0 0 1 * * /opt/cgms-tools/bin/rotate_admin_password.sh <location to csv>
```

Note
Ensure the CSV file is properly formatted and accessible. For more information, see CSV File, on page 13.

What to do next

Upon successful script execution, verify if the operations such as refresh metrics, config push, firmware upgrade are working fine in FND.

Schedule for Postgres VM Deployment

To schedule admin password rotation for Postgres VM deployment:

Before you begin

Prerequisites, on page 11

Procedure

Step 1 Install or upgrade the tools rpm in VM.

a) For install use the command **rpm -ivh** as given in the example:

```
rpm -ivh  cgms-tools-5.0.0-117.x86_64.rpm
```

b) For upgrade use the command **rpm -Uvh** as given in the example:

```
rpm -Uvh cgms-tools-5.0.0-117.x86_64.rpm
```

Step 2 Enable the db connection in pg_hba.conf with the following entry.

```
host    all             all             <VM IP with Subnet>           scram-sha-256
```

Example:

Replace <VM IP with Subnet> with `203.0.113.10/32`

Step 3 Restart postgresql.

```
service postgresql-12 stop
service postgresql-12 start
```

Step 4 Copy the following files from the docker container to the cgms-tools package.

- `docker cp fnd-container:/opt/cgms/server/cgms/conf/.fnd_psk_enc /opt/cgms-tools/conf`
- `docker cp fnd-container:/opt/cgms/server/cgms/conf/fnd_psk.keystore /opt/cgms-tools/conf`
- `docker cp fnd-container:/opt/cgms/tools/conf/jdbc.properties /opt/cgms-tools/conf/jdbc.properties`
- `docker cp fnd-container:/opt/cgms/server/cgms/conf/cgms_keystore /opt/cgms-tools/conf`
- `docker cp fnd-container:/opt/cgms/server/cgms/conf/cgms.properties /opt/cgms-tools/conf`

Step 5 Provide Postgres IP in the jdbc.properties as below.

```
jdbc.url=jdbc:postgresql://<Postgres IP>:5432/cgms
```

Step 6 Add the route in the server for the device reachability. Also, make sure the devices are reachable from the VM.

What to do next

After the script executes successfully, verify if the operations such as refresh metrics, config push, firmware upgrade are working fine in Cisco IoT FND.

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 81 .

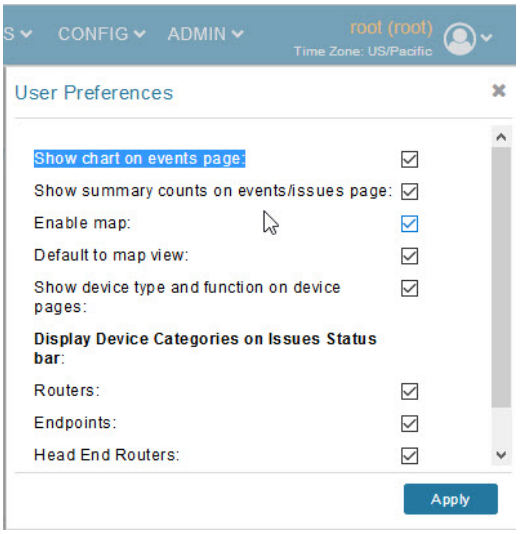
For information about the device properties that display in each view, see Device Properties, on page 195 .

For information about common actions performed in these views (for example, adding labels and changing device properties), see Common Device Operations, on page 80 .

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.

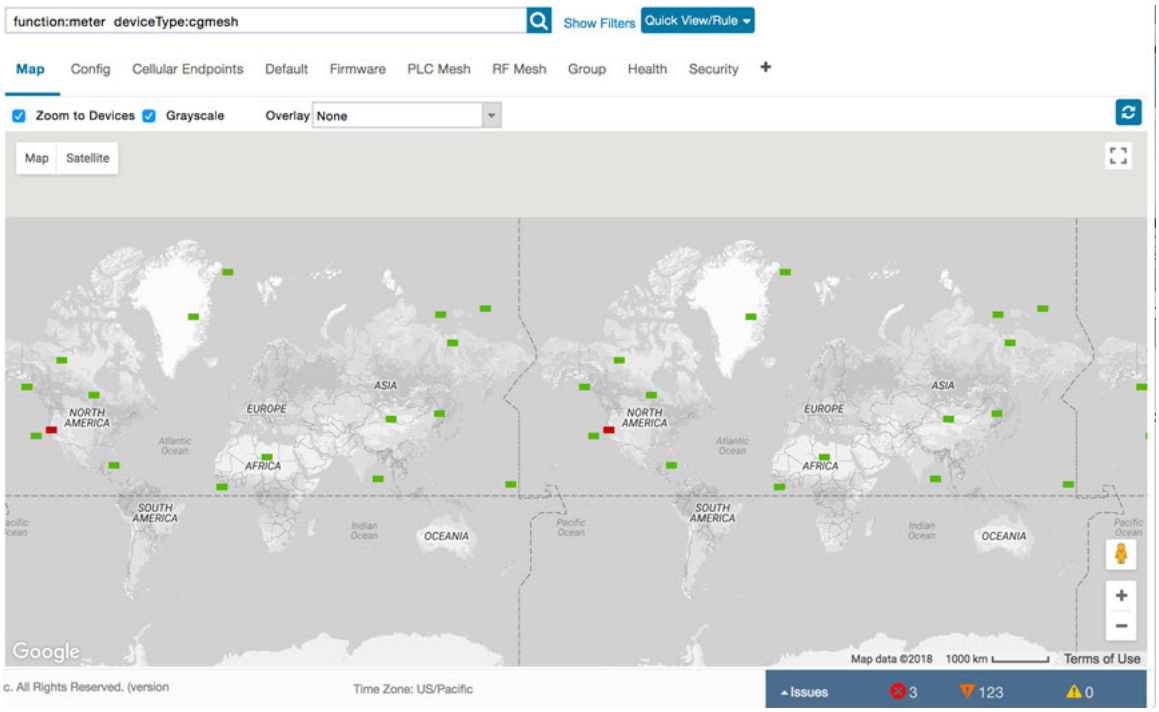
Figure 1: Setting User Preferences for User Interface Display



Note The additional options (not seen in the Figure 1: Setting User Preferences for User Interface Display, on page 18) 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.

Refreshing Router Mesh FFN Key

Using the Refreshing Router Mesh FFN Key option, you can refresh the mesh key of CGR1000 or IR8100 for the Fully Functional Nodes (FFN) such as IR500 and L+G devices (lgnn and lgelectric). The router mesh key is refreshed if you suspect unauthorized access attempts to a router or to avoid device downtime when they expire.

Note FND refreshes the mesh keys automatically when the refresh time is reached.

To refresh the router mesh FFN key:

Procedure

Step 1 Choose **DEVICES** > **FIELD DEVICES** > **Browse Devices tab**.

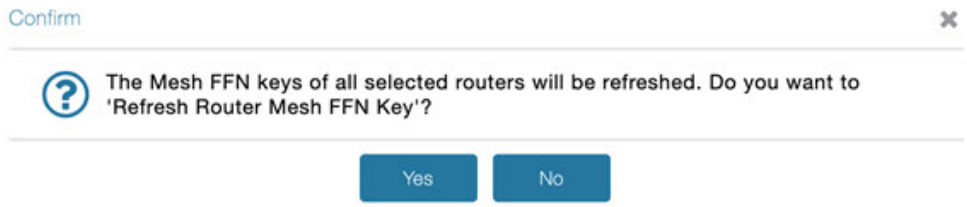
Step 2 Select CGR1000 or IR8100 routers from the left pane.

Step 3 Check the check boxes of the routers to refresh in the right pane (default view).

Step 4 Choose **More Actions** > **Refresh Router Mesh FFN Key** from the drop-down list.

Step 5 Click **Yes** to continue.

Alternatively, you can refresh the mesh key of CGR1000 or IR8100 from the Devices Details page using the **Refresh Router Mesh FFN Key** button.



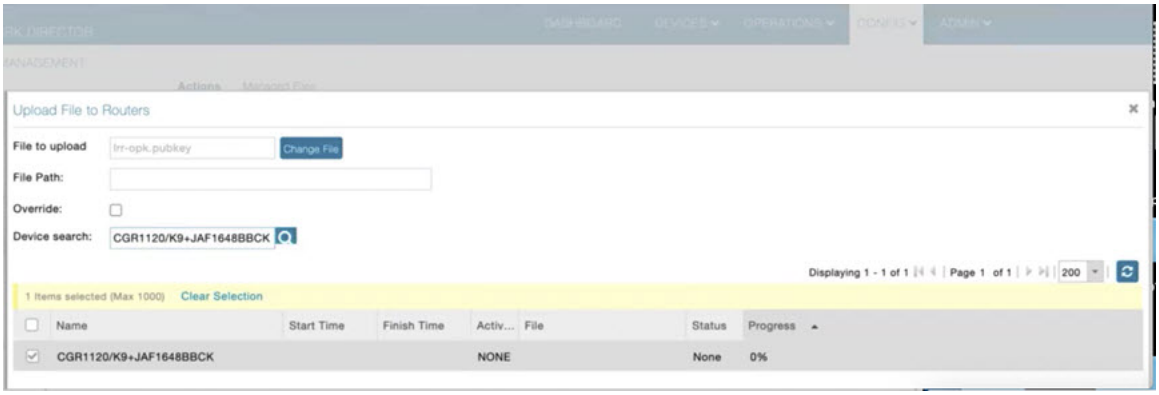
Device File Management for Routers

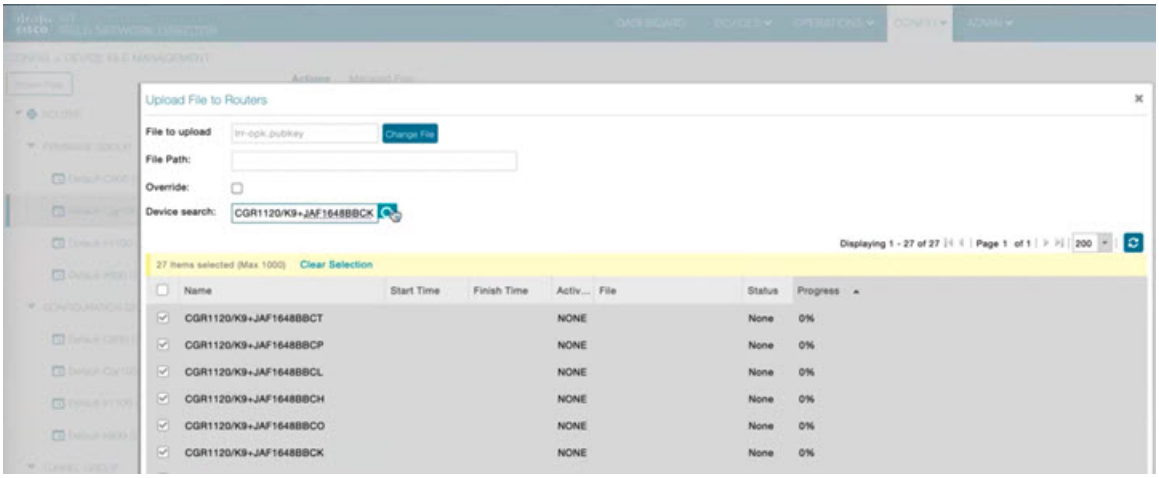
When you want to upload router device files to be managed by IoT FND, go to **CONFIG** > **DEVICE FILE MANAGEMENT** within the application. At that page, select **Actions** > **Upload** to get to the Upload File to Routers page. This page provides you the ability to:

- 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 IR829 ISRs

IoT Field Network Director allows you to manage the following embedded access point (AP) attributes on and IR829 ISRs. The embedded Access Points on the 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 IR800 routers have embedded APs. . 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.

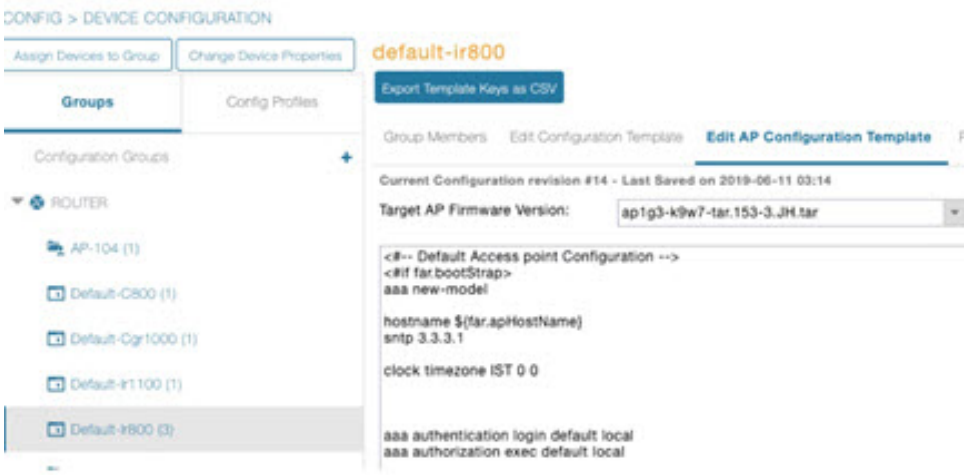
You can only define a unified image (k9w8 - factory shipped) for update via ZTD

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.

Filter routers

You can refine the list of displayed routers by using the built-in router filters under ROUTERS in the Browse Devices pane or saved custom searches in the Quick View pane.

Procedure

Step 1 Locate the desired filter under **ROUTERS** in the **Browse Devices** pane or within the **Quick View** pane.

Step 2 Click the filter to apply it.

Clicking a filter inserts the corresponding search string into the Search field. For example, clicking the **Up** group under **ROUTERS** inserts the search string **status:up**.

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.

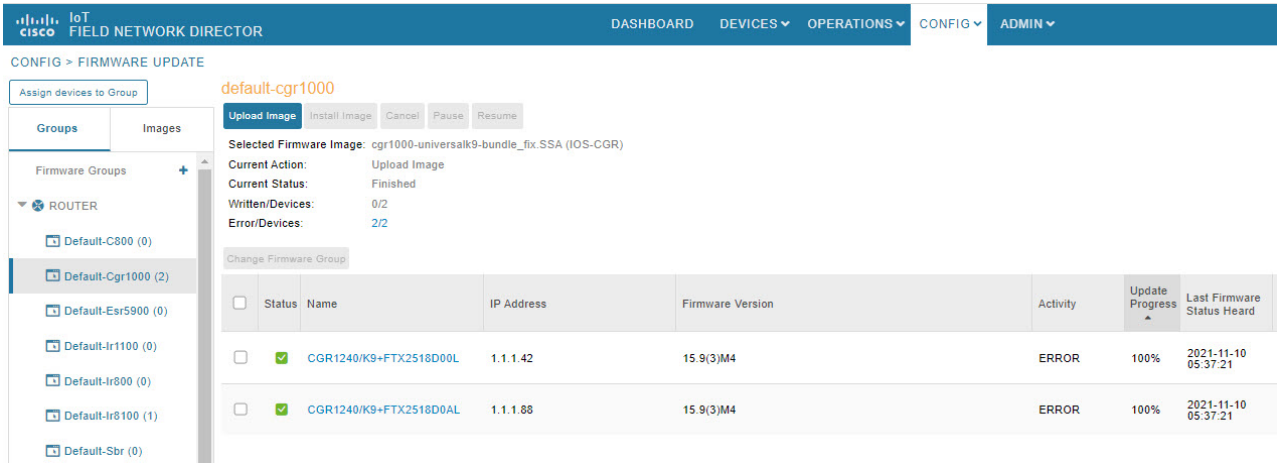
Step 2 From the **Browse Devices** pane, select the desired group listed under ROUTER to display the associated routers.

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-cgr1000, Default-ir1100, Default-ir800 or).



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.

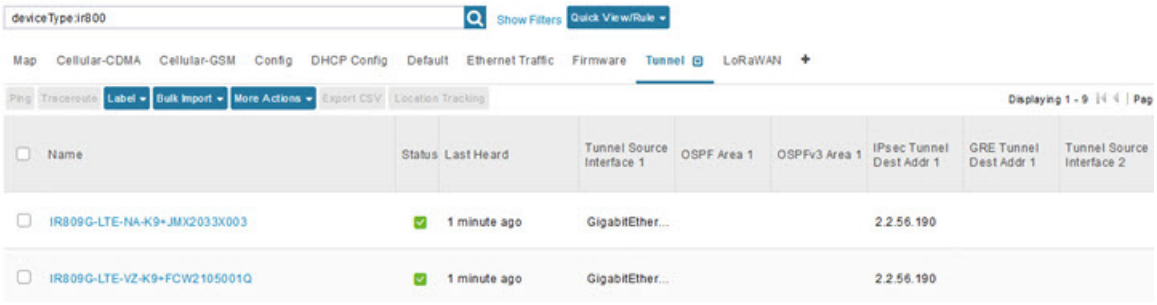
Displaying Router Tunnel Groups

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



Exporting Mesh Routing Tree Data

IoT FND provides an export option in the Mesh Routing Tree tab for exporting the routing tree information of the parent node (router) and its associated child nodes (meters) into an Excel file with xlsx format. The Excel file captures the multi-hop hierarchy (parent-child node hierarchy) in various sheets. Each Excel sheet captures information of the nodes at different hop levels. By default, the parent nodes of the current hop level appear in each sheet, however, you can use the (+) option to expand or collapse the rows to view the parent-child relationship.

This export option is available only for routers and not for other device category (such as endpoints).

Note Ensure that the production environment supports MS Excel files and has sufficient memory for storing files in the file system.

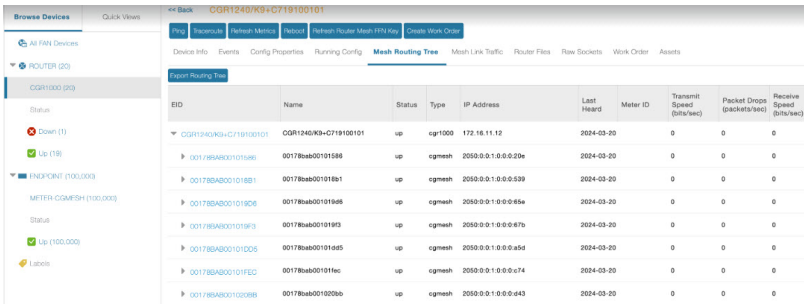
To export mesh routing tree data:

Procedure

Step 1 Choose **DEVICES** > **FIELD DEVICES** > **Browse Devices** > **ROUTERS**.

Step 2 Click the device on the right pane for which you want to export the routing tree data. The **Device Details** page appears.

Step 3 Click the **Mesh Routing Tree** tab.



Step 4 Click the **Export Routing Tree** button to export the routing tree data for the selected device.

The Excel file is stored in the file system with the following name.

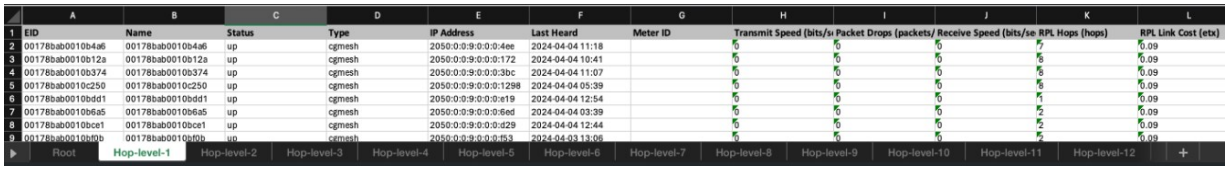
`export-routingtree-<timestamp>.xlsx`

The exported data captures the relationships between the root node and its associated child nodes in various sheets of the Excel file. The first sheet of the file is named as Root and the subsequent sheets are named as Hop-level-<hop number> (example: Hop-level-1, Hop-level-2, and so on).

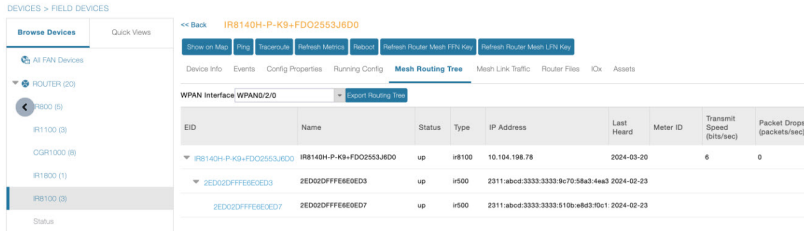
- The first **Root** sheet provides information of the parent node (router) and its associated child nodes (first hop-level child node).



- The consecutive **Hop-level-<hop number>** sheets provide information of the child nodes that are associated with the subsequent parent node.



For IR8100 routers, the exported routing tree data is based on the WPAN interface that is selected in the combo box.



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.

Manage Router Push Configuration Count

Manage Router Push Configuration Count

Table 4: Feature History

Feature Name	Release	Description
Manage Router Push Configuration Count	Cisco IoT FND Release 5.0	Define the number of router configuration changes or updates that you want to apply to routers within a specific group, simultaneously. Manage and track the number of configuration changes applied to a group of routers during the configuration push using Cisco IoT FND.

Information About Manage Router Push Configuration Count

Starting from Cisco IoT FND Release 5.0, change the **Router Push Configuration Count Per Group** directly using Cisco IoT FND. The **Router Push Configuration Count Per Group** field streamlines the configuration process, making it more efficient. The default value of the **Router Push Configuration Count Per Group** field is 5 and the maximum value is 100.

Note Define the **Router Push Configuration Count Per Group** value globally to all router push configurations using Cisco IoT FND. The maximum parallel or concurrent router push configuration count is applied to all the group of routers

Benefits of Manage Router Push Configuration Count

- You can quickly adapt configuration counts to meet changing network requirements, enhancing overall network management.

- The **Router Push Configuration Count Per Group** field minimizes the risk of errors that might occur with manual file edits.

Configure Manage Router Push Configuration Count

1. From the Cisco IoT FND menubar, choose **ADMIN** > **Server Settings** > **Property Settings**.
2. Enter the number of router push configuration you want to be pushed to a group in the **Router Push Configuration Count Per Group**. The maximum number of router push configuration you can enter is 16.
3. Click **Save**.

   The router push configuration count is set.

Viewing Router Usage Statistics

From IoT FND release 4.11 onwards, the **Device Details** page provides a new Router Usage Stats chart for the Cisco IOS (CGR1000 and IR800) and IOS-XE (IR1101, IR8100, IR1800) devices. This chart displays the historical trend of the CPU, memory, and disk usage on an hourly (6 hours), daily (one day), weekly (one week), and monthly (four weeks) basis. You can also visualize the time-specific data by customizing the date and time. However, the maximum date range that you can define is limited to the data retention period specified in the UI (**ADMIN** > **System Management** > **Data Retention**). The data retention period that you can set ranges from a minimum of one to a maximum of 90 days.

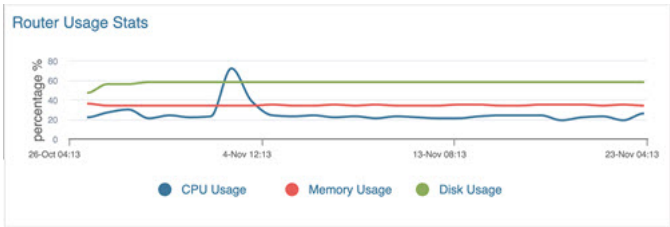
For more information, see Setting Time Filters To View Charts.

Procedure

Step 1 Choose **DEVICES** > **FIELD DEVICES** > **Browse Devices** > **ROUTER**.

Step 2 Select the device type. The Inventory tab displays the devices for the selected device type. You can also filter the usage data based on CPU, memory, or disk.

Step 3 Click the required device on the right pane to view the Router Usage Stats chart for the selected device.



Export device configuration data

Starting from Cisco IoT FND Release 5.1, you can export device configuration data from the **Device Configuration** page.

Feature name	Release information	Description
Export firmware and configuration group data	Cisco IoT FND Release 5.1	Export the firmware group update information from the **Firmware Update** page, and export the configuration group update information from the **Device Configuration** page. The export option is available only for routers and endpoints.

Export device configuration data

This task helps you export device configuration data from Cisco IoT FND.

Before you begin

- Ensure that your local system has enough space to download the firmware and configuration data.
- Ensure that your local system supports .csv files.

Here are the instructions to export device configuration data from Cisco IoT FND:

Procedure

Step 1 From the Cisco IoT FND menubar, choose **CONFIG** > **Device Configuration**

Step 2 Select a router or an endpoint group from the **Groups** tab.

a) Use the **Show Filter** option to narrow down your device group search using the available filters.

Step 3 Select a group member that you'd like to download from the group members table. You can make multiple selections as well.

Step 4 Click the export icon adjacent to the refresh icon.

The device config data is downloaded as a .csv file to your local system.

You've successfully exported the device configuration data.

Search in the Device Configuration Page

Search In The Device Configuration Page

Table 5: Feature History

Feature Name	Release	Description
Search in the Device Configuration page	Cisco IoT FND Release 5.0	The **Device Configuration** page has a new search bar to search through the various device configurations. This search helps narrow down your scope to easily identify a device.

Information About Search in the Device Configuration Page

Starting from the Cisco IoT FND Release 5.0, a search functionality is introduced on the **Device Configuration** page. This feature allows you to efficiently locate specific device configurations by entering relevant search criteria, enhancing your overall experience and productivity.

Benefits of Search in the Device Config Page

- Quickly locate specific device configurations without manually scrolling through extensive lists, saving time and effort.
- The search feature allows for precise filtering, ensuring that you find exactly what you need with minimal effort.

Use the Search in the Device Configuration Page

1. From the Cisco IoT FND menubar, choose **CONFIG** > **Device Configuration**.
2. In the **ROUTER** tab, choose a router and perform a search using the search bar. Click **Show Filter**.
3. In the Filters pane, click the first drop-down box and choose from the following options:

Option	Description
Status	Choose Status as a search criteria if you want to filter the devices based on their statuses. Here are the statuses that you can choose from: • blocked • bootstrapped • bootstrapping • down • outage • outofservice • registering • restored • unheard • unmanaged • unsupported • up
Name	Type in the name of the device that you are looking for in the text box.
EID	Type the EID of the device that you are looking for in the text box.
IP Address	Enter the IP address of the device that you are looking for in the text box.
Last Heard	Use the Last Heard filter to see devices that sent back communication to Cisco IoT between the particular timeframe of your choice.
Mesh Prefix Config	Mesh Prefix Config filter helps you filter device configurations based on their mesh prefixes.
Mesh Prefix Length Config	Filter device configurations using their mesh prefix length configurations.
Mesh PANID Config	This filter uses the Mesh PANID configurations to filter device configurations.
Mesh Address Config	Use the Mesh Address Config to filter out device configurations.
Mesh Prefix Config 2	Use the other Mesh Prefix Config to filter out device configurations.

Option	Description
Mesh Prefix Length Config 2	Use the other Mesh Prefix Length Config 2 to filer out device configurations.
Mesh PANID Config 2	This filter uses the Mesh PANID Config 2 to filter device configurations.
Mesh Address Config 2	Use the Mesh Address Config 2 to filter out device configurations.

4. In the **ENDPOINT** tab, choose an endpoint and perform a search using the search bar. Click **Show Filter**.
5. In the Filters pane, click the first drop-down box and choose from the following options:

Option	Description
Status	Choose Status as a search criteria if you want to filter the devices based on their statuses. Here are the statuses that you can choose from: • blocked • bootstrapped • bootstrapping • down • outage • outofservice • registering • restored • unheard • unmanaged • unsupported • up
Name	Type in the name of the device that you are looking for in the text box.
EID	Type the EID of the device that you are looking for in the text box.
IP Address	Enter the IP address of the device that you are looking for in the text box.
Last Heard	Use the Last Heard filter to see devices that sent back communication to Cisco IoT between the particular timeframe of your choice.

Option	Description
Config Synced	Use the Config Synced filter to see devices with configurations synched with Cisco IoT FND. Choose between true or false.
Operation Type	You can filter out endpoints based on the operation type they are functioning with. Choose from the options: • Config Push • SD Card Password Push • Access Point Config Push • Access Point Bootstrap Push • Re-Enrollment Push • Channel Notch Push • Schedule Channel Notch Push

Option	Description
Push Status	Filter out endpoints based on the configuration push status. Choose from the options: • NOT_STARTED • QUEUED • CONFIGURING • SUCCESS • ERROR • CONFIGURING_SD_CARD_PASSWORD • CONFIGURING_ACCESS_POINT • CONFIGURING_AP_BOOTSTRAP • CONFIG_PUSHED • ATTEMPTS_EXHAUSTED • INIT • ENROLLING • WAITING_ENROLL • CONFIGURING_CHANNEL_NOTCH_SETTINGS • CHANNEL_NOTCH_SETTINGS_CONFIGURED • CONFIGURING_CHANNEL_NOTCH_LOAD_REQUEST • CHANNEL_NOTCH_REQUEST_CONFIGURED • SKIPPED

6. In the **GATEWAY** tab, choose a gateway and perform a search using the search bar. Click **Show Filter**.
7. In the Filters pane, click the first drop-down box and choose from the following options:

Option	Description
Status	Choose Status as a search criteria if you want to filter the devices based on their statuses. Here are the statuses that you can choose from: • blocked • bootstrapped • bootstrapping • down • outage • outofservice • registering • restored • unheard • unmanaged • unsupported • up
Name	Type in the name of the device that you are looking for in the text box.
EID	Type the EID of the device that you are looking for in the text box.
IP Address	Enter the IP address of the device that you are looking for in the text box.
Last Heard	Use the Last Heard filter to see devices that sent back communication to Cisco IoT between the particular timeframe of your choice.

8. Click **+** button to populate the searchbar.
9. Click the **Search** icon to perform a search based on the filters.

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 81.

For information about the device properties displayed in each view, see Device Properties, on page 195.

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 80.

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.
Connectivity	Generates a device connectivity report with the following parameters: • WPAN Status • PPP Link Stats • Neighbor 802.15.4g

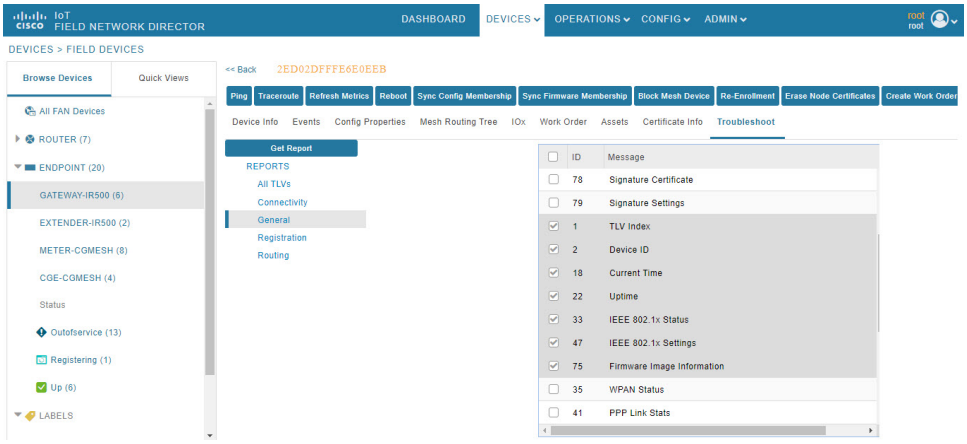
Report	Description
General	Generates a report with the following general parameters associated to the device: • TLV Index • Device ID • Current Time • Uptime • IEEE 802.1x Status • IEEE 802.1x Settings • Firmware Image Information
Registration	Generates a report with the following registration parameters: • 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
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.



Table 6: Feature History

Feature Name	Release Information	Description
Troubleshooting On-Demand Statistics for Endpoints	IoT FND 4.8	You can generate predefined system reports within IoT FND to help troubleshoot issues with endpoints such as GATEWAY-IR500, EXTENDER-IR500, METER-CGMESH, or any third-party METERS. A Troubleshoot page is displayed for each supported endpoint.

Managing MMB GEN 2 Devices

Starting from release 4.11, IoT FND manages the MMB devices. These devices function as endpoints and are supported on the CGR1000 and IR8140 platforms. Additionally, the IR8140 offers dual WPAN support. FND allows you to install and register the devices, push the configuration template to the default configuration group, and update the firmware image. For more information, see Working with MMB Devices, on page 40.

Table 7: MMB Device Information Mapping in IoT FND

Device Type	Device Category	Device Function	PID
CGMESH	Endpoints	CGE	CGEREF6
CGMESH	Endpoints	CGE	CGEREF6_IE

License

The MMB devices use the endpoint license for registering with IoT FND.

RBAC

The existing endpoint RBAC is applicable for the MMB devices as well. No new role or permission added to manage MMB devices in IoT FND.

Prerequisites

Before you install and register the MMB devices in IoT FND, ensure that the platforms, and the MMB devices have the supported firmware versions.

Devices	Firmware Version
CGR1240	15.9(3)M7a
IR8140	17.11.1a

Devices	Firmware Version
MMB	2.4.8 and later
WPAN	6.6.5

Working with MMB Devices

This section explains how to manage the MMB devices in IoT FND.

Installing and Registering

To install and register the MMB devices:

Before you begin

IoT FND manages only the MMB devices with firmware version 2.4.8 and later.

Procedure

Step 1 Choose **DEVICES** > **FIELD DEVICES** > **Browse Devices** > **ENDPOINTS**.

Step 2 In the Inventory page, click **Add Devices**. The **Add Devices** window allows you to add the MMB devices in FND through the CSV file.

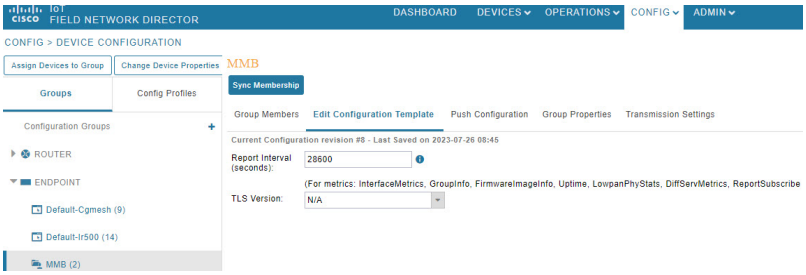
Step 3 Browse and select the CSV file, then click **Add**. The CSV file should have the minimum required fields such as EID, device type, and device function.

Step 4 Use the CSMP mechanism to register the MMB devices with FND. On successful completion of registeration, the MMB devices are listed in either MESH-CGMesh or CGE-CGMESH device type.

For more information, see OpenCSMP.

Configuration Group

From the **Device Configuration** page, you can manage the configuration group and apply the configuration template to the default configuration group. Generally, the MMB devices are added to the Default-CGMesh group. However, it is recommended to create a separate configuration group for the MMB devices or move the existing meters to another configuration group. If the MMB devices coexist with the meters in the Default-CGMesh group, then the fields that are not shown for the unsupported features of the MMB devices are unavailable for the meters as well in the UI (though the fields are applicable for the meters). For example, the EST certificate enrollment feature is not supported for the MMB devices, therefore, the related fields such as Certificate AutoRenew Settings, DTLS Settings, are not displayed in the UI.



From the **CONFIG** > **DEVICE CONFIGURATION** page, you can configure the following:

Tabs	Description
Group Members	Lists the MMB devices in the default configuration group.
Edit Configuration Template	Allows you to set the report interval in seconds and select the TLS version. **Note** **Certificate AutoRenew Settings**, **DTLS Settings**, and **Interface ACL Settings** fields are not available as EST certificate enrollment is not supported.
Push Configuration	Pushes the endpoint configuration to the default configuration group. **Note** **Push Endpoint Re-enrollment** option is not available as EST certificate enrollment is not supported.
Group Properties	Allows you to specify the markdown time for endpoints.
Transmission Settings	Allows you to set the following: • Transmission Speed: Allows you to customize the transmission speed (slow, medium, or fast). • Multicast Threshold (nodes): Enter the minimum number of nodes.

Related Topics

Unsupported Features, on page 45

Firmware Group

From the **Firmware Update** page, you can manage the firmware images for the default firmware group. Generally, the MMB devices are added to the Default-Cgmesh group, but it is recommended to create a separate group.

Tabs	Description
Firmware Management	Allows you to upload the firmware image for the selected firmware group. **Note** **Install Patch** option is disabled.
Devices	Lists the devices in the firmware group. You also have the option to filter the devices based on the device properties.
Logs	Provides the status of the firmware upload.
Transmission Settings	Allows you to specify the transmission speed.

Viewing on Dashboard

The FND Dashboard provides MMB device data in the endpoint dashlets. You can view the historical trend for the following charts:

- Endpoint states over time
- Endpoint config group template mismatch over time
- Endpoint firmware group template mismatch over time
- Endpoint inventory
- Hop count distribution
- Config group template mismatch
- Firmware group template mismatch
- RF and PLC Media utilization over time

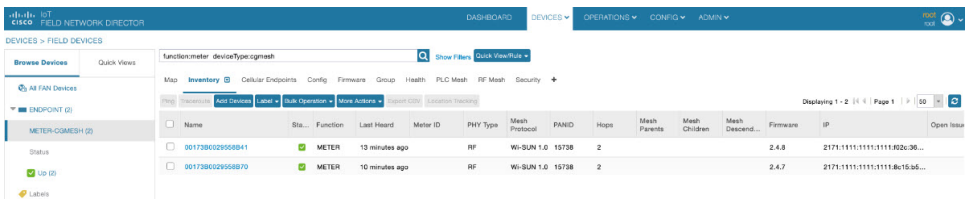
Viewing Device Details

To list and view the device details:

Procedure

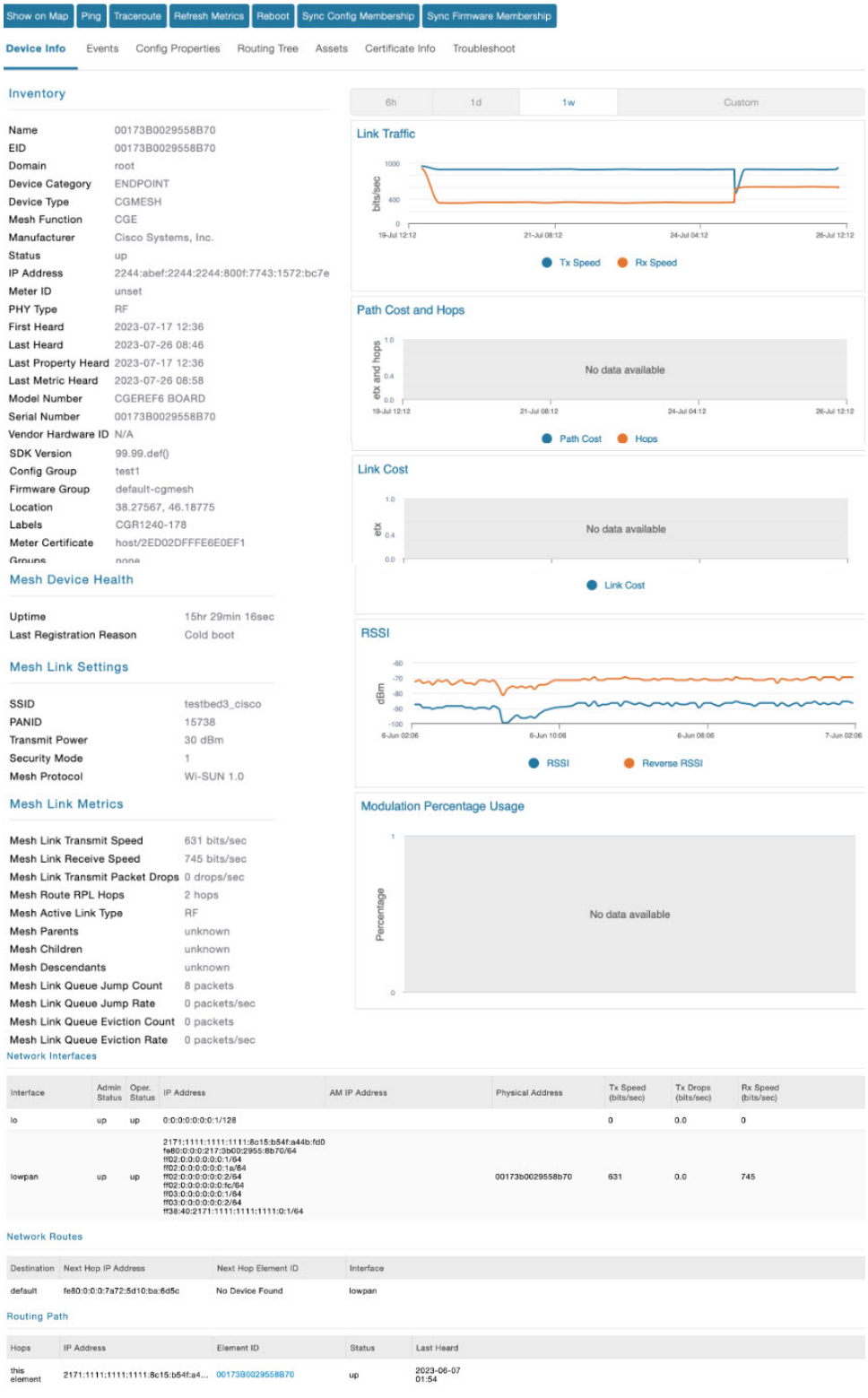
Step 1 Choose **DEVICES** > **FIELD DEVICES** > **Browse Devices** > **ENDPOINTS**.

Step 2 Select the device type, MESH-CGMesh or CGE-CGMESH, to view the device list on the right pane.



Step 3 Click the device on the right side to view the device details.

Note
As the EST certificate enrollment is not supported for the MMB devices, the **Block Mesh Device**, **Re-enrollment**, and the **Erase Node Certificate** buttons are not shown in the Device Info page.


Show on Map
Ping
Traceroute
Refresh Metrics
Reboot
Sync Config Membership
Sync Firmware Membership
Device Info
Events
Config Properties
Routing Tree
Assets
Certificate Info
Troubleshoot
Inventory
Name 00173B0029558B70
EID 00173B0029558B70
Domain root
Device Category ENDPOINT
Device Type CGMESH
Mesh Function CGE
Manufacturer Cisco Systems, Inc.
Status up
IP Address 2244:abef:2244:2244:800f:7743:1572:bc7e
Meter ID unset
PHY Type RF
First Heard 2023-07-17 12:36
Last Heard 2023-07-26 08:46
Last Property Heard 2023-07-17 12:36
Last Metric Heard 2023-07-26 08:58
Model Number CGEREF6 BOARD
Serial Number 00173B0029558B70
Vendor Hardware ID N/A
SDK Version 99.99.def()
Config Group test1
Firmware Group default-cgmesh
Location 38.27567, 46.18775
Labels CGR1240-178
Meter Certificate host/2ED02DFFFE6E0EF1
Groups none
Mesh Device Health
Uptime 15hr 29min 16sec
Last Registration Reason Cold boot
Mesh Link Settings
SSID testbed3_cisco
PANID 15738
Transmit Power 30 dBm
Security Mode 1
Mesh Protocol Wi-SUN 1.0
Mesh Link Metrics
Mesh Link Transmit Speed 631 bits/sec
Mesh Link Receive Speed 745 bits/sec
Mesh Link Transmit Packet Drops 0 drops/sec
Mesh Route RPL Hops 2 hops
Mesh Active Link Type RF
Mesh Parents unknown
Mesh Children unknown
Mesh Descendants unknown
Mesh Link Queue Jump Count 8 packets
Mesh Link Queue Jump Rate 0 packets/sec
Mesh Link Queue Eviction Count 0 packets
Mesh Link Queue Eviction Rate 0 packets/sec
6h
1d
1w
Custom
Link Traffic
bits/sec
Tx Speed
Rx Speed
Path Cost and Hops
etx and hops
No data available
Path Cost
Hops
Link Cost
etx
No data available
Link Cost
RSSI
dBm
RSSI
Reverse RSSI
Modulation Percentage Usage
Percentage
No data available
Network Interfaces
Interface
Admin Status
Oper. Status
IP Address
AM IP Address
Physical Address
Tx Speed (bits/sec)
Tx Drops (bits/sec)
Rx Speed (bits/sec)
lo up up 0:0:0:0:0:0:0:1/128 0 0.0 0
lowpan up up 2171:1111:1111:1111:8c15:b54f:a44b:fd0 fe80:0:0:0:217:3b00:2955:8b70/64 ff02:0:0:0:0:0:0:1/64 ff02:0:0:0:0:0:0:1a/64 ff02:0:0:0:0:0:0:2/64 ff02:0:0:0:0:0:0:fc/64 ff03:0:0:0:0:0:0:1/64 ff03:0:0:0:0:0:0:2/64 ff38:40:2171:1111:1111:1111:0:1/64 00173b0029558b70 631 0.0 745
Network Routes
Destination
Next Hop IP Address
Next Hop Element ID
Interface
default fe80:0:0:0:7a72:5d10:ba:6d5c No Device Found lowpan
Routing Path
Hops
IP Address
Element ID
Status
Last Heard
this element 2171:1111:1111:1111:8c15:b54f:a4... 00173B0029558B70 up 2023-06-07 01:54

Viewing Events and Issues

To view the events and issues for the MMB devices, go to **OPERATIONS** > **Events or Issues** > **ENDPOINT**.

For information on viewing and filtering the events and issues, see View Events and Viewing Issues.

Limitations

- **IoT FND Limitation**: ITRON meters and MMB devices cannot coexist in the Default-CGMesh group. We recommend you to have separate groups for ITRON meters and MMB devices for the configuration and firmware management.
- **Platform Limitation**: Registering the MMB devices with FND using LoWPAN interface is not supported. For more information, see CSCwh31845.

Unsupported Features

This section lists some of the key features that are not supported for the MMB devices in IoT FND, Release 4.11:

User Interface Components	Unsupported Features
Configuration Management (**CONFIG** > **Device Configuration**)	• EST certificate enrollment • ACL
Firmware Management (**CONFIG** > **Firmware Update**)	• Install patch • Firmware downgrade • Firmware image backup (in the upload and running slots) • Wi-SUN stack switch

Managing Out-of-Service Devices

The Out-of-Service (OOS) device state marks the end of life of a device in Cisco IoT FND. The end of life of a device is a result of meter or module change, withdrawal from services, or deletion of device from router, endpoint, or gateway. The OOS state is applicable for devices in routers, endpoints, and gateways managed by IoT FND. The OOS devices have the characteristics of both Managed and Unmanaged device status. The OOS devices do not consume license; however, the devices need license to exist in FND. The OOS state is applicable only for the classic license in FND and not for the smart license.

Note If there is no license available for the same device type, then the OOS devices move to Unmanaged state based on priority while adding new devices.

Table 8: Feature History

Feature Name	Release Information	Description
Out-of-Service (OOS) device state	IoT FND 4.8	The OOS device state marks the end of life of a device in Cisco IoT FND. The end of life of a device is a result of meter or module change, withdrawal from services, or deletion of device from router, endpoint, or gateway.

Managing OOS Devices Using CSV — IoT FND UI

This section explains how you can add, update, or delete OOS devices using a CSV file and the subsequent impact on the license count during the process.

Note The devices should have "outofservice" status in the CSV file to perform any action such as add, update, or delete in IoT FND.

Adding OOS Devices Using CSV — IoT FND UI

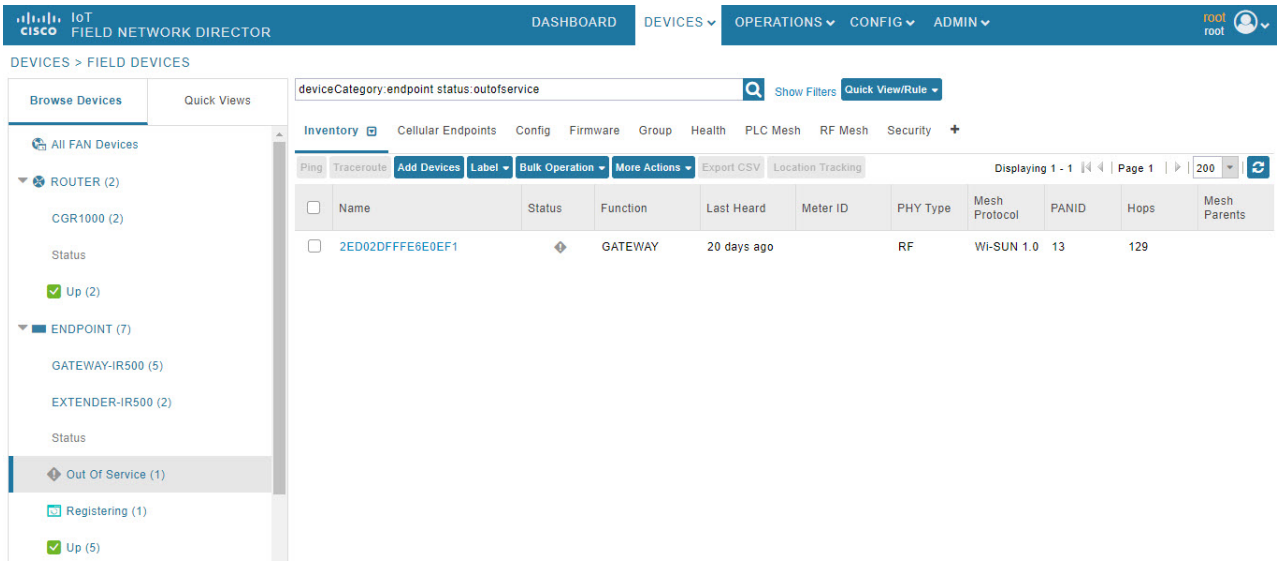
Using the CSV file, we can add OOS devices into IoT FND. The OOS devices do not consume license, however, the license should be available for them to exist in FND.

Note If the license is unavailable, then the OOS devices move to **Unmanaged** status.

To add OOS devices:

Procedure

Step 1 Choose **DEVICES** > **Field Devices** > **Browse Devices** .
Step 2 Click **Add Devices** button on the right pane to add devices of router, endpoint, or gateway.
Step 3 Click Browse to locate the csv file that has the OOS devices.
Step 4 Click **Open**.
Step 5 Click **Add**.
Step 6 Click **Close** when done.



Updating Device Status Using CSV — IoT FND UI

You can update any device state to OOS state using the **Change Device Properties** option. This action frees up the license count for adding new devices.

Note You cannot move Unmanaged devices to OOS state.

To update OOS devices:

Procedure

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

Step 2 On the right pane, choose **Bulk Operation** > **Change Device Properties**.

Step 3 Click Browse to locate the CSV file.

Step 4 Click **Open**.

Step 5 Click **Change** to change the existing device status to Out of Service status.

Step 6 Click **Close** when done.

Deleting OOS Devices Using CSV — IoT FND UI

Deleting OOS devices does not change the license count.

To delete OOS devices:

Procedure

Step 1 Choose **DEVICES** > **Field Devices** > **Browse Devices** .
Step 2 On the right pane, click **Bulk Operation** > **Remove Devices**.
Step 3 Click Browse to locate the CSV file containing the list of devices (in OOS status) to delete.
Step 4 Click **Open**.
Step 5 Click **Remove**.
Step 6 Click **Close** when done.

Managing OOS Devices Using CSV — IoT FND NB API

You can add, update, or delete OOS devices using IoT FND NB API using the CSV file. The NB API used is SOAP (Simple Object Access Protocol) UI.

Note The devices should have "outofservice" status in the CSV file to perform any action such as add, update, or delete in IoT FND.

- Adding OOS devices does not consume license. However, license should be available for the devices. If there is a request for adding new devices, then the devices in OOS state move to Unmanaged state on priority to accommodate new devices.
- Updating a device state to OOS state frees up the license count. You can update any Managed device state to OOS state. But this action prompts for license enforcement and reinstatement.
- Deleting OOS devices does not change the license count.

For more information, refer to the topic, Add, Update, or Delete OOS Devices Using CSV — IoT FND NB API.

Add, Update, or Delete OOS Devices Using CSV — IoT FND NB API

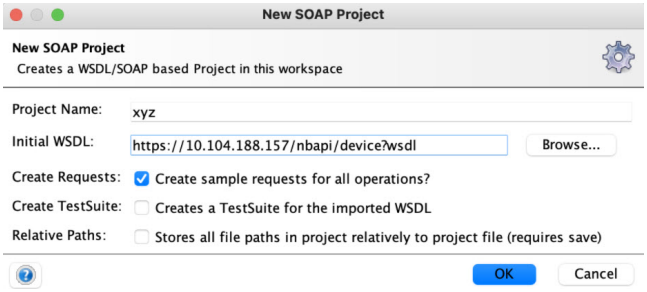
To add, update, or delete OOS devices:

Procedure

Step 1 Open the IoT FND NB API (SOAP UI:https://www.soapui.org/).
Step 2 From the **Soap** menu, select **New Soap Project**.
Step 3 In the **New SOAP Project** window, provide the following information:

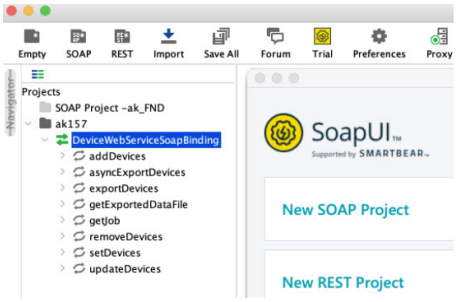
- Project Name.
- Click **Browse** to locate the Initial WSDL (Web Services Description Language).

- Check the **Create Requests** check box.



Step 4 Click **OK** when done.

The Projects tree on the left pane lists the available APIs.

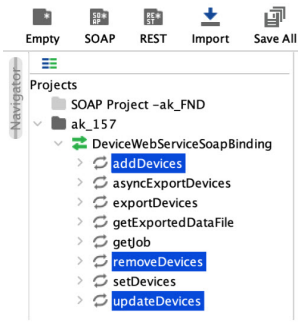


Step 5 Right-click one of the following API options and select NewRequest:

a. **addDevices** — To add OOS devices.

b. **updateDevices** — To update device status to OOS.

c. **removeDevices** — To delete OOS devices.



Step 6 In the **New Request** window, enter the request name and click **OK**.

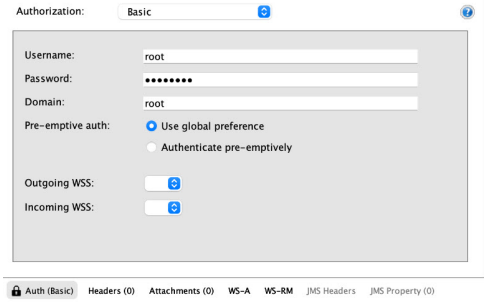
An XML window appears on the right pane.

Step 7 Click **SoapUI log** on the right lower pane.

Add Authorization window appears.

Step 8 Select the Authorization type as **Basic** and click **OK**.

Step 9 Enter **Username**, **Password**, and **Domain** details.



Step 10 Click **Attachments** tab.

Step 11 Click + icon to locate the CSV file containing the list of OOS devices.

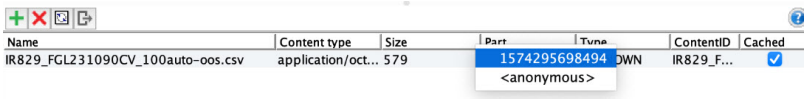
You can perform one of the following actions:

a) **Add** — Select the CSV file to add OOS devices to FND.
b) **Update** — Select the CSV file to update the device state as OOS in FND.
c) **Delete** — Select the CSV file to delete OOS devices from FND.

Step 12 Click **Open**.

Step 13 In the confirmation box, click **Yes**.

Step 14 Select the Part Number.



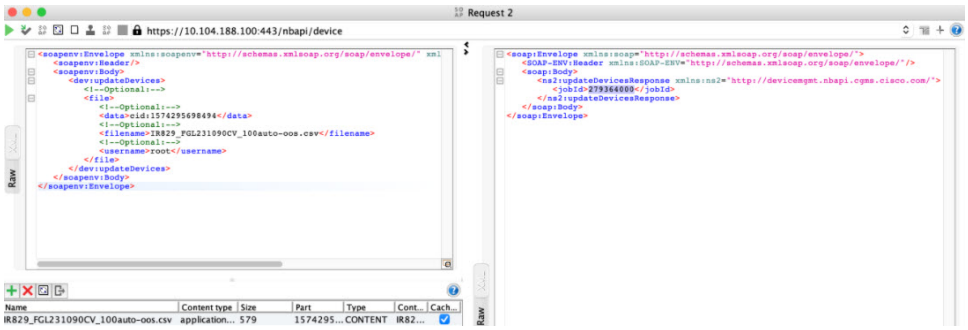
Step 15 In the XML file, provide the following information:

- Update the filename (copy the .csv filename from the Name field).
- Enter root as username.
- Update the HTTPS URL with FND IP details.

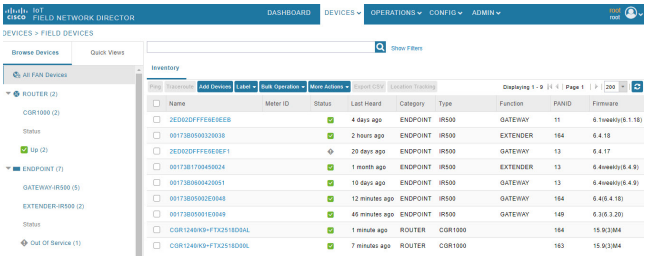


Step 16 Click the green arrow on the left top corner to send the request.

Step 17 On successful completion of the NB API request, SoapUI shows a Job ID on the right side of the pane.



Refresh FND UI. You can view the list of OOS devices based on the operation performed.



Managing License for OOS Devices

This section is moved to a different location with improved user experience. For more information see, Managing Licenses For OOS Devices.

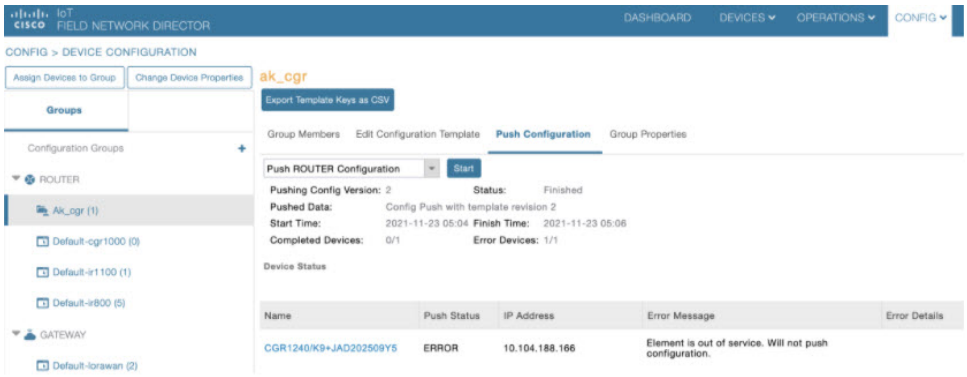
Supported Actions for OOS Devices

Cisco IoT FND enables you to ping and traceroute OOS devices of router, endpoint, or gateway on the **Device Info** page (**DEVICES** > **Field Devices** > **Browse Devices**).

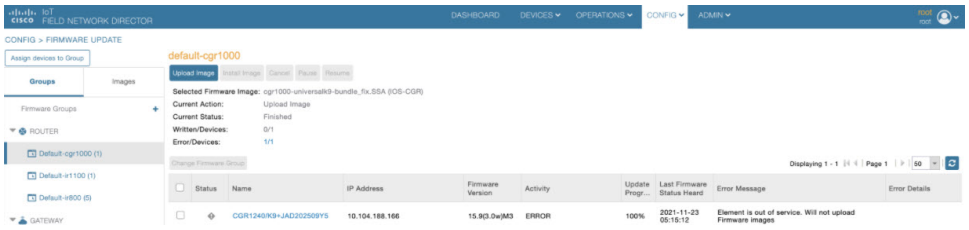
Restrictions for OOS Device Actions

The following actions are not supported for OOS device state:

- In the **Device Info** page, you can ping or traceroute OOS devices like any other device state. However, the actions such as Refresh Metrics, Reboot, Sync Config Membership, Sync Firmware Membership, Block Mesh Device, Erase Node Certificates, or Create Work Order are not supported.
- In the **CONFIG** > **DEVICE CONFIGURATION** page, when you use Push Configuration option on OOS devices, an error message appears.

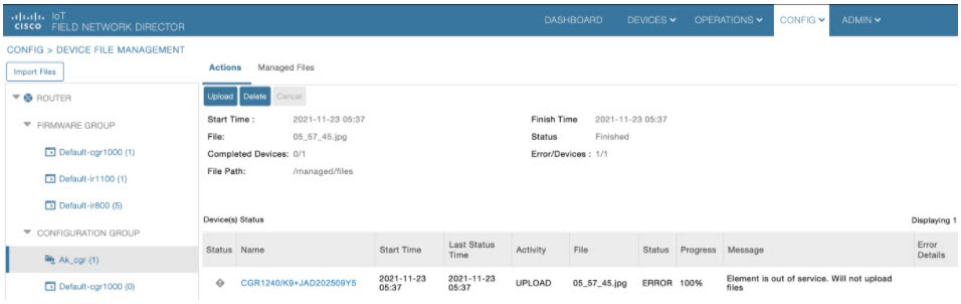


- In the **CONFIG** > **Firmware Update** page, when you use the upload or install image option on OOS devices, an error message appears.



- In the **CONFIG** > **Device File Management** page, if the upload file contains OOS devices, an error message appears.

Note You are not allowed to delete the existing file that has OOS devices now.



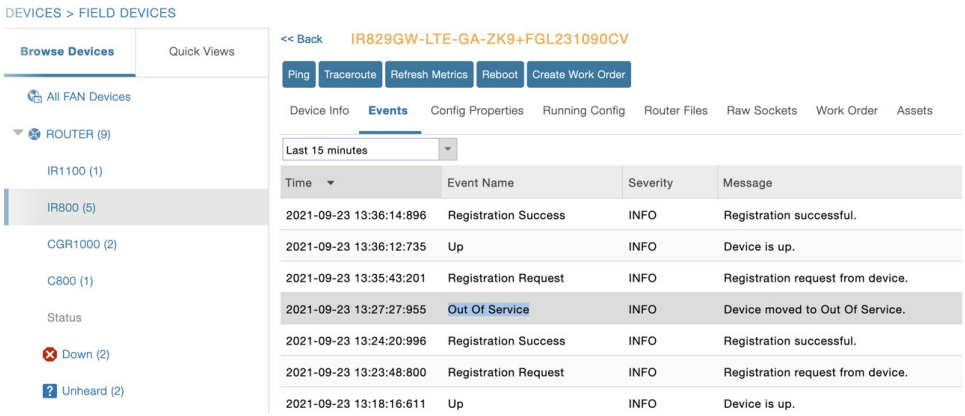
Viewing Events and Audit Trails for OOS Devices

- In the **Operations** > **Events** page, you can view only existing events for the OOS devices. The generated event provides information on when the device moved to OOS state.

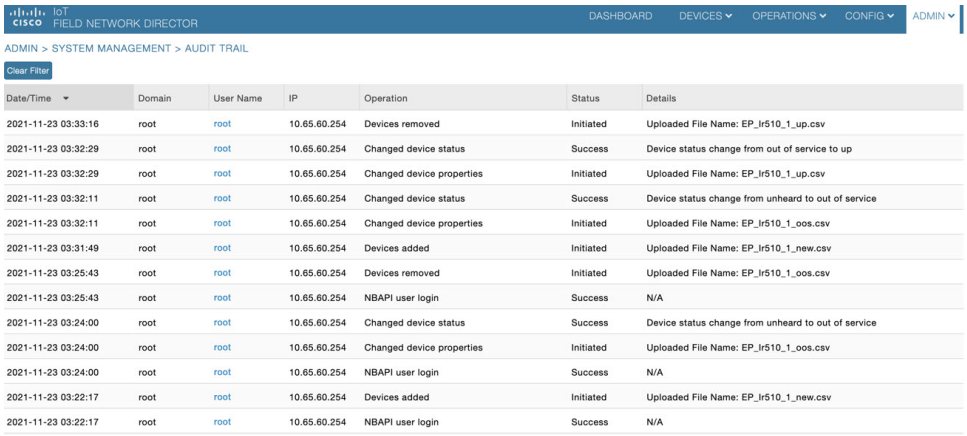
Note You cannot generate events for the devices that are currently in OOS state.

Note The Get Report option (in the Troubleshoot tab) is not supported for OOS devices.

To filter existing OOS device events, refer to Viewing OOS Devices Using Filters, on page 53.



- In the **ADMIN** > **System Management** > **Audit Trail** page, you can view the audit trail for OOS devices. The audit trail provides information on when the device moved to OOS state from Managed state and the other way round.



Viewing OOS Devices Using Filters

You can view the events generated for OOS devices using the filter option.

Procedure

Step 1 Choose **OPERATIONS** > **Events**.

Step 2 Click **Show Filter** option.

a) Select **Event Name** from the first drop-down list.

b) Select **Out of Service** option from the third drop-down list.
c) Click + icon to add the event name selected.

Step 3 Click the search icon.

The OOS device events are displayed.

Note
You can also customize your search using the **Custom Time Filter** drop-down list on the left pane. This option allows you to filter events based on relative or absolute time.

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

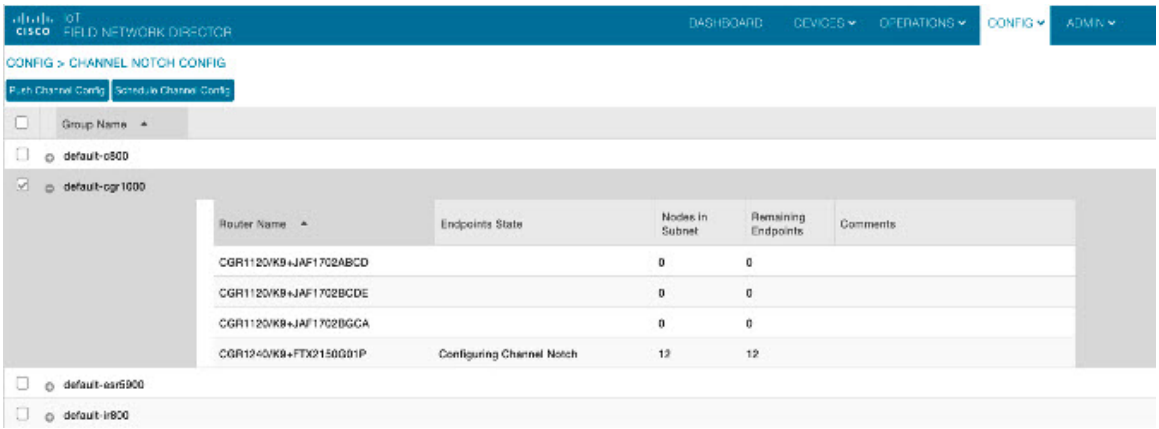
to the endpoints for all routers in the selected router config groups, you can press the Push Channel Config button. As the process of the channel config push progresses, the associated router config groups nested tables show the updated, remaining endpoint count and endpoint state of all endpoints.

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.

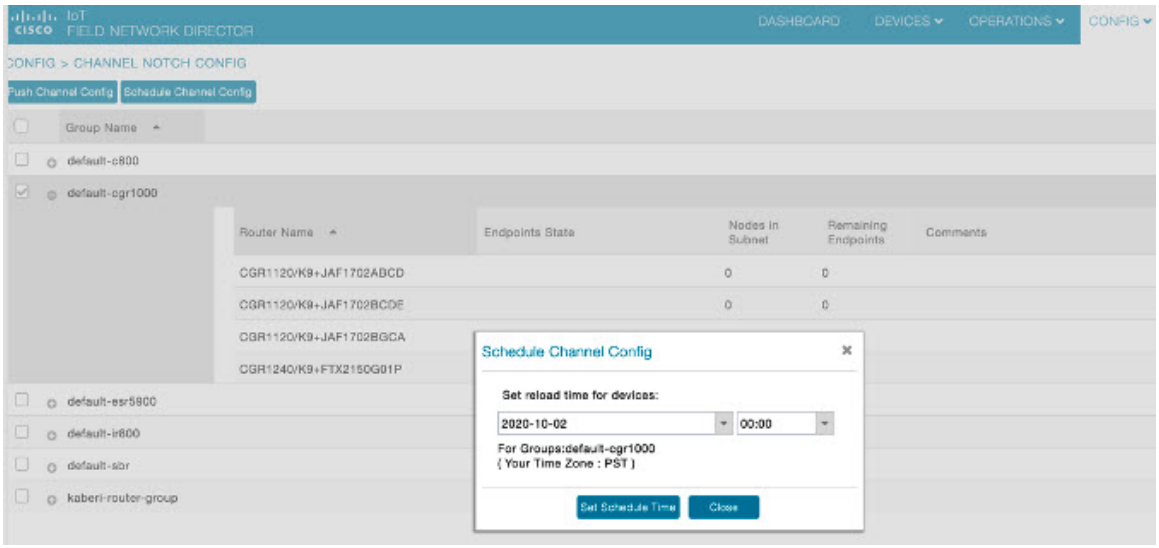


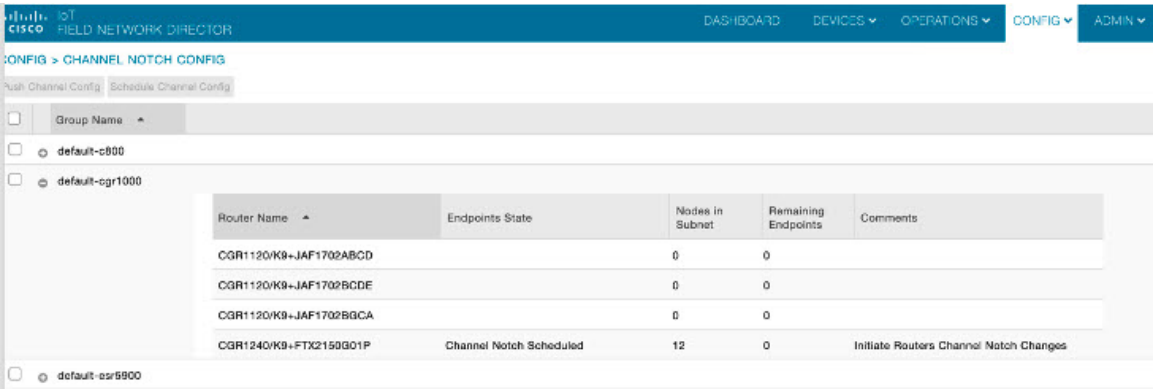


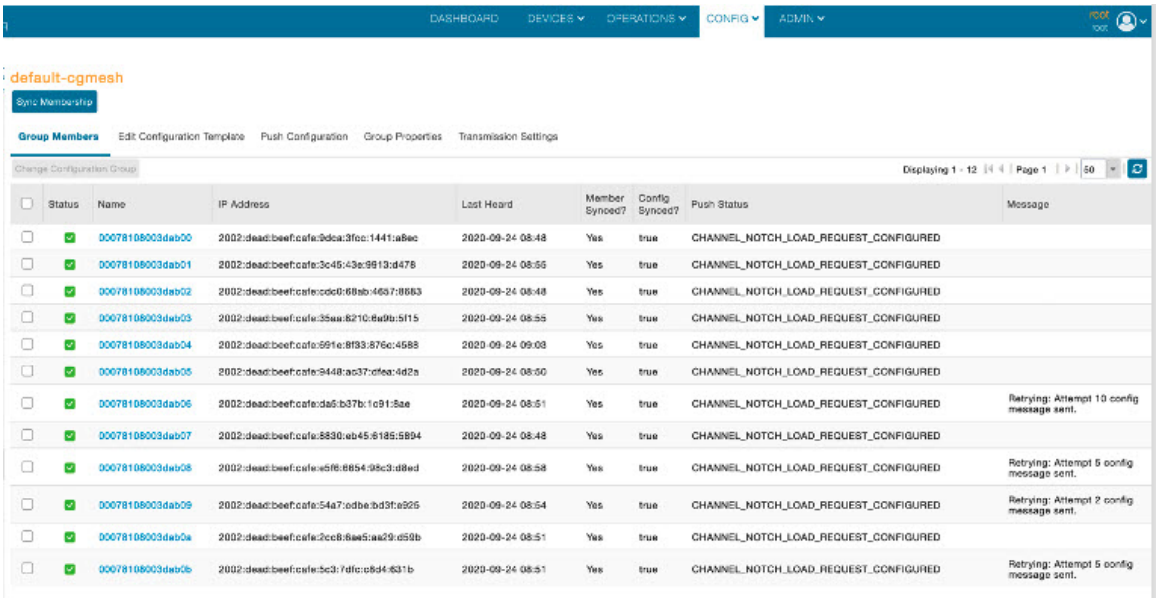
Note Before you can schedule activation of a Channel Notch Config, the router config groups must have successfully received their channel notch configuration. Note: Before you can schedule activation of a Channel Notch Config, the router config groups must have successfully received their channel notch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


IoT
FIELD NETWORK DIRECTOR
DASHBOARD
DEVICES
OPERATIONS
CONFIG
CONFIG > CHANNEL NOTCH CONFIG
Push Channel Config
Schedule Channel Config
Group Name
default-c800
default-cgr1000
Router Name
Endpoints State
Nodes in Subnet
Remaining Endpoints
Comments
CGR1120/K9+JAF1702ABCD
CGR1120/K9+JAF1702BCDE
CGR1120/K9+JAF1702BGCA
CGR1240/K9+FTX2150G01P
default-esr5900
default-ir800
default-sbr
kaberi-router-group
Schedule Channel Config
Set reload time for devices:
2020-10-02
00:00
For Groups:default-cgr1000
(Your Time Zone : PST)
Set Schedule Time
Close


IoT
FIELD NETWORK DIRECTOR
DASHBOARD
DEVICES
OPERATIONS
CONFIG
ADMIN
CONFIG > CHANNEL NOTCH CONFIG
Group Name
default-c800
default-cgr1000
Router Name
Endpoints State
Nodes in Subnet
Remaining Endpoints
Comments
CGR1120/K9+JAF1702ABCD
CGR1120/K9+JAF1702BCDE
CGR1120/K9+JAF1702BGCA
CGR1240/K9+FTX2150G01P
Channel Notch Scheduled
12
Initiate Routers Channel Notch Changes
default-esr5900


DASHBOARD
DEVICES
OPERATIONS
CONFIG
ADMIN
default-cgmesh
Sync Membership
Group Members
Edit Configuration Template
Push Configuration
Group Properties
Transmission Settings
Status
Name
IP Address
Last Heard
Member Synced?
Config Synced?
Push Status
Message
CHANNEL_NOTCH_LOAD_REQUEST_CONFIGURED

```
[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.

Landis+Gyr devices

Cisco IoT FND supports Landis+Gyr (L+G) routers and endpoints as managed field devices. L+G routers provide the routing and collection point for L+G RF mesh endpoints, while L+G endpoints represent the field devices that report meter, grid, or low-frequency network information through the L+G mesh.

In Cisco IoT FND, L+G routers appear in the `ROUTER` device category and are assigned to `Default-lgrouter` unless moved to a custom router group. L+G endpoints appear in the `ENDPOINT` device category and are assigned to endpoint groups such as `Default-lglfn`, `Default-lgelectric`, `Default-lgnn`, or `Default-lgradio`, depending on endpoint type.

For L+G border routers, the communication path depends on the deployment configuration. In secure mode, device communication uses HTTPS to the Cisco IoT FND device communication URL. In bandwidth optimization mode, only periodic metrics use HTTP while other router communication remains secure. IGMA profiles on devices that use IGMA must point to the Cisco IoT FND registration, metrics, and tunnel URLs configured for the deployment. The URL host name, port, and path must match the values configured in Cisco IoT FND provisioning settings and in the device profile.

Supported L+G devices

Cisco IoT FND supports two types of L+G devices:

- Routers
- Endpoints

CC UI Type	Device Type (Cisco)	Provisioned Type	Provisioned Subtype	Model / PID	Category	Function / Application
GAS	LGLFN	Endpoint	GASMeter	M125	ENDPOINT	METER
GAS	LGLFN	Endpoint	GASMeter	M225 GPR	ENDPOINT	METER
GAS	LGLFN	Endpoint	GASMeter	M255 GPR-PT	ENDPOINT	METER
Grid Management	LGNN	Endpoint	GSManagement	N550	ENDPOINT	NETWORK NODE
Grid Management	LGNN	Endpoint	GSManagement	OFDM N550	ENDPOINT	Not specified
Grid Management	LGNN	Endpoint	GSManagement	R650	ENDPOINT	EXTENDER
Grid Management	LGNN	Endpoint	GSManagement	R651	ENDPOINT	EXTENDER
Grid Management	LGNN	Endpoint	GSManagement	R661	ENDPOINT	EXTENDER
Electric	LGELECTRIC	Endpoint	METER-L+G-ElectricMeter	REVELO C&I	ENDPOINT	METER
Electric	LGELECTRIC	Endpoint	Not specified	REVELO	ENDPOINT	METER
Electric	LGELECTRIC	Endpoint	Not specified	OFDM S4x	ENDPOINT	Not specified
Electric	LGELECTRIC	Endpoint	Not specified	S4x-DNP	ENDPOINT	Not specified
Electric	LGELECTRIC	Endpoint	Not specified	S4x	ENDPOINT	Not specified
Electric	LGELECTRIC	Endpoint	Not specified	FOCUS-Axe	ENDPOINT	Not specified
Radio	LGRADIO	Endpoint	Not specified	N2250-R	ENDPOINT	Not specified
Radio	LGRADIO	Endpoint	Not specified	N2450-R	ENDPOINT	Not specified
Radio	LGRADIO	Endpoint	Not specified	OFDM N2450-R	ENDPOINT	Not specified
Router	LGROUTER	Router	Not specified	N2450	ROUTER	Not specified
Router	LGROUTER	Router	Not specified	OFDM N2450	ROUTER	Not specified
Router	LGROUTER	Router	Not specified	N2250	ROUTER	Not specified

Configure and verify L+G devices

Use this procedure after importing L+G routers or endpoints, after changing provisioning settings, or after moving L+G devices to a different configuration group.

Before you begin

- Confirm that the L+G device type is supported in the current Cisco IoT FND release.
- Prepare the CSV or XML import file using the supported import method for the deployment.
- Verify that Cisco IoT FND provisioning settings contain the correct Cisco IoT FND URL and periodic metrics URL.
- Verify that network security devices allow traffic from L+G routers to the configured Cisco IoT FND registration and metrics endpoints.
- For IGMA-based communication, confirm that the device IGMA profile URLs match the Cisco IoT FND provisioning settings and deployment mode.

Procedure

Step 1 Import the L+G router or endpoint into Cisco IoT FND by using the supported CSV or XML import workflow.

Step 2 From Cisco IoT FND menubar, choose **DEVICES** > **Field Devices** > **Browse Devices**.

Step 3 For L+G routers, select `ROUTER` in the left pane. For L+G endpoints, select `ENDPOINT`. Locate the L+G device by EID and open the device details page.

Step 4 Verify the device category and group membership: L+G routers should appear under `ROUTER` and use `Default-lgrouter` or the intended custom router group. L+G endpoints should appear under `ENDPOINT` and use the expected L+G endpoint group, such as `Default-lglfn`, `Default-lgelectric`, `Default-lgnn`, or `Default-lgradio`.

Step 5 Verify that the EID uses the same letter case in the import file, certificates, device profile, Cisco IoT FND UI, and logs.

Step 6 Verify that `Status`, `Last Heard`, and `Last Metric Heard` reflect the expected operational state. For routers, click `Refresh Metrics` and confirm that `Last Metric Heard` updates after the refresh completes. For endpoints, open the endpoint details and verify that inventory, mesh parent information, and endpoint metrics appear as expected. For L+G endpoints, IoT FND displays the mesh parent value as `1` when the L+G router does not report mesh parent details.

Step 7 If the device remains `Unheard`, `Down`, or has stale telemetry, use the troubleshooting procedures in the troubleshooting guide.

You've configured L+G devices and verified them using Cisco IoT FND.

What to do next

- For stale `Last Metric Heard` values or failed refresh operations, see Troubleshoot L+G device metric refresh.
- For IGMA registration, telemetry, metric, tunnel, firmware, or WebSocket session failures, see Debug IGMA websocket sessions for L+G border routers.

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=<%>
```

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): 61096E7D000000000000C
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

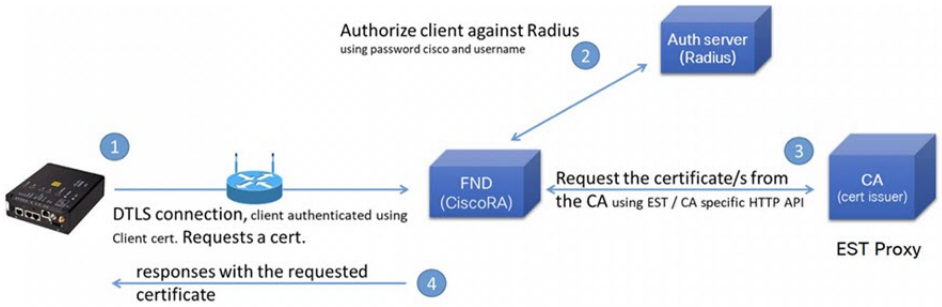
This section provides an overview of the components and configurations involved in integrating Enrollment over Secure Transport (EST) certificate enrollment for clients over the secure transport layer within the network. EST is based on public-private key exchange. This feature is supported on Itron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

Table 9: 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.



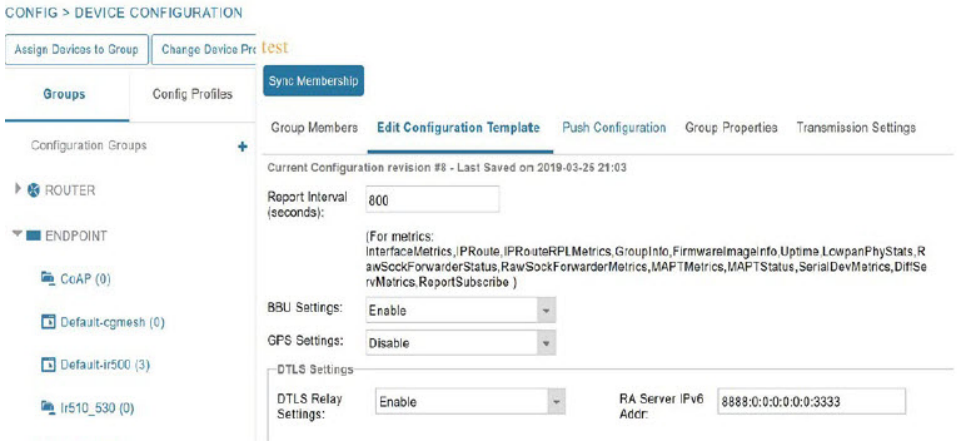
Note Supported from version 4.5.0.122 onwards.

Procedure

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

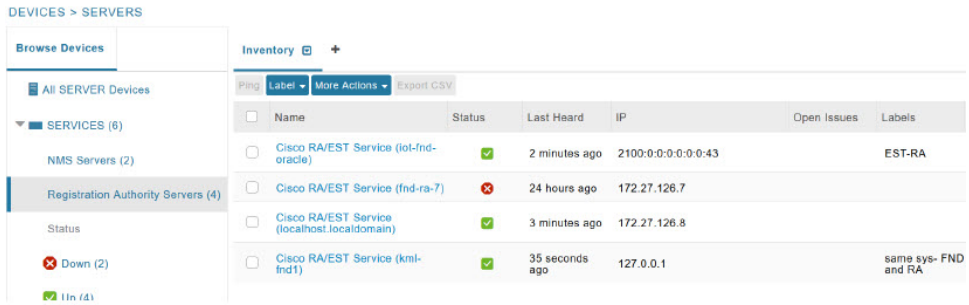
Step 2 Select **Enable** from the **DTLS Relay Settings** drop-down list.

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**.

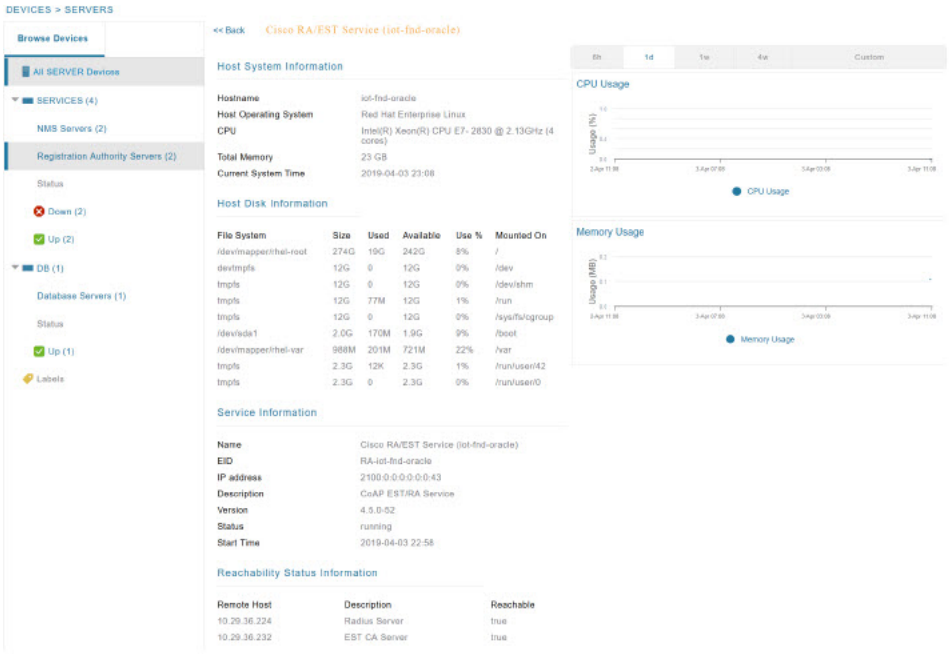


Figure 4: Events for FND-RA Service

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

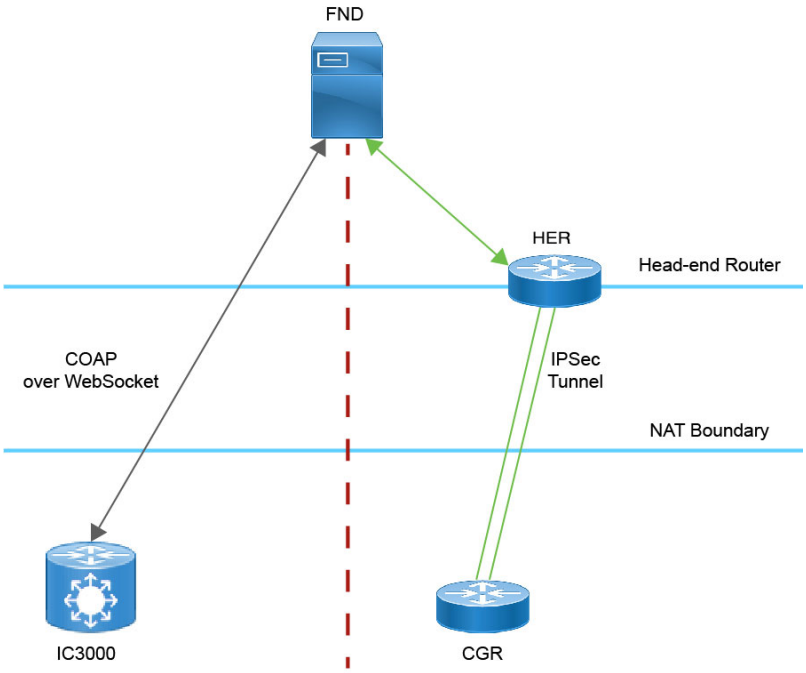
IC3000 supports edge computing and communicates with IoT FND through the IOx application, Cisco Fog Director which is accessible via IOT FND.

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.

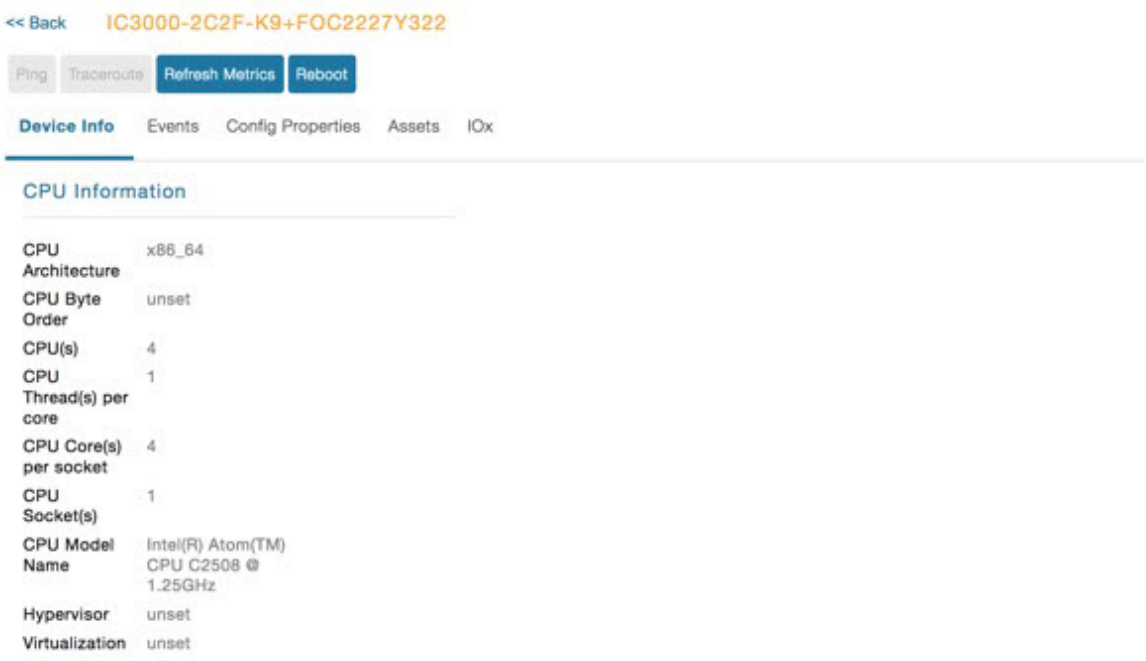


You can perform the following actions for an IC3000 device type on demand:

- 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,

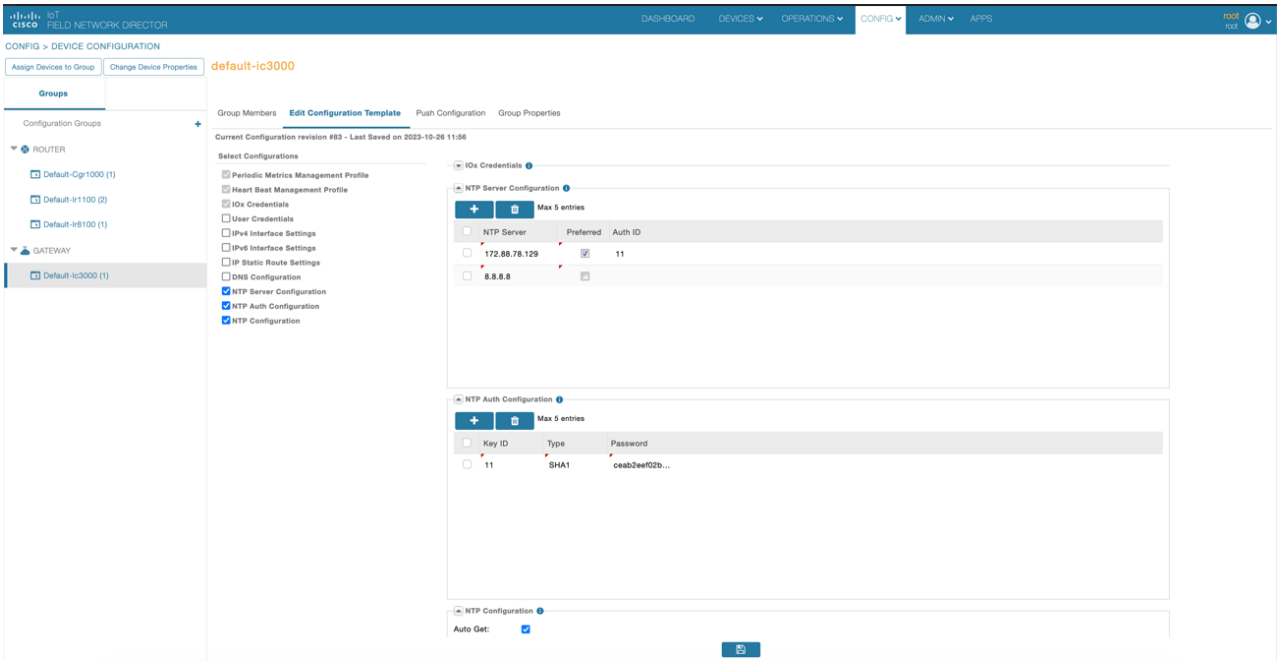
Procedure

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 74).

- 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)

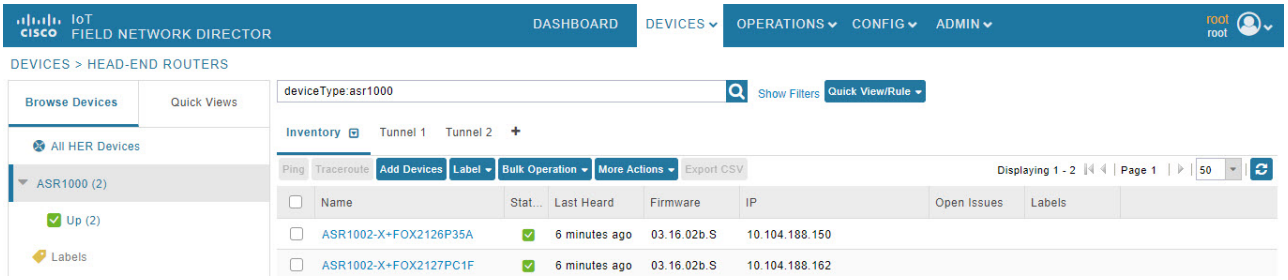

<< Back
IXM-LPWA-900-16-K9+FOC21028RJ4
Show on Map
Ping
Traceroute
Refresh Metrics
Restart Radio
Device Info
Events
Config Properties
Running Config
Assets
Inventory
Name IXM-LPWA-900-16-K9+FOC21028RJ4
EID IXM-LPWA-900-16-K9+FOC21028RJ4
Domain root
Device Category IOTGATEWAY
Device Type LORAWAN
Status 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
6h
1d
1w
4w
Custom
Load Average
% Utilization
Load Average
Modem Temperature
Degree Celsius
Modem Temperature
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

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 81

For information about the device properties displayed in each view, see Device Properties, on page 195.

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 80

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 10: Feature history

Feature name	Release information	Description
Cisco IRM-1100-4S8I expansion module	Cisco IoT FND Release 5.1	You can boost your network flexibility and industrial integration using Cisco IRM-1100-4S8I expansion module featuring 4x SFP L2/L3 ports and 8x GPIO ports.

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.

View expansion module info

This task guides you to view the expansion module info on Cisco IoT FND.

Before you begin

- Ensure that you have attached the expansion module to the Cisco IR1100 device.

- Ensure that you've restarted Cisco IR1100 and registered it once again with Cisco IoT FND. For more information see, Register IR1100 with Cisco IoT FND.

Here are the steps to view the expansion module info using Cisco IoT FND:

Procedure

Step 1 From the Cisco IoT FND menubar, choose **Devices** > **Field Devices**.

Step 2 From the **Router** list, select an IR1100 device from the left tree.

Step 3 Click the device **Name** and view the **Expansion Module Info**section.

Field	Description
PID1	Displays the exapansion module attached to the device.
Name	Displays the expansion module's name.
Description	Describes the expansion module's SFP and digital I/Os.
PID	Displays the PID of the expansion module.
SN	Displays the serial number of the expansion module found in the device.

You can see the PID and SN details.

You've viewed the expansion module info.

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.

Similarly, IOx must be running on IR8100 before you install the 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.

Note
For IR8100 device with CAM module, select Default-Ir8100 under the Groups panel and select the type as ACTD-IR8100 while uploading the image.

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

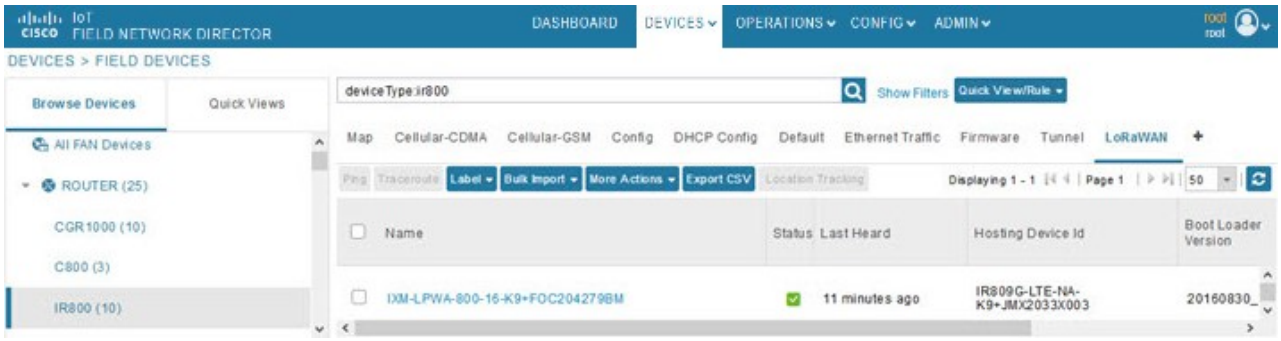
Procedure

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.

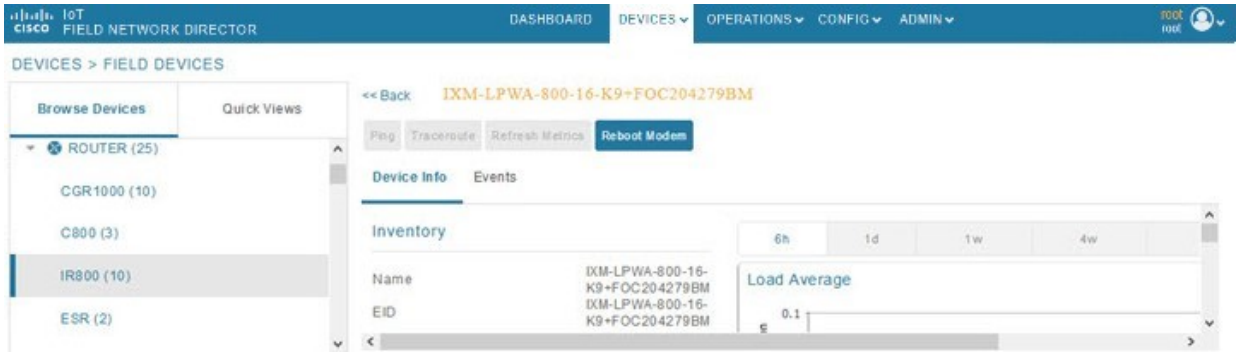
Note
IoT FND does not support discovery for the LoRaWAN module. Rather, IoT FND recognizes it as an IR800 module and will communicate with it via Cisco IOS.

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:



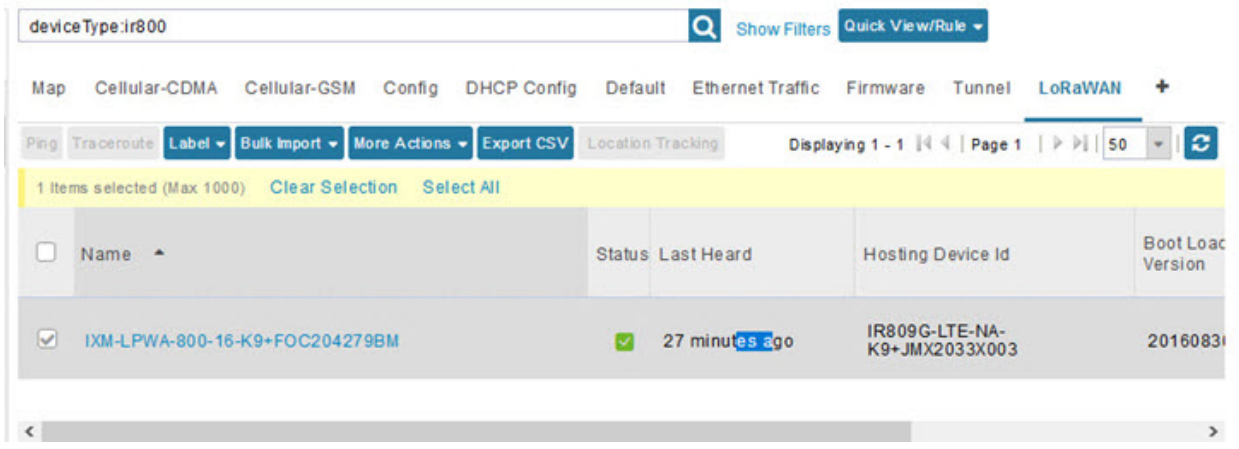
b) Click **Reboot Modem**. When the reboot completes, the date and time display in the Last Reboot Time field in the Device Info pane for the LoRaWAN module. You can only process one modem reboot at a time.

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**.

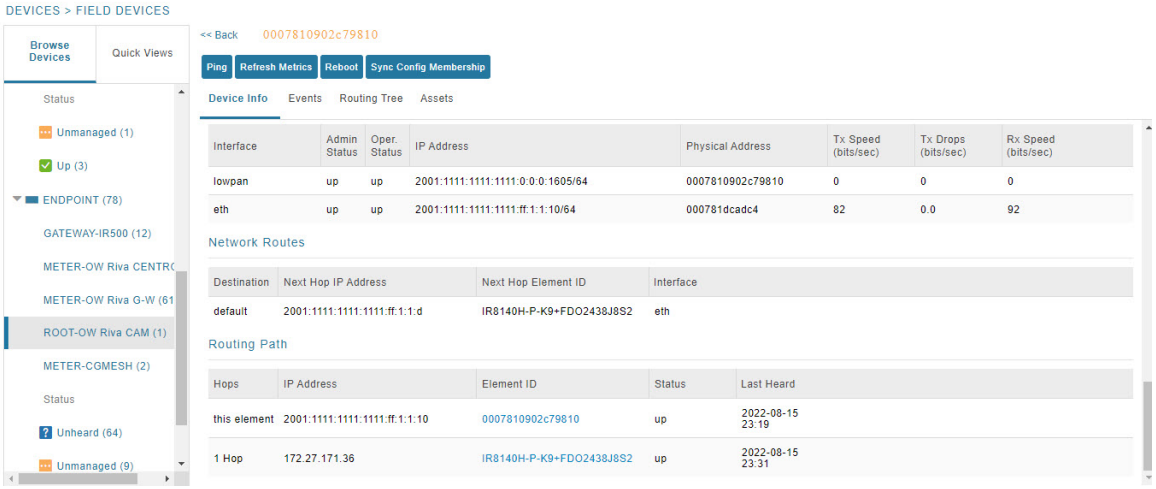
Step 5 To create a user-defined LoRaWAN (IXM) Tunnel, choose **CONFIG** > **Tunnel Provisioning**.

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.

Routing Path

In **Devices** > **Field Devices** page, in the left-pane, under Endpoint, select the CAM module. In the Device Info page, the Routing Path table shows the topological connection where the device is displayed with the Hops connected.



The following table describes the routing path fields in the Device Info page.

Field	Description
Hops	Number of hops that the element is from the root of its RPL routing tree
IP Address	IP address of the device.
Element ID	Element identifier of the device.
Status	Status of device (up/down).
Last Heard	Last date and time the device contacted IoT FND.

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 81.

For more information about the device properties displayed in each view, see Device Properties, on page 195.

For information about the common actions in this view, see Common Device Operations, on page 80 .

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,

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:

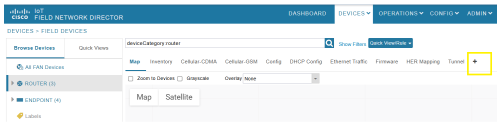
- Add and delete tabs
- Specify the properties to display in the columns for each view (see Device Properties by Category, on page 196 for available properties)
- Change the order of columns

Adding Device Views

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

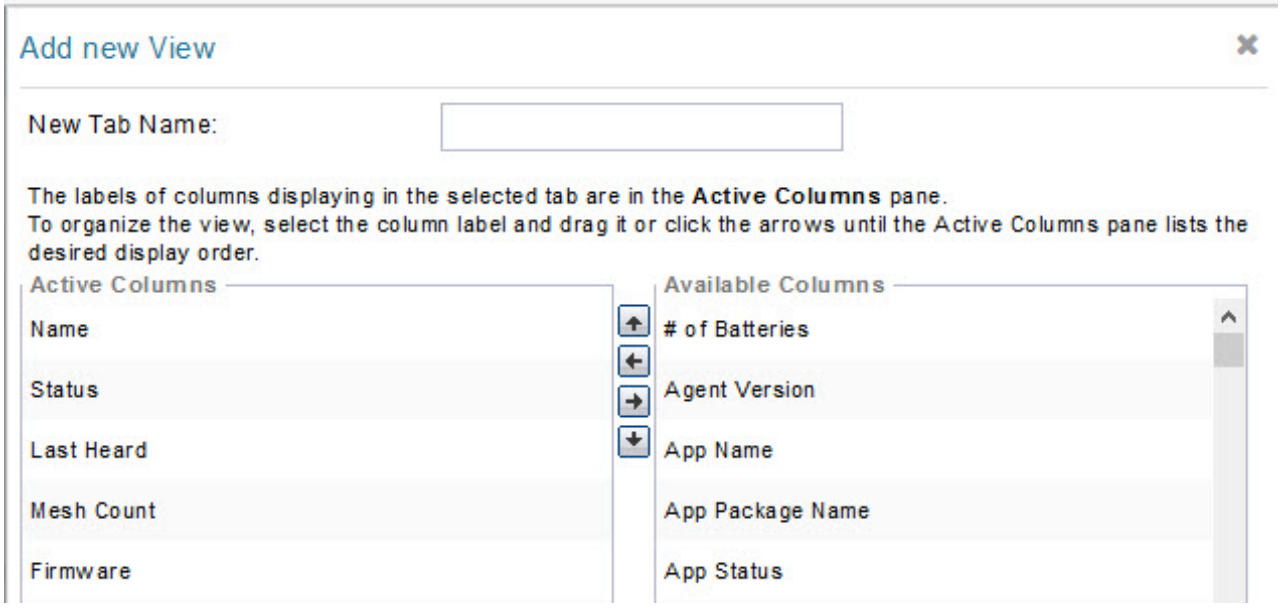
Procedure

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 11: 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.

Note
Starting from Cisco IoT FND Release 5.0, the system lists user-defined properties along with other properties under the **Available Columns**, which can be moved to **Active Columns**.

Note
In addition, the user defined properties can also be viewed and added from the drop-down 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.

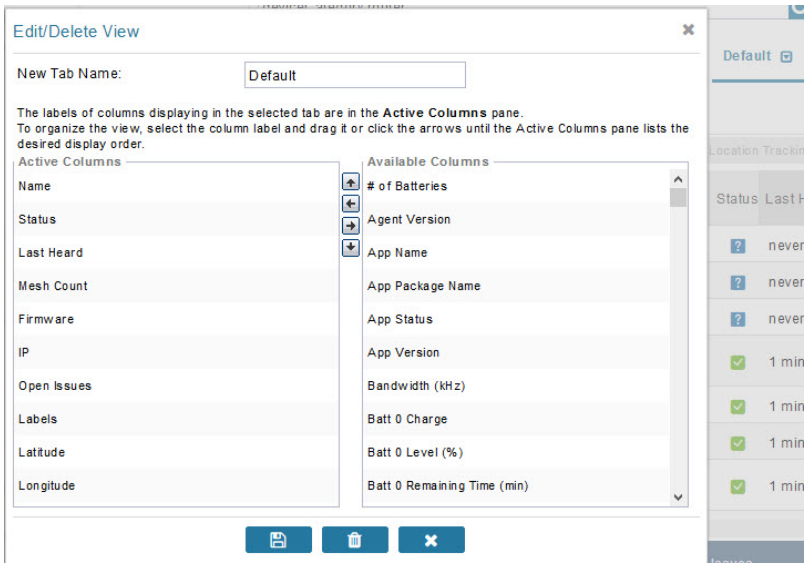
Step 5 Click the disk icon to save the view.

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.



Note
Starting from Cisco IoT FND Release 5.0, you can delete the default views as well.

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

Viewing Devices in Map View

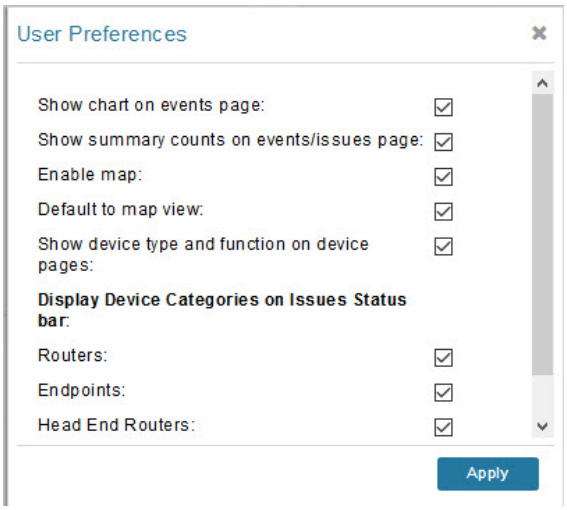
IoT FND provides a map view for visualizing device information based on geographic location. In Map view, IoT FND displays a Geographic Information System (GIS) map and uses GIS Map services to show device icons on the map based on the latitude and longitude information of the device. When this information 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)**.

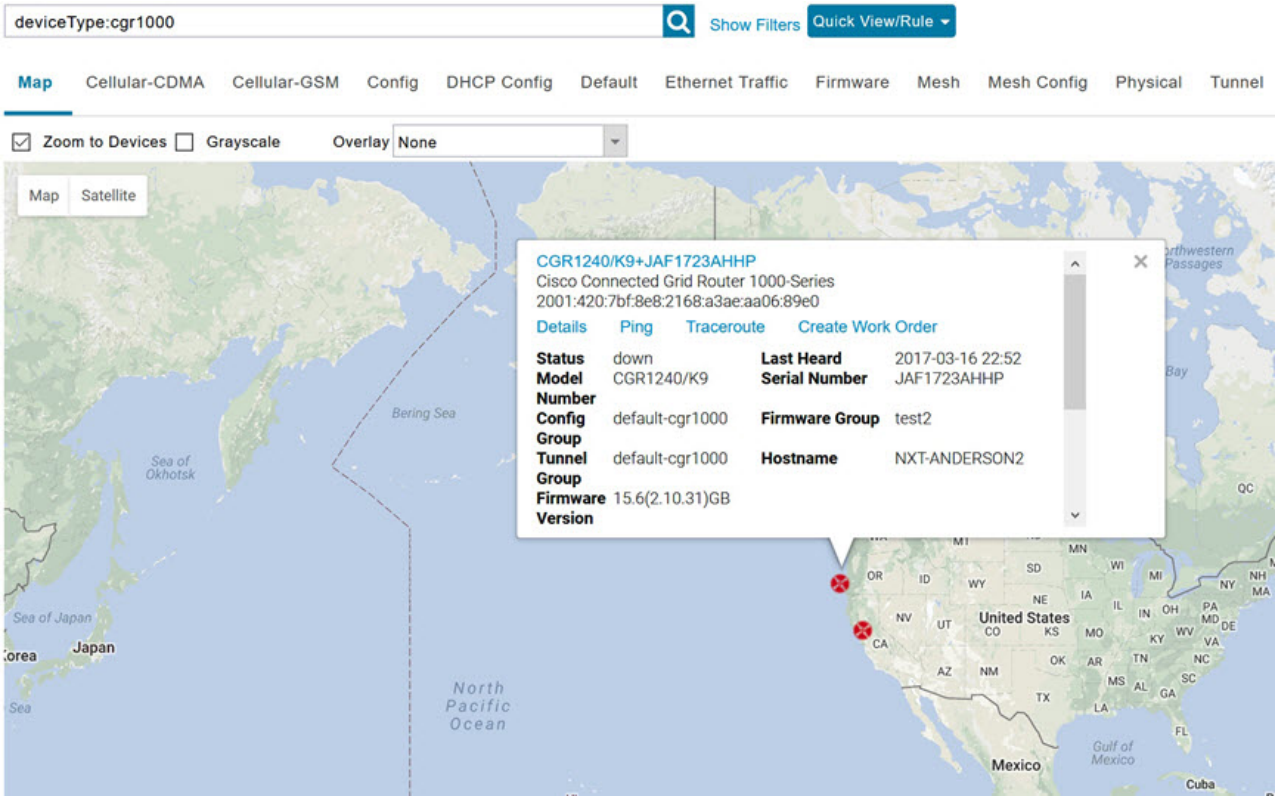
Step 2 Select the **Enable map** check box, and click **Apply**.



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 101.
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:

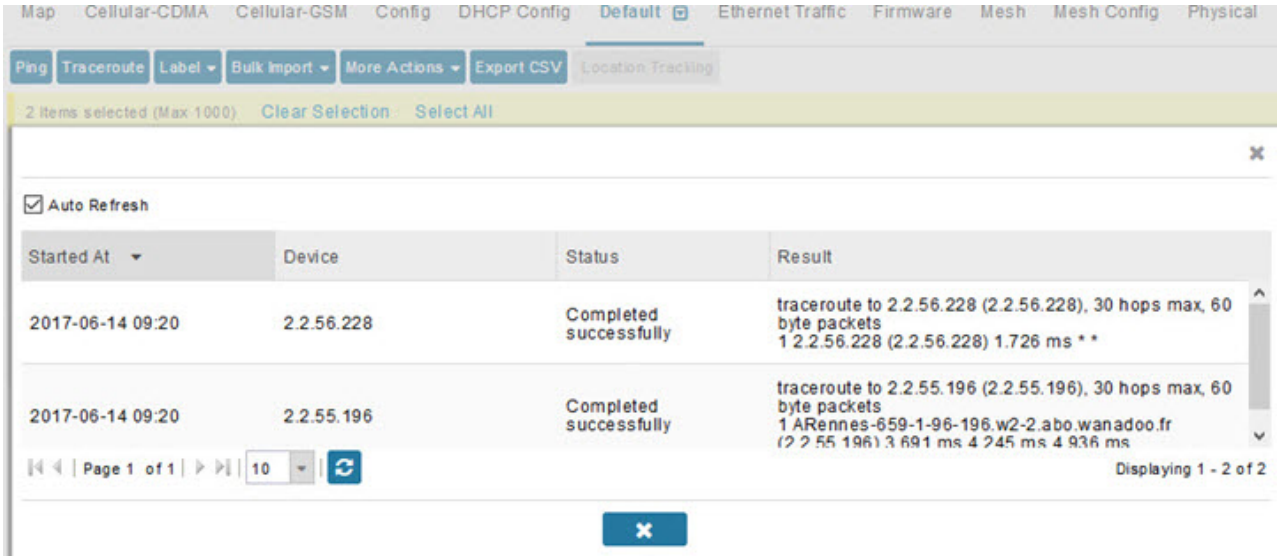
Procedure

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.

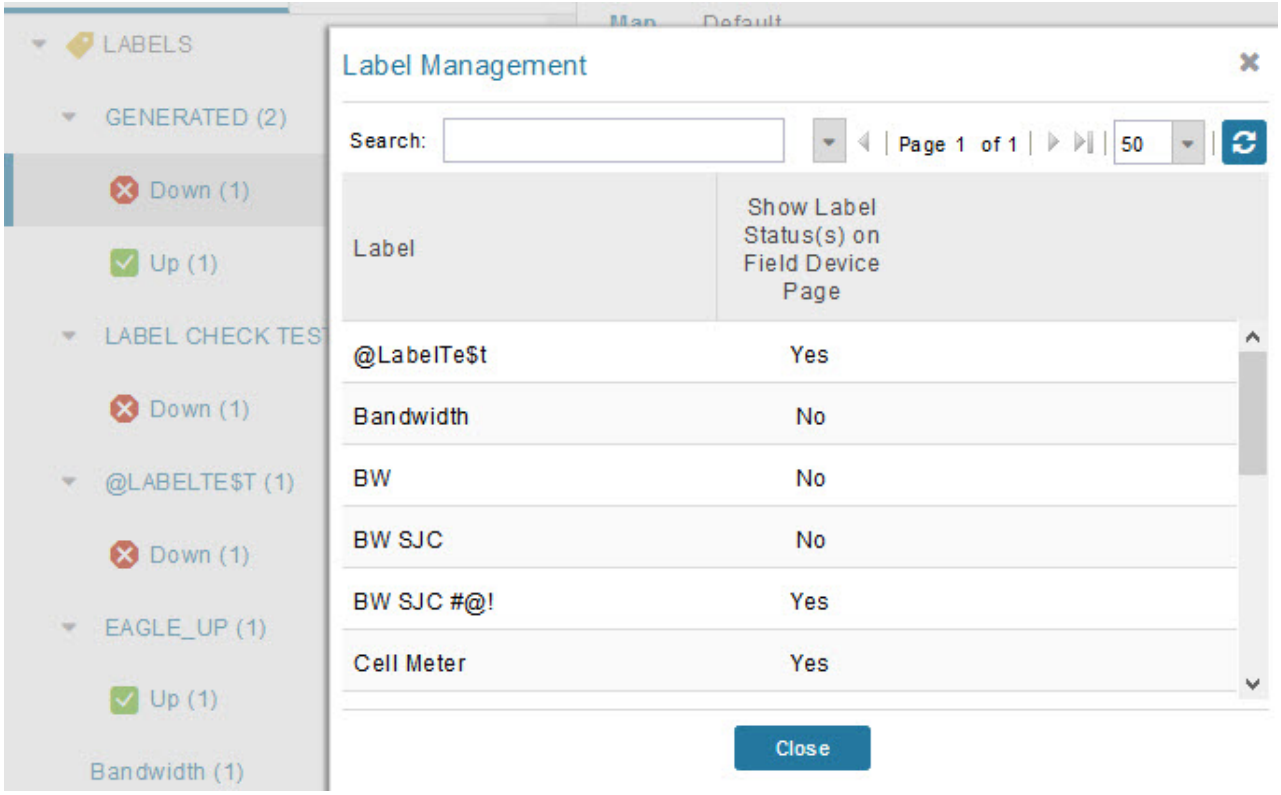
Managing Labels

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**.

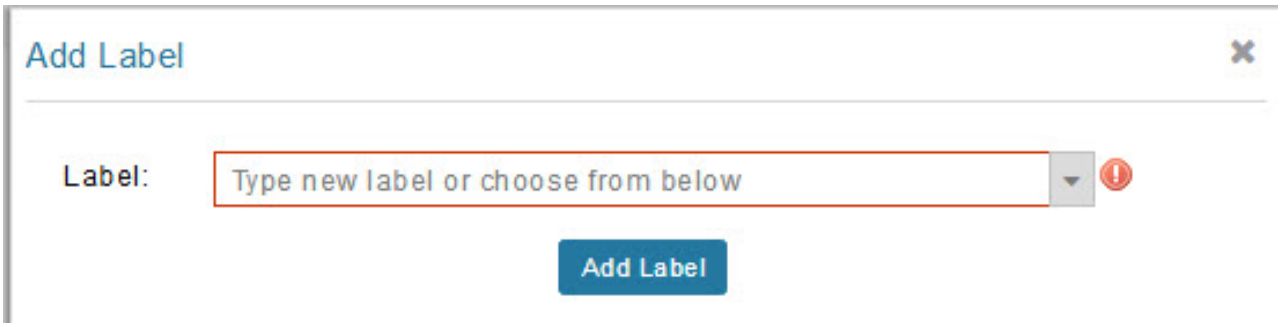
Adding Labels

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 106.

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 107.

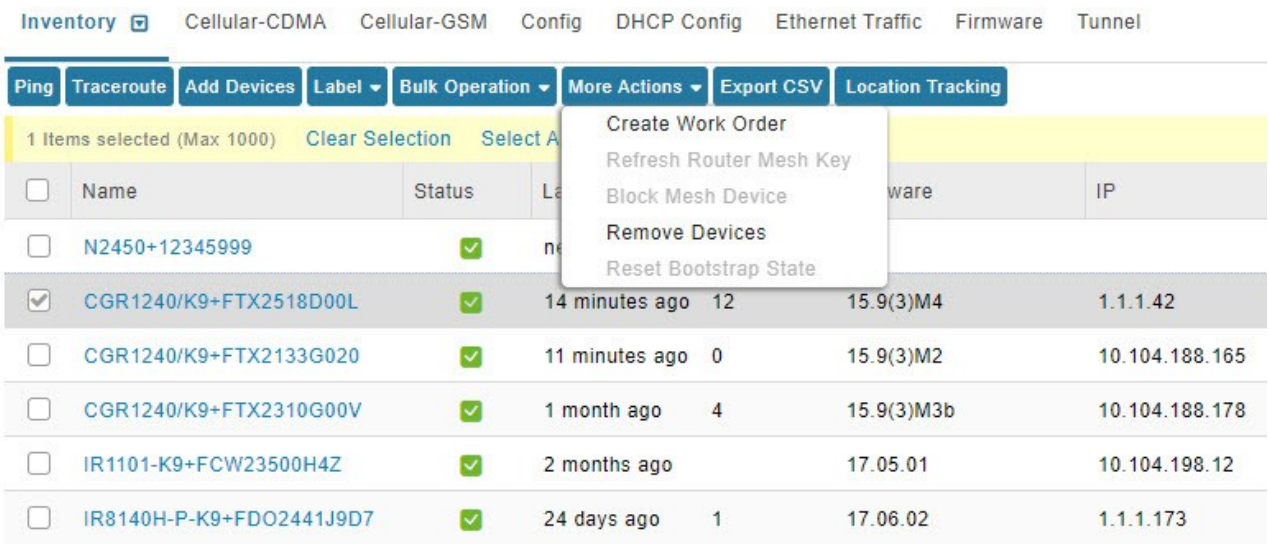
Removing Devices

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 92
- Head-end Router, Router, and Endpoint Information, on page 93

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.

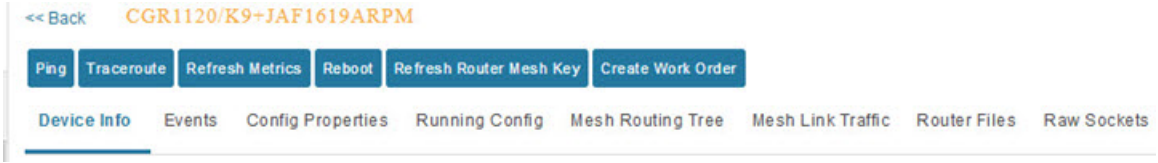
Table 12: NMS Server Pane Areas

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. For more information on viewing the chart for default or custom-defined time intervals, refer to Setting Time Filters To View Charts
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 195). 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 195). 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 115.
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 (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 (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 87.
Traceroute	Traces the route to the device. See Tracing Routes to Devices, on page 88.
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 121.
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 191.

Device filters

Filters in Cisco 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.

- Cisco 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.

Built-in device 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, Cisco IoT FND provides a device count in parenthesis. Cisco 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** .

This table lists all the filter attributes and operators and how they could be used when creating a filter.

Table 13: Filters

Filter Attribute	Operator	Resulting Action
Label	:	Filters devices by their assigned labels. Use this filter to quickly find devices that have been tagged with specific labels for organization or categorization purposes.
Asset	:	Filters devices by their asset name. Use this filter to search for devices associated with specific asset identifiers or asset management records.
Config Group	:	Filters devices by their configuration group membership. Use this filter to find all devices that belong to a specific configuration group for managing or viewing devices with similar configuration settings.
Firmware Group	:	Filters devices by their firmware group assignment. Use this filter to locate devices in a specific firmware group for tracking firmware versions or planning firmware updates.
Groups	:	Filters devices by general group membership using text search. Use this filter to find devices belonging to any group by entering group name keywords.
Tunnel Group	:	Filters devices by their tunnel group assignment. Use this filter to find devices that are part of specific tunnel configurations for network connectivity management.

Filter Attribute	Operator	Resulting Action
Category	:	Filters devices by their device category classification. Use this filter to narrow down devices to specific categories (e.g., routers, endpoints, gateways) within the fan device family.
Domain	:	Filters devices by their network domain. Use this filter to search for devices within a specific network domain or administrative boundary.
EID	:	Filters devices by their unique Element Identifier. Use this filter to quickly locate a specific device using its unique EID for troubleshooting or configuration.
Firmware	:	Filters devices by their currently running firmware version. Use this filter to find all devices running a specific firmware version for identifying devices needing updates or to verify deployment success.
Function	:	Filters devices by their functional role or purpose. Use this filter to locate devices based on their designated function in the network (e.g., gateway, repeater, collector).
Hardware ID	:	Filters devices by their hardware identifier. Use this filter to search for devices with specific hardware IDs for inventory management or hardware-specific troubleshooting.
IP	:	Filters devices by their IP address. Use this filter to find devices using IP address search (exact match or partial) for network troubleshooting or connectivity verification.
Last GPS Heard	between	Filters devices by the date/time when GPS location was last received. Use this filter to identify devices with recent or outdated GPS data for monitoring mobile devices or detecting connectivity issues.

Filter Attribute	Operator	Resulting Action
Last Heard	between	Filters devices by the date/time they last communicated with the system. Use this filter to find devices that haven't reported recently (potential offline devices) or verify recent device activity.
Latitude	between	Filters devices by their geographic latitude coordinate. Use this filter to search for devices within specific latitude ranges for geographic-based device management or mapping.
Longitude	between	Filters devices by their geographic longitude coordinate. Use this filter to search for devices within specific longitude ranges to locate devices in particular geographic areas.
Model Number	:	Filters devices by their product ID or model number. Use this filter to find all devices of a specific model for model-specific configuration, updates, or inventory reporting.
Name	:	Filters devices by their assigned device name. Use this filter to search for devices using their friendly names for quick identification and access.
Serial Number	:	Filters devices by their unique serial number. Use this filter to locate a specific device using its serial number for warranty tracking, RMA, or precise device identification.
Status	:	Filters devices by their operational status. Use this filter to find devices in specific states (e.g., up, down, unheard, unmanaged) for monitoring network health or troubleshooting issues.

Filter Attribute	Operator	Resulting Action
Type	:	Filters devices by their specific device type. Use this filter to narrow down to specific device types within the fan family for type-specific management or reporting.
Up Time	between	Filters devices by their uptime duration (in numeric range). Use this filter to find devices with specific uptime ranges for identifying recently rebooted devices or those with stability issues.

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 17.

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 14: Filter Operators

Operator	Description
:	Equal to
>	Greater than
>=	Greater than or equal to
<	Less than

Operator	Description
<=	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 15: Filter Examples

Filter	Description
`configGroup:"default-cgr1000"`	Finds all devices that belong to the default-cgr1000 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 101.

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 102

For more information about adding HERs, see Adding HERs to IoT FND, on page 102

For more information about adding routers, see Adding Routers to IoT FND, on page 103

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 195

Table 16: 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 195.

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

Table 17: 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.
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+JAE1546007O,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.

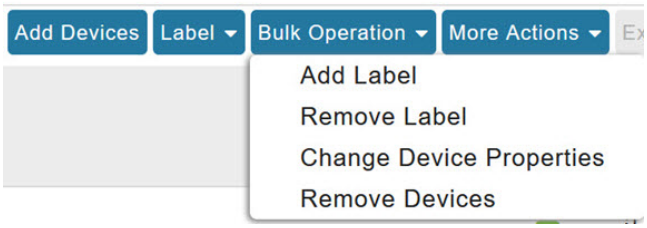
Caution When you remove routers, IoT FND returns all the leased IP addresses associated with these devices to CNR and removes the corresponding tunnels from the HERs.

To remove devices in bulk:

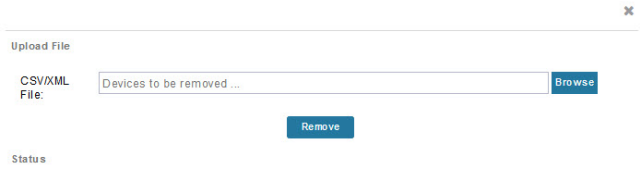
Procedure

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+JAE1546007O,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 109

Creating a Rule

To add a rule:

Procedure

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

Step 2 Click **Add**.

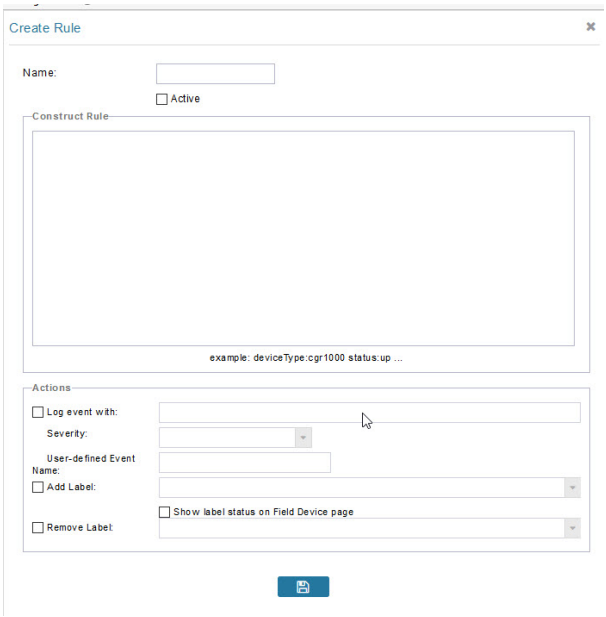
Step 3 Enter a name for the rule.

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 112
- Edit the ROUTER configuration template, on page 122
- Editing the ENDPOINT Configuration Template, on page 150
- Push configurations to routers, on page 159
- Pushing Configurations to Endpoints, on page 162

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 . 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-lglfn	By default, all L+G LFN (limited function node) battery endpoints are members of this group.
Default-lgelectric	By default, all L+G electric endpoints are members of this group.
Default-lgnn	By default, all L+G grid management endpoints are members of this group.
Default-lgrouter	By default, all L+G routers 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-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.

Group Name	Description
Default-ir8100	By default, all IR8100 (ROUTER) are members of this group.
Default-ir1800	By default, all IR1800 (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 113
- Creating Endpoint Groups, on page 114

Creating ROUTER Groups

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

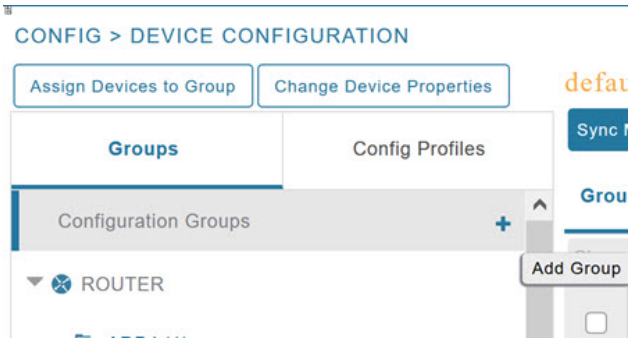
To create a router configuration group:

Procedure

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

Step 2 Select the default configuration group: **Default-cgr1000**, **Default-ir800**, , **Default-ir1100**, **Default-ir8100**, **Default-ir1800**, , or **Default-lgrouter**.

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 118
- To remove a group, see Deleting Device Groups, on page 119

Creating Endpoint Groups

To create an endpoint configuration group:

Procedure

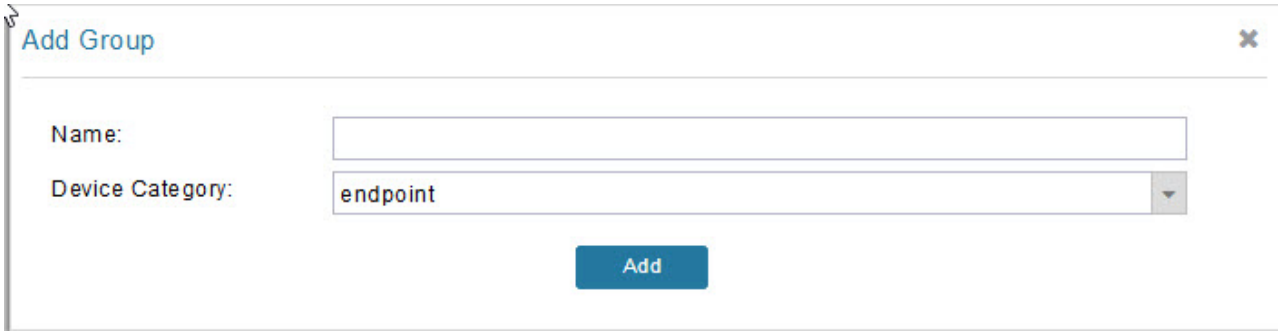
Step 1 Choose **CONFIG** > **Device Configuration**.

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

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 118
- To remove a group, see Deleting Device Groups, on page 119

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 195.

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

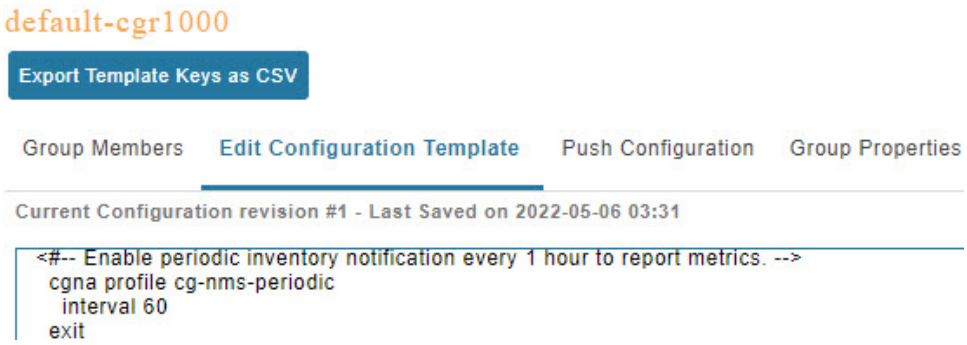
To configure the periodic inventory timer for a ROUTER configuration group:

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 60 minutes for routers and 8 hours for endpoints.



Note
We recommend you to use the default periodic value. However, you can also customize the periodic interval, but the value that is defined should be more than the default value of 60 minutes and not less. For example, if you want to enable the periodic inventory notification to report metrics every 120 minutes, then add the following lines to the template:

```
<#-- Enable periodic inventory notification every 2 hours to report metrics. -->
cgna profile cg-nms-periodic
      interval 120
    exit
```

Step 4 Click the disk icon to save the changes.

Configuring Heartbeat Notification

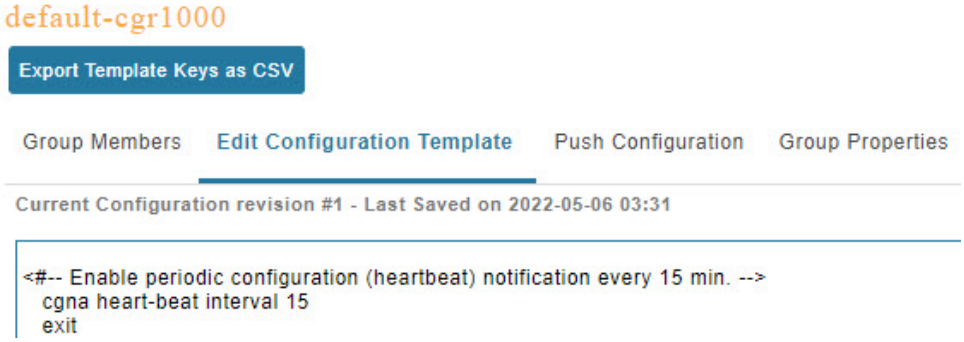
To configure the heartbeat notification for a ROUTER configuration group:

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 heartbeat notification interval is 15 minutes.



Note
We recommend you to use the default heartbeat value. However, you can also customize the default value, but the value that is defined should be more than default value and not less. For example, if you want to enable the heartbeat notification every 30 minutes, then add the following lines to the template:

```
cgna heart-beat interval 30
```

Note
Ensure that the heartbeat interval is less than the mark-down timer value set by you. For more information on the device mark-down timer, refer to Configuring Mark-Down Timer, on page 117.

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.

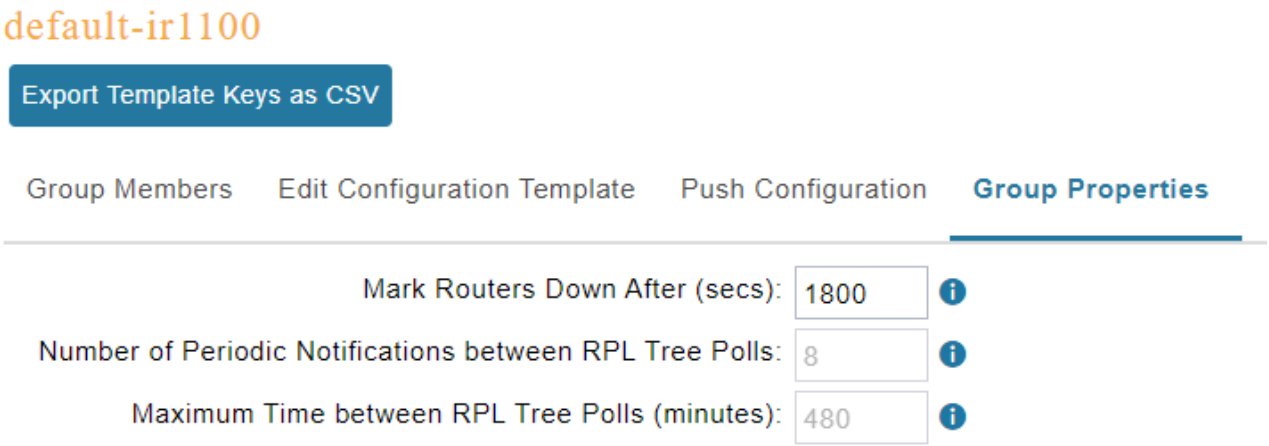
To configure the mark-down timer for a ROUTER configuration group:

Procedure

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

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

Step 3 Click **Group Properties**.



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 116.

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

Renaming a Device Configuration Group

In the **Device Configuration** page, there are two device configuration groups available, namely user-defined groups and default groups of router, endpoint, or gateway. IoT FND allows you to rename the user-defined device configuration groups only. You cannot rename the default device configuration groups.

To rename a device configuration group:

Procedure

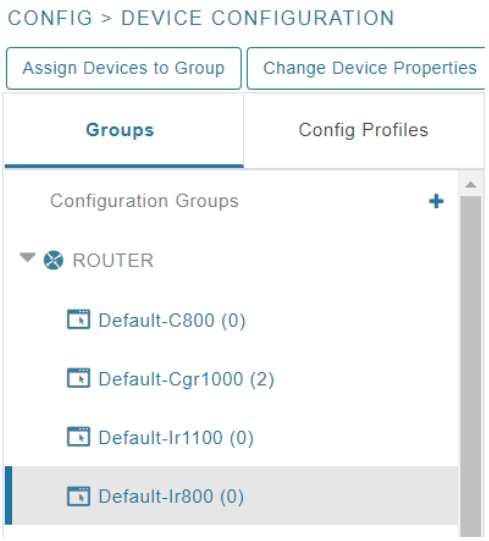
Step 1 Choose **CONFIG** > **Device Configuration**.

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.

Note
Starting with Cisco IoT FND 4.8 release, the default device configuration groups cannot be renamed, whereas the user-defined device configuration groups can be renamed. The pencil icon does not appear for the default device configuration groups.

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:

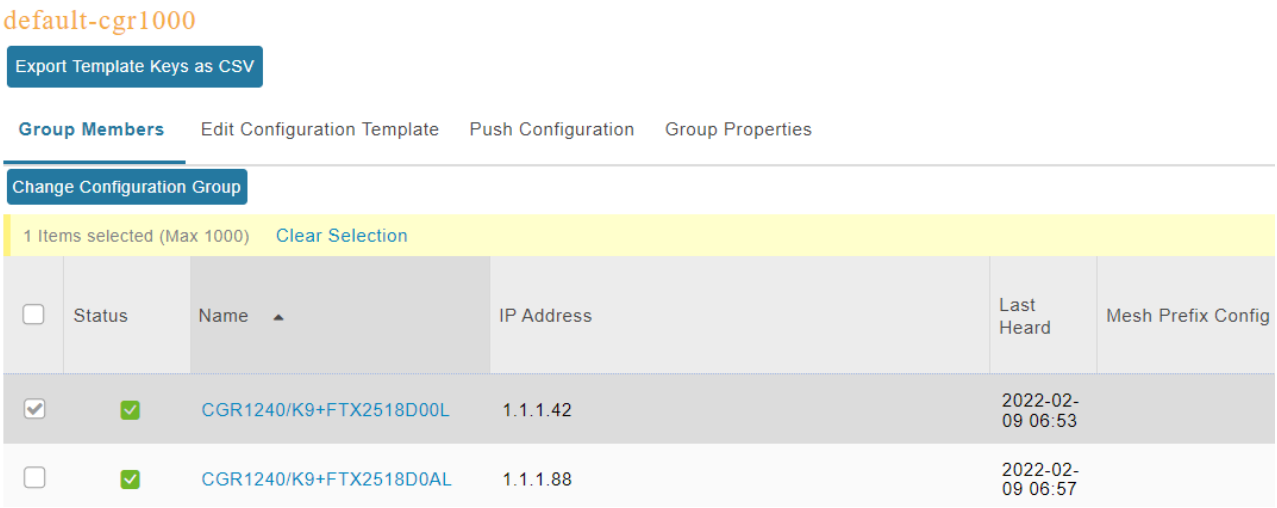
Procedure

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:

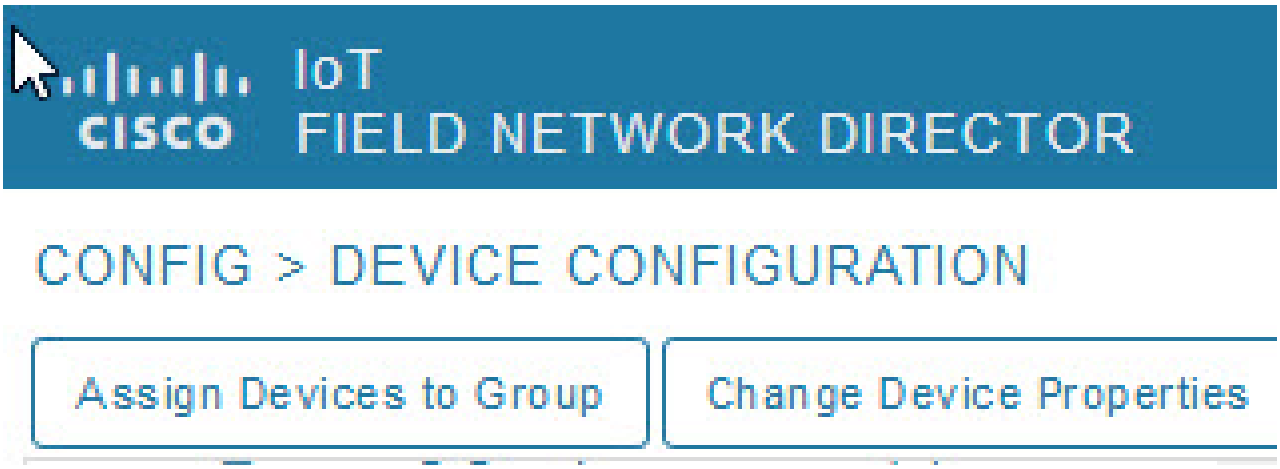
```
eid
CGR1120/k9+JS1
CGR1120/k9+JS2
CGR1120/k9+JS3
```

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**

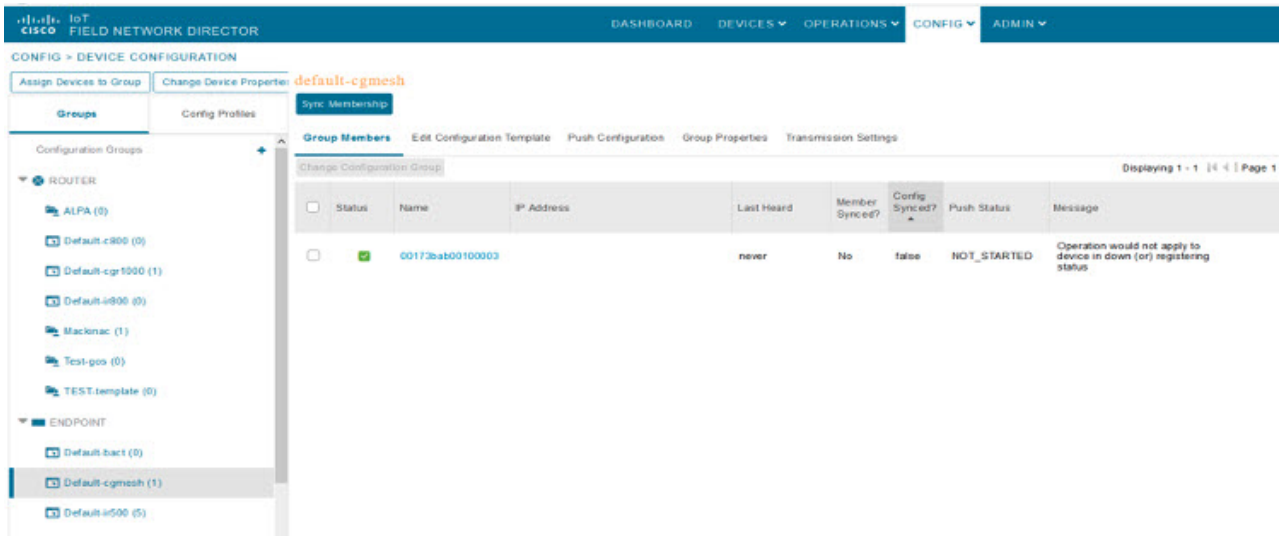
Step 2 Select an ENDPOINT group (left pane) such as Default-cgmesh.

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**.



Edit the ROUTER configuration template

Use this task to edit a ROUTER group configuration template.

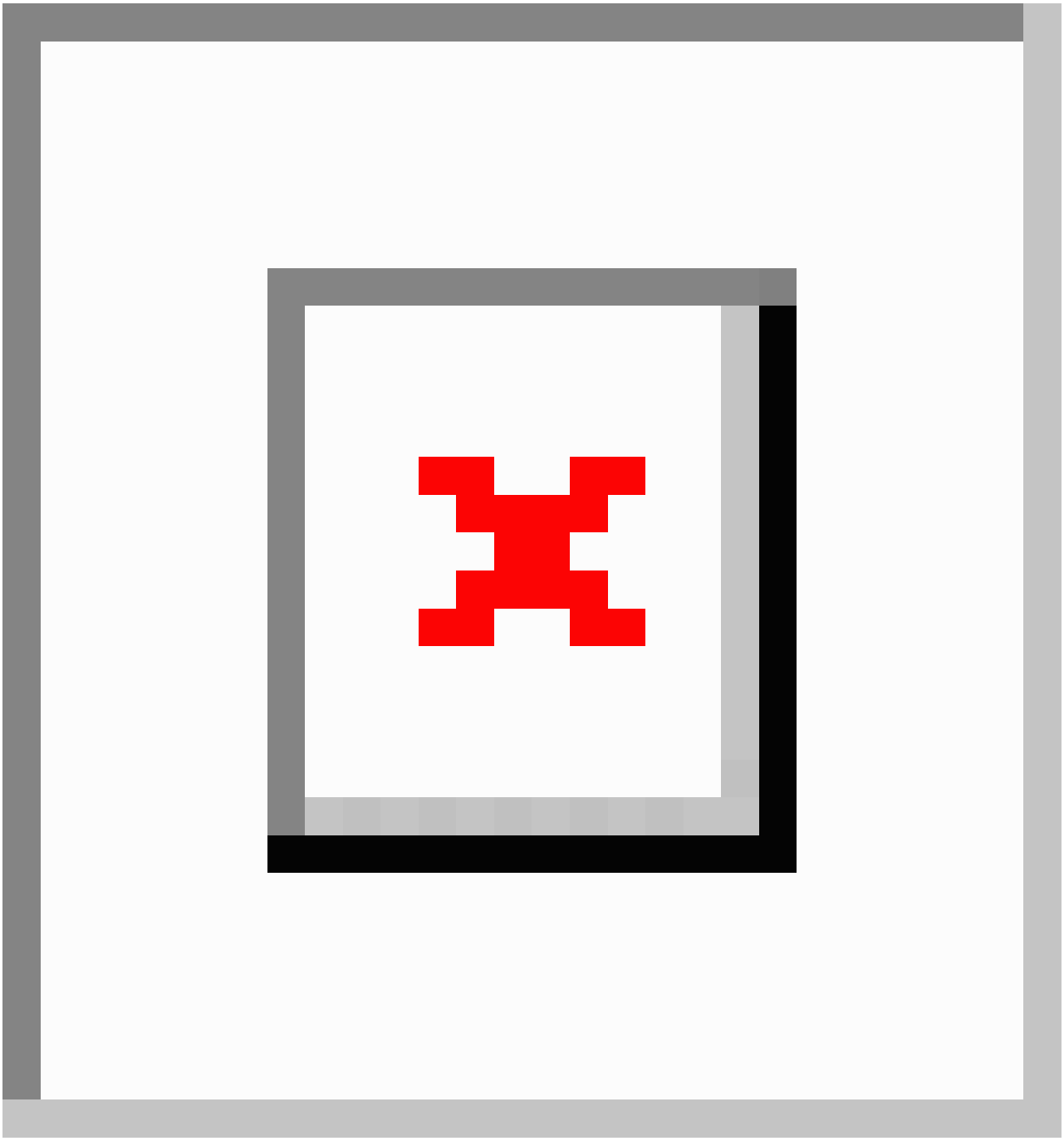
IoT FND lets you configure routers in bulk using a configuration template. When a router registers with IoT FND, IoT Field Network Director pushes the configuration defined in the default template to the device and commits the changes to the router startup configuration. IoT FND then retrieves the running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

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 Template**



Step 4 Edit the template.

The template is expressed in FreeMarker syntax

Note
The router configuration template does not validate all 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

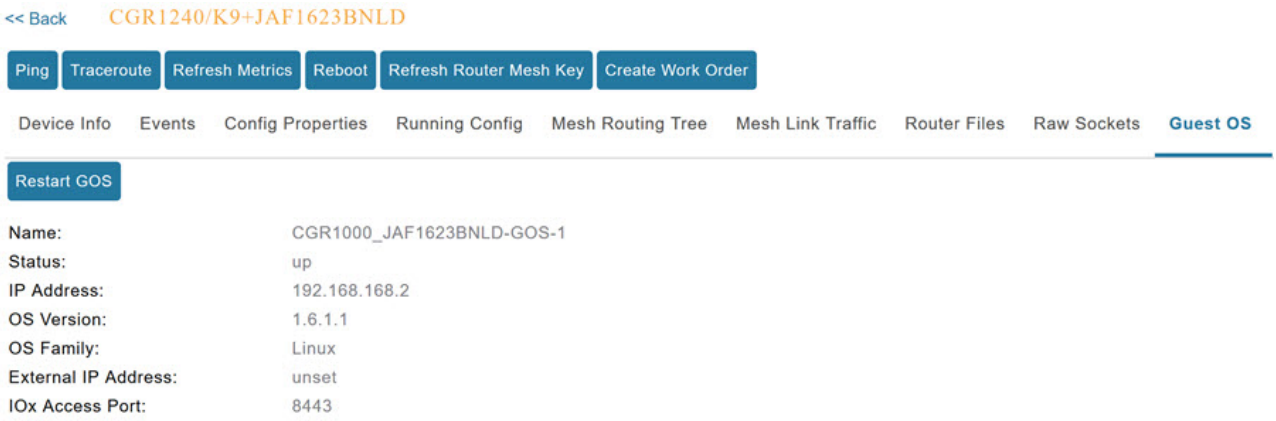
To edit an AP group configuration template:

Procedure

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

Step 2 Under CONFIGURATION GROUPS (left pane), select the 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.

Cisco IoT FND WPAN

Cisco Wireless Personal Area Network (WPAN) is a short-range wireless network that connects devices within a small area. It supports multiple network based applications and operates using Cisco routers. It is typically implemented through the Cisco Connected Grid WPAN modules for routers.

WPAN also provides robust security features for access control, device identity, key management, and encryption.

Table 18: Feature History

Release Information	Feature Name	Description
Cisco IoT FND Release 4.8.1	Support of Dual WPAN for IR8100	Cisco IoT FND 4.8.1 supports dual WPAN on IR8100 routers. The dual WPAN support allows you to add more endpoints to the router. You can insert the WPAN modules in any of the three available UIM slots in IR8100 router.

Release Information	Feature Name	Description
Cisco IoT FND Release 5.1	WPAN Reboot in Cisco IoT FND	**Reboot WPAN** button is added to the **Device info** page in Cisco IoT FND for these routers running: • Cisco IOS XE: Cisco Catalyst IR8140, • Cisco IOS: Cisco Connected Grid Router CGR1000.

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.



Note

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

Table 19: 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
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

Profile Name	Description	Properties Configurable in CSV File
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
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

Profile Name	Description	Properties Configurable in CSV File
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
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

Profile Name	Description	Properties Configurable in CSV File
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
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

Create profile

Use this task to add a new config profile.

Procedure

Step 1 From Cisco IoT FND menubar, choose **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles** tab.

Step 2 Click the **+**(plus icon) at the top of the configuration panel to open the **Add Profile** entry panel.

Step 3 Enter **Name** for the new profile and select the **Profile Type** from the drop-down list.

Step 4 Click **Add**.

A new **Profile** entry appears in the left pane under the **Profile Type** sub-heading.

The new profile is created.

Delete profile

Use this task to delete a config profile.

Procedure

Step 1 From the Cisco IoT FND menubar, choose **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles** tab.

Step 2 Select **Profile Name**.

Note
You cannot select **Default-Profile** for deletion.

Step 3 Click on the trash icon to remove the profile.

A pop-up window appears asking for your confirmation to delete.

Step 4 Click **Yes**.

The profile is deleted.

Rename a profile

Use this task to rename a config profile.

Procedure

Step 1 From the Cisco IoT FND menubar, choose **CONFIGDEVICE CONFIGURATION Config Profiles** tab.

Step 2 Select the **Profile Name** that you want to rename.

Note

You cannot select **Default-Profile** for renaming.

Step 3 Click on the pencil icon to open the **Rename Profile** pop-up window.

Step 4 Make your edit and click **OK**.

The new name appears in the list of profiles.

Clone a profile

Use this task to clone a config profile.

Procedure

Step 1 From the Cisco IoT FND menubar, choose **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles** tab.

Step 2 Select the **Profile Name** that you want to clone.

Step 3 Click on the overlapping squares icon to open the **Clone Profile** pop-up window.

Step 4 Enter a new **Profile Name**

Note
The profile name must be unique from the existing profile names.

Step 5 Click **OK**.

A new profile entry appears in the same **Profile Type** sub-heading.

Group configuration profiles

Group configuration profiles refer to the collective profiles of the members of a configuration group. The profile details are displayed in the **Configuration Group Template** page.



Note

- You are allowed to save the configuration templates and push the configuration to all devices in the **Configuration Group**.
- The profile associations within a **Configuration Group** are optional. For example, a **Configuration Group** may not require serial DCE settings, so you may select the option as None for serial DCE settings.
- 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 and the DSCP value remains the same throughout.

View WPAN configuration

Use this task to view the WPAN configuration details.

Before you begin

You can use the example in this task to retrieve the current Dual-PHY WPAN device RPL slot tree, RPL slot table, RPL IP route info table, along with the configuration information for slots 4/1 and 3/1.

Procedure

Run the command as given in the example.

Example:

```
cisco-FAR5#show run int wpan 4/1
Building configuration...
Current configuration : 320 bytes
!
interface Wpan4/1
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 ieee154 beacon-async min-interval 100 max-interval 600 suppression-coefficient 1
 ieee154 panid 5552
 ieee154 ssid ios_far5_plc
 ipv6 address 2001:RTE:RTE:64::4/64
 ipv6 enable
 ipv6 dhcp relay destination  2001:420:7BF:5F::500
end
cisco-FAR5#show run int wpan 3/1
Building configuration...
Current configuration : 333 bytes
!
interface Wpan3/1
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 ieee154 beacon-async min-interval 120 max-interval 600 suppression-coefficient 1
 ieee154 panid 5551
 ieee154 ssid ios_far5_rf
 slave-mode 4
 ipv6 address 2001:RTE:RTE:65::5/64
 ipv6 enable
 ipv6 dhcp relay destination  2001:420:7BF:5F::500
end
cisco-FAR5#show wpan 4/1 rpl stree
---------------------------- WPAN RPL SLOT TREE [4] -----------------------------
  [2001:RTE:RTE:64::4]
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1800    // SY RF nodes
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1801
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A00
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1802
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1803
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1804
\--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1805
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A03
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A07
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1806
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1807
```

```
            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1808
            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1809
            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:180A
            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:180B
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A01
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C05
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C06
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C07
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A02
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A04
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A05
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C03
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C08
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C09
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C0A
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A06
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C02
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C04
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A08
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A09
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A0A
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C00
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C01
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C0B
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A0B
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E00    // CY PLC nodes
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E01
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E02
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E03
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E04
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E05
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E06
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E07
RPL SLOT TREE: Num.DataEntries 44, Num.GraphNodes 45 (external 0) (RF 36) (PLC 8)
cisco-FAR5#ping
 2001:RTE:RTE:64:217:3BCD:26:4E01
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:RTE:RTE:64:217:3BCD:26:4E01, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 254/266/294 ms
cisco-FAR5#ping
 2001:RTE:RTE:64:207:8108:3C:1C00
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:RTE:RTE:64:207:8108:3C:1C00, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 272/441/636 ms
cisco-FAR5#
cisco-FAR5#show wpan 4/1 rpl stable

------------------------------ WPAN RPL ROUTE SLOT TABLE [4] ------------------------------
NODE_IPADDR                    NEXTHOP_IP                     SSLOT LAST_HEARD
2001:RTE:RTE:64:207:8108:3C:1800        2001:RTE:RTE:64::4                     3      17:49:12
// SY RF nodes
2001:RTE:RTE:64:207:8108:3C:1801        2001:RTE:RTE:64::4                     3      18:14:05
2001:RTE:RTE:64:207:8108:3C:1802        2001:RTE:RTE:64::4                     3      18:14:37
2001:RTE:RTE:64:207:8108:3C:1803        2001:RTE:RTE:64::4                     3      17:56:56
2001:RTE:RTE:64:207:8108:3C:1804        2001:RTE:RTE:64::4                     3      17:48:53
2001:RTE:RTE:64:207:8108:3C:1805        2001:RTE:RTE:64::4                     3      17:47:52
2001:RTE:RTE:64:207:8108:3C:1806        2001:RTE:RTE:64::4                     3      17:49:54
2001:RTE:RTE:64:207:8108:3C:1807        2001:RTE:RTE:64::4                     3      17:46:38
2001:RTE:RTE:64:207:8108:3C:1808        2001:RTE:RTE:64::4                     3      18:22:01
2001:RTE:RTE:64:207:8108:3C:1809        2001:RTE:RTE:64::4                     3      17:50:02
2001:RTE:RTE:64:207:8108:3C:180A        2001:RTE:RTE:64::4                     3      17:50:02
2001:RTE:RTE:64:207:8108:3C:180B        2001:RTE:RTE:64::4                     3      18:24:00
```

```
2001:RTE:RTE:64:207:8108:3C:1A00        2001:RTE:RTE:64:207:8108:3C:1801        3       17:56:34
2001:RTE:RTE:64:207:8108:3C:1A01        2001:RTE:RTE:64:207:8108:3C:180B        3       18:27:34
2001:RTE:RTE:64:207:8108:3C:1A02        2001:RTE:RTE:64:207:8108:3C:180B        3       18:03:06
2001:RTE:RTE:64:207:8108:3C:1A03        2001:RTE:RTE:64:207:8108:3C:1805        3       18:25:18
2001:RTE:RTE:64:207:8108:3C:1A04        2001:RTE:RTE:64:207:8108:3C:180B        3       17:57:15
2001:RTE:RTE:64:207:8108:3C:1A05        2001:RTE:RTE:64:207:8108:3C:180B        3       18:23:39
2001:RTE:RTE:64:207:8108:3C:1A06        2001:RTE:RTE:64:207:8108:3C:180B        3       18:04:16
2001:RTE:RTE:64:207:8108:3C:1A07        2001:RTE:RTE:64:207:8108:3C:1805        3       17:55:00
2001:RTE:RTE:64:207:8108:3C:1A08        2001:RTE:RTE:64:207:8108:3C:180B        3       18:19:35
2001:RTE:RTE:64:207:8108:3C:1A09        2001:RTE:RTE:64:207:8108:3C:180B        3       18:02:02
2001:RTE:RTE:64:207:8108:3C:1A0A        2001:RTE:RTE:64:207:8108:3C:180B        3       18:18:00
2001:RTE:RTE:64:207:8108:3C:1A0B        2001:RTE:RTE:64:207:8108:3C:180B        3       18:02:46
2001:RTE:RTE:64:207:8108:3C:1C00        2001:RTE:RTE:64:207:8108:3C:1A0A        3       18:22:03
2001:RTE:RTE:64:207:8108:3C:1C01        2001:RTE:RTE:64:207:8108:3C:1A0A        3       18:24:03
2001:RTE:RTE:64:207:8108:3C:1C02        2001:RTE:RTE:64:207:8108:3C:1A06        3       18:25:03
2001:RTE:RTE:64:207:8108:3C:1C03        2001:RTE:RTE:64:207:8108:3C:1A05        3       18:15:05
2001:RTE:RTE:64:207:8108:3C:1C04        2001:RTE:RTE:64:207:8108:3C:1A06        3       18:24:05
2001:RTE:RTE:64:207:8108:3C:1C05        2001:RTE:RTE:64:207:8108:3C:1A01        3       18:10:02
2001:RTE:RTE:64:207:8108:3C:1C06        2001:RTE:RTE:64:207:8108:3C:1A01        3       18:05:03
2001:RTE:RTE:64:207:8108:3C:1C07        2001:RTE:RTE:64:207:8108:3C:1A01        3       18:11:03
2001:RTE:RTE:64:207:8108:3C:1C08        2001:RTE:RTE:64:207:8108:3C:1A05        3       18:15:05
2001:RTE:RTE:64:207:8108:3C:1C09        2001:RTE:RTE:64:207:8108:3C:1A05        3       18:15:04
2001:RTE:RTE:64:207:8108:3C:1C0A        2001:RTE:RTE:64:207:8108:3C:1A05        3       18:15:04
2001:RTE:RTE:64:207:8108:3C:1C0B        2001:RTE:RTE:64:207:8108:3C:1A0A        3       18:24:03
2001:RTE:RTE:64:217:3BCD:26:4E00        2001:RTE:RTE:64::4                      4       18:21:40
// CY PLC nodes
2001:RTE:RTE:64:217:3BCD:26:4E01        2001:RTE:RTE:64::4                      4       17:47:23
2001:RTE:RTE:64:217:3BCD:26:4E02        2001:RTE:RTE:64::4                      4       18:20:16
2001:RTE:RTE:64:217:3BCD:26:4E03        2001:RTE:RTE:64::4                      4       17:49:07
2001:RTE:RTE:64:217:3BCD:26:4E04        2001:RTE:RTE:64::4                      4       18:21:49
2001:RTE:RTE:64:217:3BCD:26:4E05        2001:RTE:RTE:64::4                      4       18:22:06
2001:RTE:RTE:64:217:3BCD:26:4E06        2001:RTE:RTE:64::4                      4       18:22:51
2001:RTE:RTE:64:217:3BCD:26:4E07        2001:RTE:RTE:64::4                      4       18:24:04

Number of Entries in WPAN RPL ROUTE SLOT TABLE: 44 (external 0)
cisco-FAR5#show wpan 4/1 rpl itable
----------------------------- WPAN RPL IPROUTE INFO TABLE [4] -----------------------------
NODE_IPADDR                     RANK  VERSION     NEXTHOP_IP                      ETX_P      ETX_LRSSIR
  RSSIF HOPS  PARENTS     SSLOT
2001:RTE:RTE:64:207:8108:3C:1800        835   1     2001:RTE:RTE:64::4                      0
762   -67   -71   1     1     3    // SY RF nodes
2001:RTE:RTE:64:207:8108:3C:1801        692   2     2001:RTE:RTE:64::4                      0
547   -68   -67   1     1     3
2001:RTE:RTE:64:207:8108:3C:1802        776   2     2001:RTE:RTE:64::4                      0
711   -82   -83   1     1     3
2001:RTE:RTE:64:207:8108:3C:1803        968   2     2001:RTE:RTE:64::4                      0
968   -72   -63   1     1     3
2001:RTE:RTE:64:207:8108:3C:1804        699   1     2001:RTE:RTE:64::4                      0
643   -71   -66   1     1     3
2001:RTE:RTE:64:207:8108:3C:1805        681   1     2001:RTE:RTE:64::4                      0
627   -70   -64   1     1     3
2001:RTE:RTE:64:207:8108:3C:1806        744   1     2001:RTE:RTE:64::4                      0
683   -69   -68   1     1     3
2001:RTE:RTE:64:207:8108:3C:1807        705   1     2001:RTE:RTE:64::4                      0
648   -76   -63   1     1     3
2001:RTE:RTE:64:207:8108:3C:1808        811   2     2001:RTE:RTE:64::4                      0
811   -68   -69   1     2     3
2001:RTE:RTE:64:207:8108:3C:1809        730   1     2001:RTE:RTE:64::4                      0
692   -68   -70   1     1     3
2001:RTE:RTE:64:207:8108:3C:180A        926   1     2001:RTE:RTE:64::4                      0
926   -66   -68   1     1     3
2001:RTE:RTE:64:207:8108:3C:180B        602   2     2001:RTE:RTE:64::4                      0
314   -74   -69   1     1     3
2001:RTE:RTE:64:207:8108:3C:1A00        948   1     2001:RTE:RTE:64:207:8108:3C:1801        692
```

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

```
584   118   118   1     1     4
Number of Entries in WPAN RPL IPROUTE INFO TABLE: 44
```

The WPAN configuration details are displayed.

Enable router GPS tracking

Use this task to enable GPS traps.

You can enable GPS traps to trigger an event if the router moves a distance threshold, after a time threshold, or both.

For example, you can configure stationary, pole-top CGR monitoring for a distance threshold, to detect movement from theft or pole incident; for mobile routers, set both thresholds to determine distance over time.

Before you begin

Note

- The recommended distance threshold is 100 feet (30 m).
- Because GPS traps only generate informational logs, it is recommended that you create a rule-based event with high severity (such as **CRITICAL**) to inform the administrator of router movement. An example of this type of rule definition is:`configGroup:name eventName:deviceLocChanged`. For more information, see Creating a Rule .

Procedure

Run the command in the given example after uncommenting these lines in the default configuration template.

Example:

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

Router GPS tracking gets enabled.

Configure SNMP v3 informational events

Use this task for enabling SNMP v3 informational events.

For Cisco IOS routers you configure SNMP v3 informational events to replace the default SNMP v3 traps. For Cisco IOS routers, converting these SNMP v3 traps to SNMP v3 informational events sends an acknowledgment to the router for every event received from the router.

The router then verifies if the trap is received by Cisco IoT FND or not.

To enable SNMP v3 informational events,

Procedure

Run the commands given in the example after uncommenting the lines in the default configuration file.

Example:

```
<#-- Enable the following configurations for the nms host to receive informs
instead of traps -->
<#-- no snmp-server host ${nms.host} traps version 3 priv ${far.adminUsername} -->
<#-- snmp-server engineID remote ${nms.host} ${nms.localEngineID} -->
<#-- snmp-server user ${far.adminUsername} cgnms remote ${nms.host} v3 auth sha
${far.adminPassword} priv aes 256 ${far.adminPassword} -->
<#-- snmp-server host ${nms.host} informs version 3
priv ${far.adminUsername} -->
```

The SNMP v3 informational events are enabled.

What to do next

Once the SNMP v3 informational events are enabled you can push the new configuration file to all routers in the group.

WPAN reboot option in Cisco IoT FND

Cisco Wireless Personal Area Network (WPAN) is a type of wireless network that connects devices within a small area. It supports multiple network-based applications and operates using Cisco routers.

Starting from Cisco IoT FND Release 5.1, you can reboot WPAN on these two routers:

- Cisco IOS XE software: Cisco Catalyst IR8140.
- Cisco IOS software: Cisco 1000 Series Connected Grid Router CGR1000.

To reboot WPAN, you can use the **Reboot WPAN** button which is available in the device details page in Cisco IoT FND.

Note You can use **Reboot WPAN** option only for routers which support WPAN interface module.

Reboot WPAN

Use these steps to reboot WPAN in Cisco IoT FND.

Before you begin



Note The **Reboot WPAN** feature in Cisco IoT FND works only for routers which have a WPAN interface.

Procedure

Step 1 From the Cisco IoT FND menubar, choose:

- **DEVICES** > **FIELD DEVICES** > **Browse Devices** > **ROUTER**, or

Step 2 Select router from the **ROUTER** group.

Note
You can only select Cisco Catalyst IR8140 or Cisco Connected Grid Router CGR1000 as routers for rebooting WPAN in Cisco IoT FND.

Step 3 Click the router from the list of routers.

Step 4 Click **Reboot WPAN** in the device details page.

a) Select the WPAN slot if more than one WPAN cards are available on the router.

You will receive a confirmation message, asking whether you want to continue with the reboot or not.

Step 5 Click **Yes**.

Note
If you do not wish to continue with the WPAN reboot, then you can click **No**.

Once WPAN has rebooted successfully, the status is displayed as **Completed successfully**.



Note There are two scenarios in which WPAN reboot can fail:

- WPAN reboot fails due to missing module: In this case the **Reboot WPAN** button is not enabled in the page and you do not have to perform any action in this case.
- WPAN reboot fails even when the module is present but is not rebooting: In this case you will receive an error message asking you to wait for 30 seconds and then try rebooting again.

View WPAN reboot audit log

Use the following steps to view the status of the router after rebooting WPAN.

From Cisco IoT FND menubar, choose **ADMIN** > **System Management** :

Before you begin



Note Once you complete the WPAN reboot of selected routers, you can check the status of these routers in the audit log.

Procedure

Click **Audit Trail**.

The status of the router after WPAN reboot is displayed in the table.

View WPAN reboot events

Use this task to check the status of the routers after rebooting WPAN.

Before you begin

Once you complete rebooting WPAN for the selected routers, you can check the status of these routers in the **Events** page.

Procedure

Step 1 From Cisco IoT FND menubar, choose **DEVICES** > **FIELD DEVICES** > **Browse Devices** > **ROUTER**.

Step 2 Select and click Cisco Catalyst IR8140 or Cisco Connected Grid Router CGR1000 router from the router group.

The device inventory page is displayed.

Step 3 Click **Events**.

Note
You can also view the events listed in the Cisco IoT FND **OPERATIONS** > **Events** page.

The status of the router after WPAN reboot is displayed in the table.

Dual WPAN support for Cisco Catalyst IR8100 router

Cisco IoT FND supports dual Wireless Personal Area Network (WPAN) on Cisco Catalyst IR8100 routers. The dual WPAN support allows you to add more endpoints to the router. You can insert the WPAN modules in any of the three available UIM slots in Cisco Catalyst IR8100 router.

Cisco IoT FND uses the slot number in which the module is inserted for mapping the inventory details of the respective WPAN interface. In Cisco IoT FND, WPAN related information for the WPAN inserted in slot

number 1 is displayed by default. The WPAN related information for the WPAN inserted in slot 2 or slot 3 are suffixed with corresponding slot number.

Key considerations

Before using the Cisco Catalyst IR8100 dual WPAN, it is recommended for you to know these points:

- All parameters related to WPAN display according to slot number. User-configurable parameters display according to interface number.
- User configurable parameters are not mapped according to the slot number. The existing user configurable parameters represent the configurable parameters of first WPAN and the existing name with suffix 2 represents configurable parameters of second WPAN (for example, meshPrefixConfig, meshPrefixConfig2).
- It is recommended for you to re-register the device after WPAN addition or removal.
- Cisco IoT FND 4.8.1 supports dual WPAN feature for Cisco Catalyst IR8100 router when its firmware version is greater than or equal to 17.08.01. Cisco IoT FND maps the properties or metrics of WPAN based on the slot number in which it is inserted. If the firmware version of registered Cisco Catalyst IR8100 router is less than 17.08.01, Cisco IoT FND processes the properties or metrics the same way as it does for single WPAN and not based on slot number.

  You can consider these two scenarios to understand how dual WPAN works with slot numbers. If the WPAN is inserted in slot 2 of the Cisco Catalyst IR8100 router with firmware version less than 17.08.01, the related properties or metrics always point to a set of attributes without the slot number suffix.

  This leads to:

  - With Cisco IoT FND 4.8.1, the firmware upgrade of Cisco Catalyst IR8100 router from version less than 17.08.01 to a version greater than or equal to 17.08.01 leads the existing WPAN module to map the respective properties or metrics based on slot number.

    So the historic properties or metrics of the same Cisco Catalyst IR8100 router are mapped to one set of mesh properties or metrics (without slot number suffix) and the latest data is mapped to slot specific properties or metrics set.
  - After the Cisco IoT FND 4.8.1 upgrade process, the already registered Cisco Catalyst IR8100 device with firmware version greater than or equal to 17.08.01 starts to use the properties or metrics of the WPAN based on slot number. However, the historic properties or metrics of the same Cisco Catalyst IR8100 router is already mapped to existing set of mesh properties or metrics (without the slot number suffix).
- Because the High Availability feature is not supported in WPAN by the Cisco Catalyst IR8100 router, it is also not supported for dual WPAN in a similar way.

Prerequisites

The configuration of dual WPAN in Cisco Catalyst IR8100, requires a few prerequisites that have to be met before using it. To support dual WPAN the required prerequisites are:

- The dual WPAN interfaces are configured with: different PAN IDs and IPv6 prefixes, and same SSID or different SSID.
- Both WPANs must be in Active-Active state and in either WiSUN or CRMESH mode.

Note Mix of stack modes is not supported.

Support of dual WPAN in Field Devices page

The WPAN and related information is available in the **DEVICES** > **FIELD DEVICES** page in Cisco IoT FND. The FAN view is available in the devices list in Cisco IoT FND.

Add user configurable parameters for WPAN interfaces

Use this task to add user configurable parameters for both the WPAN interfaces.

Procedure

Step 1 From the Cisco IoT FND menubar, navigate to **DEVICESFIELD DEVICES** device list page.

Step 2 Upload a csv file from the **DEVICES** > **FIELD DEVICES** device list page.

For more information on uploading csv, see Changing Device Properties in Bulk.

Step 3 From the Cisco IoT FND menubar, navigate to **DEVICES** > **FIELD DEVICES** > **Browse Devices tab** and select **IR8100**.

Step 4 Click **Mesh Config** tab to view the uploaded values.

You can also view the uploaded values using the **Config Properties** tab in the same page which has the **Mesh Link Config** details displayed for both the WPANs along with the parameters which are suffixed according to the slot number.

The user configurable parameters for both the WPAN interfaces are added.

Support of Dual WPAN in Router Device View

In the Cisco IoT FND router device view, the Mesh Count column indicates the number of endpoints connected in the WPAN 0/1/0 inserted in slot 1. By default, the Mesh Count column is displayed. The mesh count 2 and mesh count 3 columns indicate the number of endpoints that are connected to WPAN 0/2/0 and WPAN 0/3/0. The mesh count 2 and mesh count 3 columns can be added in the Field Device page by choosing them to be in the default view. For more information, see Adding Device Views, on page 81.

View dual WPAN details in Cisco IR8100 router

Use this task to view the dual WPAN information in Cisco IR8100 router.

Procedure

From the Cisco IoT FND menubar, choose **DEVICES** > **Field Devices** > **IR8100** router.

Note

- The **Inventory** > **IR8100** device view displays the parameters for the WPAN inserted in slot 1 by default. The **Mesh** tab and **Mesh Config** tab displays the existing properties related to WPAN inserted in slot 1.
- WPAN parameters are included for the WPANs that are inserted in other slots. You can view these additional attributes by customizing your default view.

The WPAN details in Cisco IR8100 router are displayed.

Add or edit a new tab in default view

Use this task for adding or editing a new tab in the existing default view of the dual WPAN in Cisco IR8100 router.

Procedure

Step 1 From the Cisco IoT FND menubar, choose **DEVICES** > **Field Devices** > **IR8100** router.

Step 2 Click + in the devices page, or

Step 3 Click the drop-down list near the **Mesh** tab or **Mesh Config** tab to edit the current view and add WPAN specific fields.

This helps to view WPAN related details specific to WPAN 0/2/0 or WPAN 0/3/0. For more information, see Customizing Device Views.

The new WPAN related tab is added.

View additional dual WPAN fields using filters

Use this task to view the filters based on the slot number in which the WPAN is inserted

Before you begin

Note The newly added WPAN parameters are displayed in the **Show Filters** option view.

Procedure

Step 1 From the Cisco IoT FND menubar, choose **DEVICES** > **Field Devices** > **IR8100** router.

Step 2 Click **Show Filters** in the default view.

Step 3 Select the WPAN parameters from the drop-down list.

Step 4 Enter the search criteria.

The search results are displayed in the page accordingly. For more information on filters, see Using Router Filters.

Device Info tab

The **Device Info** tab in Cisco IoT FND can be used to access **Mesh Link Settings**, **Mesh Link Metrics**, **Mesh Link Keys** tabs.

The **Mesh Link Settings**, **Mesh Link Metrics**, and **Mesh Link Keys** section displays the values of the various parameters which are retrieved from both the WPANs. Under each section, the columns with WPAN interface name are displayed and the respective value of the parameters is listed under the respective column.

For more information on **Mesh Link Settings**, see Link Metrics.

For more information on Mesh Link Keys, see Mesh Link Keys.

The **Network Interface** fields in the **Device Info** page are as given in the table.

Table 20: Network interface fields

Field	Description
Interface	Indicates the name of the interface
Admin Status	Provides admin status (up/down)
Oper. Status	Provides operational status (up/down)
IP Address	Indicates the IP address of the device
Physical Address	Indicates the latitude and longitude of the device
Tx Speed (bps)	Indicates the speed (bits/sec) of data transmitted by the interface
Tx Drops (bps)	Indicates the number of packets dropped (drops/sec)
Rx Speed (bps)	Indicates the speed (bits/sec) of data received by the interface

View Device Info tab

Use this task to view the Cisco IoT FND **Device Info** tab.

Procedure

Step 1 From the Cisco IoT FND menubar, choose **DEVICES** > **Field Devices** > **IR8100** router.

Step 2 Click on router from the list of routers.

Note

- The **Network Interface** table in the **Device Info** page provides the details of both the WPAN interfaces that are connected in any of the three available slots.
- The Cisco IR8100 device is connected to CAM module through new virtual port group interface which is processed to retrieve information of the RPL tree. Based on the settings in the RPL tree, the mesh routing tree is displayed.

- The **Device Info** tab displays the **Mesh Link Traffic** chart according to the time period selected on the top-right side of the page. The information given in the chart is color coded to distinguish the slot in which the WPAN is inserted. For example, the color used for Tx or Rx speed of WPAN in slot 1 is different from that of WPAN in slot 2.
- You can click on the color code and the respective line in the chart is removed from the graph. This applies for all the charts.
- The endpoint hop count chart shows an aggregated endpoint count between the hops connected to both the WPAN interfaces.

The **Device Info** page is displayed.

View dual WPAN events

Use this task to view the dual WPAN events in Cisco IoT FND.

Procedure

Step 1 From the Cisco IoT FND menubar, choose **DEVICES** > **Field Devices** > **IR8100** router.

Step 2 Click on router from the list of routers

Step 3 Click **Events** tab.

The dual WPAN events page is displayed.

View Running Config tab

Use this task to view the **Running Config** tab in Cisco IoT FND.

Procedure

Step 1 From the Cisco IoT FND menubar, choose **DEVICES** > **Field Devices** > **IR8100** router.

Step 2 Click on router from the list of routers

Step 3 Click **Running Config** tab.

The **Running Config** page gets displayed.

View Mesh Routing Tree

Use this task to view the **Mesh Routing Tree** in the **Device Info** page in Cisco IoT FND.

The **Mesh Routing Tree** tab allows you to select the available WPAN interface for which you want to see the mesh routing table information. For example, if you want to see the mesh routing tree information of WPAN inserted in slot number one, then you must select WPAN0/1/0.

Before you begin

Note

- By default, the **WPAN Interface** drop-down list displays the WPAN interface inserted in lower slot number. Therefore, the information pertaining to the respective WPAN is displayed. So, you must select the available WPAN from the drop-down list for which you want to view the information.
- During RPL tree polling, the information is fetched from both WPAN interfaces and processed by FND. For more information on polling, refer to Configure RPL tree polling.
- For the Cisco IR8100 device with CAM module, the RPL tree information is captured from the respective CAM module and displayed in the **Mesh Routing Tree** tab. The Cisco IR8100 device as the root element and the act devices connected to the CAM module are shown.

Procedure

Step 1 From the Cisco IoT FND menubar, choose **DEVICES** > **Field Devices** > **IR8100** router.

Step 2 Click on router from the list of routers

Step 3 Click **Mesh Routing Tree** tab.

Step 4 Select the required WPAN slot number from the **WPAN Interface** drop-down list.

The table describes the fields under **Mesh Routing Tree** tab in the **Device Info** page.

Field	Description
EID	Element Identifier.
Name	Router EID (Device identifier).
Status	Provides status of device (up/down).
Type	It represents the FAR and endpoint device type.
IP Address	Indicates the IP address of the device.
Last Heard	Last date and time the device contacted IoT FND.
Meter ID	Meter ID of the device.
Transmit Speed (bits/sec)	Indicates the speed (bits/sec) of data transmitted by the interface.
Packet Drops (packets/sec)	Indicates the number of packets dropped (drops/sec).
Receive Speed (bits/sec)	Indicates the speed (bits/sec) of data received by the interface.
RPL Hops (hops)	Number of hops that the element is from the root of its RPL routing tree.
RPL Link Cost (etx)	RPL cost value for the link between the element and its uplink neighbour.
RPL Path Cost (etx)	RPL path cost value between the element and the root of the routing tree.

Field	Description
RSSI	Shows the measured RSSI value of the primary mesh RF uplink (dBm) over time.
Reverse RSSI	RSSI received from the neighbour.
Active Link Type	Determines the most recent active RF or PLC link of a meter.

The table displays the mesh routing information for the selected WPAN.

Support of dual WPAN in Device Configuration page

Dual WPAN is also supported in the Cisco IoT FND **Device Configuration** page.

View dual WPAN in Device Configuration page

Use this task to view the dual WPAN parameters in the **Device Configuration** page in Cisco IoT FND.

Procedure

From the Cisco IoT FND menubar, choose **CONFIG** > **Device Configuration** > **ROUTER** > **Default-Ir8100** router.

Note
In the **Group Members** tab, the table is updated with four more columns for representing the user configured parameters such as meshPrefixConfig2, meshPrefixLengthConfig2, meshPanIdConfig2, meshAddressConfig 2 metrics. The existing parameter represents for first WPAN and the parameters with suffix represents the configured parameter for the second WPAN.

The dual WPAN details are displayed in the **Device Configuration** page.

Edit dual WPAN user configurable parameters

Use this task to edit the user configurable dual WPAN parameters in the **Device Configuration** page in Cisco IoT FND.

The **Edit Configuration Template** page allows you to define user configurable parameters in the template. Cisco IoT FND maps the defined parameters to the WPAN parameter value configured through CSV.

Procedure

Step 1 From the Cisco IoT FND menubar, choose **CONFIG** > **Device Configuration** > **ROUTER** > **Default-Ir8100** router.
Step 2 Click **Edit Configuration Template**.
Step 3 Enter the parameter values in **Edit Configuration Template** box.
Step 4 Click **Save**.

Note

- You can change device properties by clicking the **Change Device Properties** button.
- You can export the dual WPAN related user configurable parameters in a csv file format by clicking **Export Template Keys as CSV** button.

The user configurable dual WPAN parameters are edited and saved.

View dual WPAN in Dashboard

Use this task to view dual WPAN in the **DASHBOARD** page in Cisco IoT FND.

Procedure

Step 1 From the Cisco IoT FND menubar, choose **DASHBOARD** .

Step 2 Click on the gear icon called **Settings**.

Step 3 Click **Dashlets** drop-down box in the **Dashboard Settings** window.

Step 4 Select the interface enabled devices from the **Dashlets** drop-down box.

Step 5 Click **Close**.

The **Devices with interfaces enabled but down** filter settings combo box is displayed.

Step 6 Select **Type**, **Device**, **Interface**, **WPAN *x*|*y*|*z***.

Note
The **Type** refers to the type of device, **Device** refers to the router like Cisco IR8100 router, **Interface** is the **WPAN *x*|*y*|*z*** interface type listed in the drop-down box.

Step 7 Click **Save**.

A gauge chart with device interface is displayed.

Step 8 Click on the needle of the gauge chart.

T devices for which the interfaces are enabled is displayed in the gauge chart.

The status of the device interface is displayed in the form of a gauge chart.

Refresh router mesh keys for Dual WPAN

Use this task to refresh the Cisco Catalyst IR8100 mesh keys. for the following nodes:

Refreshing the router mesh key helps to avoid the downtime of devices when they expire.

Before you begin

Consider these points before the router refresh.

- You can refresh the Cisco Catalyst IR8100 router mesh keys. for the following nodes:

Table 21: Nodes and supported devices for dual WPAN router mesh keys

Nodes	Supported Devices
Fully Functional Nodes (FFN)	IR500 and L+G devices (lgnn and lgelectric).
Limited Functional Nodes (LFN)	Battery endpoints.

- Cisco IoT FND refreshes the mesh keys automatically once the refresh time is reached.

  You can alternatively refresh Cisco IR8100 router mesh keys from the **Devices Details** page using the **Refresh Router Mesh LFN Key** button or **Refresh Router Mesh FFN Key** button.

Procedure

Step 1 From the Cisco IoT FND menubar, choose **DEVICES** > **Field Devices** > **IR8100** router.

Step 2 Click **More Actions** > **Refresh Router Mesh LFN Key** (or) **Refresh Router Mesh FFN Key**.

Step 3 Click **Yes** to continue.

The key refresh time and key expiration time values are updated under Mesh Link Keys accordingly.

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.

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

.

Device-level configuration push

Device-level configuration push is a management capability that allows administrators to apply specific configurations directly to a device using FreeMarker templates.

- Supports configuration deployment with or without rollback mechanisms.
- Integrates with registration and active running configuration views for monitoring.
- Facilitates updates during reprovisioning, ZTD, and re-ZTD processes.

Table 22: Feature History

Feature Name	Release Information	Description
Device-Level Configuration Push	Cisco IoT FND Release 5.0	Push configurations at the device level using the **Push Configuration** tab in the **CONFIG** > **Device Configuration** page.

Configuration Push Methods and Running Config Details

The following methods are available for pushing configurations to a device:

- Config Push with Rollback : Pushes the configuration by first rolling back to the before-registration-config and then applying the new configuration.
- Config Push without Rollback: Pushes the configuration to the device without rolling back to the before-registration-config.

The Running Config tab provides visibility into the following configurations:

- Registration Config : Displays the before-registration-config configuration that is baselined in Cisco IoT FND.
- Active Running Config: Displays the running configuration received from the device after the without rollback config push.

Note During the Config Push with Rollback operation, you cannot perform tunnel provisioning or firmware upgrade.

Note Cisco IoT FND supports configuration push at the group-level with rollback capabilities to prevent any misconfigurations caused by manual changes.

Push a configuration with rollback

The Push with rollback option updates the device configuration by first rolling back to the before-registration-config configuration and then applying the new configuration.

Note When applying a configuration at the device level, if you simultaneously attempt to push a configuration at the group level (for the selected device), then the group-level configuration operation is skipped for the device.

Configuration Sequence: The configuration is pushed to the device in the following sequence:

1. Roll back to (`before-registration-config`)
2. Apply group-level configuration
3. Apply device-level configuration

Note If the device-level configuration is not defined, then the configuration is pushed in this sequence:

a. Roll back to (`before-registration-config`)

b. Apply group-level configuration

Procedure

Step 1 From the main menubar, choose **Devices** > **Field Devices** > **Router** .

Step 2 Select Cisco IOS or IOS-XE device type from the left pane.

Step 3 In the right pane, click the device for which you want to push the configuration.

Step 4 Click the **Push Configuration** tab.

Step 5 Define the device configuration in the FreeMarker template.

Step 6 Click **Save** .

Step 7 Select **Push with rollback** from the **Push Router Configuration** drop-down list.

Step 8 Click **Submit** to initiate the config push operation.

- **Config Push Status** : After the config push is initiated, the status is updated in the **Device Status** section. The statuses include:
  - Queued
  - Configuring

- Success
- Error

Note
Once the config push with rollback is initiated, the config push status keeps updated every 60 seconds.

Note
The config push status is viewed from either **Push Config** tab or at the group-level (**CONFIG** > **DEVICE CONFIGURATION** > **Push Configuration** tab.

- **Viewing Running Config** : Click the **Running Config** tab to view registration config which is pushed to the device, along with group level config if it exists and the active running config is cleared.

Note
If you perform either a device level config push with roll back or group level config push both get pushed to the device and are displayed in the registration config section and the if the active running config exists, it gets cleared.

What to do next

- Viewing Config Push Events, on page 157
- Viewing the Audit Trail, on page 159

Push a configuration without rollback

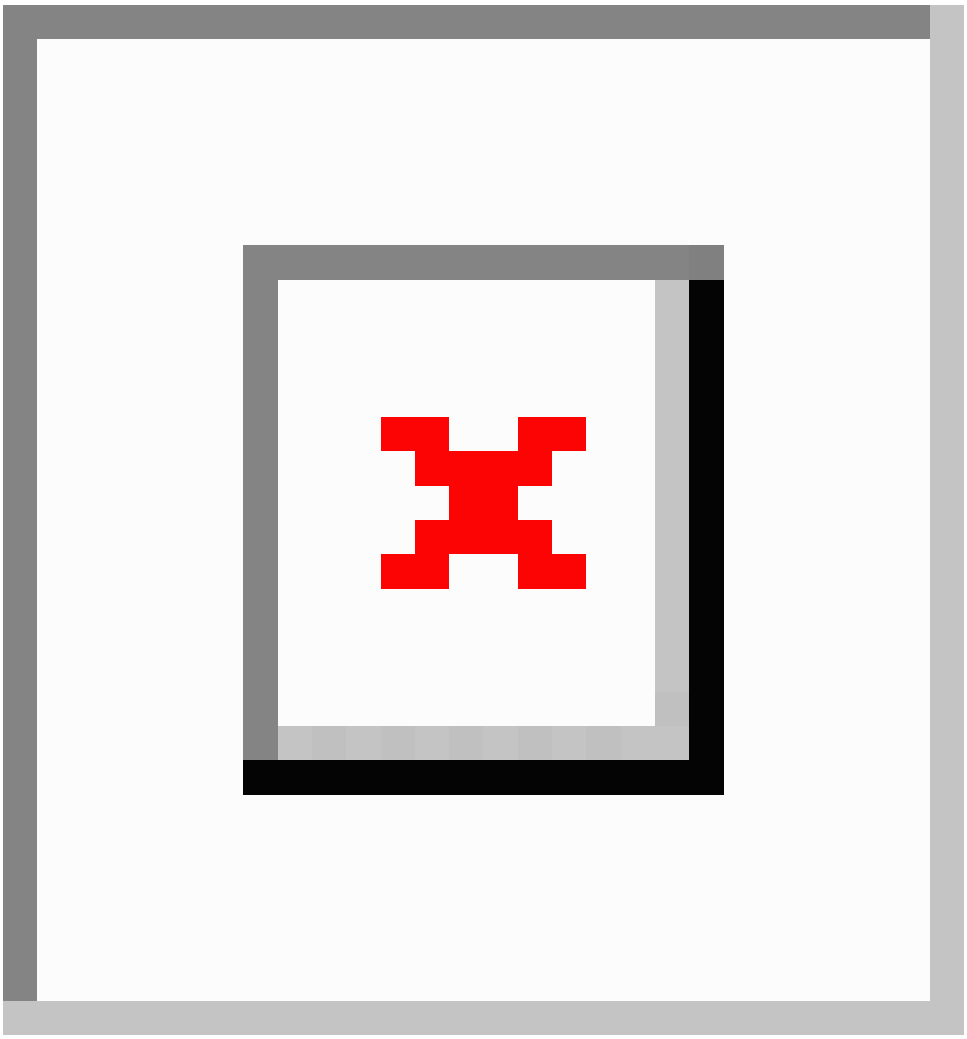
The Push without rollback option allows you to apply the configuration to the device without rolling back to the existing configuration (before-registration-config). In this scenario, FND directly pushes the config commands that are defined in the FreeMarker template to the device assuming that the device is already configured at the group level. You can also push the configuration to multiple devices simultaneously in different web sessions.

Viewing New Configuration : You can view the new configuration that is pushed to the device in the **Active Running Config** section of the **Running Config** tab.

Follow these steps to push a configuration without rollback.

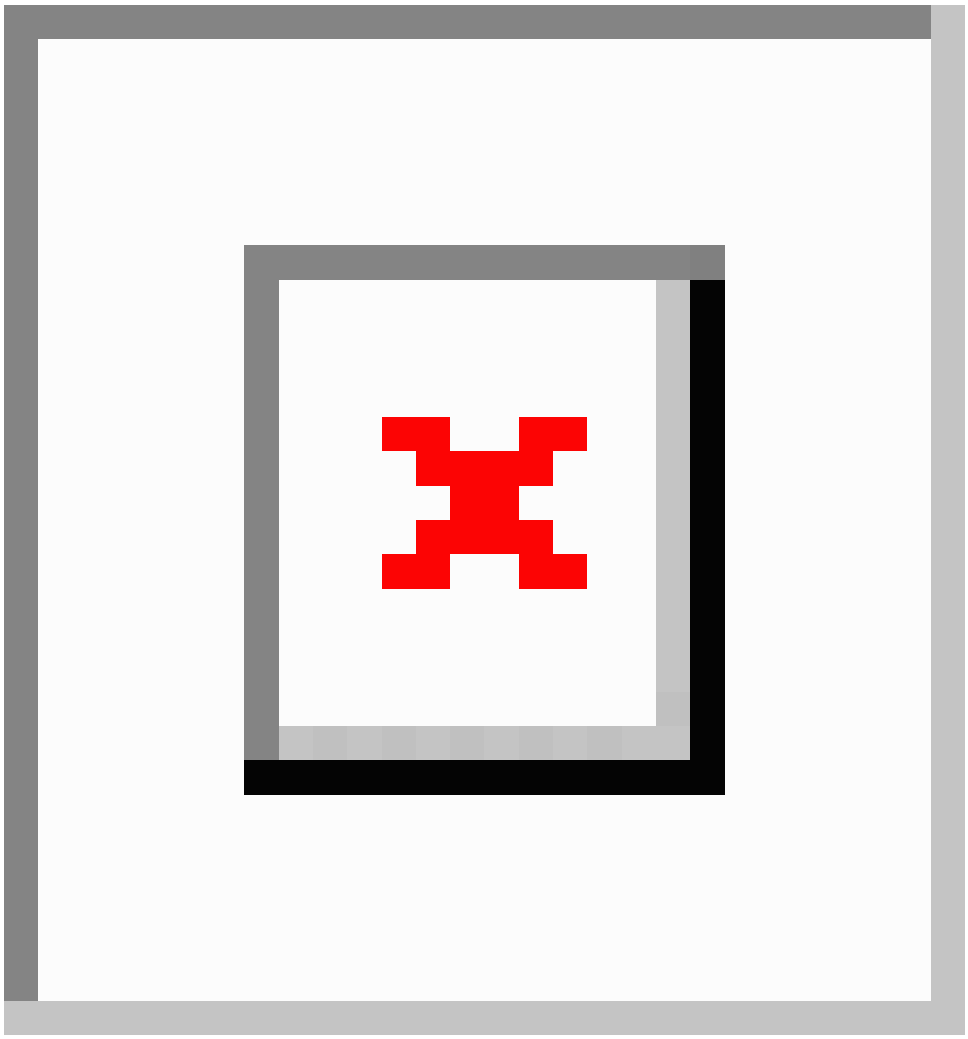
Procedure

Step 1 From the main menubar, choose **Devices** > **Field Devices** > **Router**.
Step 2 Select Cisco IOS or IOS-XE device type from the left pane. The **Inventory** page appears.
Step 3 In the right pane, click the device for which you want to push the configuration.
Step 4 In the Device Info page, click the **Push Configuration** tab.
Step 5 Define the device configuration in the FreeMarker template.
Step 6 Click **Save Template** .
Step 7 Select **Push without rollback** from the **Push Router Configuration** drop-down list.



Step 8 Click **Submit** .

Step 9 A warning message appears. Click **Yes** .



Note
For viewing running config, click the **Running Config** tab to view both the registration config and the active running config sections. The pushed configuration is displayed in the active running config section.

Config Push Status : After the config push is initiated, the status is updated in the **Device Status** section.

Note

- Both registration and active running configs are displayed when config push is performed without a rollback .
- Once the config push without rollback is initiated, the config push status keeps updated every 10 seconds.
- Maintain the history of commands in the device-level template to preserve them during the reprovisioning process or group-level config operations.

What to do next

- Viewing Config Push Events, on page 157

- Viewing the Audit Trail, on page 159

Note Once the tunnel reprovisioning is successful and the device is registered to Cisco IoT FND, the active running configs gets cleared and only registration config is displayed. If device level and group level configurations are present they are pushed to the device and will appear in the registration config section. This will clear the active running configuration.

Viewing Config Push Events

This section explains the various event statuses available for the configuration push at the device level and group level.

- Viewing config push events at the device level without rollback
- Viewing config push events at the device level with rollback
- Viewing config push events at the group level (for the selected device)

Procedure

Step 1 Choose **DEVICES** > **FIELD DEVICES** > **ROUTER**.

Step 2 Select the device type and click the required device on the right pane.

Step 3 Click the **Events** tab. The events for the selected device appear. You can also filter the events for the selected device by choosing the options from the drop-down list (example: Last 24 hours, Last 15 minutes).

a) Viewing config push events at the device level without rollback:

- The events of a successful configuration push include:
  - Device Configuration Push Initiated Without Rollback
  - Device Configuration Push Successful
- The events of a failed configuration push include:
  - Device Configuration Push Initiated Without Rollback
  - Device Configuration Push Failed

Time	Event Name	Severity	Message
2024-08-29 12:19:28:309	Device Configuration Push Failed	MAJOR	java.io.IOException: [invalid configuration commands supplied [BAD_PARAMETER][no shut1]. [PARSE_ERROR_NOMATCH]] Sent [[int loop1234, no shut1]]
2024-08-29 12:19:21:883	Device Configuration Push Initiated Without Rollback	INFO	Configuration push Initiated to Device: CGR1240/K9+FTX2518D00M , Push Type: Push Without Rollback.
2024-08-29 12:15:50:015	Device Configuration Push Successful	INFO	Configuration push successfully applied to Device: CGR1240/K9+FTX2518D00M
2024-08-29 12:15:40:926	Device Configuration Push Initiated Without Rollback	INFO	Configuration push Initiated to Device: CGR1240/K9+FTX2518D00M , Push Type: Push Without Rollback.

b) Viewing config push events at the device level with rollback:

- The different events of a successful configuration push include:
  - Device Configuration Push Initiated With Rollback

- Configuration Rollback
- Registration Request
- Registration Success
- Device Configuration Push Successful

2024-08-29 11:03:54:270	Device Configuration Push Successful	INFO	Configuration push successfully applied to Device: CGR1240/K9+FTX2518D00M
2024-08-29 11:03:51:018	Registration Success	INFO	Registration successful.
2024-08-29 11:03:17:674	Registration Request	INFO	Registration request from device.
2024-08-29 11:01:16:432	Configuration Rollback	INFO	Rolling back configuration to flash:/before-registration-config
2024-08-29 11:01:03:597	Device Configuration Push Initiated With Rollback	INFO	Configuration push Initiated to Device: CGR1240/K9+FTX2518D00M, Push Type: Push With Rollback

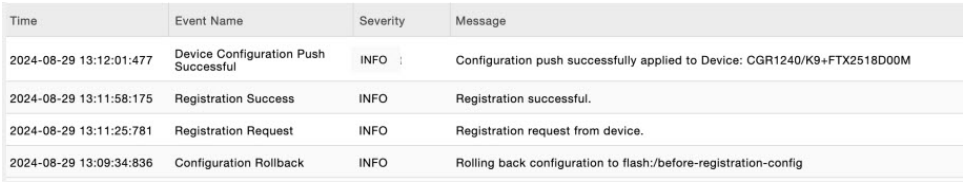
- The different events of a failed configuration push include:
  - Device Configuration Push Initiated With Rollback
  - Configuration Rollback
  - Registration Request
  - Registration Failure
  - Device Configuration Push Failed

Time	Event Name	Severity	Message
2024-09-06 15:24:47:893	Device Configuration Push Failed	MAJOR	Unable to configure element: java.io.IOException: [invalid configuration commands supplied [BAD_PARAMETER][ip scp server enable1234] [PARSE_ERROR_NOMATCH]] Sent [[cgna gzip, cgna profile cg-nms-periodic, gzip, url https://fnd.iot.cisco.com:9121/cgna/ios/metrics, interval 60, add-command show version] format flash:/managed/odm/cg-nms.odm, add-command show environment temperature | format flash:/managed/odm/cg-nms.odm, add-command show hosts | format flash:/managed/odm/cg-nms.odm, add-command show interfac
2024-09-06 15:24:47:874	Registration Failure	MAJOR	java.io.IOException: java.io.IOException: [invalid configuration commands supplied [BAD_PARAMETER][ip scp server enable1234]. [PARSE_ERROR_NOMATCH]] Sent [[cgna gzip, cgna profile cg-nms-periodic, gzip, url https://fnd.iot.cisco.com:9121/cgna/ios/metrics, interval 60, add-command show version] format flash:/managed/odm/cg-nms.odm, add-command show environment temperature | format flash:/managed/odm/cg-nms.odm, add-command show hosts | format flash:/managed/odm/cg-nms.odm, add-command show interfaces | for
2024-09-06 15:24:27:930	Registration Request	INFO	Registration request from device.
2024-09-06 15:12:54:580	Configuration Rollback	INFO	Rolling back configuration to flash:/before-registration-config
2024-09-06 15:12:45:620	Device Configuration Push Initiated With Rollback	INFO	Configuration push Initiated to Device: CGR1240/K9+FTX2518D00M, Push Type: Push With Rollback

c) Viewing config push events at the group level (for the selected device):
   - Choose **CONFIG** > **DEVICE CONFIGURATION** > **ROUTER**.
   - Select the default configuration group of the selected device.
   - Click the **Push Configuration** tab. The device status appears in the Device Status table.
     - The various events of a successful configuration push is shown in the **Events Name** column.

Time	Event Name	Severity	Message
2024-08-29 13:12:01:477	Device Configuration Push Successful	INFO	Configuration push successfully applied to Device: CGR1240/K9+FTX2518D00M
2024-08-29 13:11:58:175	Registration Success	INFO	Registration successful.
2024-08-29 13:11:25:781	Registration Request	INFO	Registration request from device.
2024-08-29 13:09:34:836	Configuration Rollback	INFO	Rolling back configuration to flash:/before-registration-config

     - The various events of a failed configuration push is shown in the **Events Name** column.



Time	Event Name	Severity	Message
2024-08-29 13:12:01:477	Device Configuration Push Successful	INFO	Configuration push successfully applied to Device: CGR1240/K9+FTX2518D00M
2024-08-29 13:11:58:175	Registration Success	INFO	Registration successful.
2024-08-29 13:11:25:781	Registration Request	INFO	Registration request from device.
2024-08-29 13:09:34:836	Configuration Rollback	INFO	Rolling back configuration to flash:/before-registration-config

Note
Alternatively, you can also view the events from the Operations menu (**OPERATIONS** > **EVENTS**.

Viewing the Audit Trail

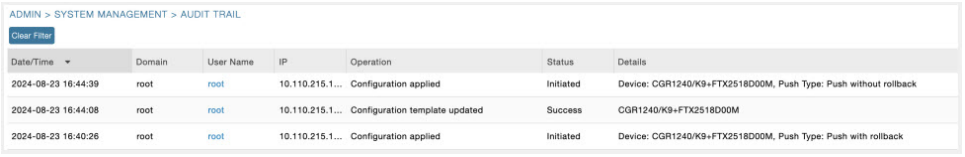
To view the audit trail:

Procedure

Choose **ADMIN** > **System Management** > **Audit Trail**.

There are two audit trail statuses:

- Success: When the device-level configuration template is saved.
- Initiated: When the configuration push starts, either with or without rollback.



ADMIN > SYSTEM MANAGEMENT > AUDIT TRAIL

Clear Filter

Date/Time	Domain	User Name	IP	Operation	Status	Details
2024-08-23 16:44:39	root	root	10.110.215.1...	Configuration applied	Initiated	Device: CGR1240/K9+FTX2518D00M, Push Type: Push without rollback
2024-08-23 16:44:08	root	root	10.110.215.1...	Configuration template updated	Success	CGR1240/K9+FTX2518D00M
2024-08-23 16:40:26	root	root	10.110.215.1...	Configuration applied	Initiated	Device: CGR1240/K9+FTX2518D00M, Push Type: Push with rollback

Push configurations to routers

Use this task to push configuration to routers.

Router configuration pushes are performed from the Push Configuration tab for selected router groups or subsets.

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

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 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 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**.

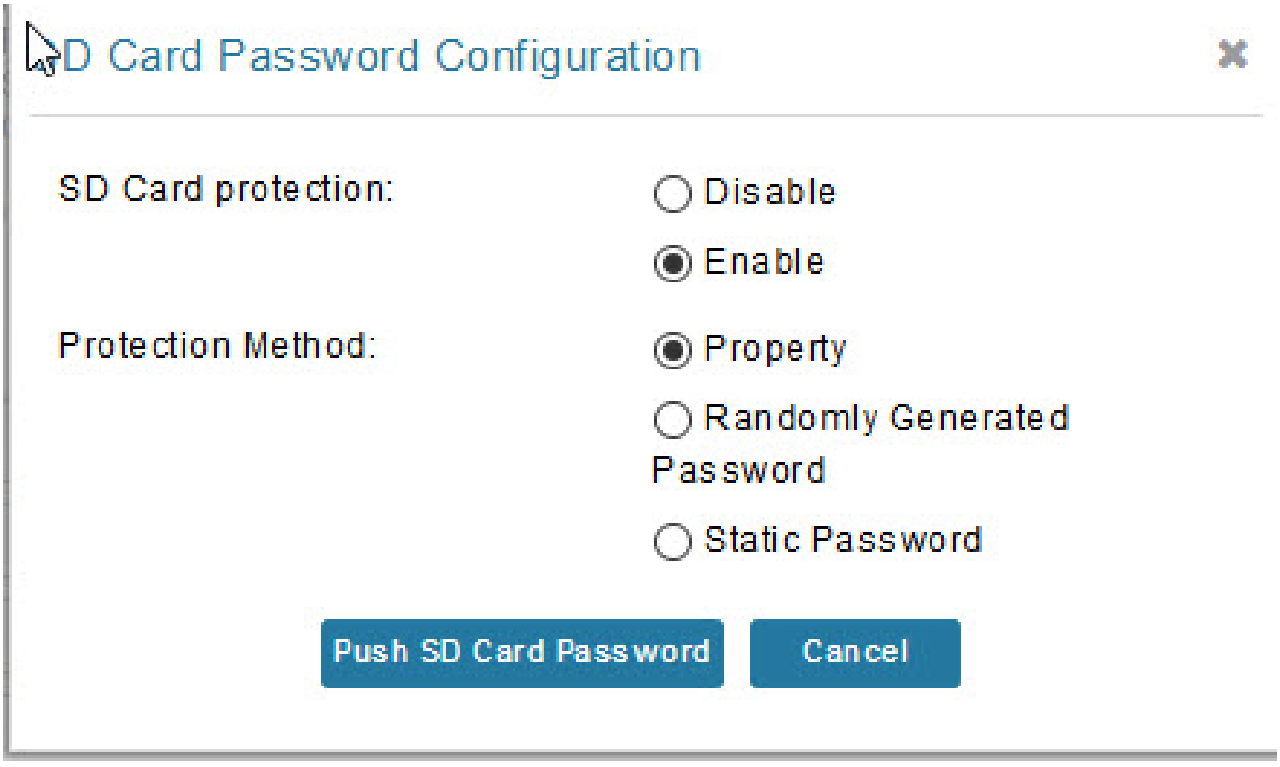
Step 2 Select the CGR group or CGRs to push the configuration to in the Configuration Groups pane

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 164
- Device Configuration page — Figure 8: CONFIG > DEVICE CONFIGURATION > Endpoint Certificate Re-enrollment, on page 165
- DTLS Relay Settings — Figure 9: Support for DTLS Relay Settings and Cert Auto-Renew Settings for ITRON30 and IR500 Devices, on page 165

- Additionally, Certificate Information is provided for IR500s — Figure 10: Certificate Information for IR500, on page 165

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

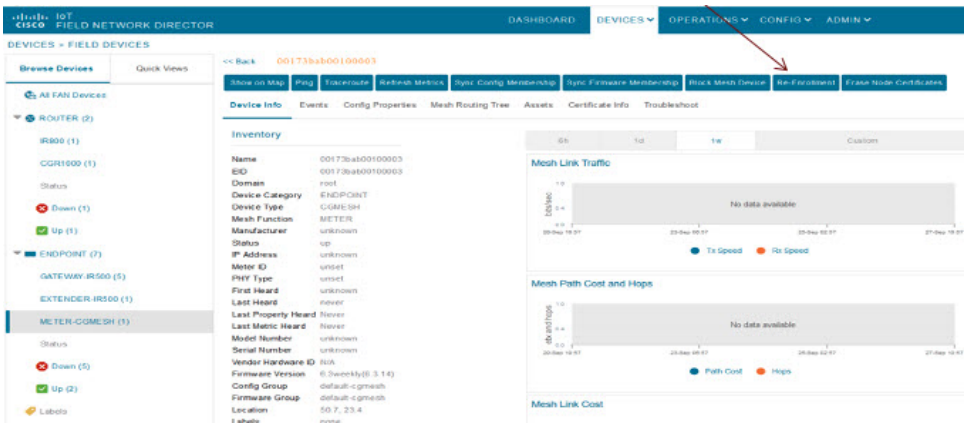


Figure 7: DEVICES > FIELD DEVICES > Endpoint Re-Enrollment (2 of 2)

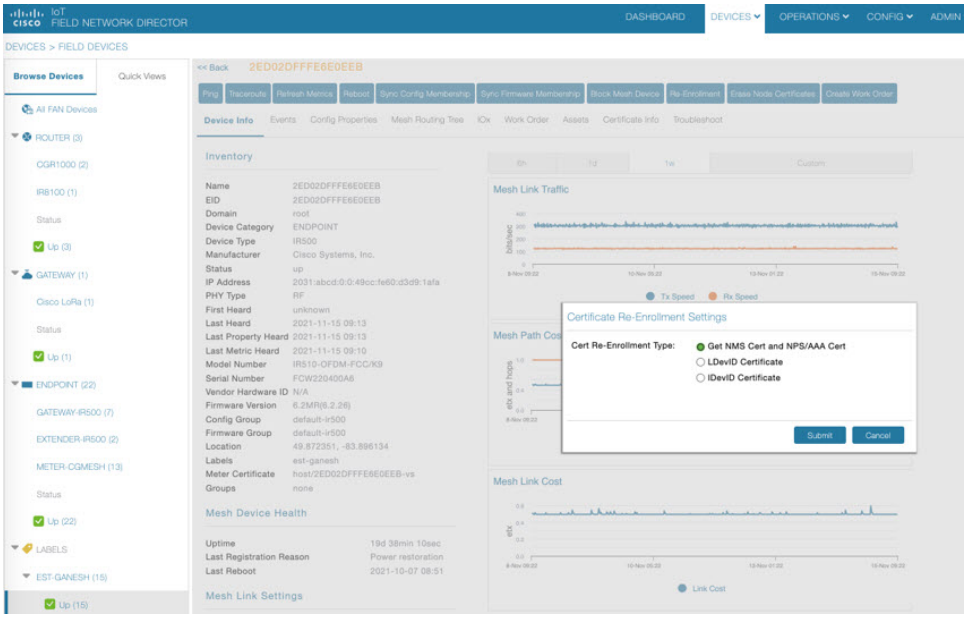


Figure 8: CONFIG > DEVICE CONFIGURATION > Endpoint Certificate Re-enrollment

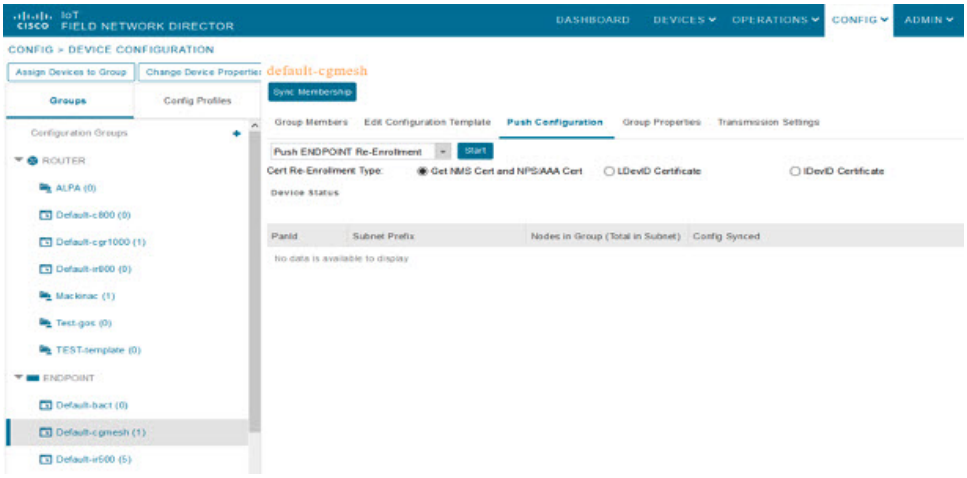
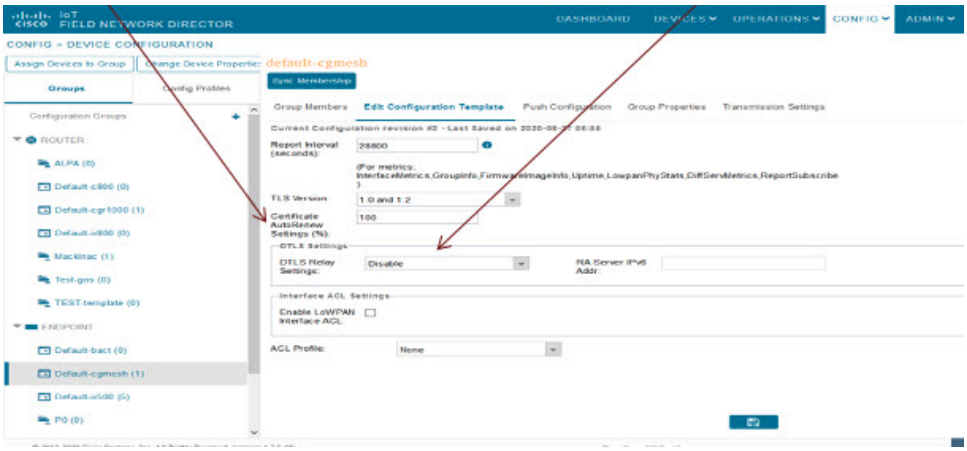
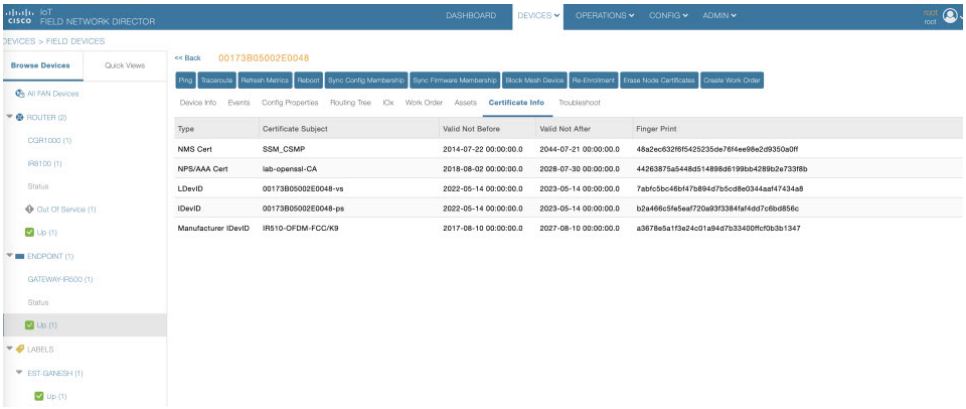


Figure 9: Support for DTLS Relay Settings and Cert Auto-Renew Settings for ITRON30 and IR500 Devices



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.

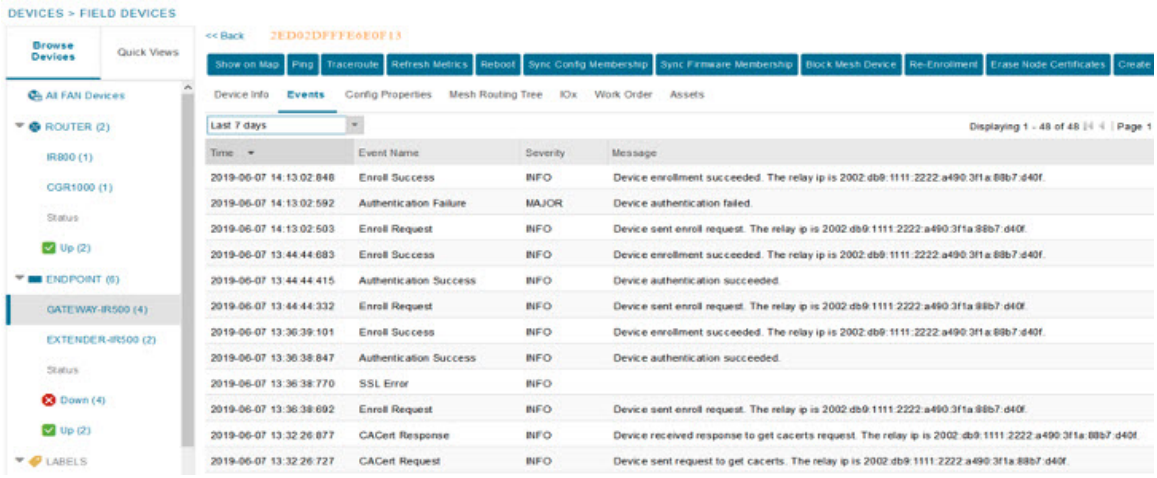
Figure 10: Certificate Information for IR500



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:**

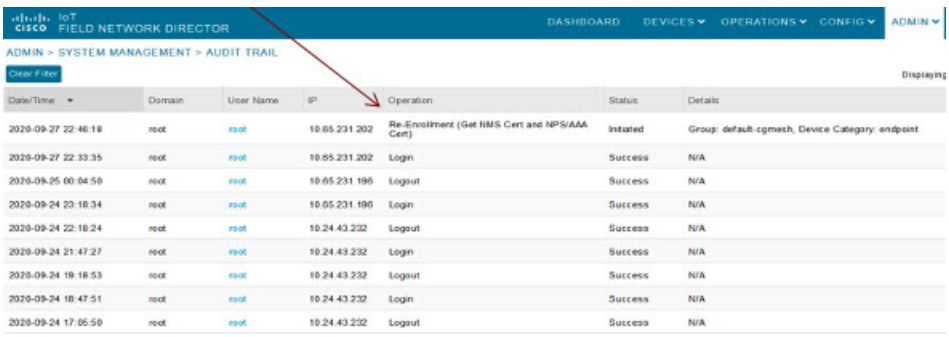
Operation: Re-enrollment (Get NMS Cert and NPS/AAA Cert)

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.

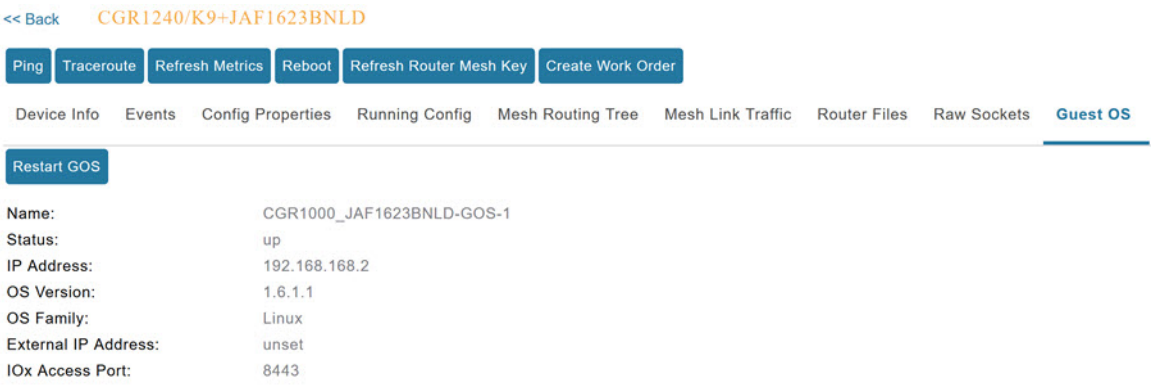
After any Cisco IOS install or upgrade, when IoT FND discovers a GOS, it checks if the initial communications setup is complete before it performs the required setup. The CGR must have a DHCP pool and Gigabit Ethernet 0/1 interface configured to provide an IP address and act as the gateway for the Guest 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 168

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

Cisco IoT FND supports application management for IR1100 and IR1800 devices. The OS used is Polaris OS (IOS-XE). IOx node can be started and stopped from the IoT FND UI. The docker applications can be installed in the IR1100 or IR1800 device and are also managed by IoT FND from the APPS main menu and from the Device Details page (App tab and IOx tab) when the IR1100 or IR1800 device is registered with IoT FND and Fog Director (FD) integrated environment.

Note The application management for IR1100 and IR1800 is supported only on OVA installations and not on standalone IoT FND installation.

Prerequisites

- The configuration required for the application hosting are:
  - Enabling IOx
  - Configuring a VirtualPortGroup to a Layer 3 Data Port

  For more configuration related information, see Cisco Catalyst IR1101 Rugged Series Router Software Configuration Guide or Cisco Catalyst IR1800 Rugged Series Router Software Configuration Guide.
- FND and FD Integrated OVA with FD version v1.18.1 and above.

Registering IR1100 or IR1800 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.

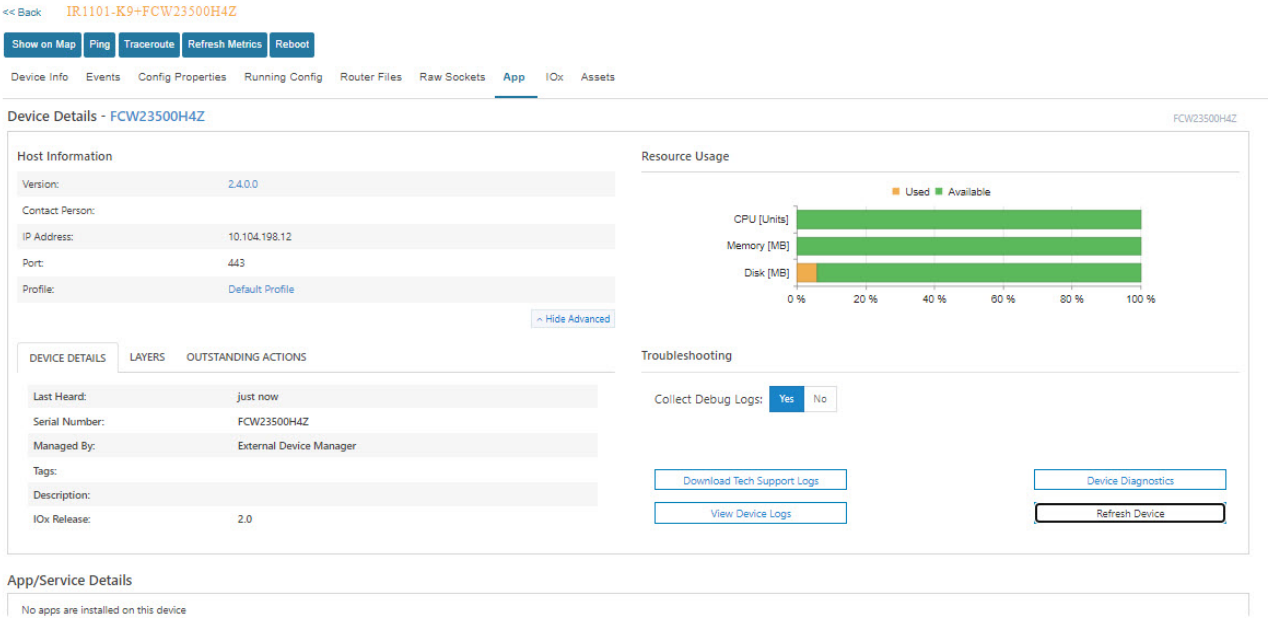


Step 3 Click **Yes** in the confirmation dialog box.

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.

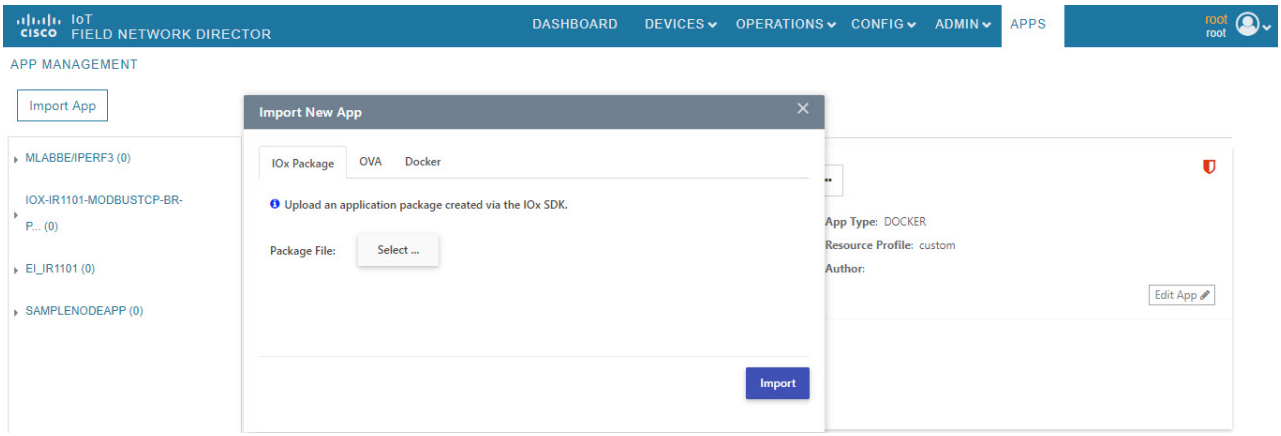
Importing the Application in APPS Main Menu

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

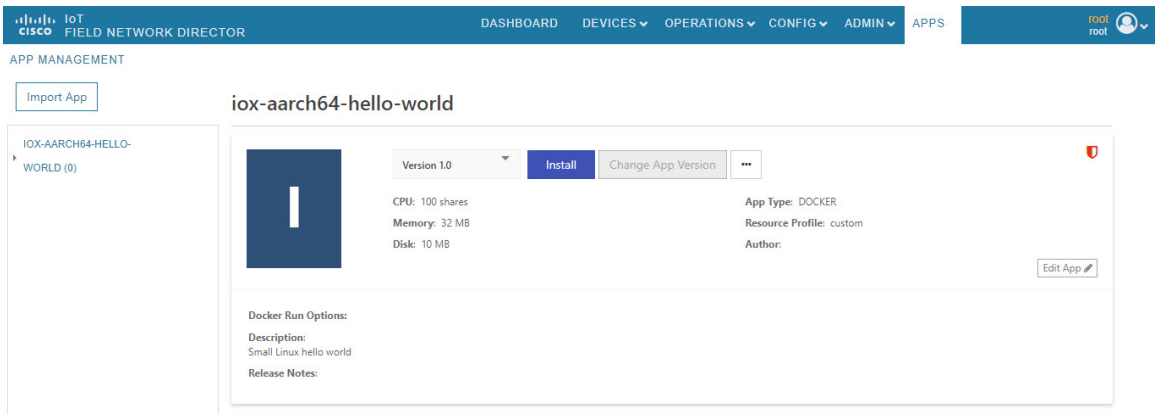
Step 1 Click **Import App**.

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.

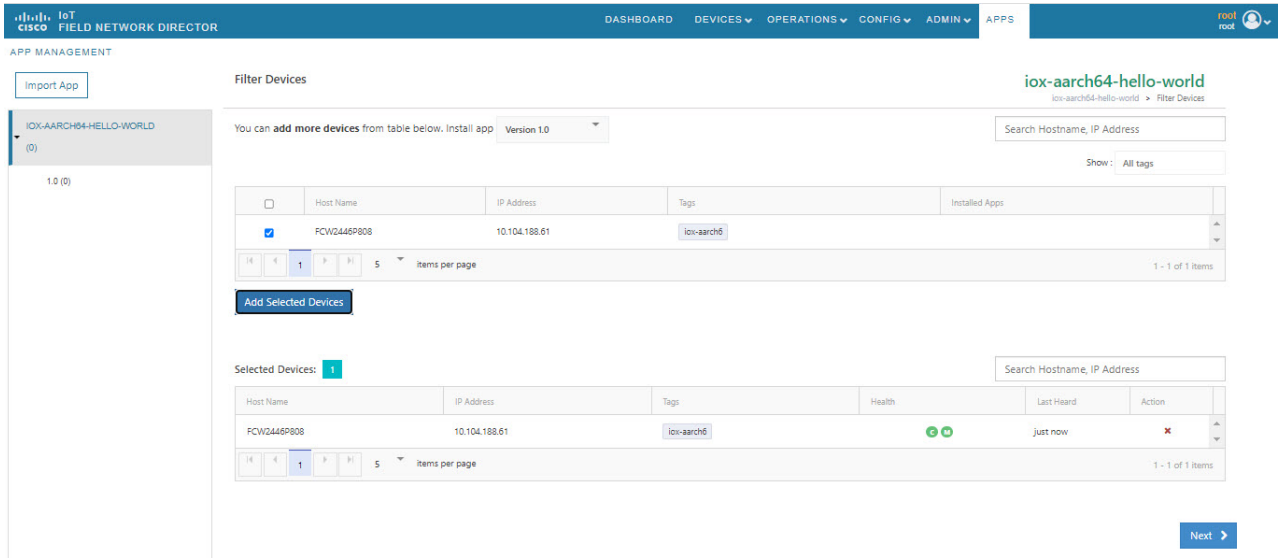
Procedure

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

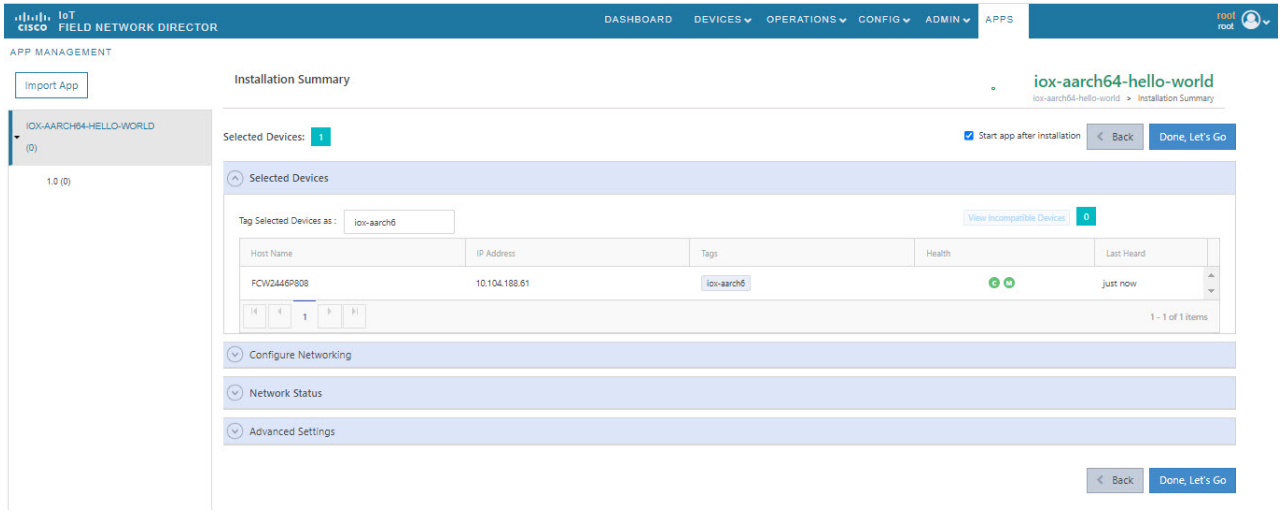
Step 2 Click **Add Selected Devices**. The device is added to the Selected Devices section where the Last Heard status of the device can be seen.

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

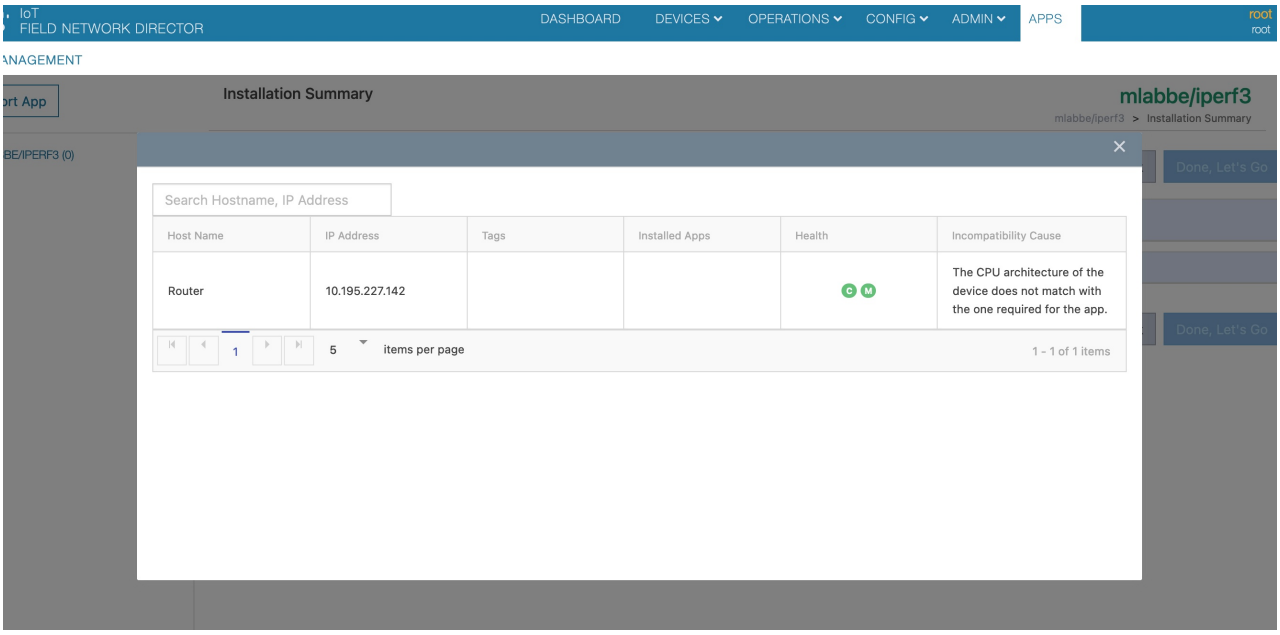
Step 3 Click **Next**.



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

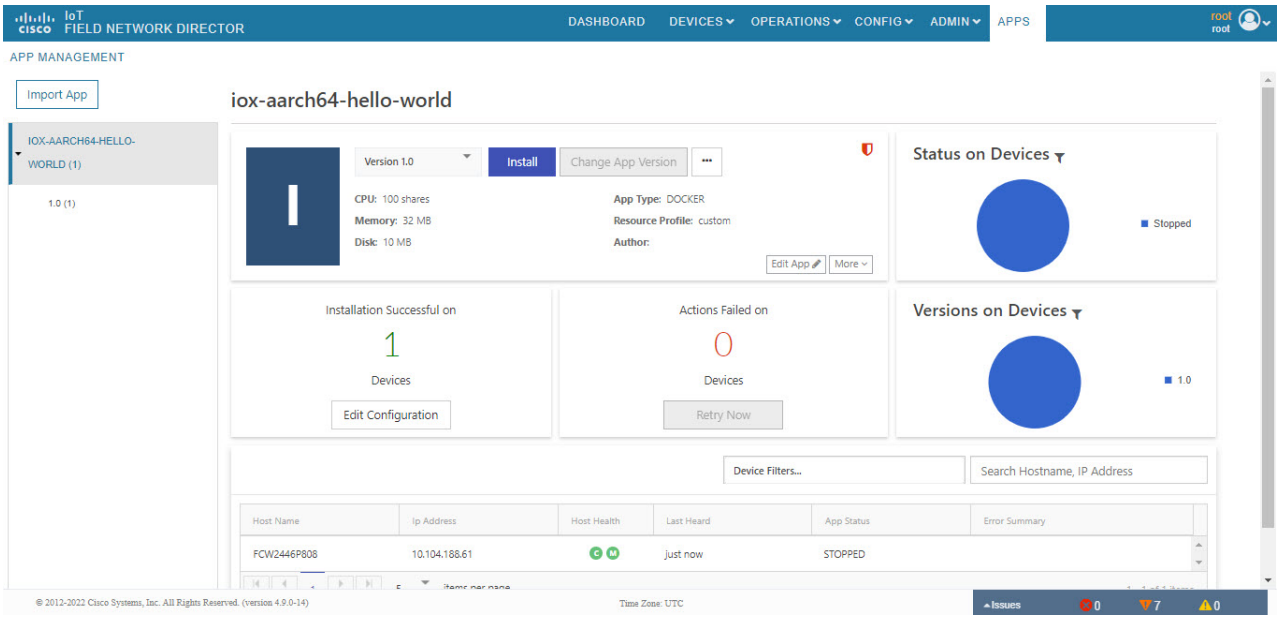


Note
If you install incompatible application, then you will get the following CPU architecture error.



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

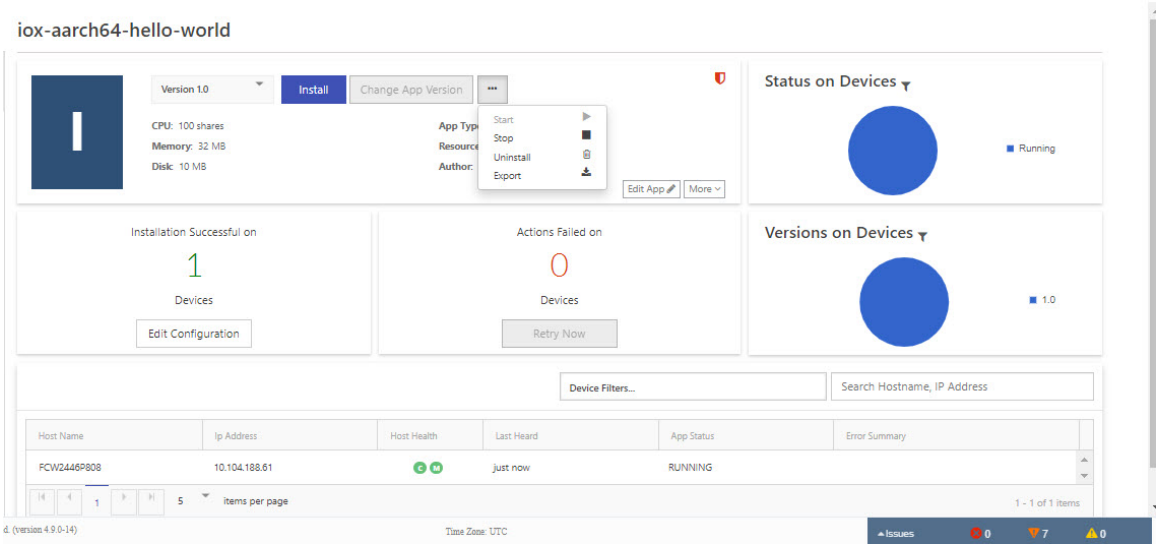
"Installation Successful on device" message appears once installation is complete. The device that is capable of IOx is discovered automatically and the Host Name, Ip Address are properly populated in IoT FND.



Managing the Application

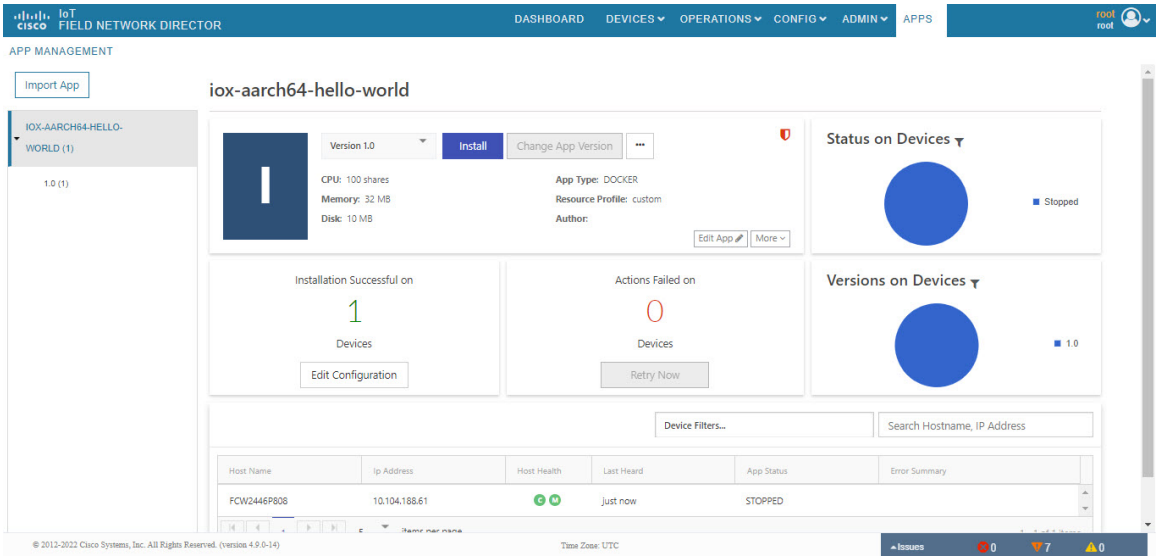
This section describes how to start, stop, and uninstall the application from the APPS menu.

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.

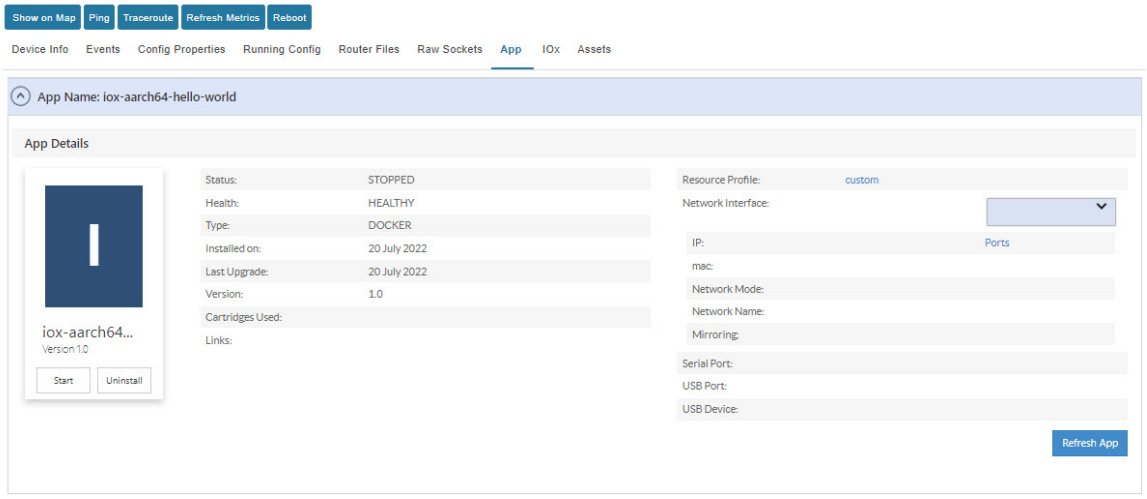


Stopping the Application

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."

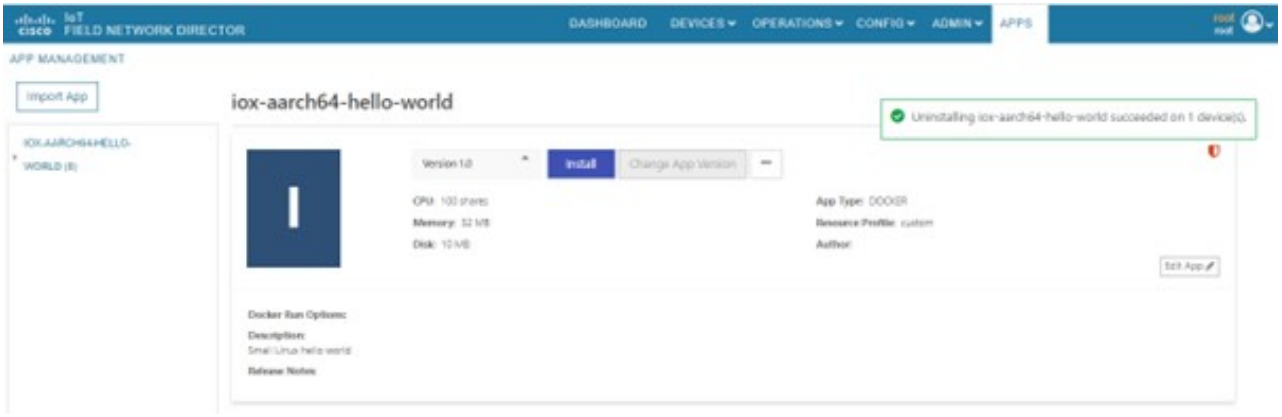
Uninstalling the Application

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 23: Feature History

Release Information	Feature Name	Description
Cisco IoT FND Release 5.1	P-5GS6-GL PIM Support for Cisco Catalyst IR1800 and Cisco Catalyst IR1100 routers	Adds support for P-5GS6-GL 5G stand alone PIM for the Cisco Catalyst IR1800 and Cisco Catalyst IR1100 routers.
Cisco IoT FND Release 5.1	IRMH-5GS6-GL and IRMH-5GR16SA PIMs Support for Cisco Catalyst IR8100 routers	Adds support for IRMH-5GS6-GL and IRMH-5GR16SA stand alone PIMs for Cisco Catalyst IR8100 routers.
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.
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
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 Name	PID	Devices Supported	Minimum Supported Cisco IoT FND Release	Cisco IoT FND Supported Device Version	Description
5G Stand Alone PIM	P-5GS6-GL	Cisco Catalyst IR1800 and Cisco Catalyst IR1100	Cisco IoT FND Release 5.1	Cisco IOS XE Release 17.7.1 and later releases	5G stand-alone pluggable module for 5G and fallback 4G cellular connectivity; supports multiple APNs and interfaces; enhances flexibility on the IR1100 and IR1800 platforms. For more details, see Cisco Catalyst IR1800 Rugged Series Router Hardware Installation Guide, Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide.
5G Stand Alone PIM	IRMH-5GS6-GL and IRMH-5GR16SA	Cisco Catalyst IR8100	Cisco IoT FND Release 5.1	Cisco IOS XE 17.17.1 and later releases	5G stand-alone pluggable module for 5G and fallback 4G cellular connectivity; robust wireless options; advanced networking for the IR8100 platform. For more details, see Cisco Catalyst IR8100 Heavy Duty Series Router

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.

Router Model	PIM Slot(s)	Supported Cellular Interfaces	Notes
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.
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 181
- Adding a Router Device File to IoT FND, on page 182
- Transferring Files, on page 183
- Viewing Files, on page 184
- Monitoring Files, on page 185
- Monitoring Actions, on page 185
- Deleting Files, on page 186



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 Edit the ROUTER configuration template, on page 122). 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 182). 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 183).

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

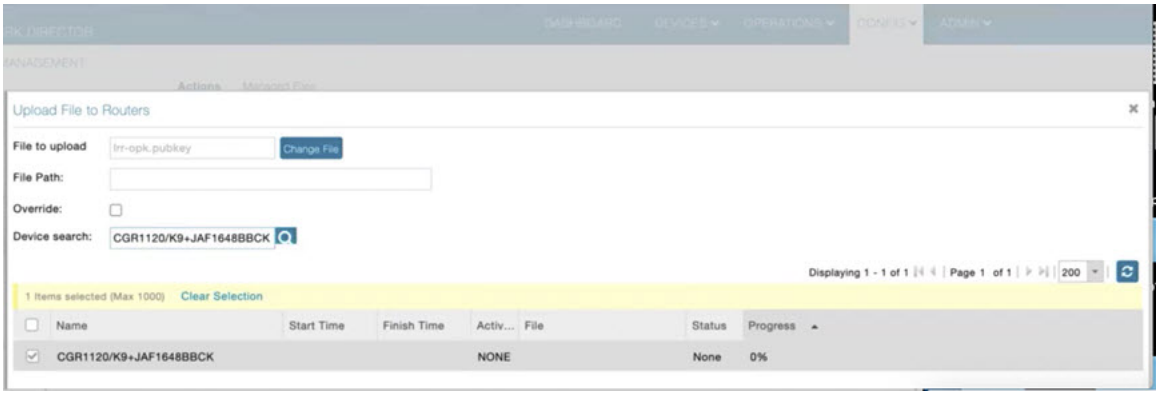
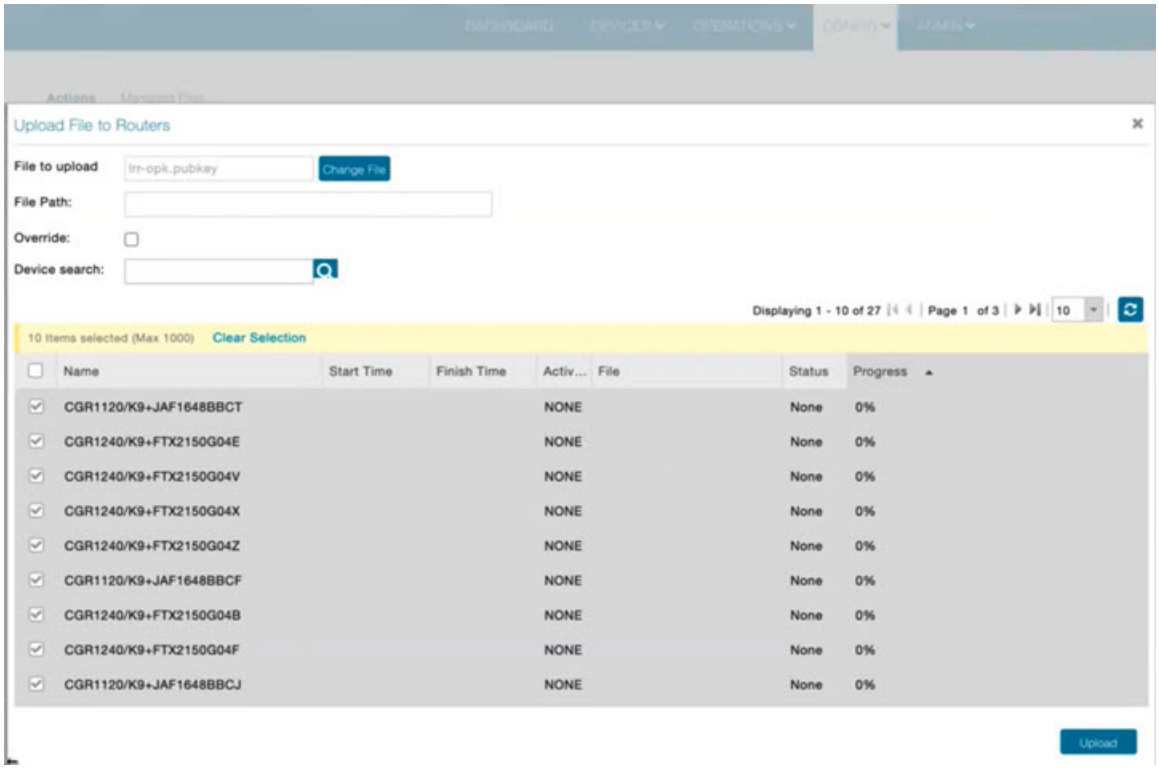


Figure 15: Upload Multiple CGR Files Within a Given String Search Range to the FND Router Page



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.

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

Improved Audit Trail

Download .CSV Files

Table 24: Feature History

Feature Name	Release	Description
Improved Audit Trail	Cisco IoT FND Release 5.0	When you add or remove or edit files using .CSV files on Cisco IoT FND, a log is generated in the **Audit Trail** page. You can download the .CSV file that you used to change the devices.

Information About Improved Audit Trail

Starting from Cisco IoT FND Release 5.0, Cisco IoT FND enhances the **Audit Trail** page and includes a direct link to download .csv files associated with device actions. Access and review changes made through .csv file uploads. This functionality improves transparency and simplifies the process of tracking device management activities. The feature ensures quick access to detailed records for auditing and compliance purposes.



Note Download the .CSV file logs even when you use NBAPIs for your device actions.

Benefits of Improved Audit Trail

- Gain immediate access to detailed records of device management actions, allowing for clear and transparent auditing of changes made via .csv files. This helps maintain accountability and ensures compliance with organizational policies.
- Downloading and storing the .csv files directly from the audit trail simplifies record-keeping practices.

Downloading .CSV Files

Here are the steps to download the .csv files:

1. From the Cisco IoT FND menubar, choose **ADMIN** > **System Management** > **Audit Trail**.
2. Find a **Devices added** or **Changed Device Properties** or **Devices removed** log from the audit trail list.
3. In the **Details** column, you'll see that the .csv is a clickable link.
4. Click the .csv file link and download.

   The .csv file contains information like timestamp, user id, device information and so on.

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 25: 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.

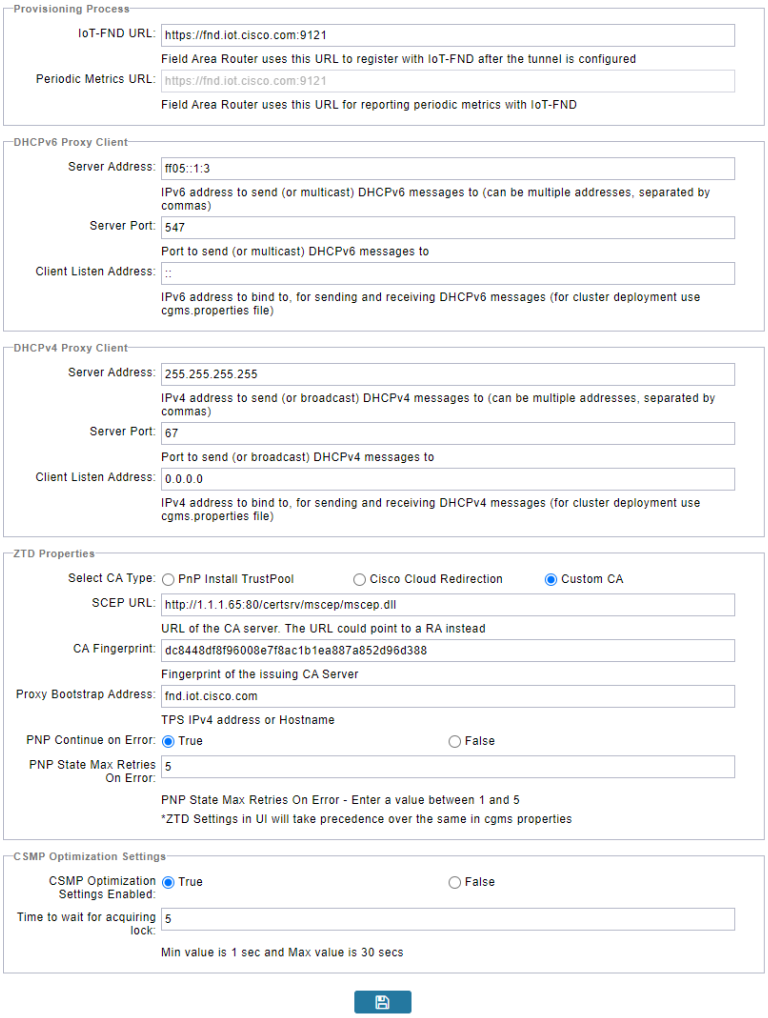
To setup Bandwidth Optimization Mode for FND and router communications:

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

Provides a comprehensive overview of device properties and their configuration status in Cisco IoT FND.

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 26: 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 SNR	CellularSnr	The Signal to Noise Ratio is the ratio of signal power to that of all other electrical signals in a location.

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
—	—	—



Note Starting with IoT FND 4.10, Cisco router IR1100 supports a new dual-active radio module that supports single modem and maximum of 3 APNs. The APNs hold interface numbers 3, 4, and 5 in IoT FND.

Additionally, the 4G LTE dual-active radio module does not support or display all fields summarized in Cellular Link Settings Fields

Table 27: 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.

Field	Key	Configurable	Description
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.
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

Field	Key	Configurable	Description
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.
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.
MSISDN	cellularMSISDN	—	The Mobile Station International Subscriber Directory Number is an unique number that identifies a mobile subscriber.

DA Gateway Properties

DA Gateway Metrics Area Fields describe the fields in the DA Gateway area of the Device Info view.

Table 28: 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.

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 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.
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 29: 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 30: 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 IR800 Device Info view.

Table 31: 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.
Wi-Fi Clients	NA	Provides client MAC address, SSID, IPv4 address, IPv6 address, device type, state, name, and parent.
Dot11Radio 0 Traffic	NA	Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps), and Rx speed (bps).
Dot11Radio 1 Traffic	NA	Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps,) and Rx speed (bps).
Tunnel3	NA	Provides admin status (up/down), operational status (up/down), Tx speed (bps), Tx drops (bps), and Rx speed (bps).
BVI1	NA	Provides admin status (up/down), operational status (up/down), IP address, physical address, Tx speed (bps), Tx drops (bps) and Rx speed (bps).
GigabitEthernet0	NA	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 32: 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.

Field	Key	Description
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 33: 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
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 34: 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 35: 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 36: Head-End Routers Tunnel 2 Config Device Fields

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

Inventory

This reference provides a comprehensive list of inventory fields, their corresponding keys, configurability status, and descriptions for CGR1000 devices.

Table 37: 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.

Field	Key	Configurable	Description
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).
Location	N/A	No	Latitude and longitude of the device.
Manufacturer	N/A	No	Manufacturer of the endpoint device.

Field	Key	Configurable	Description
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 38: 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.

Field	Key	Description
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.
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 39: 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 Metrics

You can view the mesh link metrics on both Device Info and Device Details pages.

Table 40: Mesh Link Metrics

Field	Key	Description
Receive Speed	meshRxSpeed	The rate of data received by the uplink network interface, in bits per second, averaged over a short element-specific timeframe (for example: one hour).
Transmit Speed	meshTxSpeed	The current speed of data transmission over the uplink network interface, in bits per second, averaged over a short element-specific timeframe (for example: one hour).
Mesh Endpoint Count	meshEndPointCount	Number of active connected mesh endpoints.

Mesh Link Config

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

Table 41: 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 42: 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 43: 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 44: 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 45: 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.

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 46: Raw Sockets Metrics and Sessions View

Field	Key	Description
Metrics		

Field	Key	Description
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.
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 47: 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.

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

Battery Backup Units in Cisco IoT FND

Battery Backup Units (BBUs) in Cisco IoT FND provide power to routers when the AC power supply fails or is unavailable. BBUs serve as an emergency power source whenever the AC power source is unavailable for the routers.

Each router can support up to three BBU units at a time.

Table 48: Feature History

Release Information	Feature Name	Description
Cisco IoT FND Release 5.1	Support for Enabling or Disabling Battery Backup Units (BBUs) in Cisco IoT FND with BBU Firmware Upgrade	You can use the **Enable BBU** and **Disable BBU** options in Cisco IoT FND to enable or disable Battery Backup Units (BBUs) for these routers: • Cisco CGR 1000 Series router CGR1240. • Cisco Catalyst IR8140. Additionally, you can upgrade the BBU firmware images for these routers at the router group level by uploading and installing them in Cisco IoT FND.

Considerations

Before you enable or disable BBUs, consider these points:

- If you try disabling BBU, while the AC power is turned off, then you will receive a warning message. The router shuts down if you still proceed with disbaling BBU after
- You can only enable or disable all the BBUs present in the router and not individual ones.
- In case BBUs are not present and if you try to enable or disable them, then Cisco IoT FND displays an error message letting you know that you cannot enable or disable BBUs if they are not available.
- While onboarding a new router, the BBU is disabled by default. The BBU is enabled as part of the configuration push during Zero Touch Deployment (ZTD). The default configuration template has the command which activates the battery unit automatically the first time.
- After you successfully enable or disable a BBU, you will be restricted by Cisco IoT FND from immediately enabling or disabling the BBU again. You must wait for two minutes before attempting to enable or disable the BBU again.

Supported routers

BBU enable and disable option with BBU firmware upgrade is enabled for these routers in Cisco IoT FND:

- Cisco CGR 1000 Series router CGR1240: For more information on BBUs in CGR 1000 Series router CGR1240, see BBUs in Cisco 1240 Connected Grid Router .
- Cisco Catalyst IR8140: For more information on BBUs in Cisco Catalyst IR8140 router, see BBUs in Cisco Catalyst IR8140.
- For more information on router battery session, see Router Battery.

Enable BBUs

Use this task to enable BBUs on a router in Cisco IoT FND.

Before you begin



Note

- You can use the **Enable BBU** option only if a BBU is present on the router and if it is already in the disabled state. Otherwise, this option appears disabled in the **Device info** > **Battery Backup Unit** drop-down list.
- If you attempt to enable a Battery Backup Unit (BBU) that is already enabled on a router, you will receive a message with this notification: `BBU is already Enabled. Do you forcefully want to enable BBU?`

Procedure

Step 1 From Cisco IoT FND menubar, choose **DEVICES** > **FIELD DEVICES** > **Groups**.

Step 2 Select **ROUTER**.

Step 3 Click router in the list of routers.

Step 4 Click **Battery Backup Unit** from the menu options which appear over **Device Info** page.

Step 5 Click **Enable BBU**.

Step 6 Click **Yes**.

The battery is enabled, and the status is displayed on the command status pop-up screen as completed.

Disable BBUs

Use this task to disable BBUs on a router in Cisco IoT FND.

Before you begin



Note

- You can use the **Disable BBU** option only if a BBU is present on the router and if it is already in the enabled state.
- If you attempt to disable a Battery Backup Unit (BBU) that is already disabled on a router, you will receive a message with this notification: `BBU is already Disabled. Do you forcefully want to disable BBU?`

Procedure

Step 1 From Cisco IoT FND menubar, choose **DEVICES** > **FIELD DEVICES** > **Groups**.
Step 2 Select **ROUTER**.
Step 3 Click router in the list of routers.
Step 4 Click **Battery Backup Unit** from the menu options which appear over **Device Info** page.
Step 5 Click **Disable BBU**.
Step 6 Click **Yes**.

The battery is disabled, and the status is displayed on the command status pop-up screen as completed. Otherwise, the status appears as failed and the battery is not disabled.

What to do next

Once you enable or disable BBU on the router, you can proceed with checking the BBU status in the **Router Battery** section of the **Device info** page or you can check the status in **ADMIN** > **SYSTEM MANAGEMENT** > **AUDIT TRAIL** page.

BBU firmware images

BBU firmware images in Cisco IoT FND are software files that you use to update and enhance the BBU firmware of routers in Cisco IoT FND. The BBU firmware upgrade is carried out at the router group level similar to router firmware image installations in Cisco IoT FND.

Add BBU firmware image

Use this task to add BBU firmware image.

Before you begin

Before proceeding with BBU firmware upgrade, you need to consider these points:

- Ensure that the AC power supply is ON before you begin the BBU firmware upgrade process. If the AC power is OFF, then the firmware upgrade is skipped for the supported routers during firmware installation.
- Before you start BBU firmware upgrade process, you must ensure the BBU is in the enabled state.
- Cisco Catalyst IR8140 routers with firmware version below 17.09.01 and CGR 1000 Series CGR1240 routers with firmware version below 15.9.3.M7a are not supported for BBU upgrades and they are skipped during installation.

Procedure

Follow the steps given in: Add firmware images

Note

Select **IOS-BBU** as the firmware image.

The BBU image appears in the **Firmware Images** list.

What to do next

See, Upload BBU firmware image.

Upload BBU firmware image

Use this task to upload BBU firmware image.

Before you begin

Note

- The BBU firmware image used for upload is present in the `bootflash:/bbu_fw` directory.
- You must select **IOS-BBU** in the **Select Type** drop-down list for uploading BBU firmware image.
- For BBU firmware upgrades the **Mode of installation** option is disabled during upload.

Procedure

Follow the steps given in: Upload firmware images.

BBU firmware image is uploaded.

Note In case the upload fails for any reason, you will receive a corresponding error message, after which you can retry uploading the BBU firmware image.

What to do next

See, Install BBU firmware image.

Install BBU firmware image

Use this task to install BBU firmware image.

Before you begin

Ensure BBU firmware image upload has completed successfully and without errors, before you can proceed with installing BBU firmware image.

Procedure

Follow the steps given in: Install firmware images.

The BBU firmware image is installed.

Note In case the BBU firmware image installation fails for any reason, you will receive a corresponding error message, after which you can retry the BBU firmware installation again.

What to do next

See View BBU firmware images.

View BBU firmware images

Use this task to view BBU firmware image.

Procedure

Follow the steps given in: View firmware images.

You can view the list of firware images associated with the router including the BBU firmware image you installed.

Router Config

Router Config Device View describes the fields in the Router Config area of the **Field Devices** > **Config Properties** page.

Table 49: 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 50: 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 51: 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 52: 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.

Field	Key	Configurable	Description
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 53: Router Tunnel 1 Config Device View

Field	Key	Configurable	Description
Tunnel Source Interface 1	tunnelSrcInterface1	Yes	Defines the interface over which the first tunnel is built to provide WAN redundancy.
OSPF Area 1	ospfArea1	Yes	Defines the OSPFv2 Area 1 in which the router (running IPv4) is a member.
OSPFv3 Area 1	ospfV3Area1	Yes	Defines OSPFv3 Area 1 in which the router (running IPv6) is a member.
OSPF Area 2	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 54: 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.

Field	Key	Configurable	Description
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 55: 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.
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 56: 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.

Field	Key	Configurable	Description
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 57: WiFi Interface Config Fields

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

WiMAX Config

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 58: 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 59: 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 60: WiMAX Link Settings Fields

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