# Cisco IoT Field Network Director User Guide, Release 4.8.x

**First Published:** 2021-12-10

**Last Modified:** 2024-05-15

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# CONTENTS

CHAPTER 1

# Feature History

This chapter summarizes the new and modified features that are supported in Cisco IoT FND 4.8.1 and 4.8.0 releases.

**Note** The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.



# What's New in 4.8.1

| Features | Description |
|---|---|
| **Cisco IoT Field Network Director 4.8.1** | |
| Integrating Third-Party Endpoints in IoT FND through CSMP | The CSMP code is shared with the Cisco partners which helps the partners to register their endpoint devices in FND. When registering their devices, they can define their own set of metadata files for capturing metric, property, event, or issue types for the new device type. |
| Saving Configuration After LDevID Renewal | Auto-renew LDevID certificates and save configuration after LDevID renewal. |
| Mesh Link Metrics for N2450 Router | This feature allows you to view the Tx speed, Rx speed, and endpoint count for N2450 router. |
| Support For Wi-SUN Stack Switch | This feature supports switching devices from CG-Mesh to Wi-SUN stack. |

| Features | Description |
|---|---|
| Support for RHEL OS | Cisco IoT FND 4.8.1 supports RHEL 8.5. |
| Support of Dual WPAN for IR8100 | Cisco IoT FND 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 the IR8100 router. |

# What's New in 4.8.0

| Features | Description |
|---|---|
| **Cisco IoT Field Network Director 4.8.0** | |
| Enable 8140 Licensing | The licensing for device type IR8100 is now supported in FND. The license PID for IR8100 devices is IOTFND-IR8140. After adding the license, go to **ADMIN** > **System Management** > **License Center** > **License Summary** page to view the licenses consumed and total license count for IR8100 devices.<br><br>It is also possible to allocate licenses for each domain. Go to **ADMIN** > **Access Management** > **Domains**. In the Edit Domain page, you can allocate licenses for the IR8100 devices. |
| Enhance DB queries to support scaled mesh deployment | The Oracle DB is scaled up to 8,000/ 8,000,000 routers/ endpoints. Under **ADMIN** > **System Management** > **Provisioning Settings** page, the CSMP optimization settings are introduced to configure the timeout in order to acquire lock when processing CSMP messages.<br><br>The CSMP optimization setting is available only for Oracle DB set up and not for PostgreSQL DB setup. |
| Out-of-Service (OOS) Device State | 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. |
| Single Sign-On (SSO) Authentication | SSO authentication allows you to access multiple web applications using a single login credential. |
| Troubleshooting On-Demand Statistics for Endpoints | 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. |

CHAPTER 2

# Overview of Cisco IoT Field Network Director

This section provides an overview of the Cisco IoT Field Network Director (Cisco IoT FND) and describes its role within the Cisco Internet of Things (IoT) Network solution. Topics include:



# Cisco IoT Connected Grid Network

This section provides an overview of:



The Cisco IoT Field Network Director (IoT FND) is a network management system that manages multi-service network and security infrastructure for IoT applications, such as smart grid applications, including Advanced Metering Infrastructure (AMI), Distribution Automation (DA), distributed intelligence, and substation automation. IoT FND is a scalable, highly-secure, modular, and open platform with an extensible architecture. IoT FND is a multi-vendor, multi-service, communications network management platform that enables network connectivity to an open ecosystem of power grid devices.

IoT FND is built on a layered system architecture to enable clear separation between network management functionality and applications, such as a distribution management system (DMS), outage management system (OMS), and meter data management (MDM). This clear separation between network management and applications helps utilities roll out Smart Grid projects incrementally, for example with AMI, and extend into distribution automation using a shared, multi-service network infrastructure and a common, network management system across various utility operations.

### Features

- Geographic Information System (GIS) map-based, visualization, monitoring, troubleshooting, and alarm notifications
- Group-based configuration management for routers and smart meter endpoints

- OS compatible (Cisco IOS, Guest OS, IOx) and provides application management
- Rule-engine infrastructure for customizable threshold-based alarm processing and event generation
- North Bound API for transparent integration with utility head-end and operational systems
- High availability and disaster recovery

Cisco IoT FND provides powerful Geographic Information System (GIS) visualization and monitoring capability. Through the browser-based interface, utility operators manage and monitor devices in a Cisco IoT Connected Grid Field Area Network (FAN) solution, using IPv6 over Low-power Wireless Personal Area Networks (6LoWPANs). The FAN includes the following devices:

- Cisco 1000 Series Connected Grid Routers (CGRs), also called pole-top or DIN-rail-mount routers. These devices are referred to as routers in this document and identified by model (for example, CGR1000, CGR1120, or CGR1240) on the Field Devices page. Available CGR modules provide 3G, 4G LTE, and Cisco Resilient Mesh connectivity (WPAN). CGR1000s also support the Itron OpenWay RIVA CAM module, which provides connectivity to the Itron OpenWay RIVA electric and gas-water devices.
- Cisco 800 Series Integrated Services Routers (ISR 800s) are used in most networks as edge routers or gateways to provide WAN connectivity (cellular, satellite over Ethernet, and WiFi) to an end device (energy-distribution automation devices, other verticals such as ATMs, and mobile deployments such as taxis or trucks). These devices are referred to as routers in this document; and identified by product ID on the Field Devices page. You can use IoT FND to manage the following hardened Cisco 819H ISRs:
    - C819HG-4G-V-K9
    - C819HG-4G-A-K9
    - C819HG-U-K9
    - C819HGW-S-A-K9
    - C819H-K9

  IoT FND also manages the following non-hardened Cisco 819 ISRs:
    - C819G-B-K9
    - C819G-U-K9
    - C819G-4G-V-K9
    - C819G-7-K9
- Cisco 4000 Series Integrated Services Routers (ISR 4300 and ISR4400) consolidate many must-have IT functions in a single platform, such as network, security, compute, storage, and unified communications to help you build out the digital capabilities in your enterprise branch offices. The platform is modular and upgradable, so you can add new services without changing equipment.
- Cisco 800 Series Industrial Integrated Services Routers (IR800s) are compact, ruggedized, Cisco IOS Software routers. They offer support for integrated 4G LTE wireless WAN (IR807, IR809 and IR829 models) and wireless LAN capabilities (IR829 only). These devices are referred to as routers in this document; and identified by product ID (for example, IR800) on the Field Devices page. You can use IoT FND to manage the following IR800 models:

  - IR807: Highly compact, low-power industrial router. Well-suited for industrial applications (distribution automation for utilities, transportation, manufacturing) and remote asset management across the extended enterprise.
  - IR809: Very compact, cellular (3G,4G/LTE) industrial routers that enable reliable and secure cellular connectivity for remote asset monitoring and machine-to-machine (M2M) applications such as distribution automation, pipeline monitoring and roadside infrastructure monitoring.
  - IR829: Highly ruggedized compact cellular (3G and 4G LTE with GPS and dual SIM) and WLAN (2.4/5GHz) industrial routers supporting scalable, reliable, and secure management of those IoT applications requiring mobile connectivity such as fleet vehicles and mass transit.

- Cisco 5921 Embedded Services Router (ESR) is designed to operate on small, low-power, Linux-based platforms. It helps integration partners extend the use of Cisco IOS into extremely mobile and portable communications systems. It also provides highly secure data, voice, and video communications to stationary and mobile network nodes across wired and wireless links.
- The Cisco Wireless Gateway for LoRaWAN (IXM-LPWA-800, IXM-LPWA-900) can be a standalone product that connects to Ethernet switches or routers or connects to LAN ports of the Cisco 800 Series Industrial Integrated Services Routers. This product can be configured as a radio interface of the Cisco Industrial Routers 809 and 829. One or multiple gateways are connected to the LAN port(s) of the IR809 or IR829 via Ethernet or VLANs with encrypted links. Through this configuration, it provides LoRaWAN radio access while the IR809 or IR829 offer backhaul support for Gigabit Ethernet (electrical or fiber), 4G/LTE, or Wi-Fi. You can employ either a default-group tunnel group or a user-defined tunnel group.
- Cisco Interface Module for Long Range Wide Area Network (LoRAWAN) is an extension module for the industrial routers, Cisco IR809 and IR829, and serves as a carrier-grade gateway for outdoor deployments. The module provides unlicensed low-power wide area (LPWA) wireless connectivity for a range of Internet of Things (IoT) use cases such as asset tracking, water and gas metering, street lighting, smart parking/building/agriculture, and environment monitoring. There are two models that are supported, which are differentiated by their band support (863-870 MHz ISM or 902-928 MHz ISM). The module is identified by product ID (for example, IXM-LORA-800-H-V2).
- Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR500) supply RF mesh connectivity to IPv4 and serial IoT devices (for example, recloser control, cap bank control, voltage regulator controls, and other remote terminal units).

> **Note** CGRs, C800s, IR800s, IR500s, and other types of Cisco Resilient Mesh endpoints (RMEs) can coexist on a network, but cannot be in the same device group. See Configuring Devices in the Managing Devices chapter.

- Cisco 800 Series Access Points are integrated with IR800s and C800s. These devices are referred to as routers in this document; and identified by product ID (for example, AP800). You can use IoT FND to manage the following AP800 models:
  - AP802 embedded in C800
  - AP803 embedded in IR829
- Cisco Aggregation Services Routers (ASR) 1000 series , Cisco Integrated Services Routers (ISR) 3900 series, ISR 4300, and ISR 4400 routers are referred to as *head-end routers* or HERs in this document.

- Cisco IPv6 RF (radio frequency) and PLC (power line communications).
- The IP 67-rated Cisco Catalyst IR8100 Heavy-Duty Series routers is a modular, secure, rugged and outdoor router that is suitable for harsh physical environments. It has multiple WAN (LTE, LTE-Advanced, LTE Advanced Pro, 5G Sub-6GHz1, RJ45/SFP Ethernet) and storage options. The router supports wireless and wired connectivity such as 5G, public, or private LTE, Wi-SUN, LoRaWAN, and has more connectivity options making it more adaptable. It runs on Cisco IOS XE and Cisco IOS XE provides both autonomous and controller (SD-WAN) mode support. In IoT FND, you can find the following IR8100 models:
  - IR8140H-K9
  - IR8140H-P-K9

IoT FND typically resides in the utility control center with other utility head-end operational systems, such as an AMI head end, distribution management system, or outage management system. IoT FND features enterprise-class fault, configuration, accounting, performance, and security (FCAPS) functionality, as defined in the Open Systems Interconnection (OSI) model.

The Cisco IoT FND North Bound Application Programmable Interface (NB API) allows various utility applications like DMS, OMS, or MDM to pull appropriate, service-specific data for distribution grid information, outage information, and metering data from a shared, multi-server communication network infrastructure. For more information about the Cisco IoT FND North Bound API, see the North Bound API User Guide for Cisco IoT Field Network Director, Release 4.x for your IoT FND installation.

The NB API can send events using HTTPS. NB API clients must subscribe to IoT FND by providing a valid HTTPS URL to send events. IoT FND accepts all SSL and handshake certificates that are published by the NB API client (the event consumer) while making the secure connection.

# Cisco IoT FND Features and Capabilities

- **Configuration Management** — Cisco IoT FND facilitates configuration of a large number of Cisco CGRs, Cisco C800s, Cisco ISRs, Cisco IRs, Cisco ASRs, and mesh endpoints. Use Cisco IoT FND to bulk-configure devices by placing them into configuration groups, editing settings in a configuration template, and then pushing the configuration to all devices in the group.
- **Device and Event Monitoring** — Cisco IoT FND displays easy-to-read tabular views of extensive information that is generated by devices, allowing you to monitor your network for errors. Cisco IoT FND provides an integrated Geographic Information System (GIS) map-based visualization of FAN devices such as routers and smart meters.
- **Firmware Management** — Cisco IoT FND serves as Firmware Management a repository for Cisco CGR, Cisco C800,Cisco ISR, Cisco IR, and mesh endpoint firmware images. Use Cisco IoT FND to upgrade the firmware running on groups of devices by loading the firmware image file onto the Cisco IoT FND server, and then uploading the image to the devices in the group. Once uploaded, use IoT FND to install the firmware image directly on the devices. In release 3.0.1-36 and later, a Subnet List view on the Firmware Upgrade page for Mesh Endpoints lets you filter and view subnets by PAN identifier (PAN ID) and Group (details include number of nodes within a group, hops away from the router and operational status). A subnet progress histogram has also been added.
- **OS Migration** — The CG-OS to IOS migration is supported until release 4.7.x.
- **Zero Touch Deployment** — This ease-of-use feature automatically registers (enrolls) and distributes X.509 certificates and provisioning information over secure connections within a connected grid network.

- **Tunnel Provisioning** — Protects data exchanged between Cisco ASRs and Cisco CGRs, C800s,Cisco ISRs and Cisco IRs, and prevents unauthorized access to Cisco CGRs, to provide secure communication between devices. Cisco IoT FND can execute CLI commands to provision secure tunnels between Cisco CGRs, C800s, Cisco ISRs and Cisco IRs and Cisco ASRs/Cisco 8000. Use IoT FND to bulk-configure tunnel provisioning using groups.
- **IPv6 RPL Tree Polling** — The IPv6 Routing Protocol for Low-power and Lossy Networks (RPL) finds its neighbors and establishes routes using ICMPv6 message exchanges. RPL manages routes based on the relative position of the mesh endpoints to the CGR that is the root of the routing tree. RPL tree polling is available through the mesh nodes and CGR periodic updates. The RPL tree represents the mesh topology, which is useful for troubleshooting. For example, the hop count information received from the RPL tree can determine the use of unicast or multicast for the firmware download process. IoT FND maintains a periodically updated snapshot of the RPL tree.
- **Dynamic Multipoint VPN and FlexVPN** — For Cisco C800 devices and Cisco IR800 devices, DMVPN and FlexVPN do not require IoT FND to apply device-specific tunnel configuration to the HER during tunnel provisioning. HER tunnel provisioning is only required for site-to-site VPN tunnels.
- **Embedded Access Point (AP) Management** — IoT FND provides management of embedded APs on C819 and IR829 routers.
- **Guest OS (GOS) Support** — For Cisco IOS CGR 1000 and IR800 devices that support Guest OS, IoT FND allows approved users to manage applications running on the supported operating systems. IoT FND supports all phases of application deployment, and displays application status and the Hypervisor version running on the device.
- **Device Location Tracking** — For CGR 1000, C800, IR1101, IR800, and IR8100 devices, IoT FND displays real-time location and device location history. Ensure that you enable the router GPS tracking option for this feature.
- **Software Security Module (SSM)** — This is a low-cost alternative to the Hardware Security Module (HSM), and is used for signing CSMP messages sent to meters and IR500 devices.
- **Customer Certificates** — Cisco IoT FND allows you to use your own CA and ECC-based certificates to sign smart meter messages.
- **Diagnostics and Troubleshooting** — The IoT FND rule engine infrastructure provides effective monitoring of triage-based troubleshooting. Device troubleshooting runs on-demand device path trace and ping on any CGR 1000, IR800, Cisco Series Integrated Services Routers (C800), Cisco 5921 Embedded Services Router (C5921), range extender, gateway, or meter (mesh endpoints).
- **High Availability** — To ensure uninterrupted network management and monitoring, you can deploy the Cisco IoT FND solution in a High Availability (HA) configuration. By using clusters of load-balanced IoT FND servers and primary and standby IoT FND databases, Cisco IoT FND constantly monitors the health of the system, including connectivity within clusters and server resource usage. If a server cluster member or database becomes unavailable or a tunnel fails, another takes its place seamlessly. Additionally, you can add reliability to your IoT FND solution by configuring redundant tunnels between a Cisco CGR and multiple Cisco ASRs.
- **Power Outage Notifications** — Mesh Endpoints (MEs) implement a power outage notification service to support timely and efficient reporting of power outages. In the event of a power outage, MEs perform the necessary functions to conserve energy and notify neighboring nodes of the outage. Routers relay the power outage notification to IoT FND, which then issues push notifications to customers to relate information on the outage.

- **Resilient Mesh Upgrade Support** — Over-the-air software and firmware upgrades to field devices such as Cisco CGRs and Resilient Mesh Endpoints (RMEs) (for example, AMI meter endpoints).
- **Audit Logging** — Logs access information for user activity for audit, regulatory compliance, and Security Event and Incident Management (SEIM) integration. This simplifies management and enhances compliance by integrated monitoring, reporting, and troubleshooting capabilities.
- **North Bound APIs** — Eases integration of existing utility applications such as outage management system (OMS), meter data management (MDM), trouble-ticketing systems, and manager-of-managers.
- **Role-Based Access Controls** — Integrates with enterprise security policies and role-based access control for AMI network devices.
- **Event and Issue Management** — Fault event collection, filtering, and correlation for communication network monitoring. IoT FND supports a variety of fault-event mechanisms for threshold-based rule processing, custom alarm generation, and alarm event processing. Faults display on a color-coded GIS-map view for various endpoints in the utility network. This allows operator-level custom fault-event generation, processing, and forwarding to various utility applications such as an outage management system. Automatic issue tracking is based on the events collected.

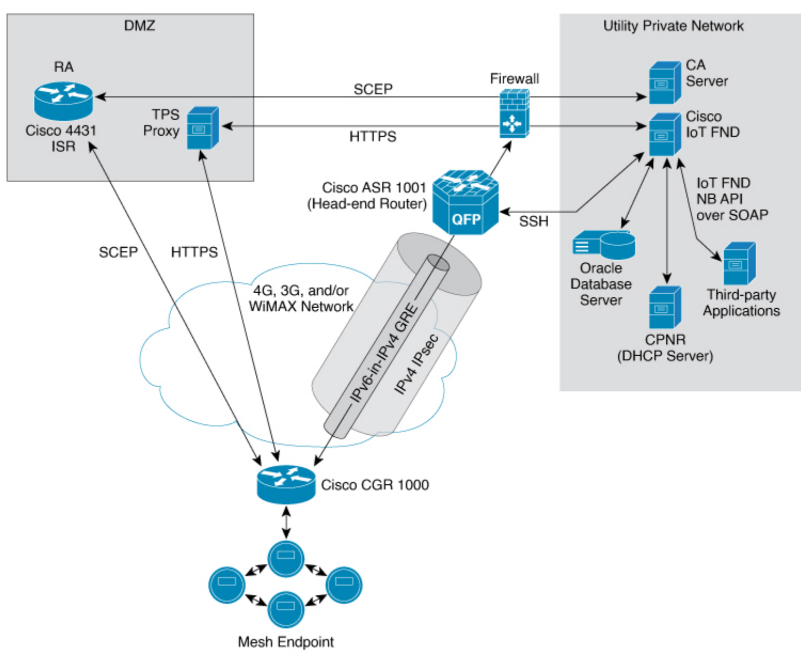
# IoT FND Architecture

Figure 1: Zero Touch Deployment Architecture, on page 8 provides a high-level view of the systems and communication paths that exist in a typical utility company operating on a Cisco CGR connected grid network in which Zero Touch Deployment is in use.

For Cisco IOS CGRs, we recommend a tunnel configuration using FlexVPN.

For Cisco C800s and IR800s, we recommend using Dynamic Multipoint VPN (DMVPN) or FlexVPN.

***Figure 1: Zero Touch Deployment Architecture***



In this example, the firewall provides separation between those items in the utility company public network (DMZ) and its private network.

The utility company private network shows systems that might reside behind the firewall such as the Cisco IoT FND, the Oracle database server, the Cisco IoT FND North Bound API, the DHCP server, and the Certificate Authority (CA). The Cisco IoT FND Tunnel Provisioning Server proxy (TPS proxy) and Registration Authority (RA) might be located in the DMZ.

After installing and powering on the Cisco CGR, it becomes active in the network and registers its certificate with the RA by employing the Simple Certificate Enrollment Protocol (SCEP).

The Registration Authority (Integrated Service Router (ISR) in Figure 1: Zero Touch Deployment Architecture, on page 8), functioning as a Certificate Authority (CA) proxy, obtains certificates for the Cisco 1000 Series Connected Grid Router (CGR1240 and CGR1120). The Cisco CGR then sends a tunnel provisioning request over HTTPS to the TPS proxy that forwards it to IoT FND.

Cisco IoT FND manages collection of all information necessary to configure a tunnel between Cisco CGRs and the head-end router ( Cisco 1000 Series Aggregation Services Routers).

## Main Components of IoT FND Solution

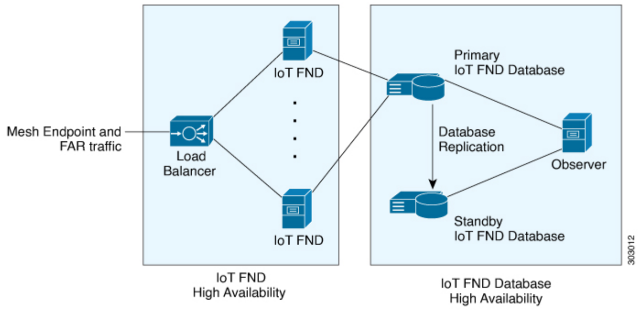
| Component | Description |
|---|---|
| IoT FND Application Server | This is the heart of IoT FND deployments. It runs on an RHEL server and allows administrators to control different aspects of the IoT FND deployment using its browser-based graphical user interface.<br><br>IoT FND HA deployments include two or more IoT FND servers that are connected to a load balancer. |
| NMS Database | This Oracle database stores all information that is managed by your IoT FND solution, including all metrics received from the MEs and all device properties such as firmware images, configuration templates, logs, event information, and so on. |
| Software Security Module (SSM) | This is a low-cost alternative to the Hardware Security Module (HSM), and is used for signing CSMP messages sent to meters and IR500 devices. |
| TPS Proxy | Allows routers to communicate with IoT FND when they first start up in the field. After IoT FND provisions tunnels between the routers and HER (ASRs), the routers communicate with IoT FND directly. |
| Load Balancer | The load balancer distributes traffic among the IoT FND servers in your network. You can employ a load balancer in your network within a Zero Touch Deployment (ZTD) architecture to provide High Availability (HA). IoT FND uses the BIG-IP load balancer from F5. |

## High Availability and Tunnel Redundancy

The example in Figure 1: Zero Touch Deployment Architecture, on page 8 is of a single-server deployment with one database and no tunnel redundancy. However, you could take advantage of Cisco IoT FND HA support to deploy a cluster of Cisco IoT FND servers connected to a load balancer, as shown in Figure 2: IoT FND Server and Database HA, on page 10. The load balancer sends requests to the servers in a round-robin fashion. If a server fails, the load balancer keeps servicing requests by sending them to the other servers in the cluster.

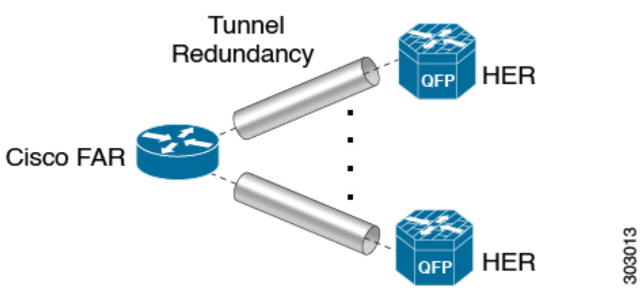
You could also deploy a standby Cisco IoT FND database to provide another layer of high availability in the system with minimal data loss.

*Figure 2: IoT FND Server and Database HA*




To provide tunnel redundancy, IoT FND allows you to create multiple tunnels to connect a CGR to multiple ASRs, as shown in Figure 3: IoT FND Tunnel Redundancy, on page 10.

*Figure 3: IoT FND Tunnel Redundancy*




For more information about HA, see Database High Availability.

# List of Standard Ports Used in IoT FND

The table provides the list of standard ports used in IoT FND solution.

| Service | Port |
|---|---|
| GUI | 443 |
| FND Demo mode | 80 |
| Tunnel Provisioning | 9120 |
| TPS | 9122 |
| FAR | 9125 |
| CG-MESH (CSMP) | 61624 |
| CG-MESH (CSMP CoAP version 18) | 61628 |
| CG-MESH (Outage) | 61625 |
| CG-MESH (Restoration) | 61626 |

| Service | Port |
|---|---|
| Oracle DB Server | 1522 |
| PostGreSql DB Server | 5432 |
| Influx | 8086 |
| Kapacitor | 9092 |
| WSMA (for IOS-XE) | 443 |
| WSMA (for Classic IOS) | 8443 |
| RADIUS (for authentication) | 1812 |
| RADIUS (for accounting) | 1813 |
| FND-RA | 61629 |
| EST Proxy | 6789 |
| Registration + Periodic | 9121 |
| Bandwidth Op Mode | 9124 |
| PnP — HTTP | 9125 |
| Web Sockets — Device Communication | 9121 |
| LwM2M | 5683 |
| DB Replication for HA | 1622 |
| DHCP IPv4 | 67 |
| DHCP IPv6 | 547 |
| SSH | 22 |
| NTP Server | 123 |
| SNMP (for polling) | 161 |
| SNMP (for notifications) | 162 |
| Syslog service | 514 |
| SSM Server | 8445 |

# Resilient Mesh Endpoints

The Cisco Field Area Network (FAN) solution brings the first multi-service communications infrastructure to the utility field area network. It delivers applications such as AMI, DA, and Protection and Control over a common network platform.

Advanced meter deployments follow a structured process designed to match the right solution to the needs of the utility company. This process moves in phases that require coordination between metering, IT, operations, and engineering. The first phase for most utilities is identification of goals, followed by analysis of data needs, and business processes. After an evaluation of the business case is complete and a technology chosen, system implementation and validation complete the process.

Once the utility company moves past the business case into system implementation, unforeseen complications can sometimes slow or delay a deployment. The true value of a plug-and-play system is that it saves cost and improves the return on investment by allowing the benefits of advanced metering to be realized sooner.

The features that enable a true plug-and-play RF or PLC mesh network system include:

- **Self-initializing endpoints**: CGRs automatically establish the best path for communication through advanced self-discovery – meters and infrastructure deploy without programming.
- **Scalability**: This type of network enables pocketed deployments where each Cisco IoT FND installation can accept up to 10 million meters/endpoints. Large capacity enables rapid, multi-team deployments to occur in various parts of the targeted AMI coverage area, while saving infrastructure and communication costs.

In a true mesh network, metering and range extender devices communicate to and through one another and decide their own best links, forming the RF Mesh Local Area Network (RFLAN) or PLC LAN. These ME devices become the network and possess dynamic auto-routing functions that eliminate the need for dedicated repeater infrastructure or intermediate (between endpoint and collector) tiered radio relay networks. The result is a substantial reduction in dedicated network infrastructure as well as powerful and more flexible fixed-network communication capability.

Range extenders are installed by the utility company to strengthen mesh coverage and provide redundancy, supplementing network reliability in difficult environmental settings such as dense urban areas where buildings obstruct the normal mesh signal propagation, or in low-meter-density geographically sparse regions and RF-challenged areas. A range extender automatically detects and connects to the mesh after installation or outage recovery, and then provides an alternate mesh path.

In a normal deployment scenario, these MEs form a stable RFLAN or PLC LAN network the same day they are deployed. Once the collector is installed, placing MEs throughout the deployment area is as simple as changing out a meter. MEs form a network and begin reporting automatically.

Mesh endpoints send and receive information. A two-way mesh system allows remote firmware upgrades, as well as system settings changes and commands for time-of-use periods, demand resets, and outage restoration notifications. Not having to physically “touch the meter” is a major value, especially when entering the advanced demand response metering domain that requires time-of-use (TOU) schedule changes and interval data acquisition changes to meet specific client needs. These commands can be sent to groups or to a specific ME. Meter commands can be scheduled, proactive, on-demand, or broadcast to the entire network.

Communication between the data center/network operations center (NOC) and the collector is accomplished by widely available and cost-efficient mass marketed TCP/IP-based public wide area network (WAN) or with the utility company-owned WAN. The flexibility and open standard public WAN architectures currently available and in the future create an environment that allows continued ongoing cost reduction and future options, without being tied into one type of connectivity over the life of the asset. It is best if the AMI system avoids using highly specialized WAN systems.

After deployment is complete, the system can transmit scheduled hourly (and sub hourly) data to support utility applications such as billing reads, advanced demand response initiatives, load research, power quality, and transformer asset monitoring.

Easy access and reliable on-demand capability allow the utility to perform grid diagnostics and load research system-wide or for selected groups of meters. Other standard features support outage management, tamper detection, and system performance monitoring.

***Table 1: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Enhance DB queries to support scaled mesh deployment | IoT FND 4.8 | The Oracle DB is scaled up to 8,000/ 8,000,000 routers/ endpoints. Under **ADMIN** > **System Management** > **Provisioning Settings** page, the CSMP optimization settings are introduced to configure the timeout in order to acquire lock when processing CSMP messages.<br><br>The CSMP optimization setting is available only for Oracle DB set up and not for PostgreSQL DB setup. |

## Grid Security

Designed to meet the requirements of next-generation energy networks, Cisco Grid Security solutions take advantage of our extensive portfolio of cybersecurity and physical security products, technologies, services, and partners to help utility companies reduce operating costs while delivering improved cybersecurity and physical security for critical energy infrastructures.

Cisco Grid Security solutions provide:

- **Identity management and access control**: Secure utility facilities, assets, and data with user authentication and access control are custom-built for grid operations.
- **Threat defense**: Build a layered defense that integrates with firewall, VPN, intrusion prevention, and content security services to detect, prevent, and mitigate threats.
- **Data center security**: Turn network, computing, and storage solutions into a secure, shared pool of resources that protects application and data integrity, secures communications between business processes and applications within the utility, and secures connectivity to external resources such as providers of renewable energy.
- **Utility compliance**: Improve risk management and satisfy compliance and regulatory requirements such as NERC-CIP with assessment, design, and deployment services.
- **Security monitoring and management**: Identify, manage, and counter information security threats and maintain compliance through ongoing monitoring of cyber events.

# How to Use This Guide

This section has the following topics to help you quickly find information on common, CGR, mesh endpoint, or administration tasks, and document conventions.

# Common Tasks

The table lists tasks that users can perform on both routers and mesh endpoints. The ability to perform tasks is role-based. For information on user roles, see System-Defined User Roles in the Managing User Access chapter.

*Table 2: Common Tasks*

| Task | Use |
|---|---|
| **Device Viewing Tasks** | |
| View Devices | Working with Router Views, on page 92 and Managing Endpoints in the Managing Devices chapter. |
| **Device Labeling Tasks** | |
| Add labels | Adding Labels in the Managing Devices chapter. |
| Remove labels | Removing Labels in Managing Devices chapter. |
| **Search and Device Filtering Tasks** | |
| Use filters | Using Filters to Control the Display of Devices, on page 158 |
| **Diagnostics and Troubleshooting Tasks** | |
| Ping | Pinging Devices, on page 151 |
| Traceroute | Tracing Routes to Devices, on page 151 |
| Download logs | Downloading Logs, on page 74 |
| **Monitoring Tasks** | |
| View and search events | Monitoring Events, on page 339 in the Monitoring System chapter. |
| View and search issues | Monitoring Issues, on page 351 in the Monitoring System chapter. |
| View tunnel status | Monitoring Tunnel Status, on page 316 in the Managing Tunnel Provisioning chapter. |
| **General Tasks** | |
| Change password | Resetting Passwords, on page 52 |
| Set time zone | “Configuring the Time Zone” in the Document Title, Release 4.x. |

# CGR Tasks

The table lists CGR tasks. For information about user roles, see System-Defined User Roles, on page 59

*Table 3: CGR Tasks*

| Task | Use |
|---|---|
| **Router Configuration Group Tasks** | |
| Add CGRs to configuration groups | Creating Device Groups, on page 172 |
| Delete a configuration group | Deleting Device Groups, on page 180 |
| List devices in a configuration group | Listing Devices in a Configuration Group, on page 181 |
| Assign devices to groups | • Adding Routers to IoT FND, on page 163<br>• Adding HERs to IoT FND, on page 162<br>• Moving Devices to Another Configuration Group in Bulk, on page 181<br>• Moving Devices to Another Configuration Group Manually, on page 180 |
| Rename configuration groups | Renaming a Device Configuration Group, on page 178 |
| **Router Configuration Tasks** | |
| Change device configuration properties | Changing Device Configuration Properties, on page 175 |
| Edit configuration templates | • Editing the ROUTER Configuration Template, on page 183<br>• Editing the AP Configuration Template, on page 185 |
| Push configurations | Pushing Configurations to Endpoints, on page 210 |
| Monitoring a Guest OS | Monitoring a Guest OS in the Managing Devices chapter. |
| **Tunnel Provisioning Tasks** | |
| Configure tunnel provisioning | See "Configuring Tunnel Provisioning" in the Managing Tunnel Provisioning chapter. |
| Edit tunnel provisioning templates | Configuring Tunnel Provisioning Templates in the Managing Tunnel Provisioning chapter. |
| Reprovisioning tunnels | • Configuring Tunnel Provisioning Templates in the Managing Tunnel Provisioning chapter.<br>• See "Factory Reprovisioning Template" in the Managing Tunnel Provisioning chapter. |
| **Firmware Management Tasks** | |
| Assign devices to firmware groups | Assigning Devices to a Firmware Group, on page 271 |
| Upload images to firmware groups | Uploading a Firmware Image to a Router Group, on page 276 |

# Mesh Endpoint Tasks

The table lists Mesh Endpoint (ME) tasks. For information about user roles, see System-Defined User Roles, on page 59.

*Table 4: Mesh Endpoint Tasks*

| Task | Use |
|---|---|
| **ME Configuration Group Tasks** | |
| Add mesh endpoint configuration groups | Creating Device Groups, on page 172 |
| Delete mesh endpoint configuration groups | Deleting Device Groups, on page 180 |
| Rename mesh endpoint configuration groups | Renaming a Device Configuration Group, on page 178 |
| Assign mesh endpoint devices to a configuration group | Moving Devices to Another Group, on page 180 |
| List devices in a configuration group | Listing Devices in a Configuration Group, on page 181 |
| **ME Configuration Tasks** | |
| Change mesh endpoint configuration properties | Changing Device Configuration Properties, on page 175 |
| Edit mesh endpoint configuration templates | Editing the ENDPOINT Configuration Template, on page 206 |
| Push configuration to mesh endpoints | Pushing Configurations to Endpoints, on page 210 |
| Add mesh endpoint firmware groups | Creating Device Groups, on page 172 |
| Assign devices to firmware groups | Moving Devices to Another Configuration Group Manually, on page 180 |
| Upload images to firmware groups | Uploading a Firmware Image to a Resilient Mesh Endpoint (RME) Group, on page 264 |

# Administration Tasks

The table lists administration tasks.

*Table 5: Administration Tasks*

| Task | Use |
|---|---|
| **Access Management Tasks** | |
| Set password policies | Managing Password Policy, on page 29 |
| Define roles | Managing Roles and Permissions, on page 57 |
| Manage user accounts | Managing Users, on page 50 |
| Manage Authentication | Managing User Authentication, on page 30 |

| Task | Use |
|---|---|
| Manage Domains | Managing Domains, on page 53 |
| **System Management Tasks** | |
| Manage active sessions | Managing Active Sessions, on page 64 |
| Display the audit trail | Displaying the Audit Trail, on page 65 |
| Manage certificates | Managing Certificates, on page 67 |
| Configure data retention | Configuring Data Retention, on page 68 |
| Manage licenses | Managing Licenses, on page 69 |
| Manage logs | Managing Logs, on page 73 |
| Configure server settings | Configuring Server Settings, on page 78 |
| Manage the syslog | Managing System Settings, on page 63 |
| Configure tunnel settings | Configuring Provisioning Settings, on page 74 |
| View logs | Managing Logs, on page 73 |

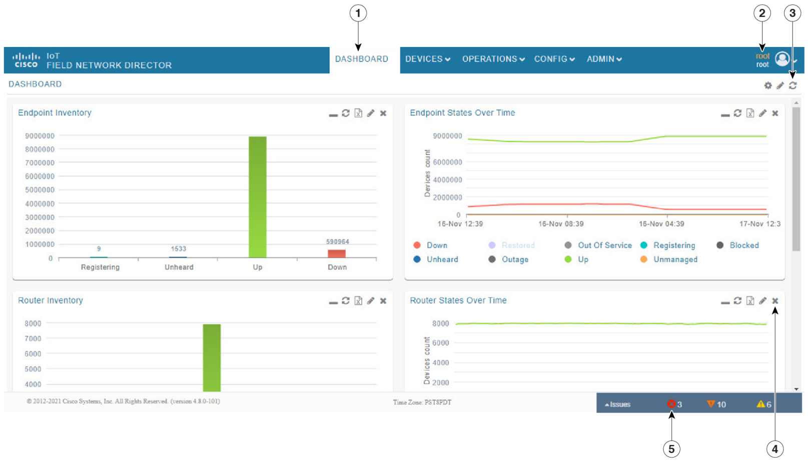
# Interface Overview

This section provides a general overview of the IoT FND GUI, including:

- Icons, on page 21
- Main Menus, on page 23

The IoT FND displays the dashboard after you log in. See “Using the Dashboard” section in the “Monitoring System” chapter of this guide.

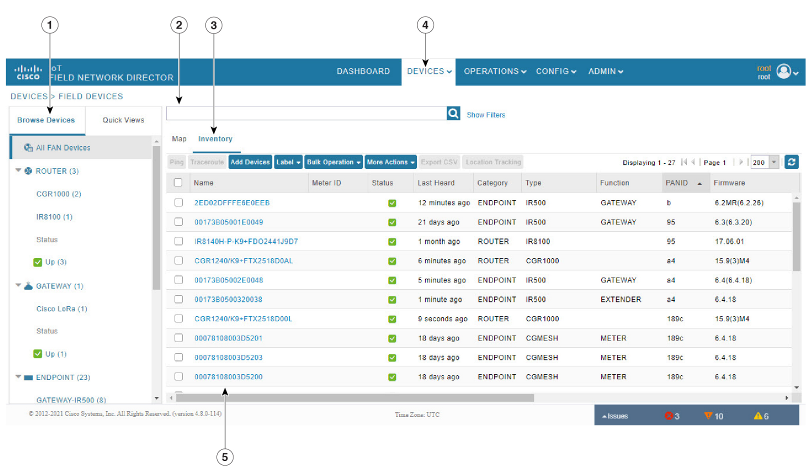
*Figure 4: IoT FND Dashboard*




| | | | |
|---|---|---|---|
| **1** | Menu and Submenu tabs.<br>Roll over the Menus to display Submenus, which display as tabs below the main menus. | **4** | Dashlet action buttons (left to right):<br>• Minimize (close) dashlet window<br>• Refresh dashlet<br>• Export data<br>• Filter (not available on all pages)<br>• Close dashlet |

| | | | |
|---|---|---|---|
| **2** | *<user name>* menu<br>• Preferences: Sets display settings of the user interface.<br>• Switch Domain<br>• Change Password<br>• Time Zone<br>• Guided Tour<br>• Log Out | **5** | Issues Status bar<br>Summary of issues by devices (routers, head-end routers, servers, endpoints) and their severity (critical, major, minor)<br>Viewing Device Severity Status on the Issues Status Bar, on page 353 |
| **3** | • Dashboard Settings-Allows you to set the refresh rate for the page and Add Dashlets to the Dashboard.<br>• Filter-Allows you to define custom filters and by selectable time periods.<br>• Refresh page. | | |

*Figure 5: Main Window Elements*




| | | | |
|---|---|---|---|
| **1** | Browse Devices Pane | **4** | Main Menu |

| | | | |
|---|---|---|---|
| **2** | Filters | **5** | Device EID links to Device Info page |
| **3** | Inventory page displays multiple entries of the same Open Issue of a given device as a single entry only. | | |

#### Working with Views

Use the Browse Devices pane (1) to view default and custom groups of devices. At the top of the Browse Devices pane the total number of registered devices displays in parenthesis. The total number of devices in groups displays in parenthesis next to the group name.

You can refine the List display using Filters (2). See Using Filters to Control the Display of Devices, on page 158. Built-in filters are automatically deployed by clicking a device group in the Browse Devices pane. Use the Quick View tab to access saved custom filters.

Click the device Name or EID (element identifier) link (5) to display a device information page. Click the **<<Back** link in the Device Info page to return to the page you were on when you clicked the device EID link. Click the refresh button on any page to update the List view.

#### Using the Tabs

Each device page has tabs in the main window to view associated information. The active tab is in bold type when you are on that tab (for example, Figure 5: Main Window Elements, on page 19).

#### Navigating Page Views

By default, device management pages display in List view, which displays devices in a sortable table. On the Routers and Mesh pages, select the Map tab to display devices on a GIS map (see Viewing Devices in Map View, on page 147 and Viewing Mesh Endpoints in Map View, on page 99).

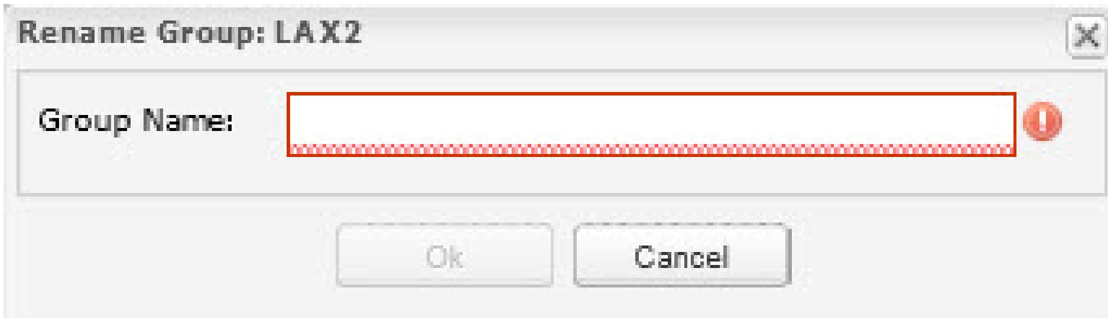
#### Working with Filters

Create custom filters by clicking the Show Filters link (the Hide Filters link displays in the same place in Figure 5: Main Window Elements, on page 19) and using the provided filter parameters (2) to build the appropriate syntax in the Search Devices field (2). Click the Quick Views tab to display saved custom filters (see Creating and Editing Quick View Filters, on page 159).

#### Completing User-entry Fields

Figure 6: Errored Group Name User-entry Field, on page 21 shows an error in the user-entry field. IoT FND displays a red alert icon, highlights the field in red, and disables the **OK** button. These errors occur, for example, on an invalid character entry (such as, @, #, !, or +) or when an entry is expected and not completed.

*Figure 6: Errored Group Name User-entry Field*

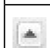
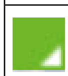
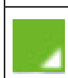


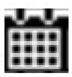
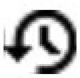

# Icons

The table lists the icons that display in the UI.

*Table 6: IoT FND Icons*

| Icon | Description |
| --- | --- |
|  | This router icon is used for CGRs, ISRs, and IRs (routers), and HERs. |
|  | This is the server icon. |
|  | This is the DA gateway (IR500) device icon. |
|  | This is a meter icon. |
|  | This is an endpoint icon. Its color varies based upon status of the device. |
|  | The up icon indicates that the device is up and online. |
|  | The down icon indicates that the device is down. |
|  | The unheard icon indicates that the device has not yet registered with IoT FND. |
|  | The outages icon indicates that the device is under power outage. |

| Icon | Description |
|---|---|
|  | The restored icon indicates that the device has recovered from an outage. |
|  | The default group icon indicates that this is the top-level device group. All devices appear in this group after successful registration. |
|  | This is the Add Group icon. |
|  | These are the Edit and Delete Group icons. |
|  | On the Events page, click this button to initiate an export of event data to a CSV file. |
|  | The Group icon indicates that this is a custom device group. |
|  | The Custom Label icon indicates a group of devices. Use labels to sort devices into logical groups. Labels are not dependent on device type; devices of any type can belong to any label. A device can also have multiple labels. |
|  | On the Dashboard page, click this button to set the refresh data interval and add dashlets. |
|  | On the Dashboard page, click this button to initiate an export of dashlet data to a CSV file. |
|  | On the Dashboard page, click this button to refresh dashlet data. |
|  | On the Dashboard page, click this button to change the data retrieval interval setting and add filters to the dashlets. On line-graph dashlets, this button not only provides access to the data retrieval interval setting and filters, but you can also access graph-specific data settings. This icon is green when a filter is applied. |
|  | On the Dashboard page in the dashlet title bar, click this button to show/hide the dashlet. When the dashlet is hidden, only its title bar displays in the Dashboard. |
|  | In Map view, this is the RPL tree root device icon. This can be a CGR or mesh device, as set when Configuring RPL Tree Polling. The colors reflect the device status: Up, Down, and Unheard.<br>The RPL tree connection displays as blue or orange lines.<br>• Orange lines indicate that the link is up.<br>• Blue lines indicate that the link is down. |
|  | In Map view, this is a device group icon. The colors reflect the device status: Up, Down, and Unheard. |

| Icon | Description |
|---|---|
|  | On the Events and Issues pages, and on the Issues Status bar, these icons indicate the event severity level, top-to-bottom, as follows:<br>• Critical<br>• Major<br>• Minor<br>• Info<br><br>Each event type has a preset severity level. For example, a Router Down event is a Major severity level event. |
|  | On the Firmware Update page, click the Schedule Install and Reload button to configure firmware updates. |
|  | On the Firmware Update page, click the Set as Backup button to set the selected image as the firmware image backup. |

# Main Menus

This section describes the IoT FND menus such as dashboard, admin, config, devices, and operations available in the title bar at the top of the page.

## Dashboard Menu

This user-configurable page displays information about the connected grid.

## Devices Menu

The Devices menu provides access to the device management pages:

- Field Devices-This page displays a top-level view of registered routers and mesh endpoints in your grid.
- Head-End Routers-This page displays a top-level view of registered HERs in your grid.
- Servers-This page displays a top-level view of IoT FND and database servers in your network.
- Assets-This page displays non-Cisco equipment that is mapped to Cisco equipment that is managed by IoT FND. Up to five assets can be mapped to a Cisco device and you can upload up to five files (such as .jpeg or .txt) that support those assets.

## Operations Menu

The Operations menu provides access to the following tabs:

- Events—This page displays events that have occurred in your grid.
- Issues—This page displays unresolved network events for quick review and resolution by the administrator.

- Tunnel Status—This page lists provisioned tunnels and displays information about the tunnels and their status.
- Work Orders – This page allows users to add, edit, or delete a work order.

## Config Menu

The Config menu provides access to the following tabs:

- Device Configuration—Use this page to configure device properties.
- Firmware Update—Use this page to install a new image on one or multiple devices, change the firmware group of a device, view the current firmware image on a device (routers, endpoints) and view subnet details on mesh endpoints.
- Device File Management—Use this page to view device file status, and upload and delete files from FARs.
- Rules—Use this page to create rules to check for event conditions and metric thresholds.
- Tunnel Provisioning—Use this page to provision tunnels for devices.
- Groups—Use this page to assign devices to groups.

## Admin Menu

The Admin menu is divided into two areas for managing system settings and user accounts:

- Access Management pages:
    - Domains—Use this page to add domains and define local or remote administrators and users.
    - Password Policy—Use this page to set password conditions that user passwords must meet.
    - Authentication—Use this page to configure local, remote, or Single Sign-On authentication for IoT-DM users.
    - Roles—Use this page to define user roles.
    - Users—Use this page to manage user accounts.
- System Management pages:
    - Active Sessions—Use this page to monitor IoT FND sessions.
    - Audit Trail—Use this page to track user activity.
    - Certificates—Use this page to manage certificates for CSMP (CoAP Simple Management Protocol), IoT-DM, and the browser (Web) used by IoT FND.
    - Data Retention—Use this page to determine the number of days to keep event, issue, and metric data in the NMS database.
    - License Center—Use this page to view and manage license files.
    - Logging—Use this page to change the log level for the various logging categories and download logs.

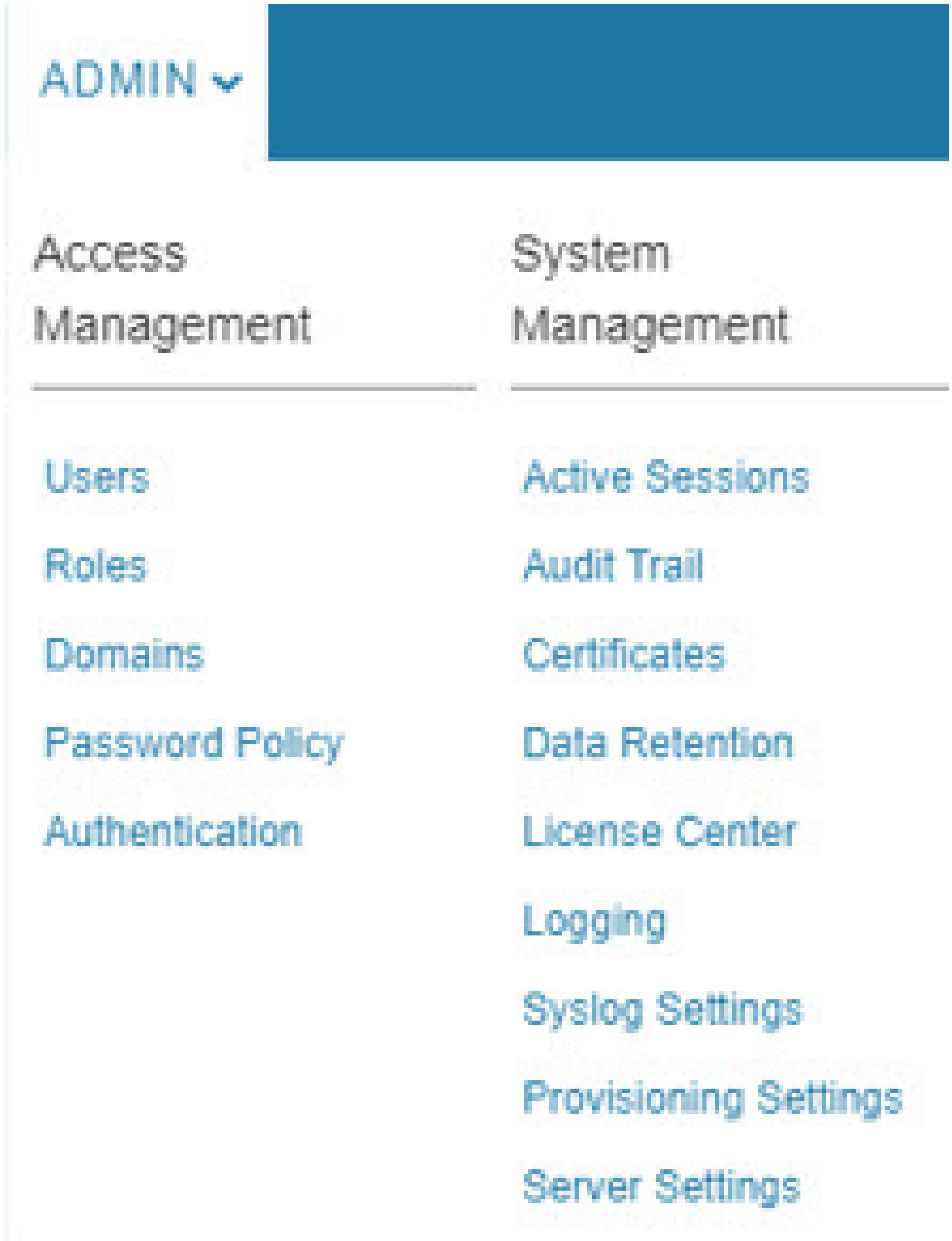
- Provisioning Settings—Use this page to configure the IoT FND URL, and the Dynamic Host Configuration Protocol v4 (DHCPv4) Proxy Client and DHCPv6 Proxy Client settings to create tunnels between CGRs and ASRs.
- Server Settings—Use this page to view and manage server settings.
- Syslog Settings—Use this page to view and manage syslog settings.
- Jobs – Use this page to view the detailed summary of the jobs and their respective sub jobs.

CHAPTER 3

# Managing User Access

This section explains how to manage users and roles in IoT FND.

All user management actions are accessed through the **Admin** > **Access Management** menu.





- Managing Password Policy, on page 29
- Managing User Authentication, on page 30

# Managing Password Policy

IoT FND provides default password policy values that you can enforce among IoT FND users.

**Note** To modify these values, you must be logged in either as root or as a user with Administrative Operations permissions.

**Caution:** In some cases, changing password policies immediately terminates all user sessions and resets all passwords.

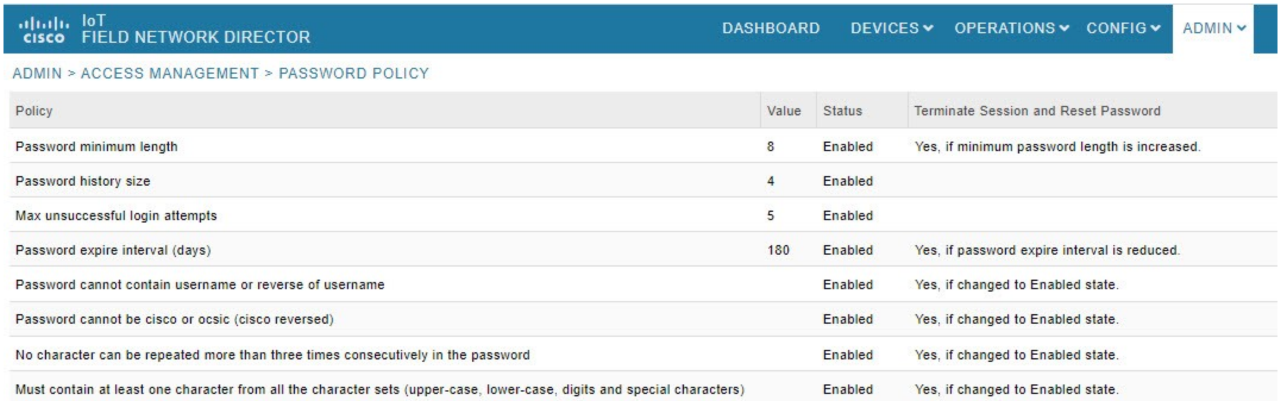
**Note** The “Password history size” and “Max unsuccessful login attempts” policies do not apply to IoT FND North Bound API users.

These changes ***invalidate*** all user sessions and expire their passwords (including the root user):

- When you increase the minimum length of passwords
- When you decrease the password expiry interval
- When you enable **"Password cannot contain username or reverse of username"**
- When you enable **"Password cannot be cisco or ocsic (cisco reversed)"**
- When you enable **"No character can be repeated more than three times consecutively in the password"**
- When you enable **"Must contain at least one character from all the character sets (upper-case, lower-case, digits and special characters)"**

To edit password policies:

**Step 1** Choose **ADMIN** > **Access Management** > **Password Policy**.




| Policy | Value | Status | Terminate Session and Reset Password |
|---|---|---|---|
| Password minimum length | 8 | Enabled | Yes, if minimum password length is increased. |
| Password history size | 4 | Enabled | |
| Max unsuccessful login attempts | 5 | Enabled | |
| Password expire interval (days) | 180 | Enabled | Yes, if password expire interval is reduced. |
| Password cannot contain username or reverse of username | | Enabled | Yes, if changed to Enabled state. |
| Password cannot be cisco or ocsic (cisco reversed) | | Enabled | Yes, if changed to Enabled state. |
| No character can be repeated more than three times consecutively in the password | | Enabled | Yes, if changed to Enabled state. |
| Must contain at least one character from all the character sets (upper-case, lower-case, digits and special characters) | | Enabled | Yes, if changed to Enabled state. |

**Step 2** To enable or disable a policy, choose the appropriate option (**Enabled** or **Disabled**) from the Status drop-down menu.

**Note** IoT FND supports a maximum password length of 32 characters.

**Step 3** To modify the value of a policy, if applicable, enter the new value in the Value field.

**Step 4** Click **Save** to start enforcing the new policies.

**Note** The password policy you configure in IoT FND applies only to local users and not to remote Active Directory (AD) users. The password policy for AD users is determined and enforced by the AD admin.

# Managing User Authentication

This section explains how to configure remote and single sign-on authentication in Cisco IoT FND.

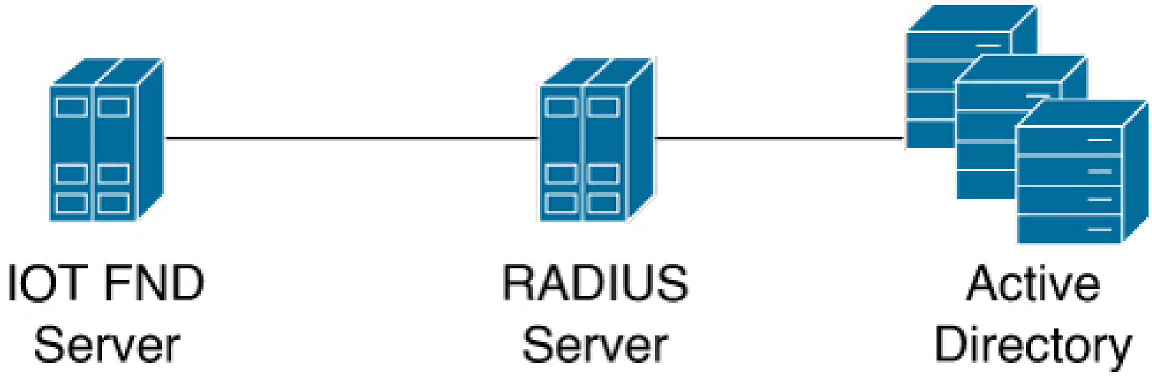
## Configuring Remote Authentication

To configure remote authentication for IoT FND, you need to perform the configurations steps (listed below) in Active Directory (AD) and IoT FND.

### Support for Remote Authentication

With Remote Authentication, it is easier to integrate IoT FND into an existing AD and Network Policy Server (NPS) infrastructure. This allows administrators to configure IoT FND access for users in AD.

When you configure remote authentication in IoT FND, it hands over the authentication and authorization responsibility to AD and NPS. AD performs user authentication to check the validity of user credentials. The RADIUS server performs user authorization to check whether a user belongs to a group that defines the user role. If so, the server returns the role name to IoT FND.




The following is the flow of user authentication and authorization by AD and NPS:

1. The user enters their credentials.

| |
|---|
| If user was created locally on the NMS server, authentication and authorization occurs locally. |
| If IoT FND determines that the user is a remote user, authentication and authorization occurs on the configured RADIUS server. |
| If remote authentication is not configured, authentication fails and user is denied access. |

2. For remote users, if authentication and authorization are successful, the assigned user role returns to the NMS server from the RADIUS server.
3. If the role that returns is valid, the user is granted access.

**Note** When remote authentication is enabled, user management is done in AD. If an AD user logs in who was deleted from IoT FND, their profile is added back to IoT FND. To prevent access to IoT FND, their AD user profiles must first be deleted from AD.

## Configuring Remote Authentication in IoT FND

To configure remote authentication:

**Step 1** Choose **ADMIN** > **Access Management** > **Authentication**.

**Step 2** Select the authentication type as **Local or Remote Authentication**.

**Step 3** Enter information about the Radius Server:

| Field | Description |
|---|---|
| IP | The IP address of the RADIUS server. |
| Radius Server Description | A descriptive name of the RADIUS server. |
| Shared Secret | The shared secret you configured on the RADIUS server. |
| Confirm Shared Secret | |

| Field | Description |
|---|---|
| Authentication Port | The RADIUS server port that IoT FND uses to send request to. The default port is 1812. |
| Accounting Port | The RADIUS server accounting port. The default port is 1813. |
| Retries | The number of times to send a request to the RADIUS server before IoT FND times out and remote authentication fails because no response was received from the RADIUS server. |
| Timeout (seconds) | The number of seconds before IoT FND times out and remote authentication fails because no response was received from the RADIUS server. |

**Step 4** To ensure that IoT FND can reach the RADIUS server, click **Test Connectivity**.

a) Enter your Remote (AD) username and password.
b) Click **Submit**.

The results of the configuration test displays.

c) Click **OK**.

**Step 5** Click **Save** when done.

## Configuring Security Policies on the RADIUS Server

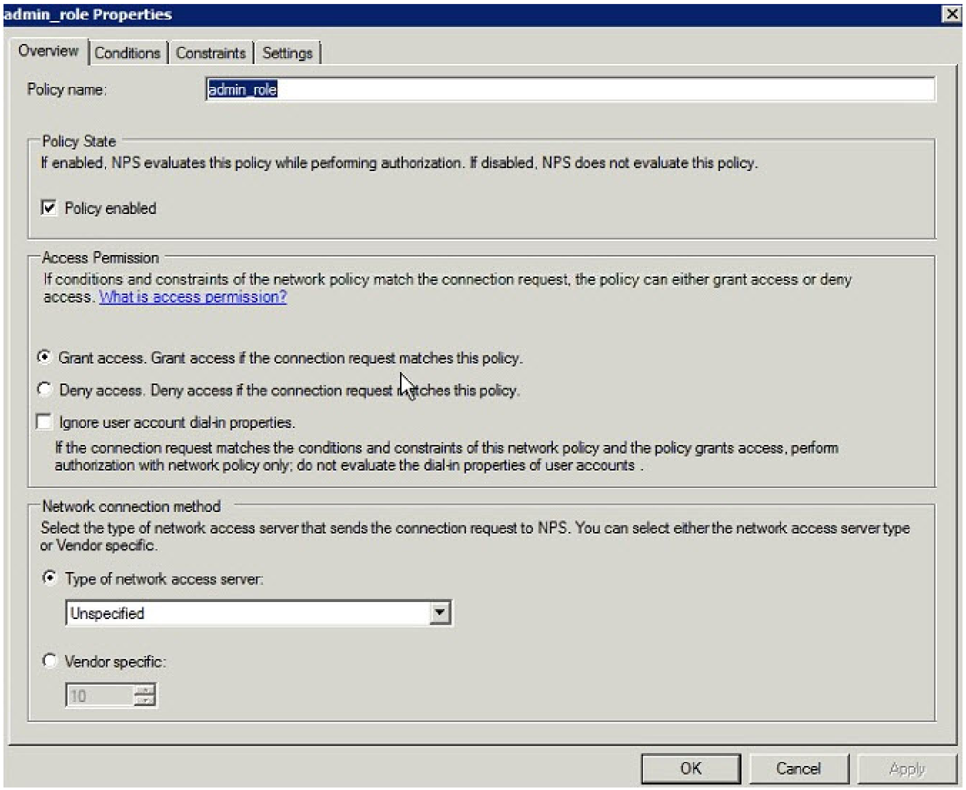
To authorize users for IoT FND access, configure security policies for the RADIUS server.

To configure security policies on the RADIUS server, follow these steps:

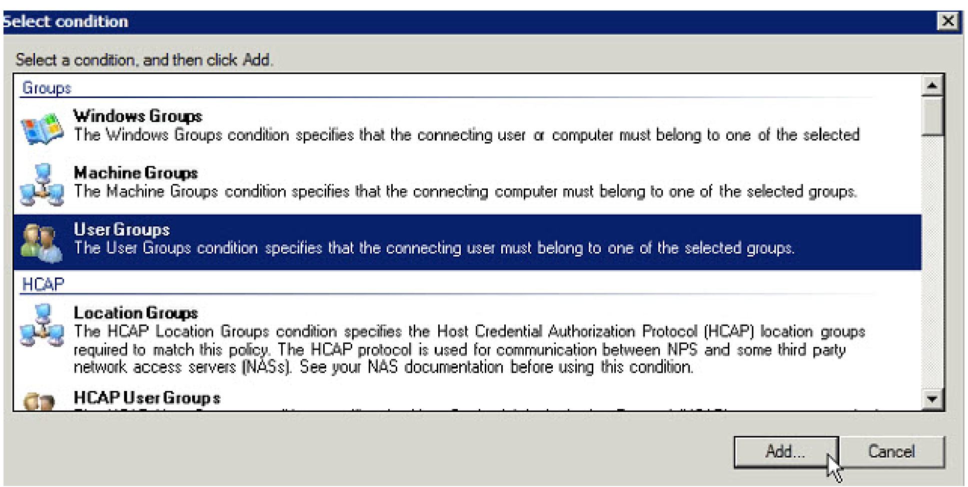
**Step 1** Create a network policy for each security group you created in AD.

**Step 2** Configure the policy as follows:

a) In the **Overview** tab, define the policy name, enable it, and grant access permissions.

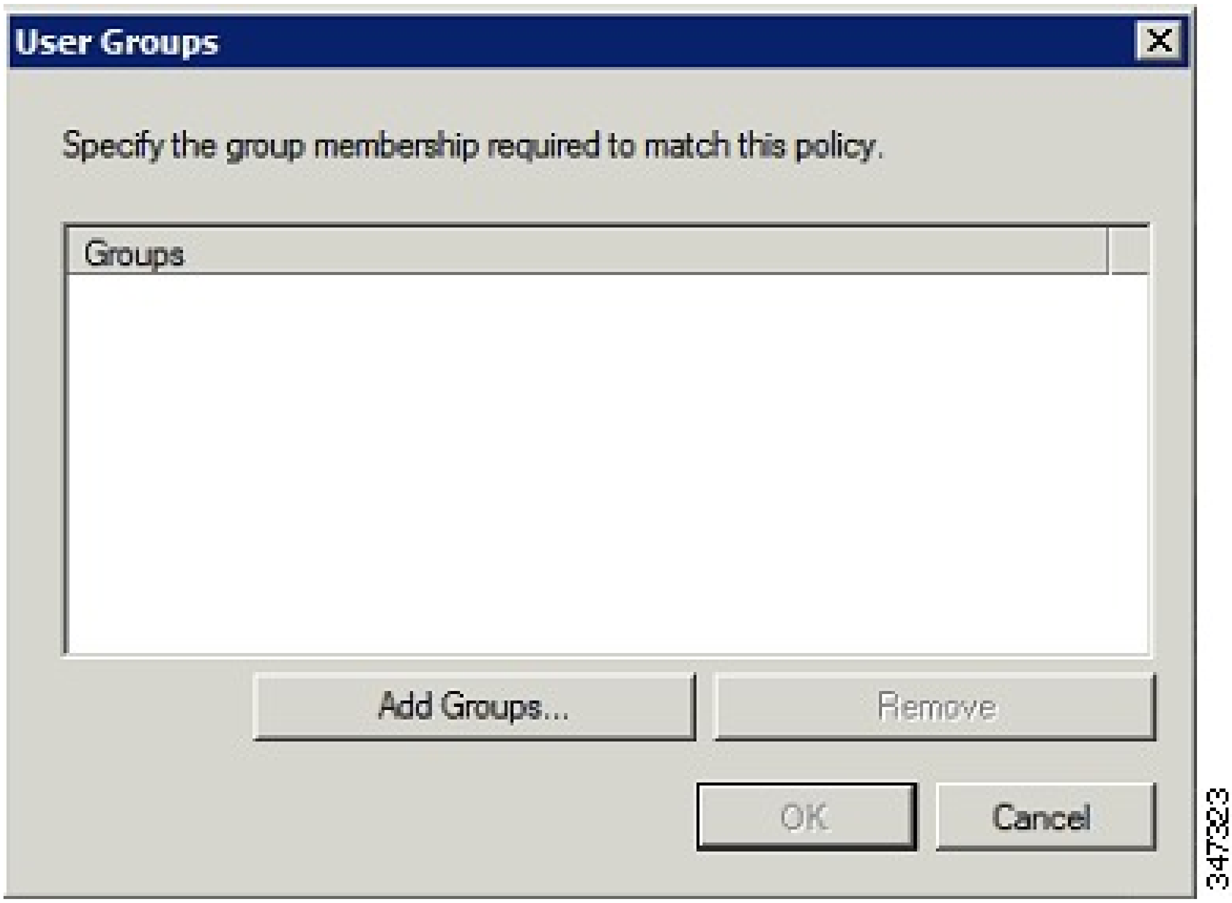



b) Click the **Conditions** tab, select the User Groups condition, and click **Add** .

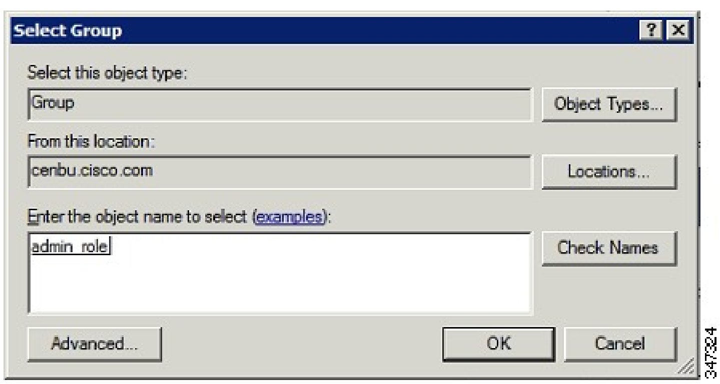



The User Groups condition specifies that the connecting user must belong to the selected group. For this policy to pass, the user being authorized must belong to the user group configured in this policy.

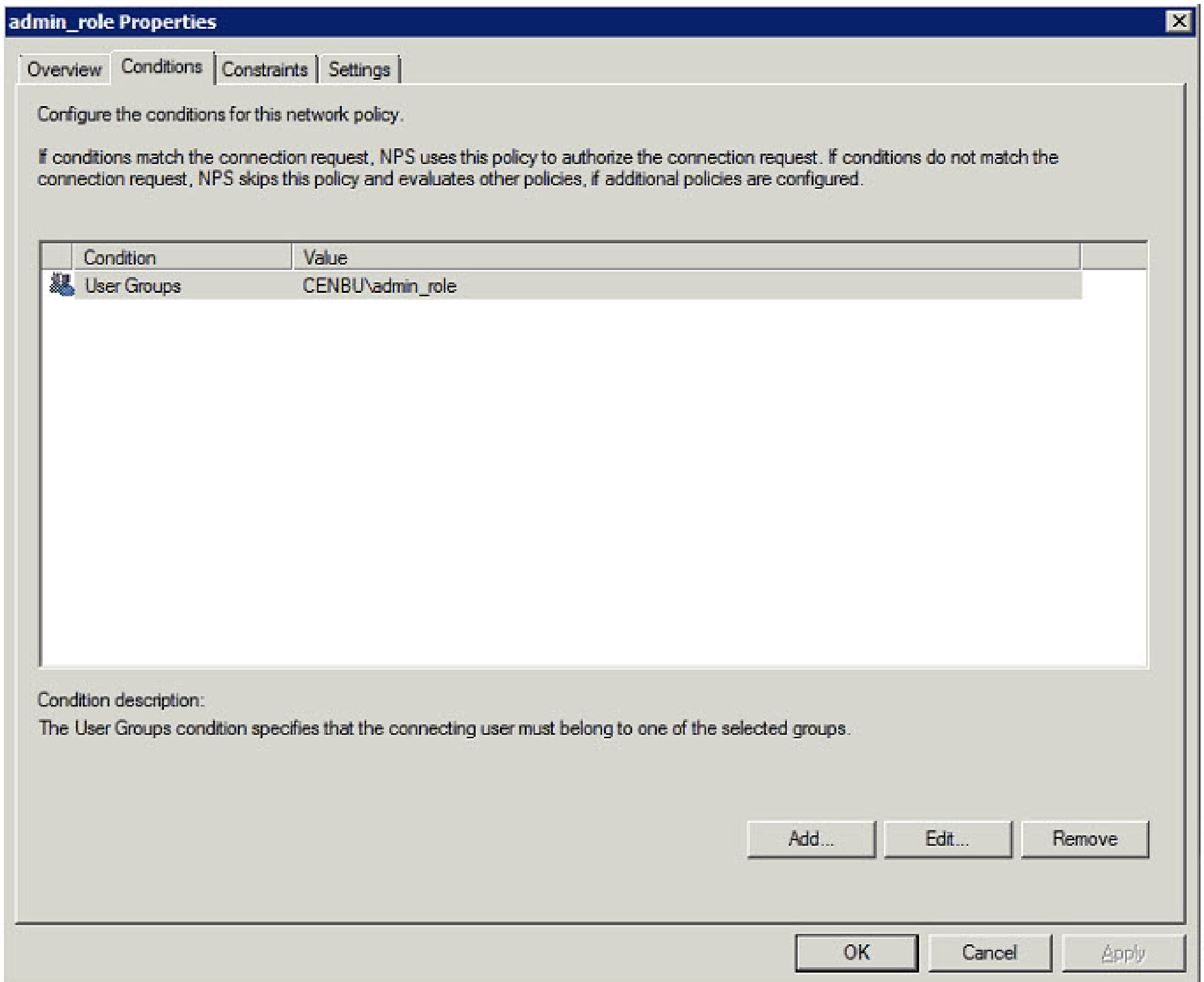
c) In the **User Groups** window, click **Add Groups**.




d) In the **Select Group** window, enter the name of the group
e) Click **OK** to close the **Select Group** dialog box, and then click **OK** to close the User dialog box.

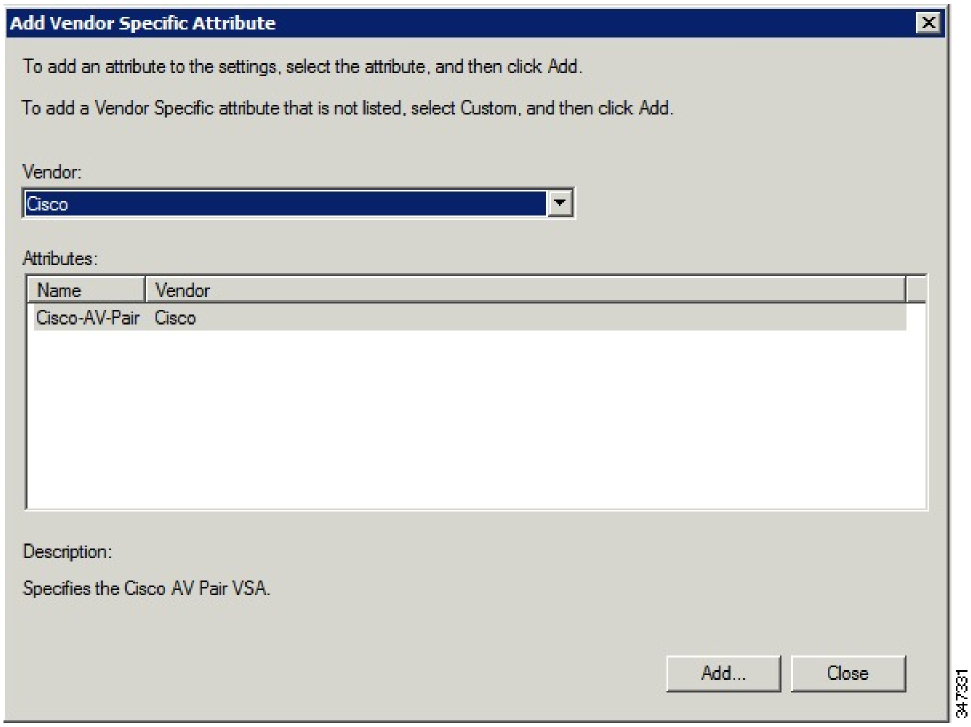



f) Click **Cancel** to close the Select condition window. The condition appears in the Conditions pane.




347321

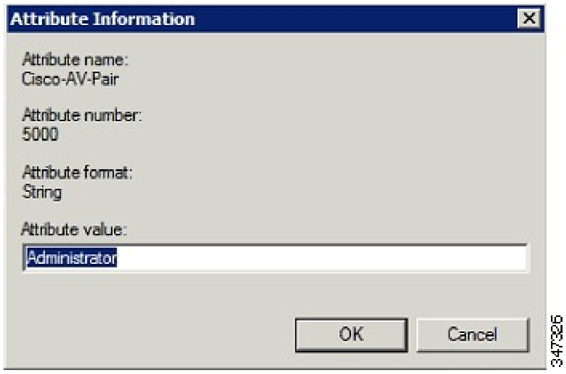
g) Click the Settings tab, and then click **Add** to display the Attribute Information window.



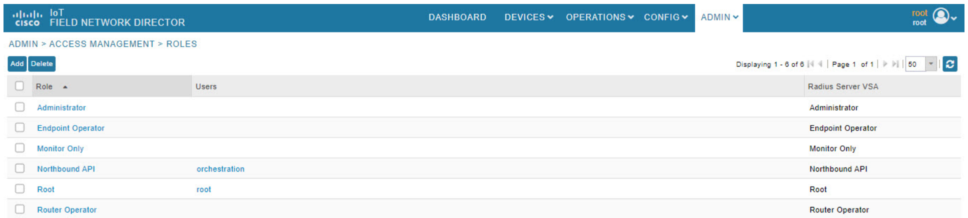

h) Click **Add** to define a Vendor Specific Attribute (VSA) that is sent to IoT FND (RADIUS client) after the user credentials and security group membership are verified.

The VSA to configure is:

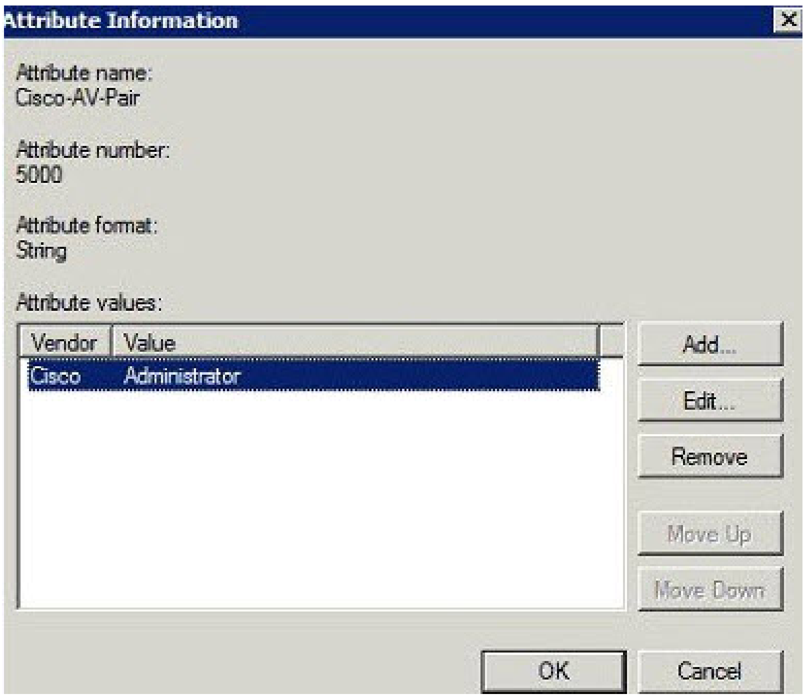
| Configure VSA |
|---|
| Attribute Name: Cisco-AV-Pair |
| Attribute number: 5000 |
| Attribute format: String. |
| Attribute value: Enter the attribute value to send to IoT FND. |



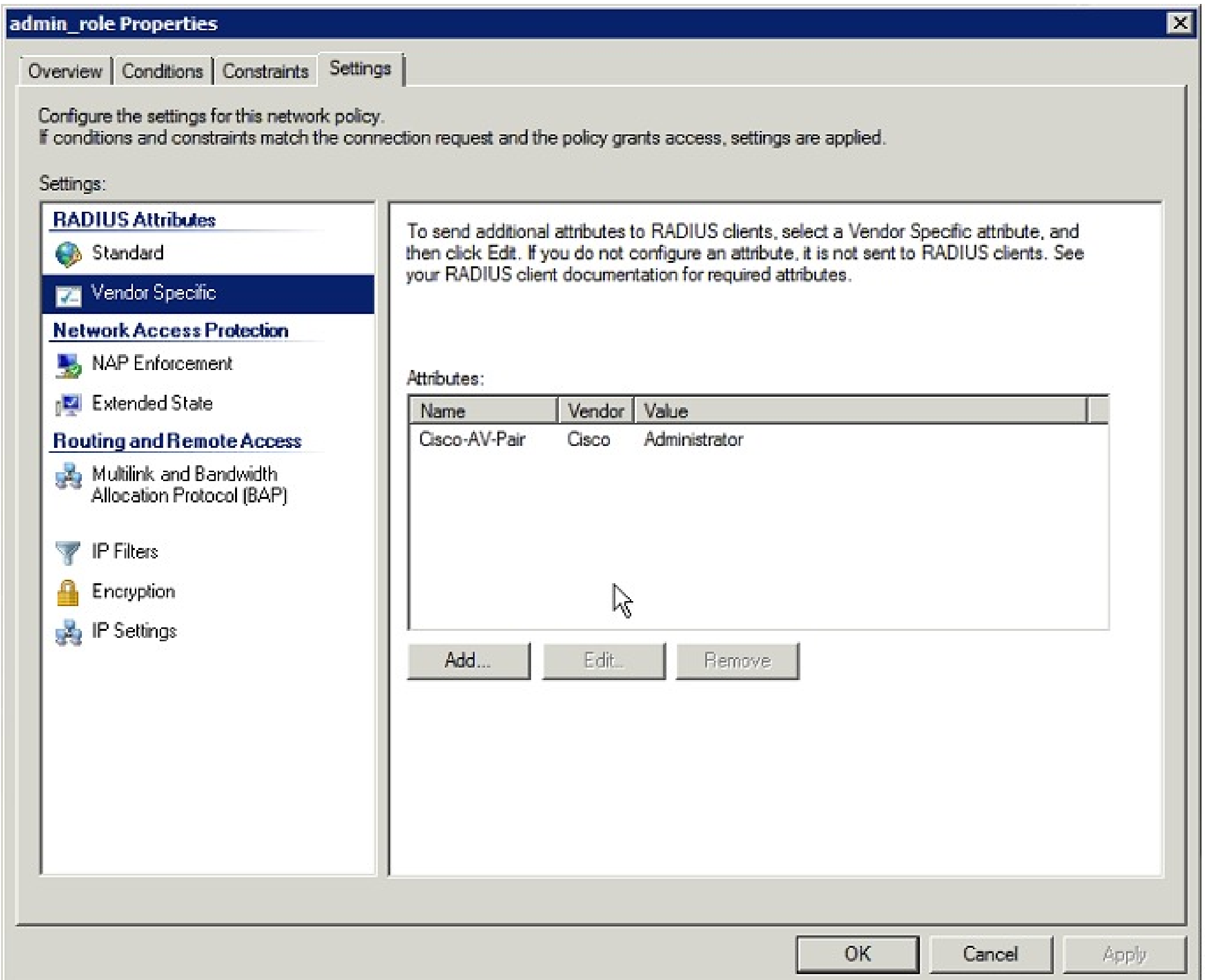

**Note** The string entered in the Attribute value field must be the exact string listed in the Radius Server VSA column on the Roles page in IoT FND (**ADMIN** > **Access Management** > **Roles**).




i) Click **OK**.




The VSA attribute appears in the Settings pane.



347327

j) Click **OK**.

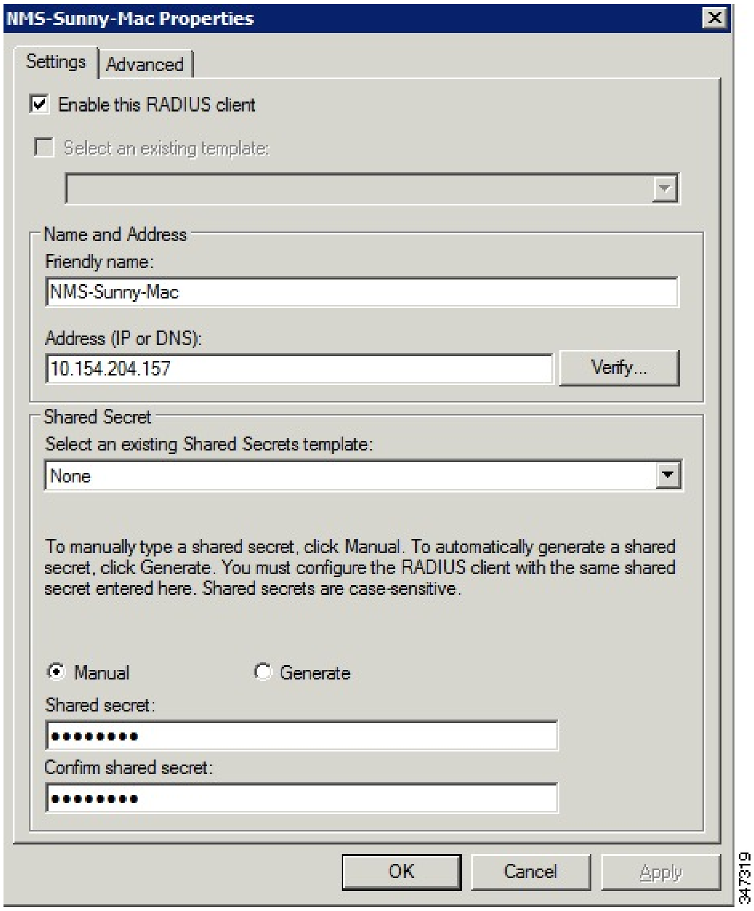
## Configuring Remote Authentication in AD

To allow IoT FND to remotely authenticate users, configure the following within Active Directory

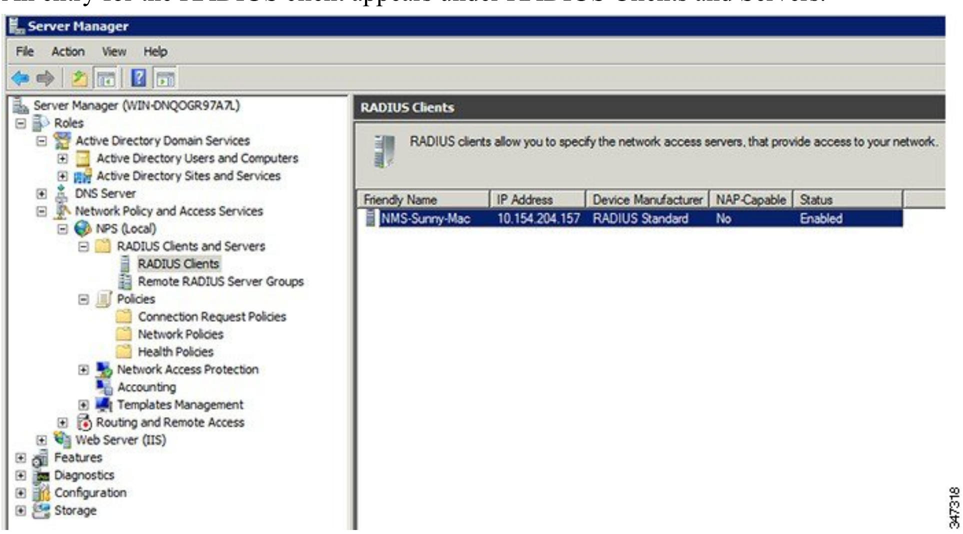
**Step 1** Log in to NPS.

**Step 2** Add IoT FND as a radius client on the RADIUS server.

Provide a friendly name, and IP address or DNS name of the IoT FND server and configure the shared secret that IoT FND uses to connect to the RADIUS server.

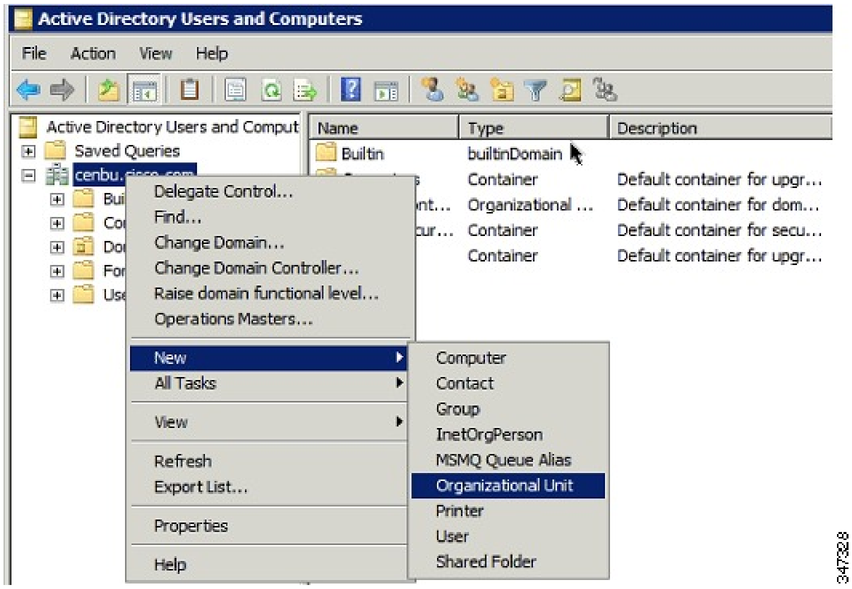



An entry for the RADIUS client appears under RADIUS Clients and Servers.



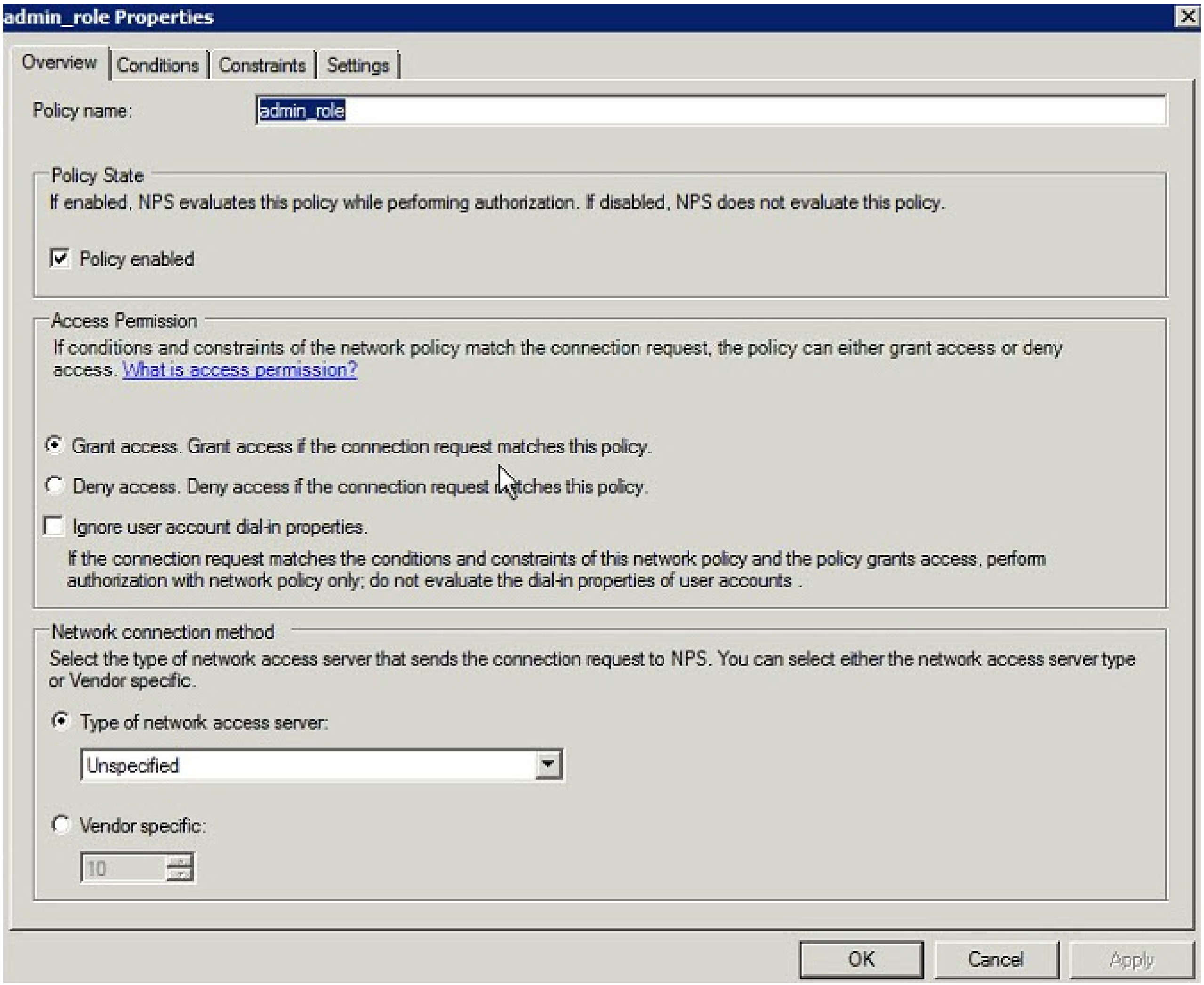

**Step 3** Log in to AD and create an Organizational Unit.

Cisco recommends that you create all security groups (IoT FND roles) within this Organizational Unit.



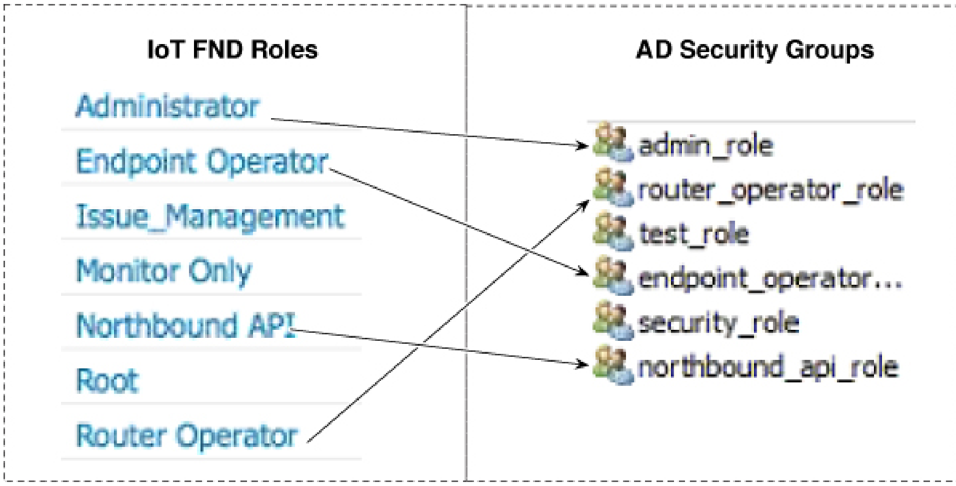

**Step 4** Add security groups corresponding to IoT FND roles to the Organizational Unit.

The following example shows the security groups defined in the NMS_ROLES Organizational Unit.




**Tip:** When creating the security groups, ensure that they map one-to-one to IoT FND roles (that is, every role defined in IoT FND maps to only one AD security group). The name of the security group does not have to match a role name in IoT FND, but for organizational purposes, Cisco recommends using names that correlate the security group name to a IoT FND role.

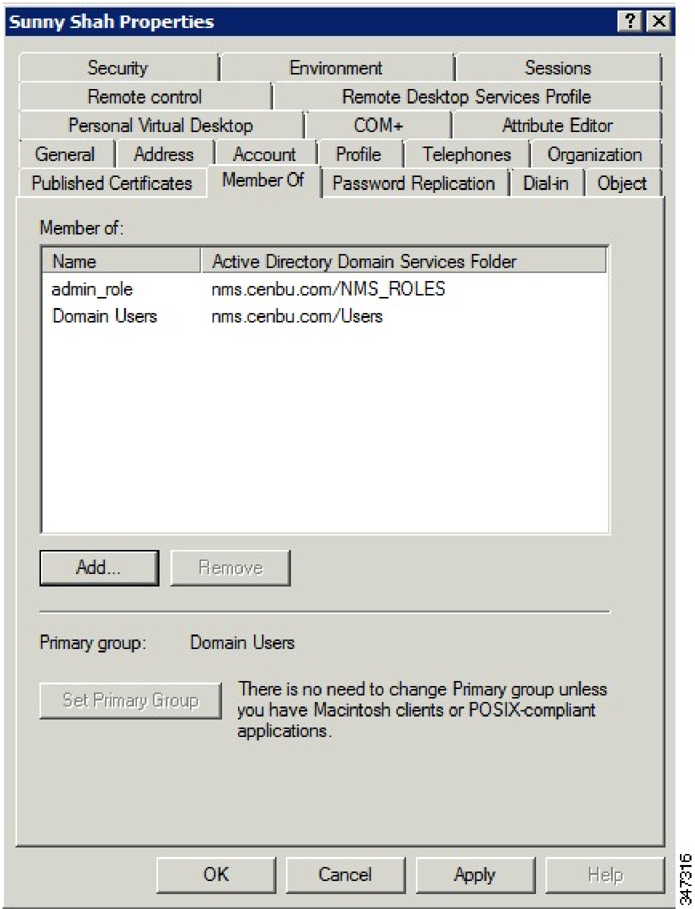
**Note** You cannot create or assign the IoT FND root role in AD.



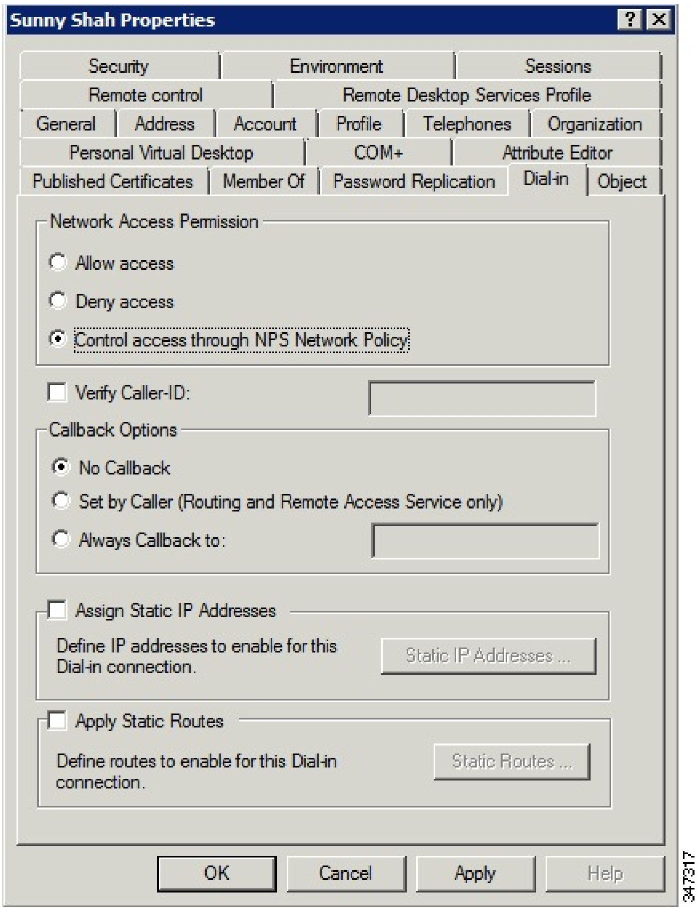

**Step 5** Assign AD users a role by adding them to the security group mapping to that role.

Since, users can only belong to one security group, the IoT FND role that the user is assigned after log in is dependent on their assigned AD security group.

**Tip:** In AD, users cannot be assigned multiple IoT FND roles, and cannot belong to multiple security groups. To assign permissions from more than one role to a group of users, create a new IoT FND role with the required permissions, and a create the corresponding AD security group. Users in this new group can then carry out the tasks allowed by this role.




**Step 6** Configure the Dial-in Network Access Permission to use the NPS Network Policy.




## Enabling and Disabling Remote User Accounts

In IoT FND you cannot enable or disable remote AD user accounts. To enable or disable remote AD user accounts, use your AD server.

## Deleting Remote User Accounts

In IoT FND, you can delete remote user accounts. However, this only removes the user from the IoT FND Users page (**ADMIN** > **Access Management** > **Users** ); it does not delete the user account from AD. If a deleted user logs in to IoT FND and AD authentication is successful, an entry for the user is added to the IoT FND Users page.

## Logging In to IoT FND Using a Remote User Account

Logging in to IoT FND using a remote AD user account is transparent to the user. In the background, IoT FND checks whether the account is local, and for remote users sends an authentication request to the RADIUS server configured on the Remote Authentication page (**ADMIN** > **Access Management** > **Remote Authentication** ). If both authentication and authorization are successful, IoT FND adds an entry for the user in the Users page (**ADMIN** > **Access Management** > **Users** ).

Unlike entries for local users on the Users page, the user name filed in remote user entries is not a link. You cannot click the name of a remote user to obtain more information about the user.

**Note** Remote users cannot be managed through IoT FND. If a remote user wants to update their password, they must use their organization's AD password update tool. Remote users cannot update their password using IoT FND.

# Configuring Single Sign-On Authentication

Starting with Cisco IoT FND 4.8 release, Single Sign-On (SSO) authentication is supported. SSO allows you to access multiple web applications using one set of login credentials. With SSO enabled, the time and effort are minimized as you need not sign-in and sign-out separately while accessing multiple applications.

You can enable SSO on IoT FND using the following ways:

- Configure IDP Manually
- Import IDP Metadata File into FND

*Table 7: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Single Sign-On (SSO) | IoT FND 4.8 | SSO allows you to access multiple web applications using one set of login credentials. |

## Single Sign-On Authentication

Single Sign-On (SSO) is an authentication process that allows you to sign into one application and then securely access other authorized applications without the need to resupply your credentials. SSO allows you to sign on only once with a username and password to access browser-based applications and services within a single browser instance. SSO uses Security Assertion Markup Language (SAML) for authentication.

**Note**
- SSO is an optional feature
- Only HTTPS protocol is required to access all the web applications. HTTP access to web application is not supported when the SSO is enabled.

For more information on SSO—SAML solution, refer to:

- Elements in SSO SAML Solution , on page 46
- How SAML Works, on page 47
- Limitations for SSO Authentication, on page 50
- Configuring IDP Manually for SSO Authentication, on page 47
- Importing IDP Metadata for SSO Authentication, on page 48

## SAML 2.0 Protocol

Security Assertion Markup Language (SAML) is an XML-based standard or framework to exchange user authentication details between an Identity Provider (IdP) and a service provider.

The identity provider authenticates the user credentials and issues SAML assertions. Each assertion is an XML document that contains security information, which is transferred from the identity provider to the service provider.

A generic SAML authentication flow consists of:

- Client—A browser-based user.
- Service Provider—An application or service the user tries to access.
- Identity Provider—An entity performing the user authentication

For more information, refer to Elements in SSO SAML Solution , on page 46

## Elements in SSO SAML Solution

SAML uses the following elements to authenticate and authorize the user credentials.

| Elements | Description |
|---|---|
| Client | A browser-based client such as FND users.<br>**Note** Firefox and MS Edge are the officially supported browsers for FND. |
| Service Provider | An application or service that trusts the SAML assertion and relies on the IDP to authenticate the users. |
| Identity Provider (IDP) server | A third-party server, which authenticates user credentials and issues SAML assertions. |
| IDP Store | Storage that maintains user credentials and their associated roles. Available stores are LDAP store, Active Directory, or RDBMS. |
| SAML Assertion | An assertion is an XML document that contains trusted statements about a user. Example: username. SAML assertions are digitally signed to ensure their authenticity. It consists of pieces of security information, which are transferred from IDP to the service provider for user authentication. |
| SAML Request | An authentication request generated by the service provider. |

| Elements | Description |
|---|---|
| Metadata | An XML file generated by the service provider application and an IDP server.<br>• The service provider metadata file contains information such as entity ID, redirect URLs, certificate key.<br>• The IDP metadata file contains server information to configure the service provider. |
| Assertion Consumer Service (ACS) URL | A URL that instructs the IDP where to post SAML assertions. |

## How SAML Works

A synopsis of SAML workflow:

- Administrator logs into FND and enables SSO for all users.
    - Configuring IDP Manually for SSO Authentication, on page 47
    - Importing IDP Metadata for SSO Authentication, on page 48
- FND performs web certification checks. If the verification is successful, the SSO users are directed to the IDP login page; else, an error message appears.
- IDP checks whether the session is active.
    - For active session, you receive a SAML token.
    - For inactive session, you are redirected to IDP login page.
- IDP validates the credentials of the user.
- On successful login, SAML response is sent to ACS URL.
- FND server receives SAML response and extracts information such as user ID and roles associated with the user.
- FND maps the roles received to the roles in FND and gets the associated permissions for the user.
- User information is stored in the FND database and SSO is enabled for the user.

## Configuring IDP Manually for SSO Authentication

To configure IDP manually for SSO authentication:

**Step 1** Choose **ADMIN** > **Access Management** > **Authentication**.

**Step 2** In the Authentication Settings page, select the **Single Sign-On Authentication** radio button.

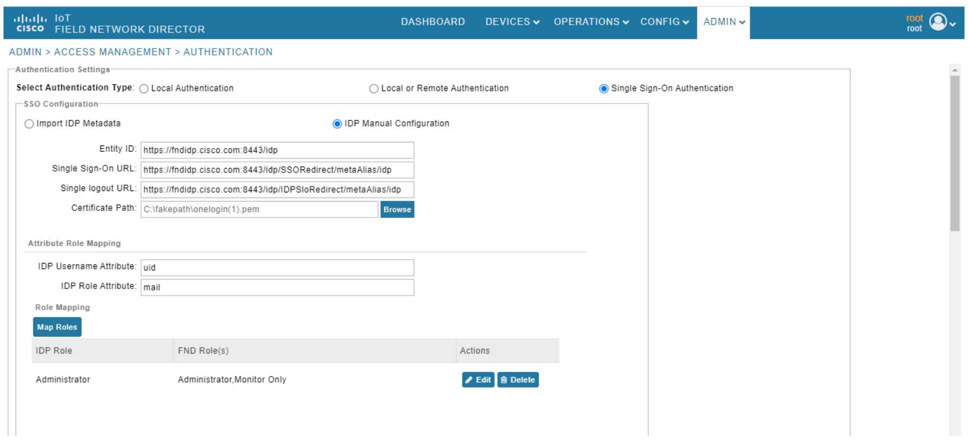
**Step 3** Select the **IDP Manual Configuration** radio button.

**Step 4** In the SSO Configuration section, provide the following information:

| Fields | Description |
|---|---|
| Entity ID | IDP URL. |
| Single Sign-On URL | Target URL of IDP, where the service provider sends the authentication request message. |
| Single logout URL | URL location of IDP, where the service provider sends the SLO request. |
| Certificate Path | Browse and select the public certificate keys for IDP. |

**Step 5** Enter **IDP Username Attribute** and **IDP Role Attribute**.

**Note** The username and role attributes specified are validated with the username and role in the SAML XML response. The same information is configured on the IDP server as well.




**Step 6** Click **Map Roles**. The Role Mapping window appears.

**Step 7** Enter **IDP Role**.

**Step 8** Check the **FND Role** check box.

**Note** You can map one IDP role to one or more FND roles.

**Step 9** Click **Map**.

The Role Mapping section displays the mapping of IDP role to FND roles.

**Step 10** Click **Save**. The IDP data gets saved in the IDP_SERVER_DETAILS DB table.

**Step 11** Click **Export FND Metadata** to export the FND metadata file.

The generated XML file is saved in the local drive. The file contains information on the service provider (entity ID, single sign-on URL, single logout URL, and certificate path). This file is used for importing IDP to avoid manual configuration.

## Importing IDP Metadata for SSO Authentication

To import IDP metadata for SSO authentication:

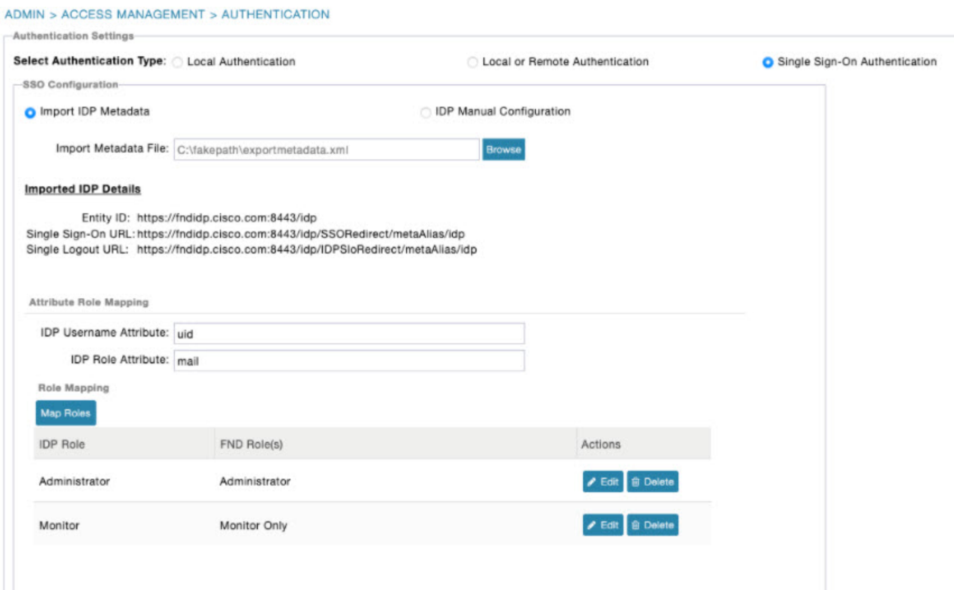
**Step 1** Choose **ADMIN** > **Access Management** > **Authentication**.

**Step 2** In the Authentication Settings page, select the **Single Sign-On Authentication** radio button.

**Step 3** Select the **Import IDP Metadata** radio button.

**Step 4** Browse and select **Import Metadata File** from the local drive.

On importing, the **Imported IDP Details** section has information on Entity ID, Single Sign-On URL, and Single Logout URL.




**Step 5** Enter **IDP Username Attribute** and **IDP Role Attribute**.

> **Note** The username and role attributes specified are validated with the username and role in the SAML XML response. The same information is configured on the IDP server as well.

**Step 6** Click **Map Roles**. The Role Mapping window appears.

**Step 7** Enter **IDP Role**.

**Step 8** Check the **FND Role** check box.

> **Note** You can map one IDP role to one or more FND roles.

**Step 9** Click **Map**.

The Role Mapping section displays the mapping of IDP role to FND roles.

**Step 10** Click **Save**.

The IDP data gets saved in the IDP_SERVER_DETAILS DB table.

**Step 11** Click **Export FND Metadata** to export the FND metadata file.

The generated XML file is saved in the local drive. The file contains information on the Service Provider information (entity ID, single sign-on URL, single logout URL, and certificate path). This file is used for importing IDP to avoid manual configuration.

## Limitations for SSO Authentication

- Supports only browser-based logins; therefore, Northbound (NB) API is not supported.

> **Note** NB API needs local authentication, which SAML does not support.

- Supports only root domain.

## Logging out of SSO

- On successful logout, IDP login page appears. For example, if you manually log out of FND, then FND sends a SAML logout request to IDP and IDP in-turn logs out of the third-party application as well .
- On inactive session, FND resends SAML authentication request to IDP to see if the session is still active.

## Fallback URL When SSO Fails

Use the FND console URL as a fallback URL to configure the authentication settings when SSO login fails. The root users and the users with administrative privileges only can access the FND console URL.

| | |
|---|---|
| FND Console URL | `https://<FND-IP>/console/home.seam` |

> **Note** The FND console URL is not used for the IDP authentication.

# Managing Users

This section explains about managing users.

## Adding Users

To add users to IoT FND:

**Step 1** Choose **ADMIN** > **Access Management** > **Users**.

**Step 2** Click + icon to **Add User**.

**Step 3** Enter the following user information:

| Field | Description |
|---|---|
| User Name | Enter the user name. |
| New Password | Enter the password. The password must conform to the IoT FND password policy. |
| Confirm Password | Re-enter the password. |
| Time Zone | Choose a time zone from the drop-down menu. |

**Step 4** Click **Assign Domain** to open the configuration panel:

a) Select the domain name from the drop-down menu.
b) Assign Role(s) and its associated Permission for the user by selecting the role check box.

**Step 5** Click **Assign to save the entries**.

IoT FND creates a record for this user in the IoT FND database.

**Step 6** To add the new user, click the **Disk** icon; otherwise, click **X** to close the window and return to the Users page.

**Note** A new user account is enabled by default. This means that the user can access IoT FND.

You can make future edits to the User entry by selecting the Edit or Delete buttons that appear under the Actions column.

# Enabling Users

You must enable the user account for users to access IoT FND. When users log in for the first time, IoT FND prompts them to change their password.

To enable user accounts in IoT FND:

**Step 1** Choose **Admin** > **Access Management** > **Users**.
**Step 2** Check the check boxes for the user account(s) to enable.
**Step 3** Click the solid person icon.
**Step 4** To confirm action, click **Yes**.

# Editing Users

To edit user settings in IoT FND:

**Step 1** Choose **Admin** > **Access Management** > **Users**.
**Step 2** To edit user credentials:

a) Click the user name link.
b) Edit the role assignments.

c) Click **Save**.

# Resetting Passwords

As the root user of the Linux server on which IoT FND runs, you can reset your password and use the password utility to reset the password for any other IoT FND user.

To reset a password:

Enter this command **[root@yourname-lnx1 bin}**`#./password_admin.sh root`

IoT FND manages its own user account database; therefore, you must add all new local users from the IoT FND user interface at the **Admin** > **Access Management** > **Users** page.

**Note** Remote users are automatically added to the database. You can also enable, disable, edit, or delete users on this page.

**Note** A user with a disabled account cannot log in until an administrator enables their account. After a user account is active, the user must reset their password. There is no limit to the number of users that you can define on the system other than the available database storage.

**Note** Starting from Cisco IoT FND release 4.8.0, in case you forgot your Cisco IoT FND password, the user with the role of **administrator** can assist you in resetting your password without you having to know your old password.

# Viewing Users

To view IoT FND users:

Choose **ADMIN** > **Access Management** > **Users** to open the Users page.

IoT FND displays this information about users:

| Field | Description |
|---|---|
| User Name | Specifies the user name. |
| Default Domain | Shows the default domains for each user. |
| Enabled | Indicates whether the user account is enabled. |
| Time Zone | Specifies the user’s time zone. |
| Roles | Specifies the roles assigned to the user. |
| Audit Trail | A link to the user’s audit trail. |

| Field | Description |
|---|---|
| Remote User | Indicates whether the user account is stored locally. If the value is false, the user account is stored in Active Directory and is accessed via the RADIUS server configured in the Remote Authentication page (**ADMIN** > **Access Management** > **Users** > **Remote Authentication**). |

## Deleting Users

Deleting user accounts removes user preferences such as the default map location from the system. Disable a user account to temporarily deactivate it.

To delete users from IoT FND:

**Step 1** Choose **ADMIN** > **Access Management** > **Users**.

**Step 2** Check the box next to the User Name entry that you want to remove from the User Account list.

**Step 3** To delete the entry, click the trash can icon.

**Step 4** To confirm action, click **Yes**.

## Disabling Users

To prevent users from accessing IoT FND, disable their accounts. Disabling user accounts does not delete their records from the IoT FND database.

To disable user accounts in IoT FND:

**Step 1** Choose **Admin** > **Access Management** > **Users**.

**Step 2** Check the check boxes for the user account(s) to disable.

**Step 3** Click the outlined person icon.

**Note** If you disable a user account, IoT FND resets the user password.

**Step 4** To confirm action, click **Yes**.

# Managing Domains

In IoT FND, you can add domains and define local or remote administrators and users.

# Viewing Domains

To view IoT FND domains, open the Domains page (**ADMIN** > **Access Management** > **Domains**).


IoT FND displays the following information about domains:

| Field | Description |
|---|---|
| Domains | Specifies domains with root or non-root access.<br>• Root - The Admin user who defines root access for other users while creating a domain.<br>• Non-root - Admin creates the domain without root access. |
| Users | Defines local or remote administrators and users. |
| Description | Provides a brief information about the domain. |
| Hierarchy | Specifies the level of domains where the root domain is the top most in the structure. |
| CGK1K | Lists the total number of CGR1K devices mapped to the domain. |
| C800 | Lists the total number of C800 devices mapped to the domain. |
| IR800 | Lists the total number of IR800 devices mapped to the domain. |
| LORAWAN | Lists the total number of LORAWAN devices mapped to the domain. |
| IR500 | Lists the total number of IR500 devices mapped to the domain. |
| ENDPOINT | Lists the total number of ENDPOINT devices mapped to the domain. |
| CELL_ENDPOINT | Lists the total number of CELL ENDPOINT devices mapped to the domain. |
| IR8100 | Lists the total number of IR8100 devices mapped to the domain. |

# Adding Domains

The user can add a domain and map an existing user to the created domain or create a new user and map the domain to the newly created user.

To add a domain in IoT FND:

**Step 1** Choose **ADMIN** > **Access Management** > **Domains**.

**Step 2** Click + icon to open the **Add Domain** page.

**Step 3** Enter the following domain information.

| Field | Description |
|---|---|
| Domain Name | Enter a name for the domain. |
| Domain Hierarchy | Specify the level of domains, where the root domain is the top most in the structure. |
| Domain Administrator | Indicates the user who can modify any information in the domain. You can choose either one of the following options:<br>• Local - The domain administrator can add new user or choose an existing user.<br>• Remote - The domain administrator can only add new users. |
| User Name | Enter the name of the new user. |
| Password | Enter the password. |
| Confirm Password | Re-enter the password. |
| Existing User | Select the existing user from the **Existing User** drop-down list. |

The License allocation section shows the devices available along with the following information:

- **Licenses Assigned**
- **Licenses Consumed**
- **Licenses Available**

Enter the number of licenses that can be assigned under each device for the newly created domain in the **Licenses Assigned** section.

**Step 4** Click the Disk icon; otherwise, click **X** to close the window and return to the **Domains** page.

# Editing Domains

To edit user settings in IoT FND:

**Step 1** Choose **ADMIN** > **Access Management** > **Domains**.

**Step 2** To edit domain details:

a) Click the domain link.
b) Edit the licenses assigned for each device type.
c) Click the Disk icon to save the details; otherwise, click **X** to close the window and return to the **Domains** page.

## Deleting Domains

The user cannot delete a domain if any device or user is associated with the domain. The root domain cannot be deleted.

To delete domains from IoT FND:

**Step 1** Choose **ADMIN** > **Access Management** > **Domains**.
**Step 2** Check the box next to the domain name that you want to remove from the Domain list.
**Step 3** To delete the entry, click the trash can icon.
**Step 4** To confirm action, click Yes.

# Managing Roles and Permissions

Roles define the type of tasks specific role IoT FND users can perform. The operations the user can perform are based on the permissions enabled for the role.

IoT FND lets you assign a system-defined role to a user such as admin or operator (**ADMIN** > **Access Management** > **Roles**). The operations the user can perform are based on the permissions enabled for the role.

## Basic User Permissions

The table describes basic IoT FND user permissions.

***Table 8: IoT FND User Permissions***

| Permission | Description |
|---|---|
| Add/Modify/Delete Devices | Allows users to import, remove, and change router and endpoint devices. |
| Administrative Operations | Allows users to perform system administration operations such as user management, role management, and server configuration settings. |
| Asset Management | Allows users to view details on Assets (non-Cisco equipment) that are associated with an FND managed device. |
| Battery Endpoint Operations | IoT FND supports the following special battery-powered endpoints:<br>• ACT, BACT, CAM<br>• L+G LFN<br>The interaction with these endpoints should be kept to a minimum in order to reduce draw down of battery within the endpoints. |
| Endpoint Certificate Management | Permission for erasing node certificates on IR500 gateways. |

| Permission | Description |
|---|---|
| Endpoint Configuration | Allows users to edit configuration templates and push configuration to mesh endpoints. |
| Endpoint Firmware Update | Allows users to add and delete firmware images and perform ME firmware update operations. |
| Endpoint Group Management | Allows users to assign, remove, and change devices from ME configuration and firmware groups. |
| Endpoint Reboot | Allows users to reboot the ME device. |
| GOS Application Management | Allows uses to add and delete Guest OS applications. |
| Issue Management | Allows users to close issues. |
| Label Management | Allows users to add, change, and remove labels. |
| LoRA Modem Reboot | Permission for rebooting LoRaWAN gateways and modems. |
| Manage Device Credentials | Allows users to view router credentials such as Wi-Fi pre-shared key, admin user password, and master key. |
| Manage Head-End Devices Credentials | Allows users to view the ASR admin NETCONF password. |
| NB API Audit Trail | Allows users to query and delete audit trails using IoT FND NB API. |
| NB API Device Management | Allows users to add, remove, export, and change router and endpoint devices using IoT FND NB API. |
| NB API Endpoint Group Management | Permission for accessing the Group Management NB API. |
| NB API Endpoint Operations | Allows users to manage endpoint operations using IoT FND NB API. |
| NBAPI Event Subscribe | Allows users to search events, subscribe and unsubscribe from events (including Outage events) using IoT FND NB API. |
| NB API Issues | Allows users to search issues. |
| NB API Orchestration Services | Permission for IOK Orchestration Service to access the Orchestration NB APIs. |
| NB API Reprovision | Allows users to reprovision devices using IoT FND NB API. |
| NB API Rules | Allows users to search, create, delete, activate, and deactivate rules using IoT FND NB API. |
| NB API Search | Allows users to search devices, get device details, group information, and metric history using IoT FND NB API. |
| NB API Tunnels | Permission for accessing the Tunnel Status NB APIs. |
| Password Policy | Provides a flexible password policy system to manage user passwords. It contains configurable properties for password expiration, failed login attempts, password strength and other aspects of password maintenance. |
| Router Configuration | Allows users to edit router configuration templates and push configuration to routers. |
| Router File Management | Permission for managing router files on the Device File Management GUI page. |

| Permission | Description |
|---|---|
| Router Firmware Update | Allows users to add and delete firmware images and perform firmware update operations for routers. |
| Router Group Management | Allows users to assign, remove, and change device assignments to router configuration and firmware groups. |
| Router Reboot | Allows users to reboot the router. |
| Rules Management | Allows users to add, edit, activate, and deactivate rules. |
| Security Policy | Allows users to block mesh devices, refresh mesh keys, and so on. |
| Tunnel Provisioning Management | Allows users to manage tunnel groups, edit/apply tunnel-related templates, and perform factory reprovisioning. |
| View Device Configuration | Allows users to view field device configuration. |
| View Head-End | Allows users to view ASR configuration, tunnel provisioning, and HER events. |

# System-Defined User Roles

**Note** The system-defined Root role cannot be assigned to users.

The table lists system-defined roles. These roles cannot be modified.

*Table 9: System-defined User Roles*

| Role | Description |
|---|---|
| Administrator | This role combines these basic permissions:<br>• Administrative Operations<br>• Label Management<br>• Rules Management |
| Endpoint Operator | This role combines these basic permissions:<br>• Label Management<br>• Endpoint Configuration<br>• Endpoint Firmware Update<br>• Endpoint Group Management<br>• Endpoint Reboot |
| Monitor Only | Optional role. This role is not defined for every user. |

| Role | Description |
|---|---|
| North Bound API | This role combines these basic permissions:<br>• NB API Audit Trail<br>• NB API Device Management<br>• NB API Endpoint Operations<br>• NB API Event Subscribe<br>• NB API Orchestration Service<br>• NB API Rules<br>• NB API Search |
| Root | The system-defined root role cannot be assigned to users. This role can use the password utility to reset the password for any IoT FND user. |
| Router Operator | This role combines these basic permissions:<br>• Label Management<br>• Router Configuration<br>• Router Firmware Update<br>• Router Group Management<br>• Router Reboot |

# Custom User Roles

In IoT FND you can define custom roles. For each role you create, you can assign it one or more basic user permissions (see Basic User Permissions, on page 57). These permissions specify the type of actions users with this role can perform.

# Adding Roles

To add IoT FND user roles:

**Step 1** Choose **ADMIN** > **Access Management** > **Roles**.

**Step 2** Click **Add**.

**Step 3** Enter the name of the role.

**Step 4** Check the appropriate check boxes to assign permissions.

**Step 5** Click **Save** .

**Step 6** To continue to add roles, click **Yes**; otherwise, click **No** to return to the Roles page.

# Editing Roles

You cannot edit system-defined roles, but you can edit custom roles.

To edit IoT FND custom roles:

**Step 1** Choose **ADMIN** > **Access Management** > **Roles**.
**Step 2** Click the role to edit.
**Step 3** Make changes to the permission assignments by checking or unchecking the relevant check boxes.
**Step 4** Click **Save**.

# Deleting Roles

You cannot delete a custom role if it is in use.

To delete IoT FND user roles:

**Step 1** Choose **ADMIN** > **Access Management** > **Roles**.
**Step 2** Check the check boxes of the roles to delete.
**Step 3** Click **Delete**.
**Step 4** Click **Yes**.
**Step 5** Click **OK**.

# Viewing Roles

To view IoT FND user roles:

**Step 1** Choose **ADMIN** > **Access Management** > **Roles**.

For every role, IoT FND lists the Users assigned to this role and the RADIUS Server VSA.

**Step 2** To view permission assignments for the role, click the role link.

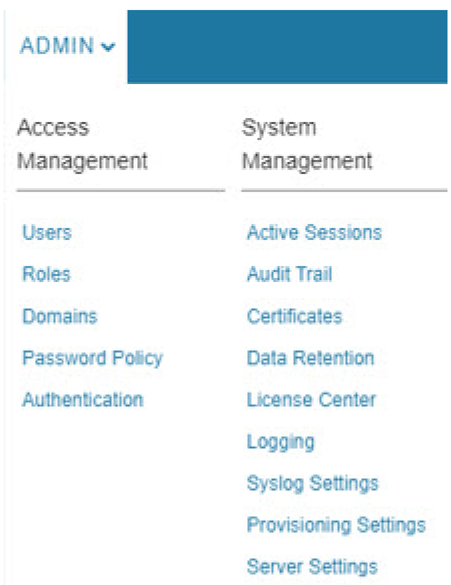
CHAPTER 4

# Managing System Settings

This section describes how to manage system settings.

> **Note** To manage system settings, you must be logged in either as root or as a user with Administrative Operations permissions.

System settings are managed from the **ADMIN** > **System Management** menu.



# Managing Active Sessions

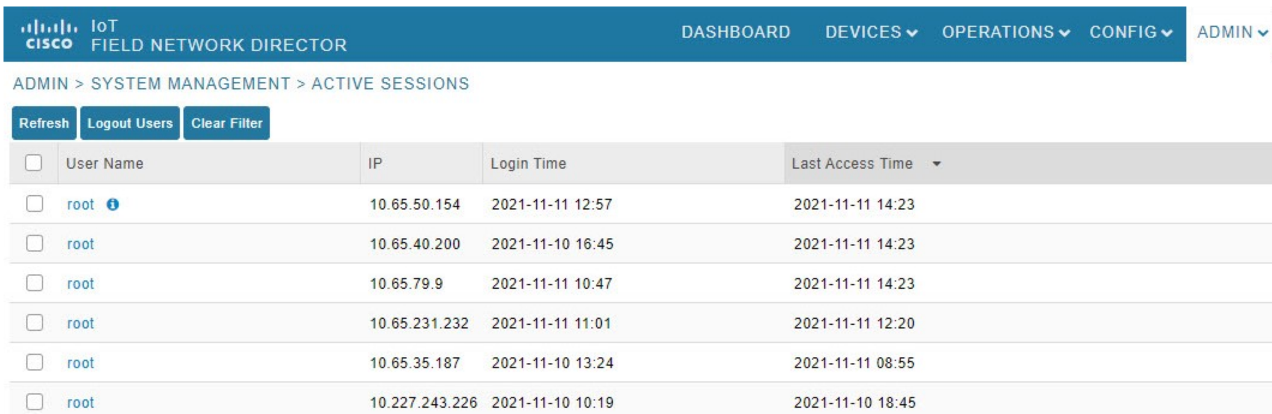
IoT FND tracks active user sessions and lets you log out users.

## Viewing Active Sessions

To view active user sessions:

Choose **ADMIN** > **System Management** > **Active Sessions**.

IoT FND displays the Active Sessions page.




The table describes the Active Session fields:

| Field | Description |
|---|---|
| User Name | The user name in the session record. To view user settings, click the user name. |
| IP | The IP address of the system the user employs to access IoT FND. |
| Login Time | The log in date and time for the user. |
| Last Access Time | The last time the user accessed the system. |

**Tip** Click the **Reload** button (upper-left hand corner) to update the users list.

## Logging Out Users

To log out an IoT FND user:

**Step 1** Choose **ADMIN** > **System Management** > **Active Sessions**.

**Step 2** Select the check boxes for those users you want to log out.

**Step 3** Click **Logout** Users.

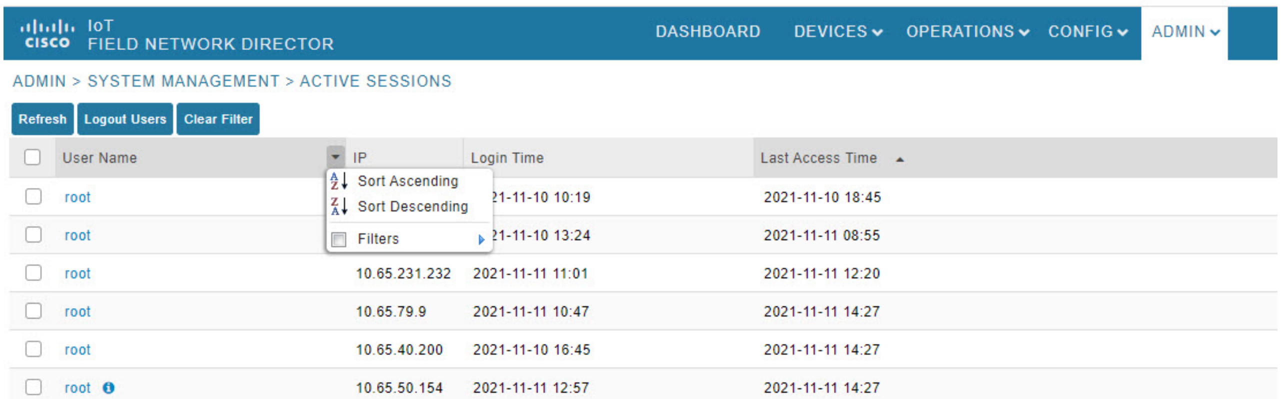
**Step 4** Click **Yes** to confirm logout of the users.

# Filtering the Active Sessions List

To filter the Active Sessions list using column filtering:

**Step 1** Choose **ADMIN** > **System Management** > **Active Sessions**.

**Step 2** Hover the mouse over the User Name column heading to expose the filter icon (triangle). Enter the user name or the first characters of the user name to filter the list.




For example, to list the active sessions for the root user, enter **root**.

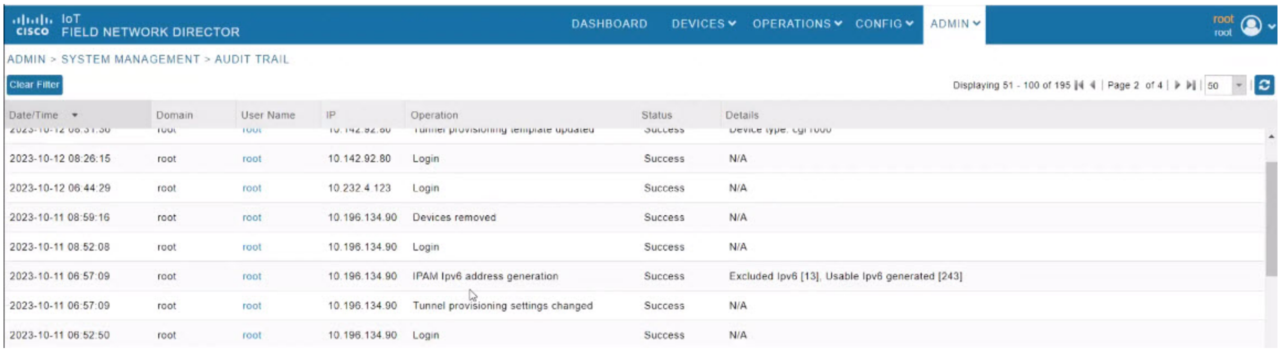
**Tip** To remove the filter, from the User Name drop-down menu, clear the **Filters** check box or click **Clear Filter**.

# Displaying the Audit Trail

Use the audit trail to track IoT Field Network Director user activity.

To display the Audit Trail:

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




The table below describes the Audit Trail Fields:

| Field | Description |
|---|---|
| Date/Time | Date and time of the operation. |
| Domain | Specifies domains with root or non-root access.<br>• Root - The Admin user who defines root access for other users while creating a domain.<br>• Non-root - Admin creates the domain without root access. |
| User Name | The user who performed the operation. To view user settings, click the user name. |
| IP | IP address of the system that the user employs to access IoT FND. |
| Operation | Type of operation performed. |
| Status | Status of the operation. |
| Details | Operation details. |

**Tip** Click the **Refresh** icon (far right) to update the list.

# Filtering the Audit Trail List

To filter the Audit Trail list using column filtering:

**Step 1** Choose **ADMIN** > **System Management** > **Audit Trail**.

**Step 2** From the User Name drop-down menu, pass over Filters option and in the field that appears enter the user name or the first characters of the user name to filter the list.

For example, to list the Audit Trail entries for the user jane, enter **jane**.

**Tip** To remove the filter, from the User Name drop-down menu, uncheck the **Filters** check box or click **Clear Filter (left of the screen)**.

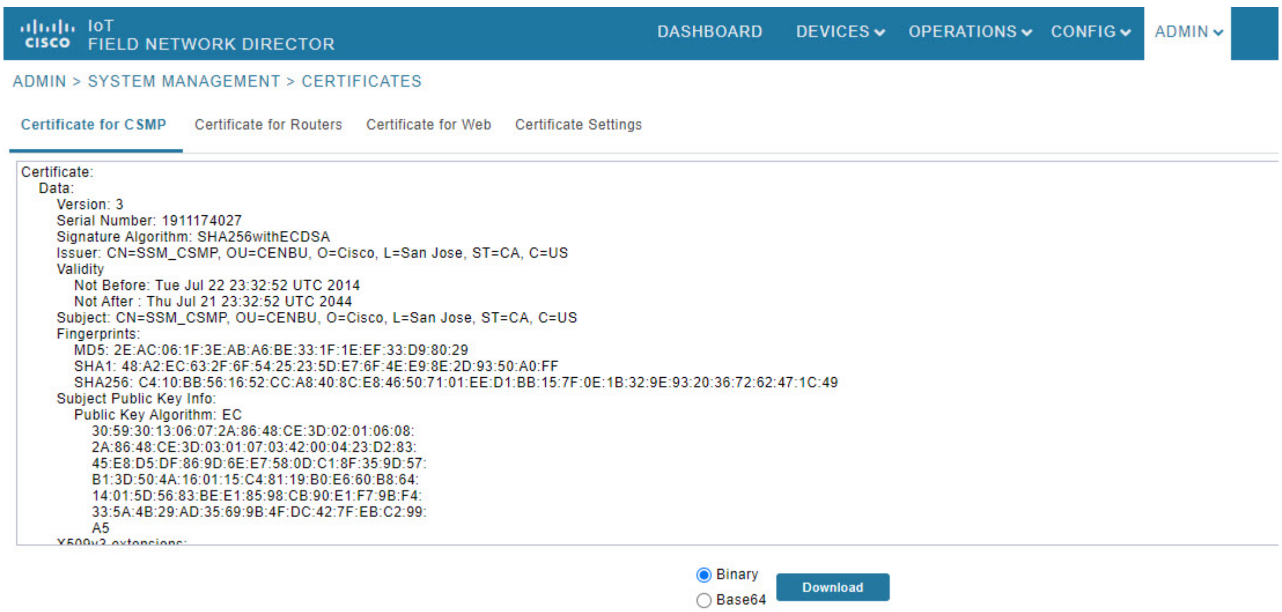
# Managing Certificates

The Certificates page displays the certificates for CSMP (CoAP Simple Management Protocol), and Web certificates used by IoT FND and lets you download these certificates.

To display the CSMP, and Web certificates:

**Step 1** Choose **ADMIN** > **System Management** > **Certificates**.

**Step 2** To view a certificate, click its corresponding heading (such as Certificate for Routers).




**Step 3** To download a certificate, select encoding type (**Binary** or **Base64**) radio button, and then click **Download**.

For more information about certificates, see Generating and Installing Certificates in the Cisco IoT Field Network Director Installation Guide.

# Configuring CA Certification to verify the App Signature

Allows you to import and add a trust anchor to the default profile for a Cisco IOx device that is being managed by IoT FND such as IC3000 or IR800. (The default profile is not visible to the user). You can enable this capability on the Application Security tab of the Certificate page.

The Application Security tab only appears when both of the following conditions are met:

- The user should have application management permission.

- At least one IOx device is being managed such as IC3000 or IR800.

To import and add a trust anchor to a default profile for a Cisco IOx device:

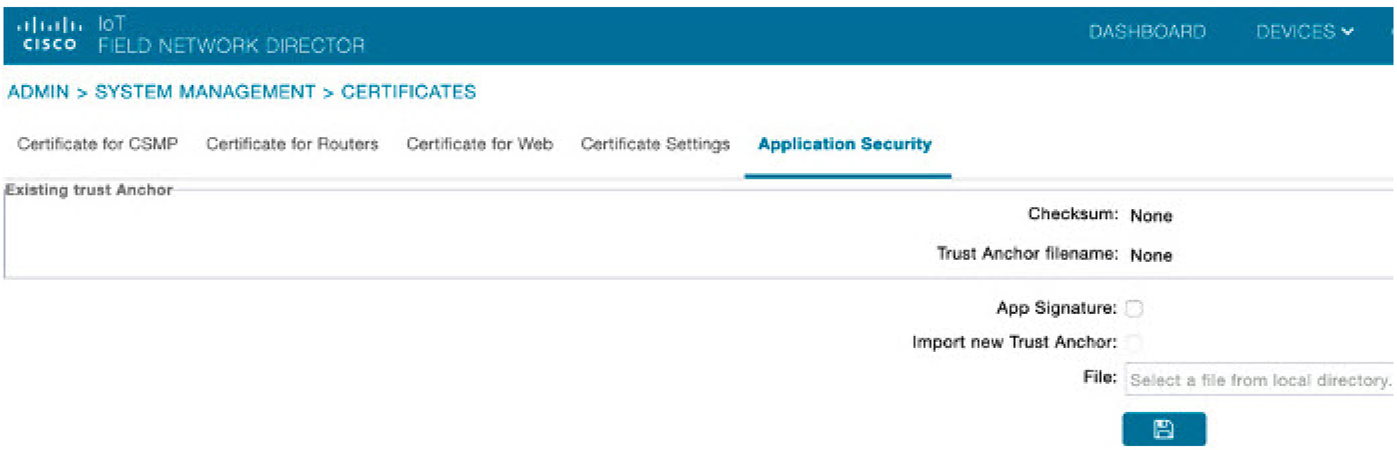
**Step 1** Choose **ADMIN** > **System Management** > **Certificates**.

**Step 2** Select the Application Security tab. The page that appears displays any existing trust anchors.

**Note** By default, no information will display for new installations or updates and the fields for Checksum and Trust Anchor will display a value of **'None'**.)

**Step 3** To import a new a new trust anchor, check the boxes next to App Signature and Import New Trust Anchor and then enter a path to the file. Click the disk icon to Save your entries. File will also be pushed to Fog Director.

**Note** After you save and reload the Certificates page, the Checksum and Trust Anchor File name appear on the page replacing the previous values of None.




# Configuring Data Retention

The Data Retention page lets you determine the number of days to keep event, issue, and metric data in the IoT FND database.

**Note** Data retention prunes events even if they have associated open issues.

To set IoT FND data retention:

**Step 1** Choose **ADMIN** > **System Management** > **Data Retention**.

**Step 2** For each of the retention categories, specify the number of days to retain the data as specified in the table.

*Table 10: Data Retention Field Allowable Maximum Values*

| Field | Minimum Values in Days | Maximum Values in Days | Default Values in Days |
|---|---|---|---|
| Keep Event data for | 1 | 90 | 31 |
| Keep Endpoint Firmware Operation data for | 7 | 180 | 7 |
| Keep Historical Dashboard data for | 1 | 90 | 62 |
| Keep Dashboard data for | 1 | 7 | 7 |
| Keep Historical Endpoint Metrics for | 1 | 7 | 7 |
| Keep Closed Issues data for | 1 | 90 | 30 |
| Keep JobEngine data for | 1 | 30 | 30 |
| Keep Historical Router Statistics data for | 1 | 90 | 30 |
| Keep Device Network Statistics data for | 1 | 7 | 7 |
| Keep Service Provider down routers data for | 1 | 31 | 31 |

**Step 3** To save the maximum values, click the disk icon.

**Step 4** To revert to default settings, click **Reset**.

# Managing Licenses

The License Center page, **ADMIN** > **System Management** > **License Center**, lets you view and manage license files.

**Note** IoT FND performs license enforcement when importing devices. If you add licenses, IoT FND only allows the permitted number of devices to be imported, as defined in the licenses.

Without licenses, IoT FND allows only 3 routers and 100 mesh endpoints.

## Adding License Files

To add a license file:

**Step 1** Choose **ADMIN** > **System Management** > **License Center**.

**Step 2** Click **Classic Licenses**.

**Step 3** Click **Add**. An **Upload License File** window appears.

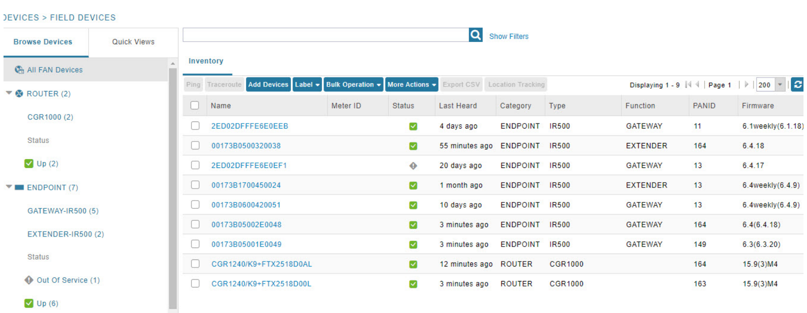
**Step 4** Click **Browse** to locate the license file and then click **Open**.

**Step 5** Click **Upload**.

**Note** The license is consumed only by devices in the Managed device category. The devices in OOS device category do not consume license.

**Step 6** Click **Reset** to cancel the selected file and search for another file.

**Note** If you import more devices that your Classic License allows, the import process will not fail. Any devices imported beyond the license limit will be marked as 'Unmanaged' and listed under Status in the Browse Devices panel. No other license types other than Classic Licenses support this capability.




# Viewing License Summary

To view IoT FND license summary:

**Step 1** Choose **ADMIN** > **System Management** > **License Center**.

**Step 2** Click **License Summary**. A list of devices with their license information is displayed.

**Note** The License Summary page displays the license information for devices in the Managed status only. The OOS devices are not displayed on this page, as they do not consume the license.


For every license, IoT FND displays the information as described in the table.

**Note** IR500s use mesh endpoint licenses and require no special license.

*Table 11: Device License Summary Information*

| Field | Description |
|---|---|
| Package Name | Name of license package. |
| CGR1K Licenses Consumed / Total | Lists the number of CGR1K devices currently active in the network and the maximum number of CGR1000s supported by the license. |
| C800 Licenses Consumed / Total | Lists the number of C800 devices currently active in the network and the maximum number of C800 devices supported by the license. |
| IR800 Licenses Consumed / Total | Lists the number of IR800 (IR809 and IR829) devices currently active in the network and the maximum number of IR800 devices supported by the license. |
| LORAWAN Licenses Consumed / Total | Lists the number of Cisco interface modules for LoRaWAN devices currently active in the network and the maximum number of Cisco interface modules for LoRaWAN devices that are supported by the license. |
| IR500 Licenses Consumed / Total | Lists the number of IR509 devices currently active in the network and the maximum number of IR509 devices supported by the license. |
| ENDPOINT Licenses Consumed / Total | Lists the number of endpoint devices currently active in the network and the maximum number of endpoint devices supported by the license. |
| CELL_ENDPOINT Licenses Consumed / Total | Lists the number of cell_endpoint devices currently active in the network and the maximum number of cell_endpoint devices supported by the license. |
| IR8100 Licenses Consumed / Total | Lists the number of IR8100 devices currently active in the network and the maximum number of IR8100 devices supported by the license. |
| Days Until Expiry | Number of days remaining until the license expires. |

*Table 12: Feature History*

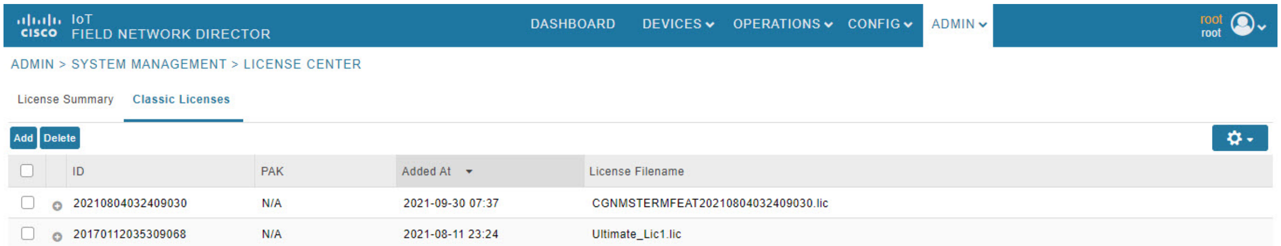
| Feature Name | Release Information | Description |
|---|---|---|
| Enable 8140 Licensing | IoT FND 4.8 | The licensing for device type IR8100 is now supported in FND. The license PID for IR8100 devices is IOTFND-IR8140. After adding the license, go to **ADMIN** > **System Management** > **License Center** > **License Summary** page to view the licenses consumed and total license count for IR8100 devices.<br><br>It is also possible to allocate licenses for each domain. Go to **ADMIN** > **Access Management** > **Domains**. In the Edit Domain page, you can allocate licenses for the IR8100 devices. |

# Viewing License Files

To view IoT FND license files:

**Step 1** Choose **ADMIN** > **System Management** > **License Center**.

**Step 2** Click **Classic Licenses** to display details on all active licenses.




For every file, IoT FND displays the fields as described in the table:

*Table 13: License File Fields*

| Field | Description |
|---|---|
| ID | License ID. |
| PAK | Number for issuing license fulfillment. Displays as N/A. |
| Added At | Date and time the license was added to IoT FND. |
| License Filename | Filename of the license. |

# Deleting the License Files

**Note** Ensure that you have access to license files before deleting existing license files. Without licenses, IoT FND only allows registration of 3 routers and 100 mesh endpoints.

To delete a single license or multiple license files:

**Step 1** Choose **ADMIN** > **System Management** > **License Center**.

**Step 2** Click **Classic Licenses**.

**Step 3** Check the license file ID check box that you want to delete.

**Step 4** Click **Delete**.

**Note** On deleting the license file, devices in Out of Service (OOS) status move to Unmanaged status. If license is added again, the devices move back to OOS status.

**Step 5** Click **Yes** to confirm deletion or click **No** to cancel the action.

# Managing Logs

This section explains about configuring and downloading logs.

## Configuring Log Settings

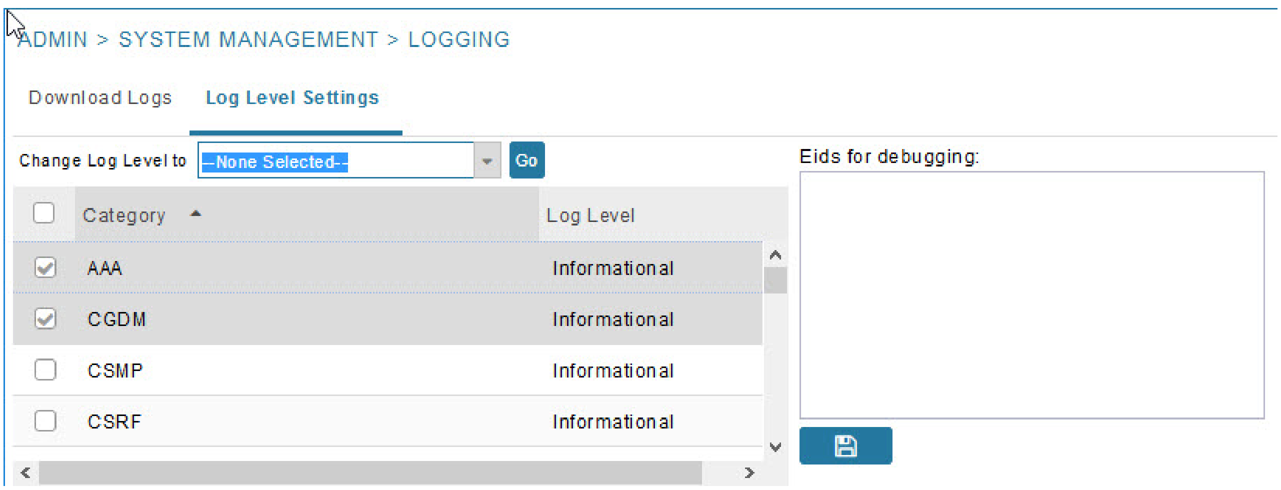
IoT FND lets you change the logging level for the various log categories and download the logs. Logs incur a certain amount of disk space. For example, for 5 million meters at an 8-hour reporting interval and 5000 routers at a 60-minute periodic inventory notification, disk consumption is approximately 7MB/sec. Ensure that your server has enough disk space to contain your logs.

To configure the logging level:

**Step 1** Choose **ADMIN** > **System Management** > **Logging**.

**Step 2** Select **Log Level Settings**.

**Step 3** Check the check boxes of all logging categories to configure.




**Step 4** From the **Change Log Level** drop-down menu, choose the logging level setting (**Debug or Informational**).

- To generate all possible logging messages, use the **Debug** level.

**Note** Running the **Debug** logging category can impact performance.

- To generate a subset of these messages, use the **Informational** logging level.

**Note** The **Informational** logging level is the default for all categories when IoT FND opens. Custom logging level settings are retained between log-in sessions, but not after IoT FND restarts.

**Step 5** To apply the configuration, click **Go**.

**Note** The server.log file is rotated based on size.

**Step 6** Click the disk icon to save the configuration.

# Downloading Logs

To download logs:

**Step 1** Choose **ADMIN** > **System Management** > **Logging**.

**Step 2** Click the **Download Logs** tab.

**Step 3** Click the **Download Logs** button.

- When you click this button in a single-server deployment, IoT FND compresses the log files into a single zip file and adds an entry to the Download Logs pane with a link to the zip file.

- In IoT FND cluster deployments, when you click this button, the IoT FND server to which you are connected:
  - Compresses the log files on the server into a single zip file and adds an entry to the Download Logs pane with a link to the zip file.
  - Initiates the transfer of the log files in .zip format from the other servers to this server. As files become available, the server adds entries for these files to the Download Logs pane.

**Step 4** To download a zip file locally, click its file name.

**Tip** In a cluster environment, if you need to send log files to Cisco Support, ensure that you send the log files of all cluster servers.

# Configuring Provisioning Settings

The Provisioning Settings page (**ADMIN** > **System Management** > **Provisioning Settings**) lets you configure the IoT FND URL, DHCPv4 Proxy Client, and DHCPv6 Proxy Client settings required for IoT FND to create tunnels between routers and ASRs (Provisioning Settings page). For an example of tunnels as used in the IoT FND, see Tunnel Provisioning Configuration Process topic in the Managing Tunnel Provisioning chapter.

During Zero Touch Deployment (ZTD), you can add DHCP calls to the device configuration template for leased IP addresses.

**Note** For Red Hat Linux 7.x server installations, you must configure specific IPv4 and IPv6 addresses from the IoT FND Linux host server to which to bind DHCP IPv4 and IPv6 clients by setting the following values in IoT FND:

| | |
|---|---|
| **ADMIN** > **Provisioning Settings** > **DHCPv6 Proxy Client** > **Client Listen Address** | Set the value to the IPv6 address of the interface to use to obtain IPv6 DHCP leases from the DHCP server. The default value is "::". Change the default setting to an actual IPv6 address on the Linux host machine. |
| **ADMIN** > **Provisioning Settings** > **DHCPv4 Proxy Client** > **Client Listen Address** | Set the value to the IPv4 address of the interface to use to obtain IPv4 DHCP leases from the DHCP server. The default value is "0.0.0.0". Change the default setting to an actual IPv4 address on the Linux host machine. |

**Note** To configure tunnel and proxy settings, you must be logged in either as root or as a user with Administrative Operations permissions.

Under **ADMIN** >**System Management** > **Provisioning Setting** page, the CSMP optimization settings help to configure the timeout to acquire lock when processing the csmp messages. By default, the timeout value is 5 seconds which can be configured between 1 to 30 seconds.

**Note** This csmp setting is applicable only for Oracle deployments.

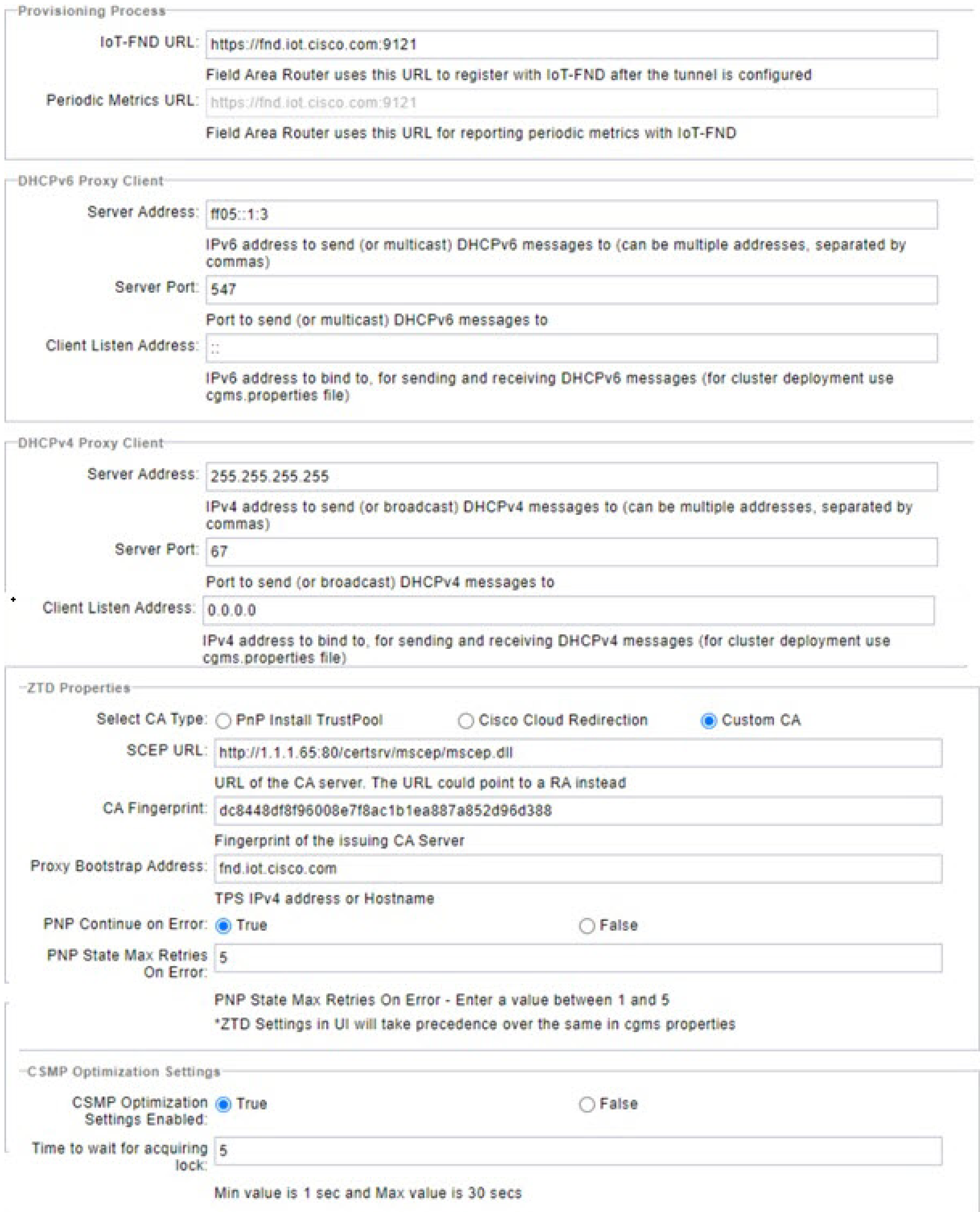
If the timeout happens, then during registration, the following message is displayed in the server.log file.

```
"Failed to acquire lock for <Endpoint Eid> during registration.
Another Operation seems to be in progress."
```

During csmp notification, the following log message is displayed in the server.log file when handing csmp messages.

```
"Failed to acquire lock to update Endpoint Status. Another Operation seems to be in progress."
```

**Provisioning Settings Page**


Provisioning Process
IoT-FND URL:
https://fnd.iot.cisco.com:9121
Field Area Router uses this URL to register with IoT-FND after the tunnel is configured
Periodic Metrics URL:
https://fnd.iot.cisco.com:9121
Field Area Router uses this URL for reporting periodic metrics with IoT-FND
DHCPv6 Proxy Client
Server Address:
ff05::1:3
IPv6 address to send (or multicast) DHCPv6 messages to (can be multiple addresses, separated by commas)
Server Port:
547
Port to send (or multicast) DHCPv6 messages to
Client Listen Address:
::
IPv6 address to bind to, for sending and receiving DHCPv6 messages (for cluster deployment use cgms.properties file)
DHCPv4 Proxy Client
Server Address:
255.255.255.255
IPv4 address to send (or broadcast) DHCPv4 messages to (can be multiple addresses, separated by commas)
Server Port:
67
Port to send (or broadcast) DHCPv4 messages to
Client Listen Address:
0.0.0.0
IPv4 address to bind to, for sending and receiving DHCPv4 messages (for cluster deployment use cgms.properties file)
ZTD Properties
Select CA Type:
PnP Install TrustPool
Cisco Cloud Redirection
Custom CA
SCEP URL:
http://1.1.1.65:80/certsrv/mscep/mscep.dll
URL of the CA server. The URL could point to a RA instead
CA Fingerprint:
dc8448df8f96008e7f8ac1b1ea887a852d96d388
Fingerprint of the issuing CA Server
Proxy Bootstrap Address:
fnd.iot.cisco.com
TPS IPv4 address or Hostname
PNP Continue on Error:
True
False
PNP State Max Retries On Error:
5
PNP State Max Retries On Error - Enter a value between 1 and 5
*ZTD Settings in UI will take precedence over the same in cgms properties
CSMP Optimization Settings
CSMP Optimization Settings Enabled:
True
False
Time to wait for acquiring lock:
5
Min value is 1 sec and Max value is 30 secs

# Configuring the IoT FND Server URL

The IoT FND URL is the URL that routers use to access with IoT FND after the tunnel is established. This URL is also accessed during periodic inventories. During ZTD, routers transition from accessing IoT FND through the TPS proxy to using this URL, which must be appropriate for use through the tunnel.

To configure the IoT FND URL:

**Step 1** Choose **ADMIN** > **System Management** > **Provisioning Settings**.

**Step 2** In the **IoT FND URL** field, enter the URL of the IoT FND server.

The URL must use the HTTPS protocol and include the port number designated to receive registration requests. By default, the port number is 9121. For example:

```
https://nms.sgbu.example.com:9121
```

**Step 3** Click **Save**.

# Configuring DHCP Option 43 on Cisco IOS DHCP Server

To configure for IPv4, enter:

```
ip dhcp pool fnd-pool
network 192.0.2.0 255.255.255.0
default-router 192.0.2.1
option 43 ascii "5A;K4;B2;I192.0.2.215;J9125"
```

```
5 - DHCP type code 5
A - Active feature operation code
K4 - HTTP transport protocol
B2 - PnP/FND server IP address type is IPv4
I - 192.0.2.215 - PnP/FND server IP address
J9125 - Port number 9125
```

# Configuring DHCPv4 Proxy Client

To configure DHCPv4 Proxy client settings:

**Step 1** Choose **ADMIN** > **System Management** > **Provisioning Settings**.

**Step 2** Configure the DHCPv4 Proxy Client settings:

a) In the **Server Address** field, enter the address of the DHCPv4 server that provides tunnel IP addresses.

**Note** You can enter multiple addresses separated by commas. However, in most cases, you only need one server. IoT FND tries to get the tunnel IP addresses from the first server in the list. If it cannot, it moves to the next server in the list, and so on.

b) In the **Server Port** field, enter the port address on the DHCP server to send DHCPv4 requests to.

**Note** Do not change the default port number (67) unless you have configured your DHCP server to operate on a non-standard port.

c) In the **Client Listen Address** field, enter the address to bind to for send and receive DHCPv4 messages.

**Note** This is the address of the interface that the DHCP server uses to communicate with IoT FND. You can enter multiple backup addresses separated by commas.

**Step 3** Click **Save**.

## Configuring DHCPv6 Proxy Client

To configure DHCPv6 Proxy client settings:

**Step 1** Choose **ADMIN** > **System Management** > **Provisioning Settings**.

**Step 2** Configure the DHCPv6 Proxy client settings:

a) In the **Server Address** field, enter the address of the DHCPv6 server that provides tunnel IP addresses.

You can enter multiple addresses separated by commas. However, in most cases, you only need one server. IoT FND tries to get the tunnel IP addresses using DHCP protocols. If it cannot, it goes to the next server in the list and so on.

b) In the **Server Port** field, enter the port address on the DHCP server to send DHCPv6 requests.

**Note** Do not change the default port number (547) unless you have configured your DHCP server to operate on a non-standard port.

c) In the **Client Listen Address** field, enter the address to bind to for DHCPv6 send and receive messages.

This is the address of the interface that the DHCP server uses to communicate with IoT FND. You can enter multiple backup addresses separated by commas.

**Tip** For IoT FND installations where the host has multiple interfaces, the client sends requests using each listed source address. The default values, “0.0.0.0” (IPv4) and “::” (IPv6), cause the client to send requests out each interface. Usually, one interface faces the DHCP server(s). In these installations, setting the **Client Listen Address** field to the IP address of the facing interface sends all client requests out that interface.

**Step 3** Click **Save**.

# Configuring Server Settings

The Server Settings page (**ADMIN** > **System Management** > **Server Settings**) lets you view and manage server settings.

## Configuring Download Log Settings

**Note** Configuring download log settings is only required for IoT FND cluster setup.

The Download Logs page lets you configure the Keystore settings.

To configure download log settings:

**Step 1** Choose **ADMIN** > **System Management** > **Server Settings**.

**Step 2** Click the **Download Logs** tab.

**Step 3** Configure these settings:

*Table 14: Keystore Settings*

| Field | Description |
|---|---|
| Keystore Filename | Click **Upload Keystore File** to upload a Keystore file with the public key of the X.509 certificate that IoT FND uses. You can reuse the same Keystore file. |
| Keystore Password | Enter the password that IoT FND uses to access the Keystore file on start up. |
| Confirm Keystore Password | |
| FTP Password | Enter the FTP password. |
| Confirm FTP Password | |

**Step 4** To save the configuration, click the disk icon.

# Configuring Web Sessions

The Web Sessions page lets you specify the number of timeout seconds after which IoT FND terminates web sessions and logs users out.

To configure web session timeout:

**Step 1** Choose **ADMIN** > **System Management** > **Server Settings**.

**Step 2** Click the **Web Session** tab.

**Step 3** Enter the number of timeout seconds.

The valid values are 0–86400 (24 hours).

**Note** If a web session is idle for the specified amount of time, IoT FND terminates the session and logs the user out.

**Step 4** To save the configuration, click the disk icon.

# Configuring Device Down Timeouts

The **Server Settings** page allows you to configure the device down timeout globally for head-end routers (ASR) and other devices that are managed by IoT FND such as routers (CGR1000, IR800, IR8100, C800, ESR), endpoints, and gateways. On reaching the specified device down timeout interval, the devices move to

*Down* state in the IoT FND GUI based on the last heard value from the device (must be greater than the down timeout value) and the tunnel interface state. If the tunnel interface that is associated with the device is *Down* as well, then devices are marked *Down* in IoT FND GUI. Otherwise, IoT FND must wait until the tunnel interface goes *Down* to mark the device as *Down* in IoT FND GUI.

From the Device Configuration page (**CONFIG** > **DEVICE CONFIGURATION**), you can configure the device downtime for a specific router or endpoint configuration group. For more information, refer to Configuring Mark-Down Timer, on page 177

**Note** For HER, you can set the device down timeout only in the Server Settings page.

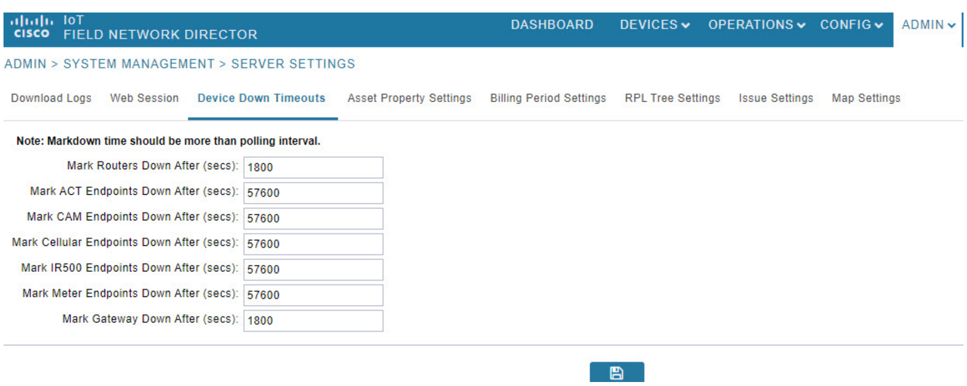
Device status changes to *Up* when IoT FND detects any of the following:

- Periodic inventory notifications
- Events
- Manual metric refreshes
- Device registrations

To configure device down timeout settings:

**Step 1** Choose **ADMIN** > **System Management** > **Server Settings**.

**Step 2** Click the **Device Down Timeouts** tab.




**Note** The device down timeout value must be greater than the corresponding polling intervals. For example, if the polling interval for routers is 30 minutes (1800 seconds), then the value in the Mark Routers Down After (secs) field must be 1801 or greater.

**Step 3** Click the disk icon to save the configuration.

# Configuring Billing Period Settings

IoT FND lets you configure the start day of the monthly billing periods for cellular and Ethernet (satellite) services.

To configure the billing period settings:

**Step 1** Choose **ADMIN** > **System Management** > **Server Settings**.

**Step 2** Click the **Billing Period Settings** tab.

**Step 3** Enter the starting days for the cellular and Ethernet billing periods.

**Step 4** From the drop-down menu, choose the time zone for the billing period.

**Step 5** To save the configuration, click the disk icon.

# RPL Tree Settings

The RPL tree routing table is generated using the CSMP messages from the Mesh nodes. The data that is obtained from the Mesh nodes is often outdated. The proposed solution is to use the RPL tree routing data from FAR which is more up to date.

IoT FND uses the command below to fetch the RPL tree data:

```
show rpl dag 1 itable | xml
```

- RPL Tree Update from Mesh Nodes
- RPL Tree Update from Routers

## RPL Tree Update from Mesh Nodes

The default RPL tree update is always set to `'Mesh Nodes'`. This is a global setting for the entire FND.

Traditionally, the RPL data has been reported to the FND by the mesh nodes as part of `IPRoute` and `IPRouteRPLMetrics` during the periodic inventory reporting.

**Global RPL Tree Settings for Entire FND**

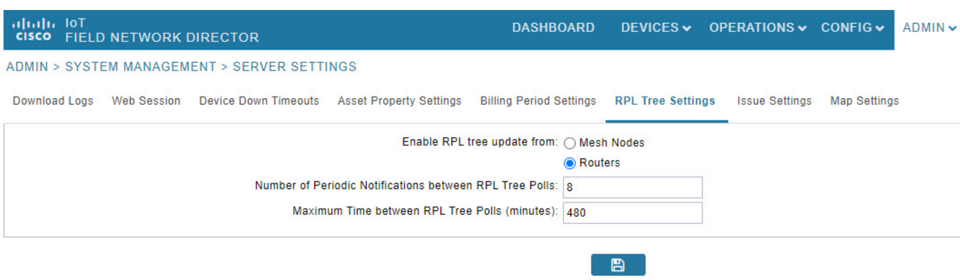



*Table 15: Global RPL Tree Settings for Entire FND*

| Field | Description |
|---|---|
| Enable RPL tree update from | Select Routers.<br>**Note** By default, Mesh Nodes is selected. |
| Number of Periodic Notifications between RPL Tree Polls | Number of periodic notification from CGR between each RPL pull. |

| Field | Description |
|---|---|
| Maximum Time between RPL Tree Polls (minutes) | Maximum time FND waits to pull RPL from a CGR for the associated PAN. |

### RPL Tree Update from Routers

As the Mesh nodes data is often outdated, the proposed solution is to use the RPL tree routing from FAR, which is more up to date. The RPL tree is not pushed from the FAR with the periodic notification. Therefore, the FND explicitly needs to pull the RPL tree at regularly configured intervals based on the Device Configuration Group properties. The FND depends on the periodic notification to determine when to poll next for the RPL tree. The FND is configured to poll the FAR for RPL tree update after every "N" periodic notifications. At times, some periodic notifications are missed. If that happens, after an absolute maximum time value, the RPL tree is fetched from the FAR.

The FAR pulls at a much higher frequency than the mesh nodes. Therefore, the RPL data is more accurate and provides a snapshot of entire PAN at any given point in time. The FND invokes **show rpl dag 1 itable** command on the CGR to obtain the RPL tree for the associated PAN.

**Device Configuration Group Properties**

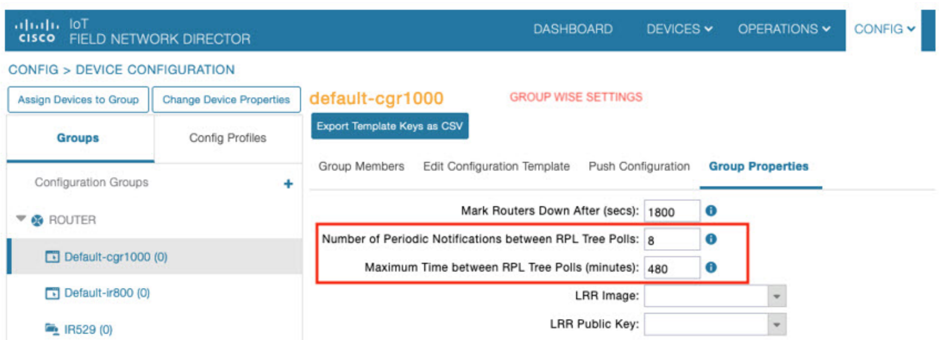



*Table 16: Device Configuration Group Properties*

| Field | Description |
|---|---|
| **RplTreePullingCycle** | The number of periodic notification intervals.<br>**Note** The default maximum number of **RplTreePullingCycle** is 8. |
| **RplTreePullingMaxTime** | The maximum time interval between the pulls in minutes.<br>**Note** The default maximum time between pulls is 480 minutes (8 * 60). |

When processing a periodic notification event, if either of these Table 16: Device Configuration Group Properties have passed, then the FND starts RPL tree retrieval from FAR.

The RPL pull times can be configured to each CGR configuration group as shown in the Device Configuration Group Properties. For the settings to take effect, the Global Settings must be set to `'Routers'`, refer to Global RPLTree Settings for Entire FND.

## RPL Tree Retrieval

The FND currently collects the following information from CGR as part of the RPL tree data:

- Node IP address
- Next hop IP address
- Number of parents
- Number of hops from root node
- ETX for path
- ETX for link
- Forward RSSI
- Reverse RSSI

**Note** No changes are required on FAR configuration when RPL updates setting is changed to routers or vice versa. When changed, the FND automatically schedules for gathering the RPL updates from FARs.

# Configuring RPL Tree Polling

RPL tree polls are derived from router periodic notification events. Since the RPL tree is not pushed from the router with the periodic notification event, Cisco IoT FND must explicitly poll for the RPL tree at the configured intervals. IoT FND lets you configure the RPL tree polling cycle (that is, how many periodic notification events occur between RPL tree polls), and set the maximum amount of time between tree polls.

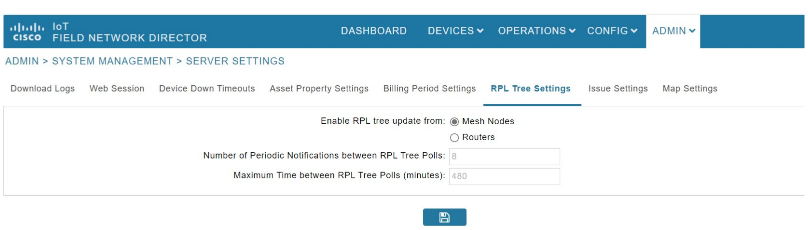
**Step 1** Choose **ADMIN** > **System Management** > **Server Settings**.

**Step 2** Choose the **RPL Tree Settings** tab.

**Step 3** In the **Enable RPL tree update from** option, click the **Mesh Nodes** or **Routers** radio button to receive the RPL tree update from those devices at the specified intervals.

**Note** The **Mesh Nodes** radio button is ON, by default.

**Note** Select the **Mesh Nodes** option in the **RPL Tree Settings** tab in order to ensure proper functionality of the L+G endpoints graph.




**Step 4** For Router polling, enter the number of events that pass between RPL tree polling intervals in the **Number of Periodic Notifications between RPL Tree Polls** field.

**Note** The default value is 8. If thresholds are exceeded during periodic notification events, IoT FND performs a RPL tree poll.

**Step 5** In the **Maximum Time between RPL Tree (minutes)** field, enter the maximum amount of time between tree polls in minutes.

**Note** The default value is 480 minutes (8 hours).

**Step 6** To save the configuration, click the disk icon.

## Configuring the Issue Status Bar

The Issue Status bar displays issues by device type (as set in user preferences) and severity level in the lower-left browser frame.

To enable the Issue Status bar and configure the refresh interval:

**Step 1** Choose **ADMIN** > **System Management** > **Server Settings** > **Issue Settings**.

**Step 2** To display the Issue status bar in the browser frame, check the **Enable/Disable Status Bar** > check box.

**Step 3** In the Issue **Status Bar Refresh Interval (seconds)** field, enter a refresh value in seconds.

The valid values are 30 secs (default) to 300 secs (5 minutes).

**Step 4** In the Certificate Expiry Threshold (days) field for all supported routers or an IoT FND application server, enter a value in days.

The valid value is 180 days (default) to 365 days.

**Note** When the configured Certificate Expiry Threshold default date is met, a Major event, certificateExpiration, is created. When the Certificate has expired (>180 days), a Critical event, certificateExpired, is created.

# Managing the Syslog

When IoT FND receives device events, it stores them in its database and sends syslog messages to a syslog server that allows third-party application integration.

**Note** The syslog server receives only the IoT FND device events (listed on Operations > Events page) and not the other IoT FND application logs in the server.log.

To configure Syslog forwarding:

**Step 1** Choose **ADMIN** > **System Management** > **Syslog Settings**.

**Step 2** In the **Syslog Server IP Address** field, enter the IP address of the Syslog server.

**Step 3** In the **Syslog Server Port Number** field, enter the port number (default is 514) over which to receive device events.

- Click **Enable Syslog Sending Events** to enable message forwarding to the Syslog server.
- Click **Disable Syslog Sending Events** to disable message forwarding to the Syslog server.

For IoT FND cluster solutions, each server in the cluster sends events to the same Syslog server.

CHAPTER 5

# Managing Devices

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

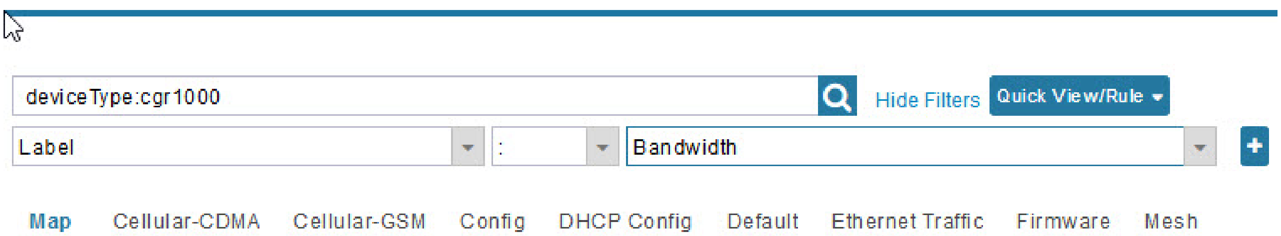
# Overview

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

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

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

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




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

**Pluggable Module Info**

**PID** P-LTEA-LA

**Details :**

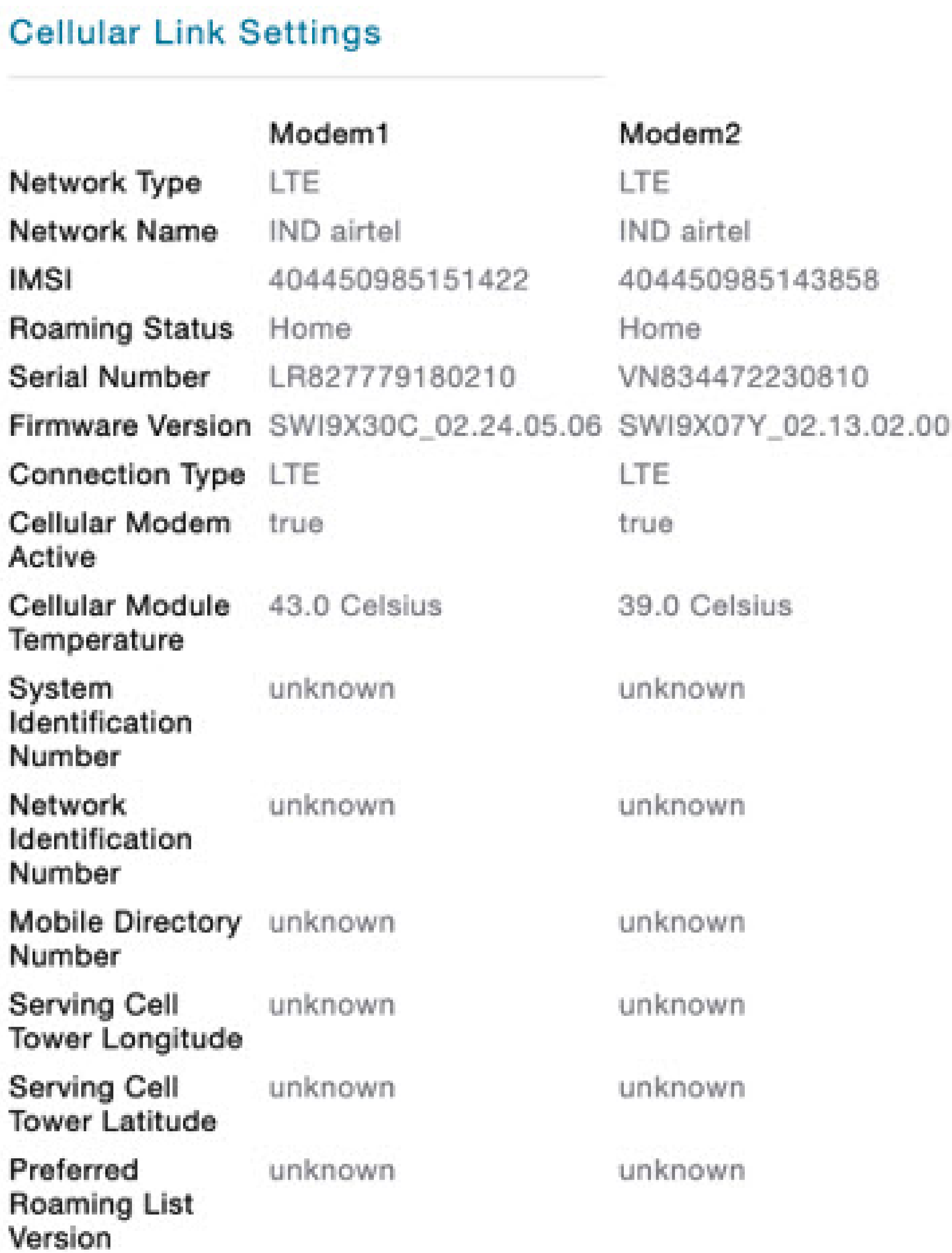
| Name | Description | PID | SN |
|---|---|---|---|
| Modem on Cellular0/1/0 | Sierra Wireless EM7430 | EM7430 | 355813070197162 |

**Expansion Module Info**

**PID** IRM-1100-SPMI

**Details :**

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



## Cellular Link Settings

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

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

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

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

# Guided Tours

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

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

**Step 2** Click GUIDED TOUR.

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

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

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

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

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

# Enabling Google Snap to Roads

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

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

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

# Managing Routers

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

## Working with Router Views

The router or routers you select determine which tabs display.

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

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

For information on how to customize router views, see Customizing Device Views, on page 144.

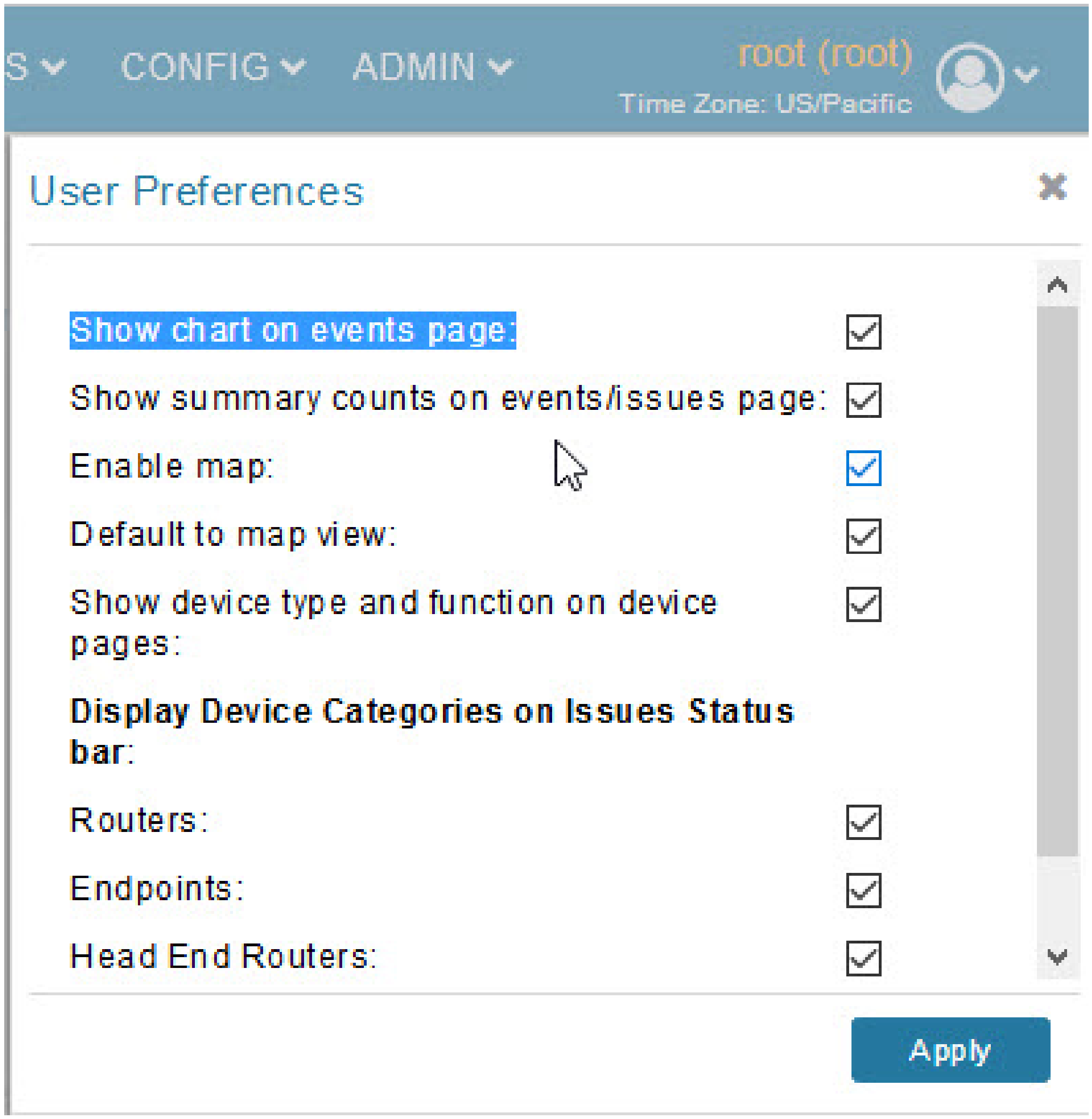
For information about the device properties that display in each view, see Device Properties, on page 236.

For information about common actions performed in these views (for example, adding labels and changing device properties), see Common Device Operations, on page 143.

## 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.

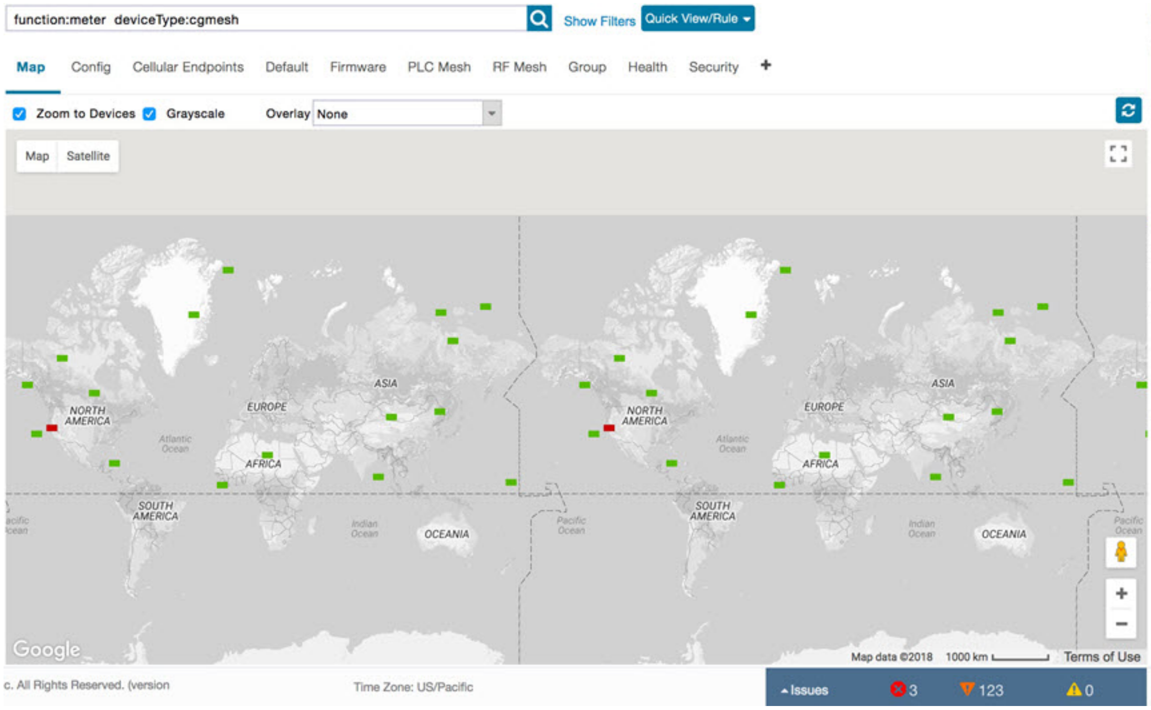
*Figure 7: Setting User Preferences for User Interface Display*




**Note** The additional options (not seen in the Figure 7: Setting User Preferences for User Interface Display, on page 93) 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 8: 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 the Router Mesh Key

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

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

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

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

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

**Step 3** Click **Yes** to continue.

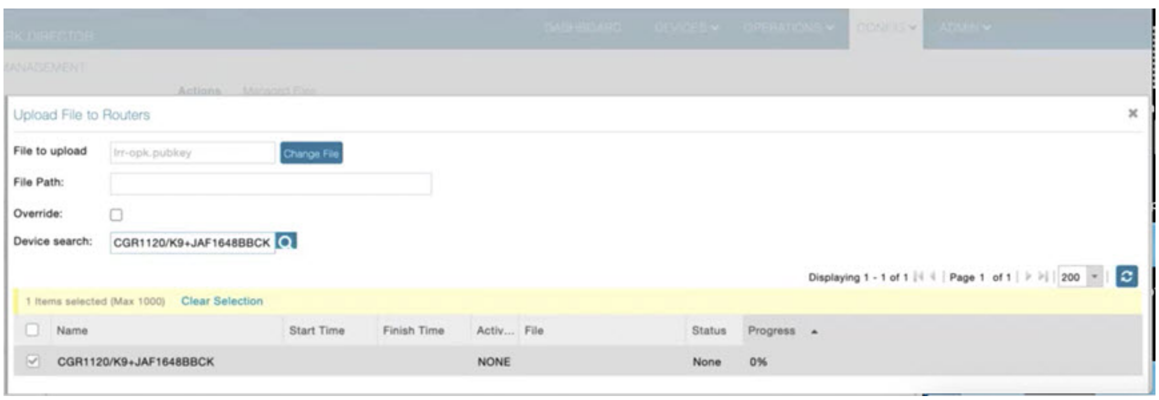
# Device File Management for Routers

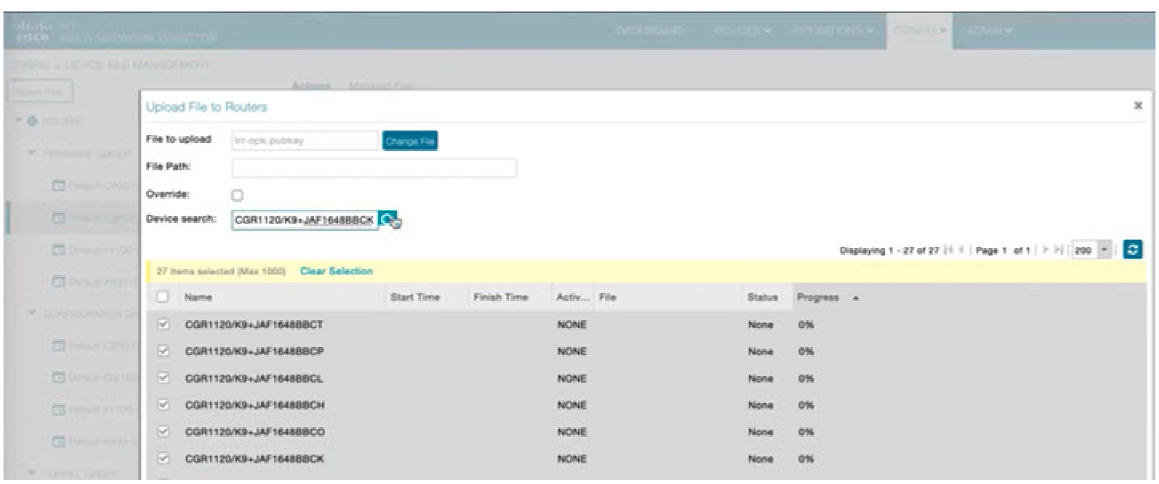
When you want to upload router device files to be managed by IoT FND, go to **CONFIG** > **DEVICE FILE MANAGEMENT** within the application. At that page, select **Actions** > **Upload** to get to the Upload File to Routers page. This page provides you the ability to:

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

The number of router files available to upload (based on your search criteria) displays and all listed routers are selected (checked boxes) by default. You can define the number of routers that display, by using the drop-down menu on that page. Options are 10 (default), 50, 100 and 200. You can remove the check mark next to any router, that you do not want to upload.

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



# Managing Embedded Access Points on Cisco C800 and Cisco IR829 ISRs

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

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

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

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

**Note** Not all C800 Series and IR800 routers have embedded APs. A C800 ISR features matrix is here. The IR829 ISR features matrix is here.

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

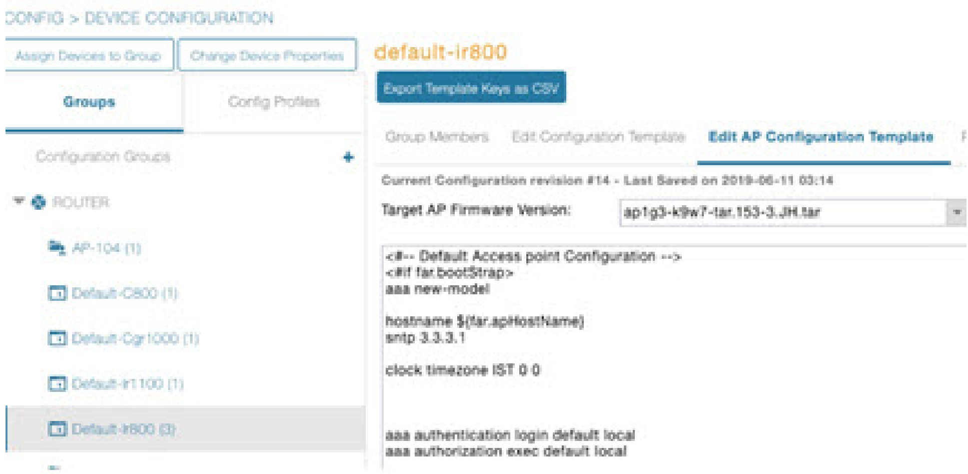
You must define a specific firmware image to use during ZTD.

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

# Defining the Unified Mode Option

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

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




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

```
ip dhcp pool embedded-ap-pool
network <router_ip> 255.255.255.0
dns-server <dns_ip>
default-router <router_ip>
option 43 hex f104.0a0a.0a0f (single WLC IP address(10.10.10.15)
in hex
format)
ip address <router_ip> 255.255.255.0
!
service-module wlan-ap 0 bootimage unified
```

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

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

# Using Router Filters

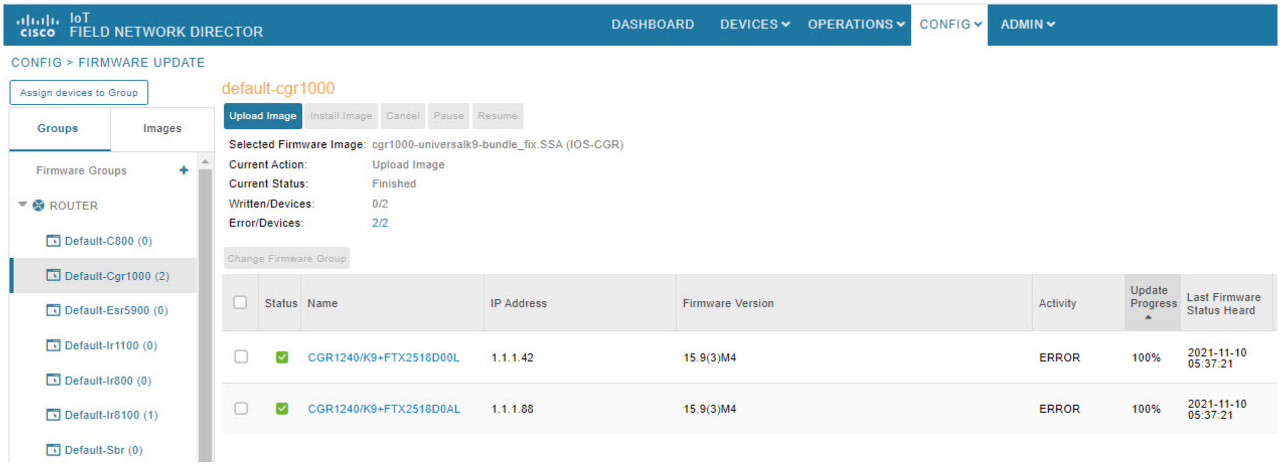
To refine the list of displayed routers, use the built-in router filters under ROUTERS in the Browse Devices pane or saved custom searches in the Quick View pane (right pane). For example, to display all operational routers, click the **Up** group under ROUTERS in the Browse Devices pane. Click a filter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

# Displaying Router Configuration Groups

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

# Displaying Router Firmware Groups

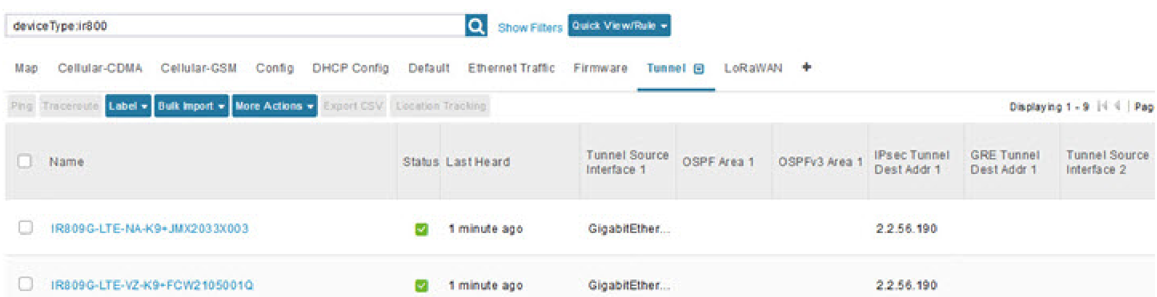
**Step 1** At the **CONFIG** > **Firmware Update** page, select the Groups tab (left pane) and then choose one of the ROUTER Groups (such as Default-c800, Default-cgr1000, Default-esr5900, Default-ir1100, Default-ir800 or Default-sbr).




**Step 2** The firmware image available for the router displays under the Name field in the right-pane. In the case of the Default-ir800, it includes both the IR809 and IR829, so there are two different firmware images listed.

# Displaying Router Tunnel Groups

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




# 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 144.

For information about the device properties displayed in each view, see Device Properties, on page 236.

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 143.

# Viewing Mesh Endpoints in Map View

To view mesh endpoints in Map view:

**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**).

**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:<br>• WPAN Status<br>• PPP Link Stats<br>• Neighbor 802.15.4g |
| **General** | Generates a report with the following general parameters associated to the device:<br>• TLV Index<br>• Device ID<br>• Current Time<br>• Uptime<br>• IEEE 802.1x Status<br>• IEEE 802.1x Settings<br>• Firmware Image Information |

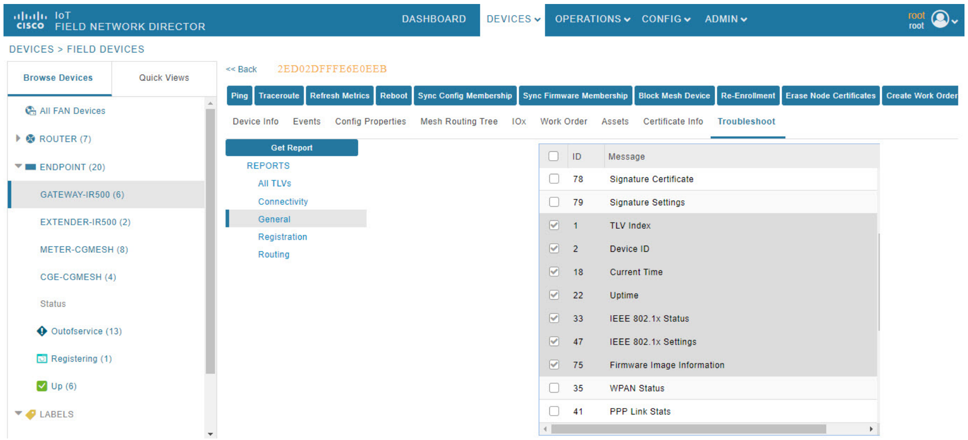
| Report | Description |
|---|---|
| **Registration** | Generates a report with the following registration parameters:<br>• Network Management System Redirect Request<br>• Report Subscribe<br>• Connected Grid Management System Settings<br>• Connected Grid Management System Status<br>• Connected Grid Management System Notification<br>• Connected Grid Management System Stats<br>• Signature Certificate<br>• Signature Settings |
| **Routing** | Generates a report with the following routing parameters:<br>• IP Address<br>• RPL Settings<br>• IEEE 802.11i Status<br>• DHCPv6 Client Status<br>• IEEE 802.15.4 Beacon Stats<br>• Stored Information<br>• Fast Synchronization Status<br>• 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.

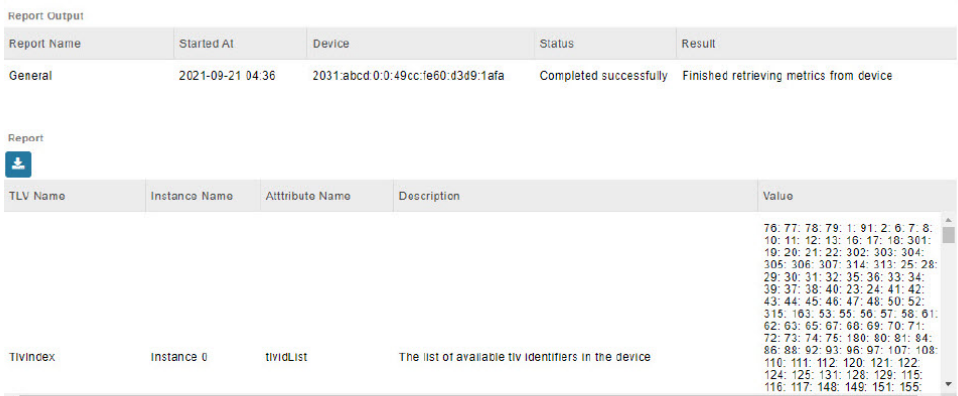



*Table 17: Feature History*

| 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 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 18: 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:

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

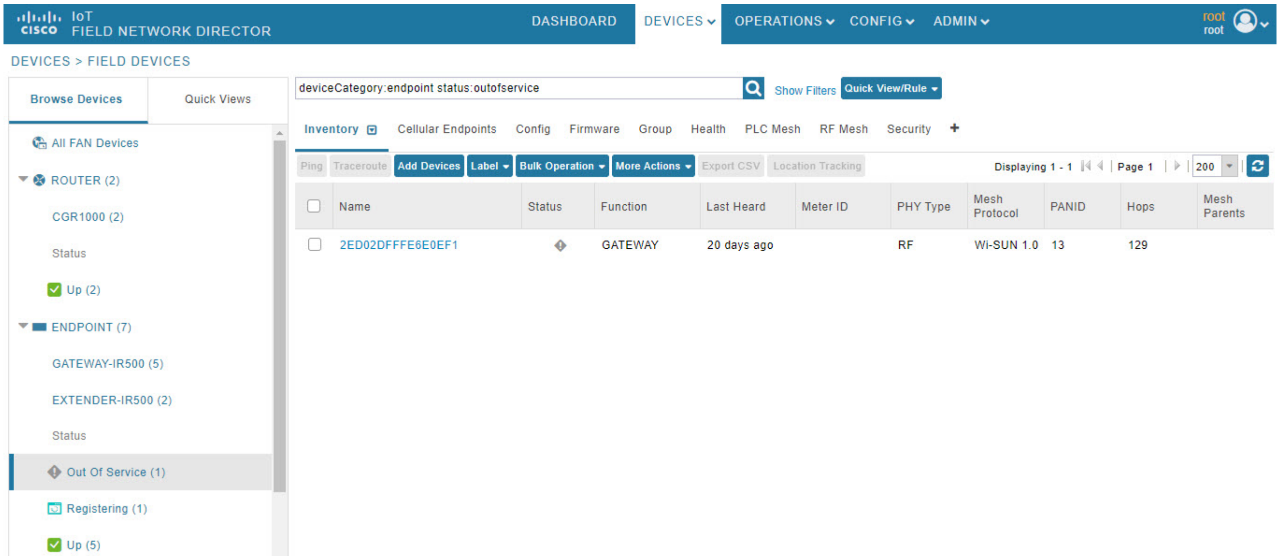
**Step 2** Click **Add Devices** button on the right pane to add devices of router, endpoint, or gateway.

**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:

**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:

**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

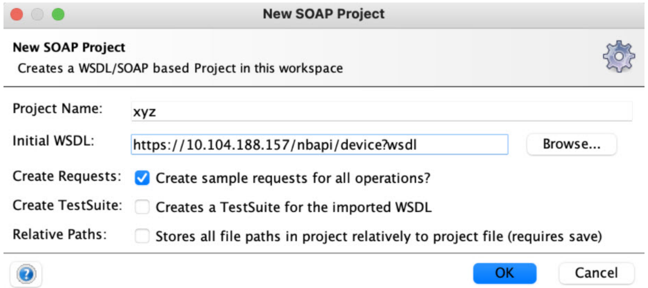
To add, update, or delete OOS devices:

**Step 1** Open the IoT FND NB API (SOAP UI:https://www.soapui.org/).

**Step 2** From the **Soap** menu, select **New Soap Project**.

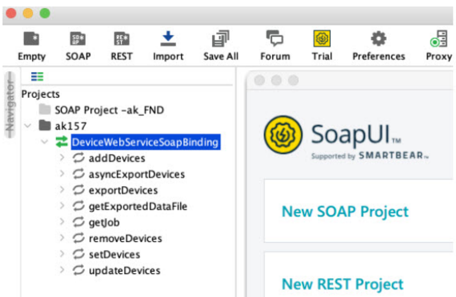
**Step 3** In the **New SOAP Project** window, provide the following information:

- 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.

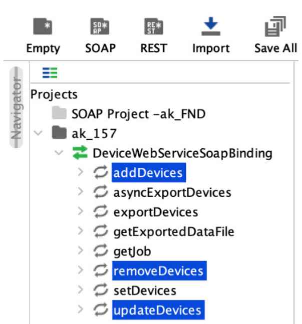



**Step 5** Right-click one of the following API options and select NewRequest:

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**.

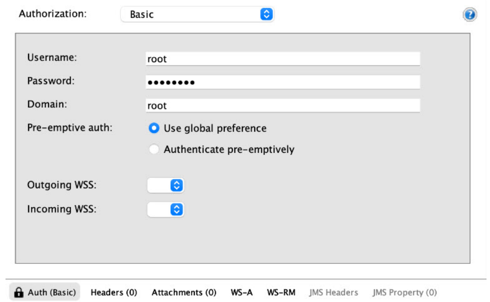
An XML window appears on the right pane.

**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.

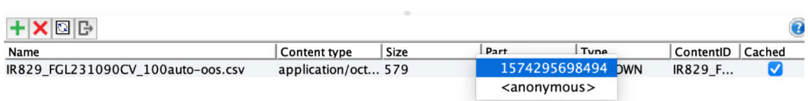
You can perform one of the following actions:

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.

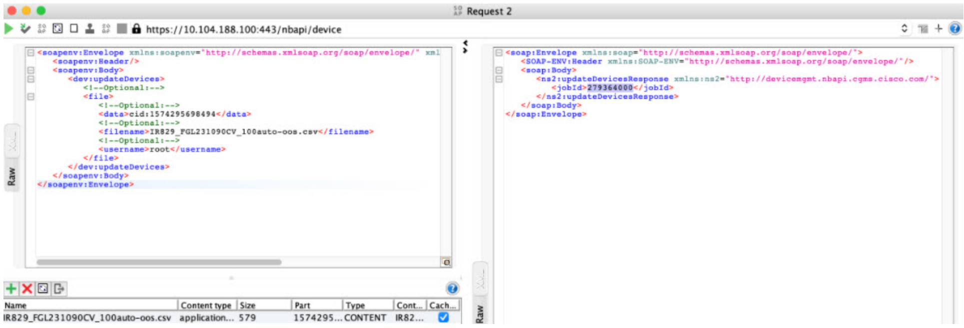



**Step 15** In the XML file, provide the following information:

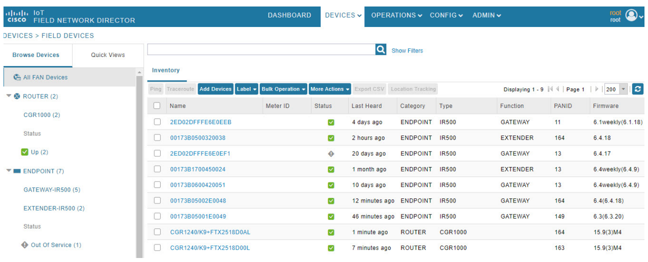
- Update the filename (copy the .csv filename from the Name field).
- Enter root as username.
- Update the HTTPS URL with FND IP details.


**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 explains how the license is managed for OOS devices in IoT FND.

| Action | Description |
|---|---|
| Adding a license file | There is no change in the license count, as OOS devices do not consume the license.<br><br>The devices in Managed status are given priority while adding the license file. The license consumed by them are displayed on the License Summary page.<br><br>To know more about adding a license file, refer to Adding License Files, on page 69 |
| Removing a license file | Changes the device status from OOS to Unmanaged.<br><br>**Note** On re-adding the license, the devices move back to OOS status.<br><br>To know more, refer Deleting the License Files, on page 72. |
| License expiry | OOS devices move to Unmanaged status on priority. |

| Action | Description |
|---|---|
| License summary page | OOS devices do not consume license, hence they are not displayed on the summary page.<br>To know more about viewing the license summary page, refer to Viewing License Summary, on page 70. |
| Registration | IoT FND accepts registration or tunnel provisioning request from OOS devices, but consumes license. |
| Tunnel Provisioning | |
| Periodic or on-demand Metric Refresh | If there is a periodic or on-demand metric refresh request from OOS devices, then the request is dropped. |
| SNMP Trap Processing | The SNMP trap request is not processed for OOS devices. The user is notified with DEBUG and INFO level message on FND server.log. |
| Deleting OOS devices | You can delete OOS devices directly from the Device Info page, but this action does not change the license count.<br>**DEVICES** > **Field Devices** > **Browse Devices** > **Devices** > **More Actions** > **Remove Devices**. |

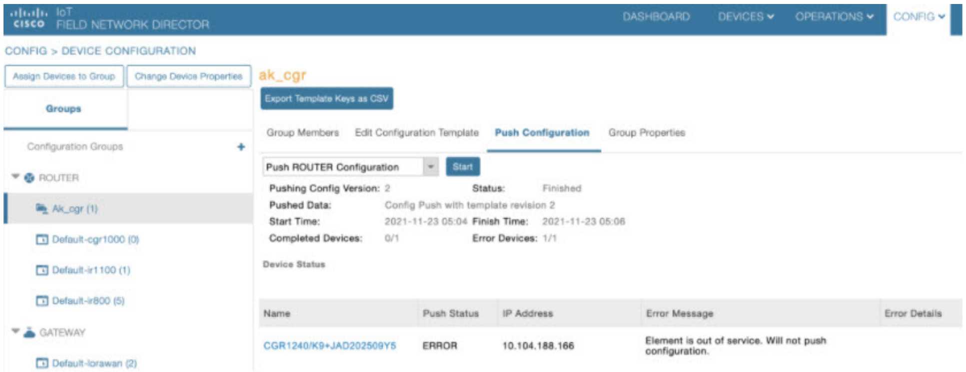
# Supported Actions for OOS Devices

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**).

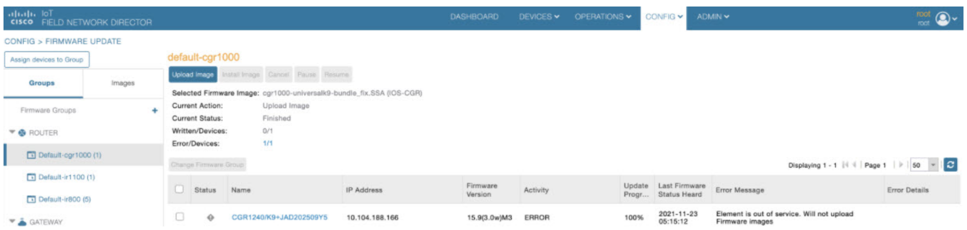
# Restrictions for OOS Device Actions

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.

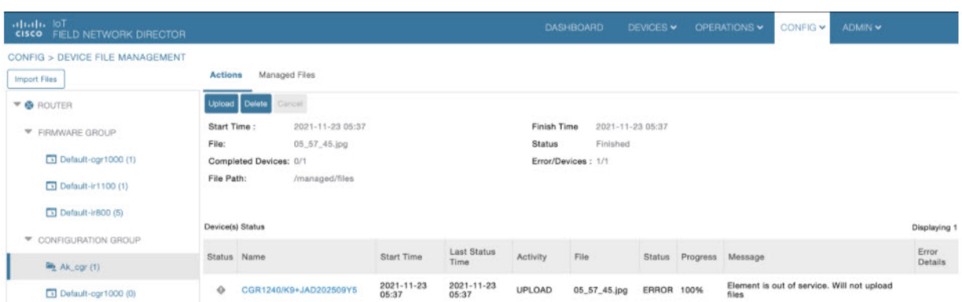


- In the **CONFIG** > **Firmware Update** page, when you use the upload or install image option on OOS devices, an error message appears.



- 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.



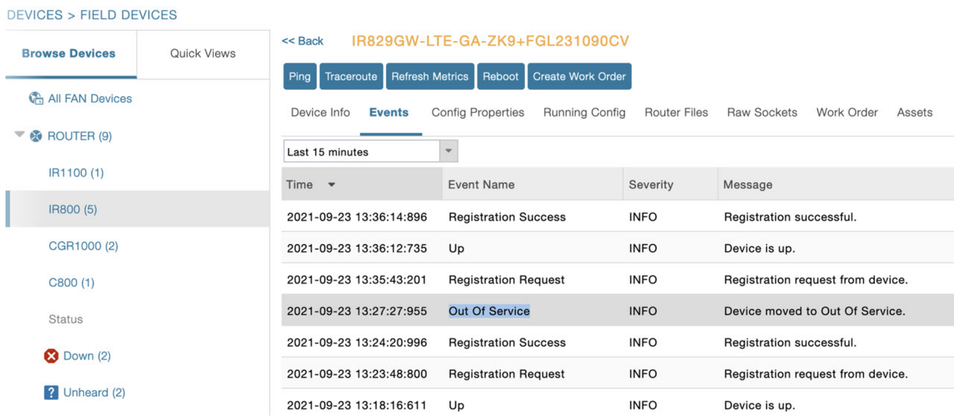
# Viewing Events and Audit Trails for OOS Devices

- 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.

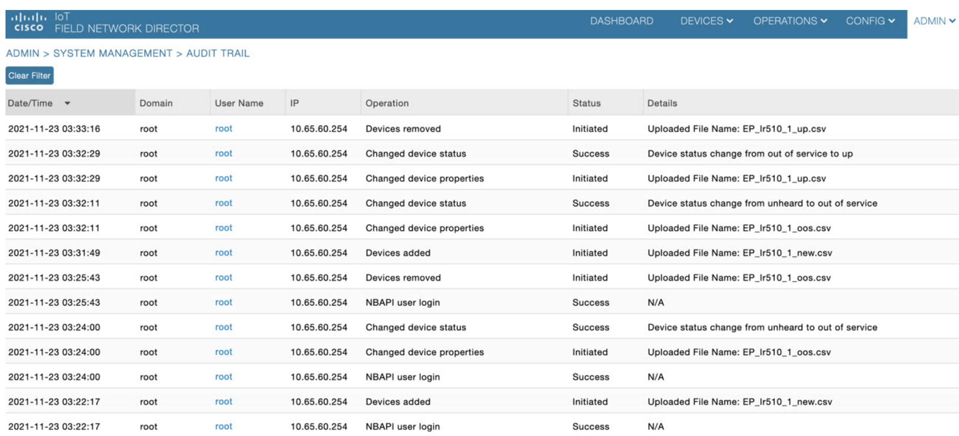
**Note** You cannot generate events for the devices that are currently in OOS state.

**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 111.




- 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.

**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.

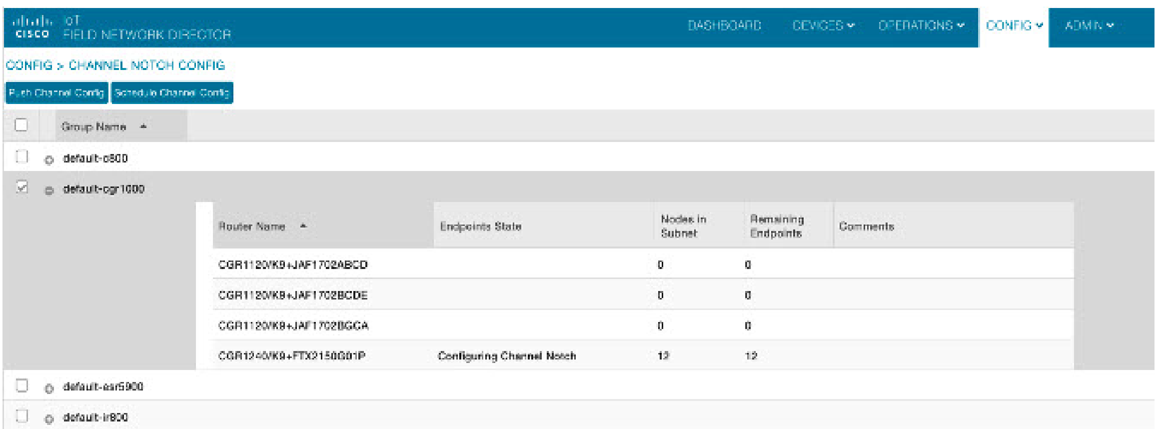
You can define up to four pairs of Notch Range Start and End Channels on the Channel Notch Settings page. These channel ranges must have increasing channel numbers for each range and cannot have any overlapping ranges. The ranges are blacklist ranges which are used to prohibit nodes from using the ranges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

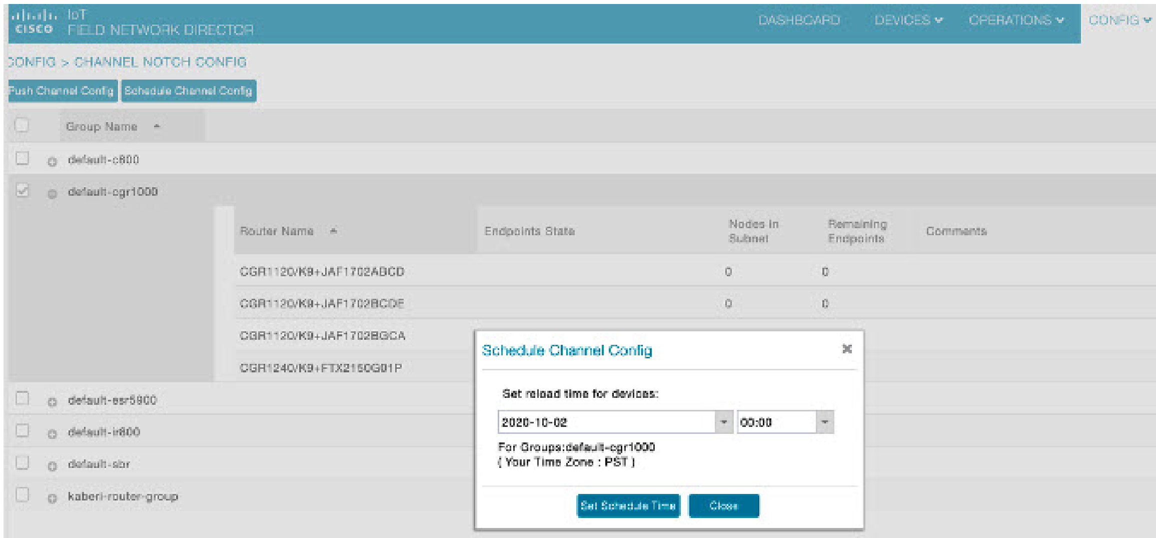
- channelNotchMaxAttempts = 20: This setting defines the maximum attempts that the software will attempt to send the config and schedule information to all of the endpoints.
- allowNewNotchSettings=true: This setting allows notch settings to be changed at will and defines those setting that will be used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

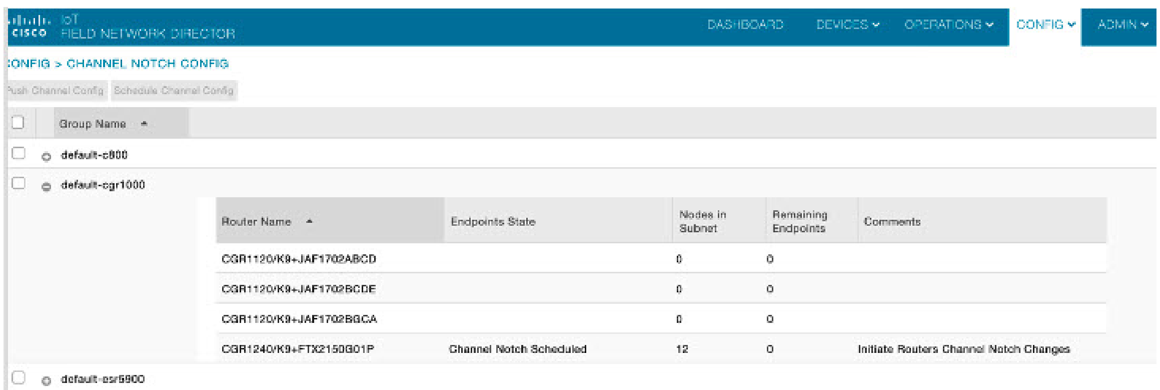



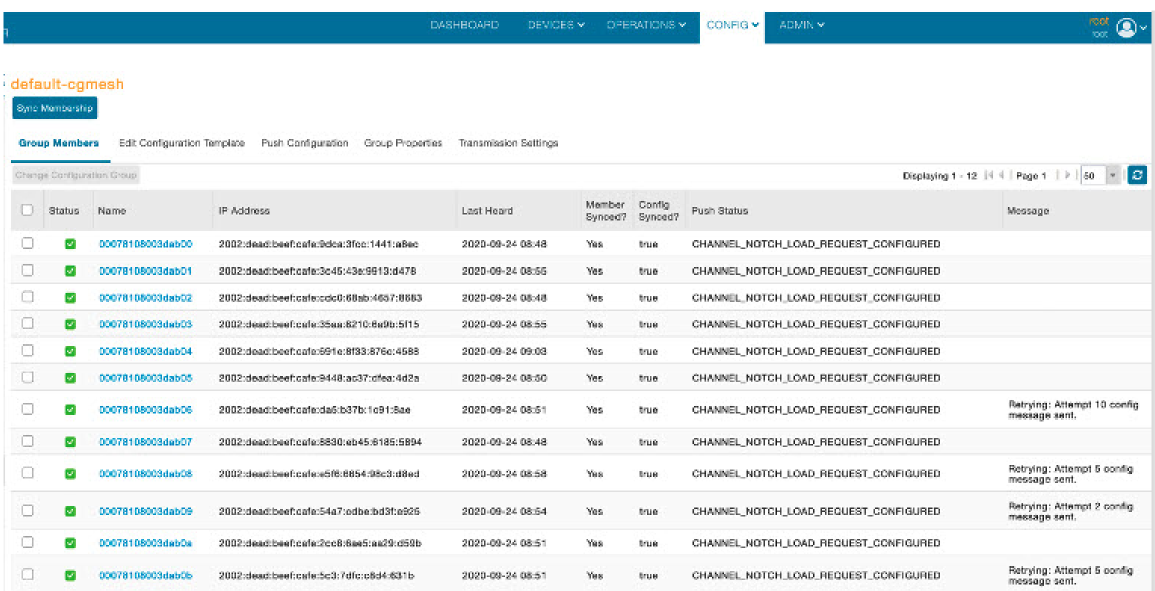

**Note** Before you can schedule activation of a Channel Notch Config, the router config groups must have successfully received their channel notch configuration. Note: Before you can schedule activation of a Channel Notch Config, the router config groups must have successfully received their channel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

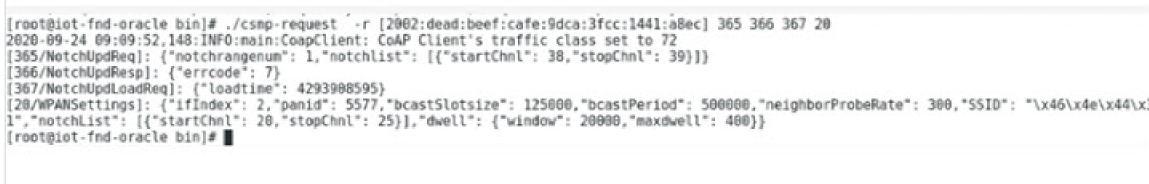
When you select the Schedule Channel Notch Config button, a pop up panel appears for you to set a reload time (day and time) that the Channel Notch Config will be activated.

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
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
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
Change Configuration Group
Displaying 1 - 12
Page 1
50
Status
Name
IP Address
Last Heard
Member Synced?
Config Synced?
Push Status
Message
00078108003dab00
00078108003dab01
00078108003dab02
00078108003dab03
00078108003dab04
00078108003dab05
00078108003dab06
00078108003dab07
00078108003dab08
00078108003dab09
00078108003dab0a
00078108003dab0b
CHANNEL_NOTCH_LOAD_REQUEST_CONFIGURED
Retrying: Attempt 10 config message sent.
Retrying: Attempt 5 config message sent.
Retrying: Attempt 2 config message sent.
Retrying: Attempt 5 config message sent.




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

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

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

# LDevID: Auto-Renewal of Certs and Saving Configuration

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

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

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

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

### LDevID Certificate Renewal for IoT FND Release 4.8.1

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

To enable this feature, you must set the following property value to "true" in the cgms properties file.

```
enable_ldevid_renewal_tcl= true
```

**Note** Restart IoT FND services after enabling this feature.

**Note** Once this feature is enabled, you cannot disable it even by setting the property value to "false".

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

- `before-tunnel-config`
- `before-registration-config files`

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

**Note** Disable the auto-renewal and update of LDevID certs feature before upgrading to Cisco IOS-XE 17.10.1 and above versions.

### LDevID Certificate Renewal for IoT FND Release 4.8.0

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

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

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

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

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

**Note** Disable the auto-renewal and update of LDevID certs feature before upgrading to Cisco IOS-XE 17.10.1 and above versions.

### LDevID Certificate Renewal for FND Releases, 4.7.1 and 4.7.2

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

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

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

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

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

# Support Expired SUDI Certificate

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

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

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

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

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

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

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

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

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

### Example Display

```
SUDI Certificate:

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

Issuer:
cn=ACT2 SUDI CA
o=Cisco

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

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

cn=Cisco Root CA 2048
o=Cisco Systems
```

```
Subject:
cn=ACT2 SUDI CA
o=Cisco

CRL Distribution Points:

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

Validity Date:

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

Associated Trustpoints: CISCO_IDEVID_SUDI
```

# Configuring Enrollment over Secure Transport

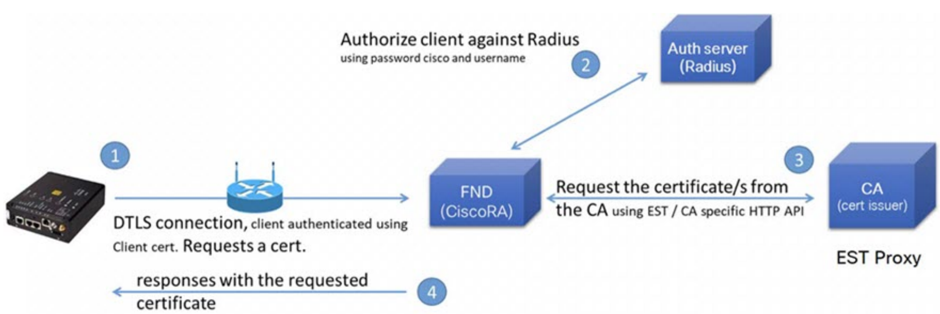
This section provides an overview of the components and configurations involved in integrating Enrollment over Secure Transport (EST) certificate enrollment for clients over the secure transport layer within the network. EST is based on public-private key exchange. This feature is supported on Itron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

***Table 19: 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:

**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

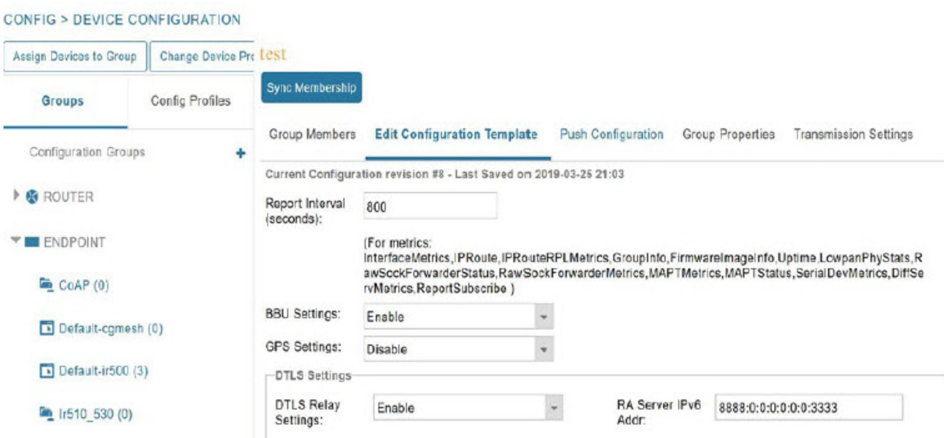
Set the DTLS relay configuration and Watchdog Cisco-RA monitoring in FND.

**Note** Supported from version 4.5.0.122 onwards.

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

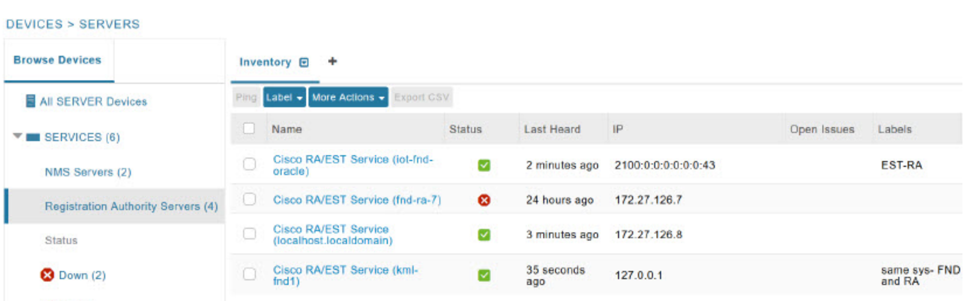
**Step 2** Select **Enable** from the **DTLS Relay Settings** drop-down list.

**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**.

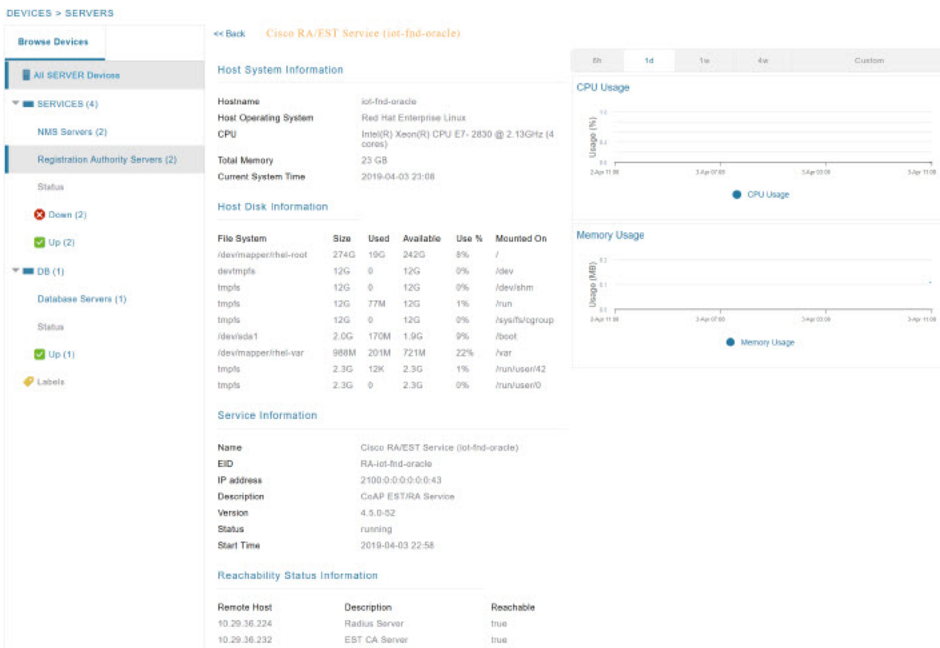



*Figure 9: Events for FND-RA Service*

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

*Figure 10: 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

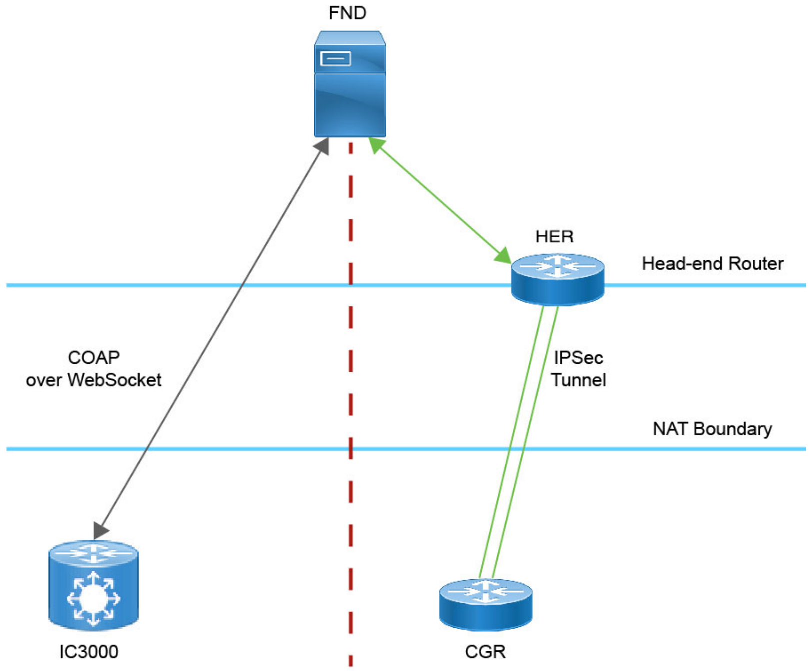
IC3000 supports edge computing and communicates with IoT FND through the IOx application, Cisco Fog Director which is accessible via IOT FND.

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.

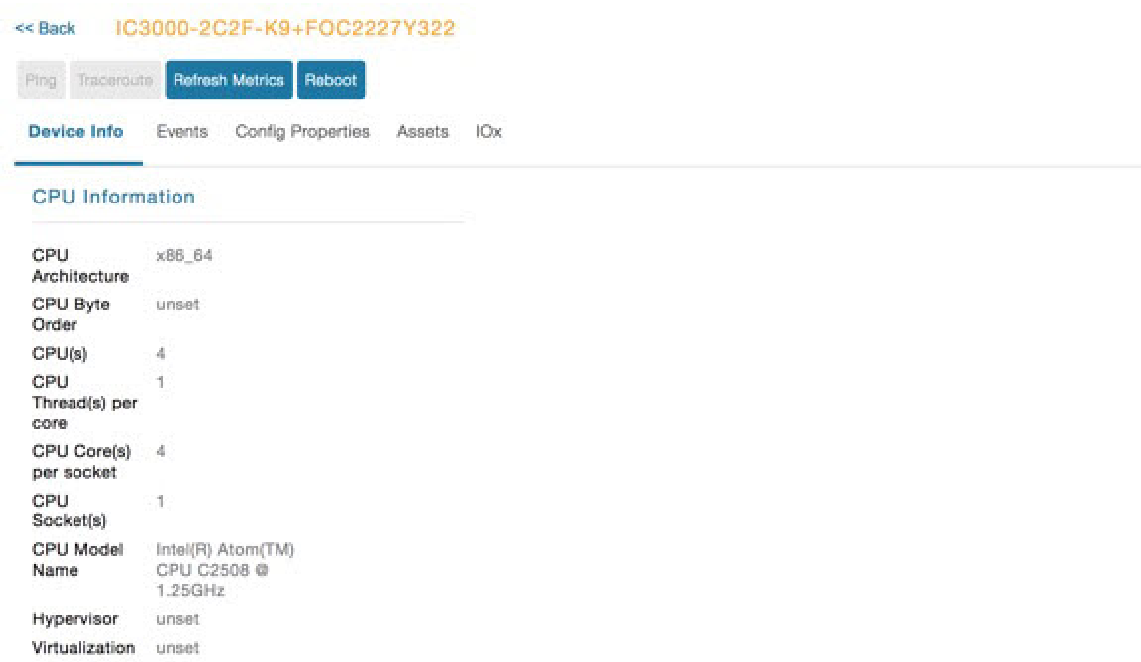



You can perform the following actions for an IC3000 device type on demand:

- 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:

**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

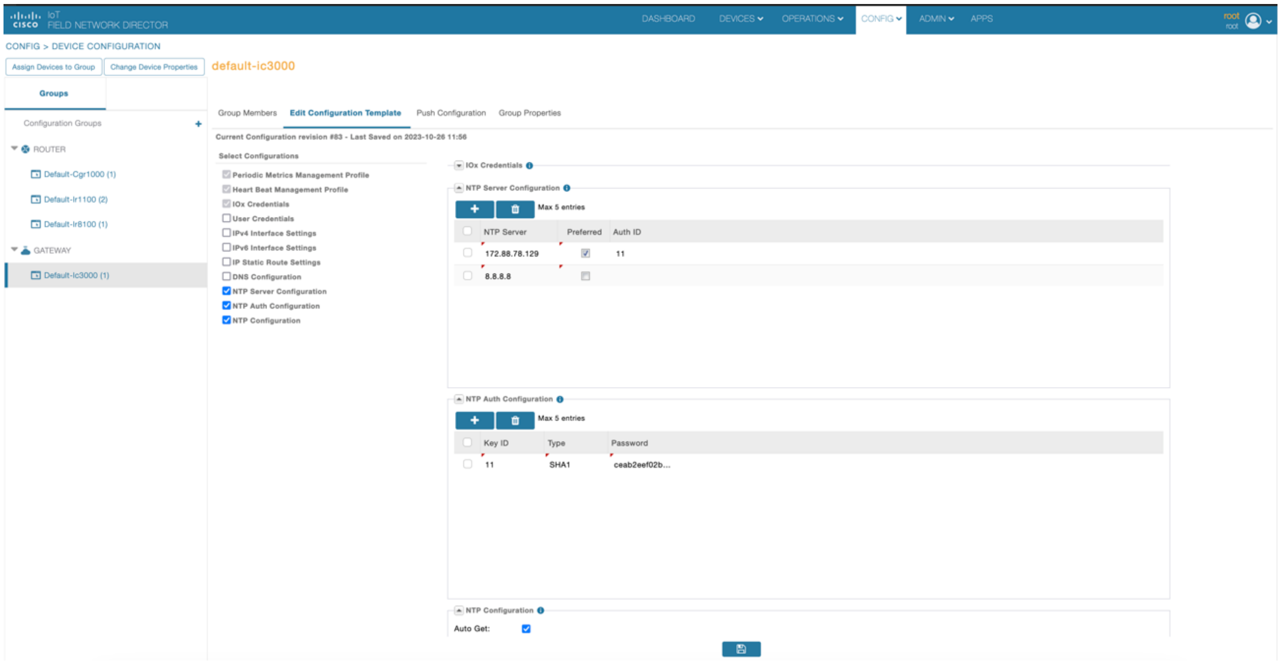
To push the NTP configuration via FND,

**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 Managing External Modules, on page 140).
- 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:

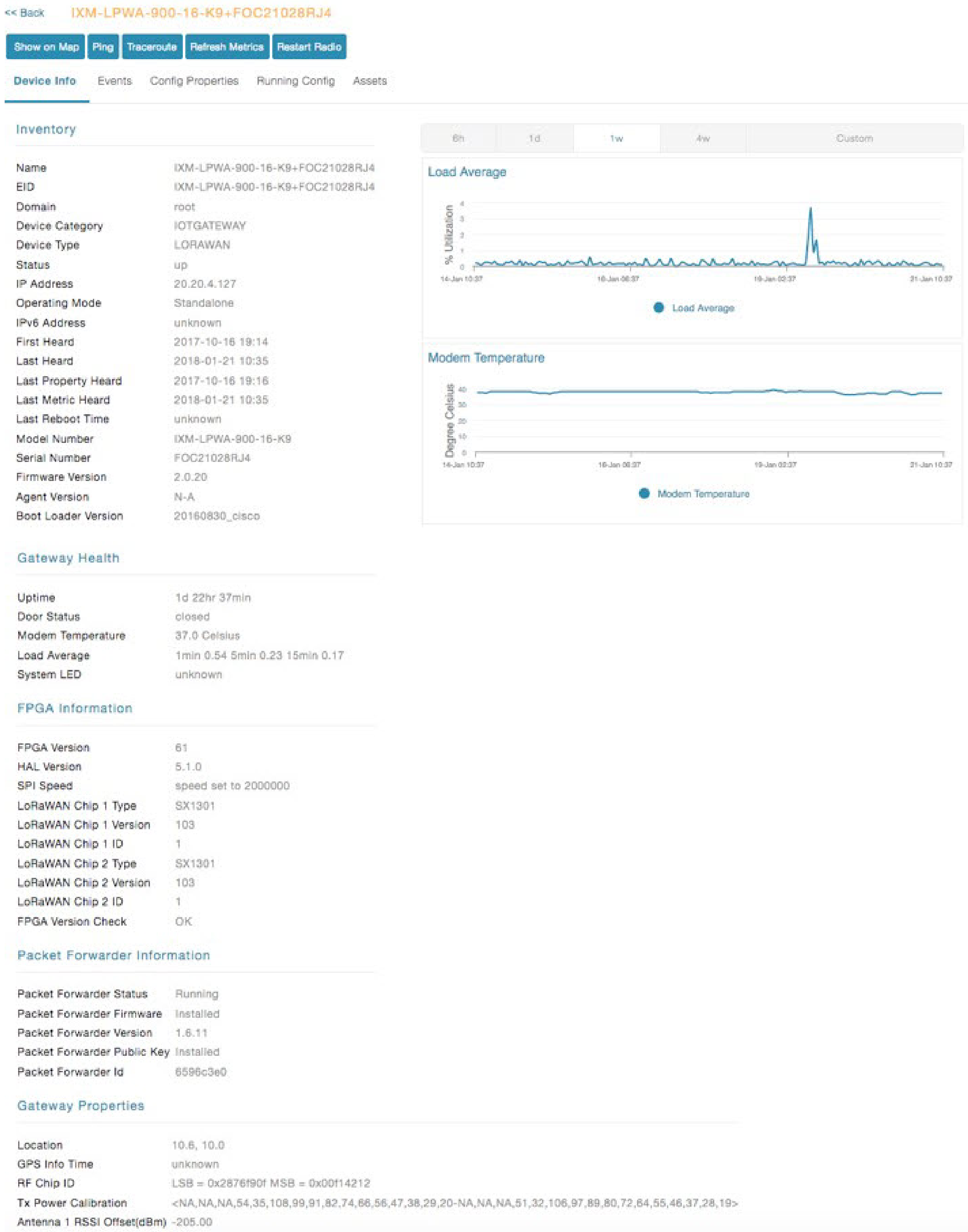
1. Choose **DEVICES** > **Field Devices**.

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 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 Internet of Things (IoT) applications such as smart grid, distribution automation (DA), and supervisory control and data acquisition (SCADA). As the next generation of the DA gateway, IR510 provides higher throughput, distributed intelligence, GPS, and enhanced security. unlicensed 915-MHz industrial, scientific, and medical band WPAN communications.

**Note** IR510 is identified and managed as an ENDPOINT in IoT FND (**DEVICES** > **FIELD DEVICES** > **ENDPOINT** > **GATEWAY**).

**Note** When updating an existing installed software base for IR510 and IR530 devices, IoT FND uploads only the new software updates rather than the full image using bsdiff and bspatch files.

## Profile Instances

IoT FND employs Profile-based configuration for IR510s. This allows you to define a specific Profile instance (configuration) that you can assign to multiple IR500 configuration groups. Table 6. Pre-defined Profiles for IR510 lists the supported Profile types.

Note the following about the Profiles:

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

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


To create a new profile:

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

To delete a profile:

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

To rename a profile:

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

To clone a profile:

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

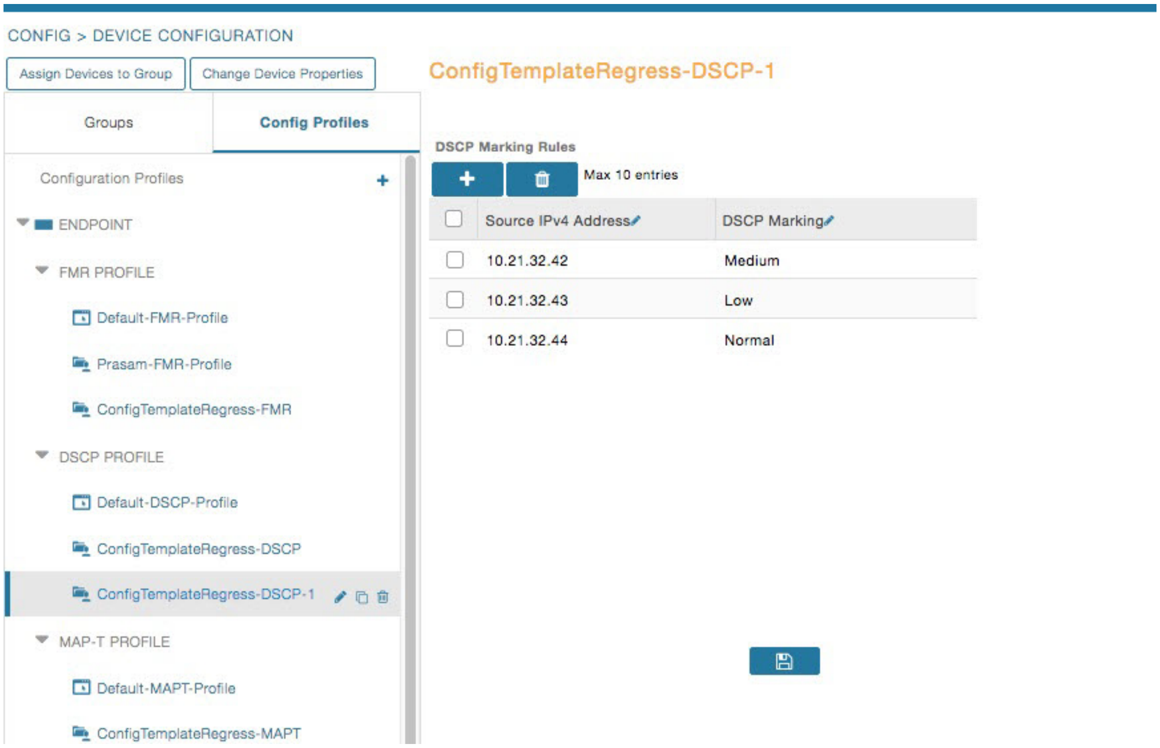
*Table 20: Pre-defined Profiles for IR510*

| Profile Name | Description | Properties Configurable in CSV File |
|---|---|---|
| Forward Mapping Rule (FMR) Profile<br>**CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **FMR PROFILE**<br>Interface configuration<br>**CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template**<br>Select the FMR profile from the drop-down menu | Processes IPv4 traffic between MAP nodes that are in two different MAP domains.<br>Each FMR rule has IPv4 Prefix, IPv4 Prefix Length and EA Bits Length.<br>You can define up to 10 FMR Profiles.<br>FMR settings are pushed to the device as a part of MAP-T Settings during configuration push. | Forward Mapping Rule IPv6 Prefix:<br>fmrIPv6Prefix0 to fmrIPv6Prefix9<br>Forward Mapping Rule IPv6 Prefix Length:<br>fmrIPv6PrefixLen0 to fmrIPv6PrefixLen9 |
| DSCP profile<br>**CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **DSCP PROFILE**<br>Interface configuration<br>**CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template**<br>Select the DSCP profile from the drop-down menu | Sets the DSCP marking for the Ethernet QoS configuration.<br>DSCP marking has eight (8) marking options to choose.<br>- User Controlled<br>- Default Queue (Best Effort)<br>- Normal Queue: Low drop probability (AF11)<br>- Normal Queue: Medium drop probability (AF12)<br>- Normal Queue: High drop probability (AF13)<br>- Medium Queue: Low drop probability (AF21)<br>- Medium Queue: Medium drop probability (AF22)<br>- Medium Queue: High drop probability (AF23)<br>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<br>**CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **MAP-T PROFILE**<br>Interface configuration **CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template**<br>Configures Basic Mapping Rule (BMR) and Default Mapping Rule (DMR) settings for IR509/IR510 | Configures endUser properties. | endUserIPv6PrefixbmrIPv6PrefixLen |
| Serial Port Profile (DCE and DTE)<br>**CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **SERIAL PROFILE**<br>Interface configuration<br>**CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template**<br>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).<br>You can configure the following settings on the serial interface:<br>• Port affinity<br>• Media Type<br>• Data Bits<br>• Parity<br>• Flow Control<br>• DSCP Marking<br>• Baud rate<br>• Stop Bit<br>**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<br>**CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **DHCP CLIENT PROFILE**<br>Interface configuration<br>**CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template**<br>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.<br>FND configures this static binding supports up to 10 client mappings.<br>The DHCP Client ID binding profile configuration associates a client ID to an IPv4 Host address.<br>The Client-id of each Client is expected to be unique within a single IR510.<br>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<br>**CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **DHCP SERVER PROFILE**<br>Interface configuration<br>**CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template**<br>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<br>DHCP server profile configuration includes:<br>**1.** Lease Time<br>**2.** DNS server list | NA |

| Profile Name | Description | Properties Configurable in CSV File |
|---|---|---|
| NAT44 Profile<br>**CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **NAT 44 PROFILE**<br>Interface configuration<br>**CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template**<br>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:<br>- CSV import method<br>- NAT44 profile instance within FND user interface<br>You configure three fields for NAT44: Internal Address, Internal Port and External Port<br>You can configure up to fifteen NAT 44 Static Map entries<br>**Note** Before you push the configuration, be sure to:<br>1. Enable Ethernet on the configuration group to which the device belongs (select check box)<br>2. Save Configuration Group | NA |
| Access Control List (ACL) Profile<br>**CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **ACL PROFILE**<br>Interface configuration<br>**CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template**<br>Select the ACL Profile from the drop-down menu. | Perform packet filtering to control which packets move through the network for increased security.<br>You can define up to 20 ACL Profiles. Each defined ACL has one associated Access Control Entry (ACE) for a maximum of 20 ACEs.<br>The check process goes through ACL from 1 to 20.<br>There is an implicit deny for all ACL at the end of 20 ACL unless configured differently.<br>To configure the interface for the Default-IR500, with Groups tab selected:<br>In the right-pane, choose Edit Configuration Template tab and select the Enable Interface ACL check box. | NA |

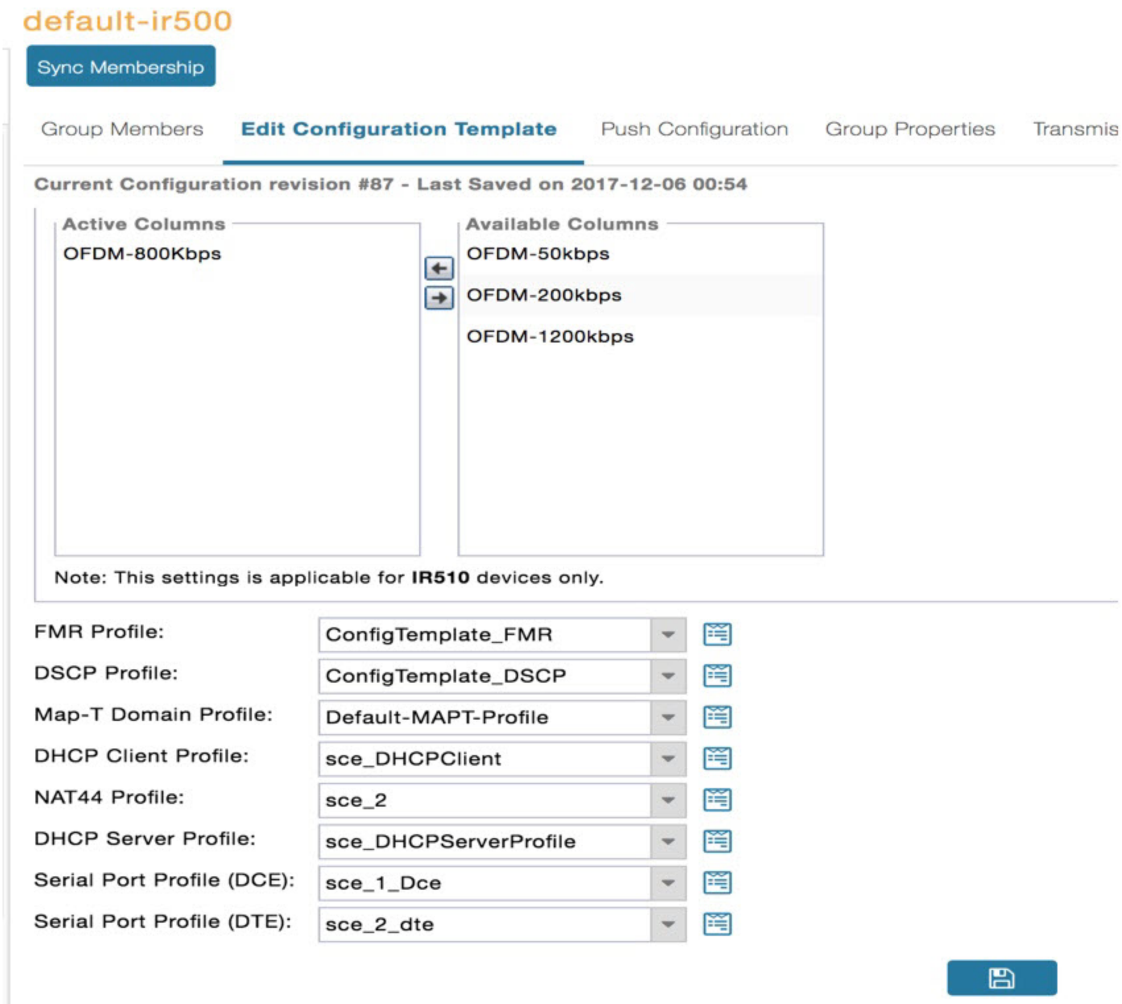



Configuration Notes:

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

# Configuration Profile for a Group

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




# Wi-SUN 1.0 Support

At the **CONFIG** > **DEVICE CONFIGURATION** and **DEVICES** > **FIELD DEVICES** > **ENDPOINTS** pages, you can now define and review the following actions for Wi-SUN 1.0 on the IR509 and IR510 WPAN gateways and the IR529 and IR530 Resilient Mesh Range Extenders as wells as an WPAN OFDM module installed within a CGR 1000 platform.

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 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 (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 IR510 only.

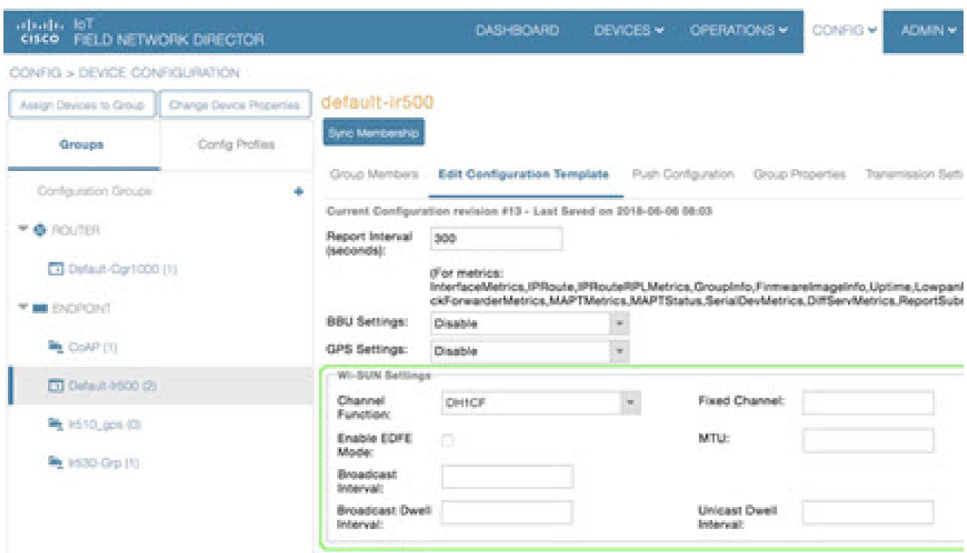
**Note** In Mesh Software 6.3, only the Wi-SUN 1.0 protocol is supported for all mesh endpoints. It displays Wi-SUN 1.0 from the mesh 6.3 firmware onward under the Mesh Protocol heading on the **DEVICES** > **FIELD DEVICES** > **ENDPOINT** > **Inventory** page.

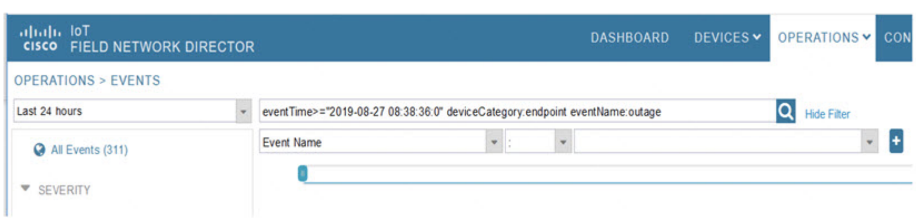
The Wi-SUN settings have been removed from the IR500 Config Group template: **CONFIG** > **DEVICE CONFIGURATION** > **Default-ir500** > **Edit Configuration Template** in IoT FND 4.7.

When using Mesh Software 6.2, for an 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 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 FND port 61625 as UDP messages. There are no changes in the events that are generated by the new PON and PRN CSMP messages.



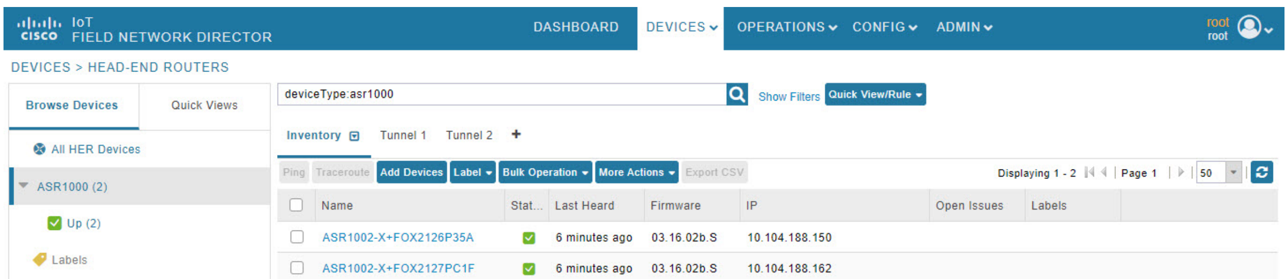



# Managing Head-End Routers

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

- Tunnel 1
- Tunnel 2

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




For information on how to customize HER views, see Customizing Device Views, on page 144

For information about the device properties displayed in each view, see Device Properties, on page 236.

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 143

# Managing External Modules

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

You can manage the following external modules using IoT FND.

## Itron CAM Module

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

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

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

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

```
manage-actd=true
```

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

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

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

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

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

c) Click + to open the Upload Image panel.

d) Select the type ACTD-CGR and select the appropriate Image from the drop-down menu such app-actd-ver-x.y.z.tar. In the confirmation box, click **Upload Image**.

e) Click Yes to confirm upload.

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

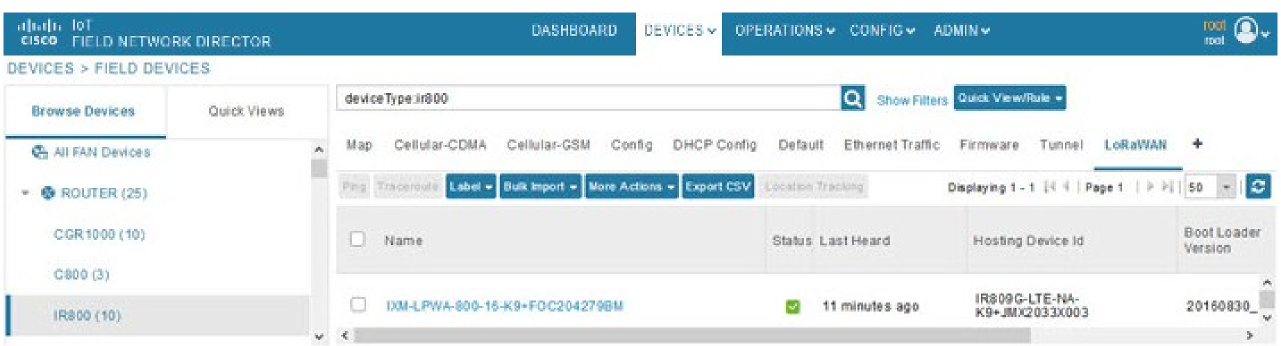
# Lorawan Gateway Module

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

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

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

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




**Step 3** To reboot the modem on the LoRaWAN module:

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

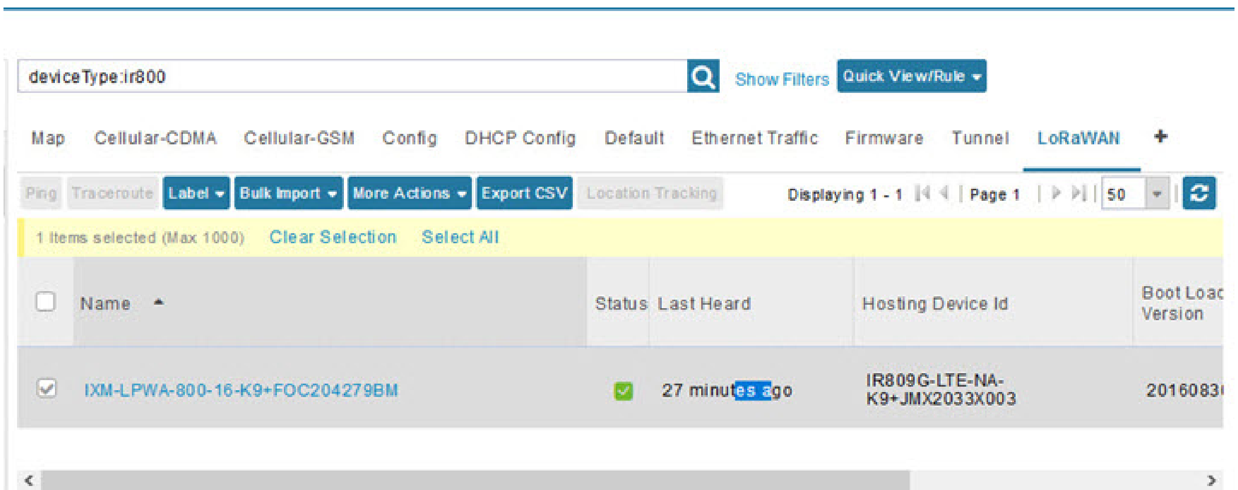

b) Click **Reboot Modem**. When the reboot completes, the date and time display in the Last Reboot Time field in the Device Info pane for the LoRaWAN module. You can only process one modem reboot at a time.

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

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

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

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




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

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

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

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

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

d) Click **Add**.

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

# Managing Servers

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

To add additional views, see Customizing Device Views, on page 144.

For more information about the device properties displayed in each view, see Device Properties, on page 236.

For information about the common actions in this view, see Common Device Operations, on page 143 .

## Managing NMS and Database Servers

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

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

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

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

## Managing Application Management Servers

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

# Common Device Operations

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

## Tracking Assets

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

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

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

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

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

  Example of Asset content in CSV file:

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

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

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

Guidelines for Adding or Associating an Asset with a Device:

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

# Selecting Devices

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

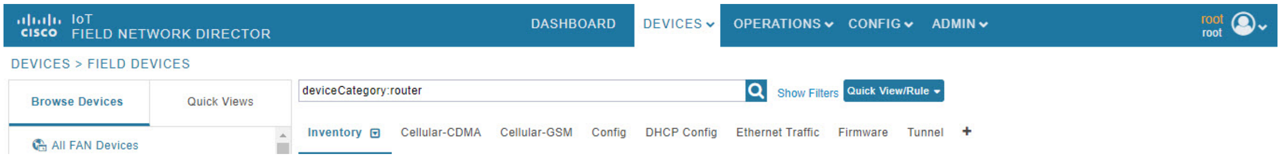
# Customizing Device Views

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

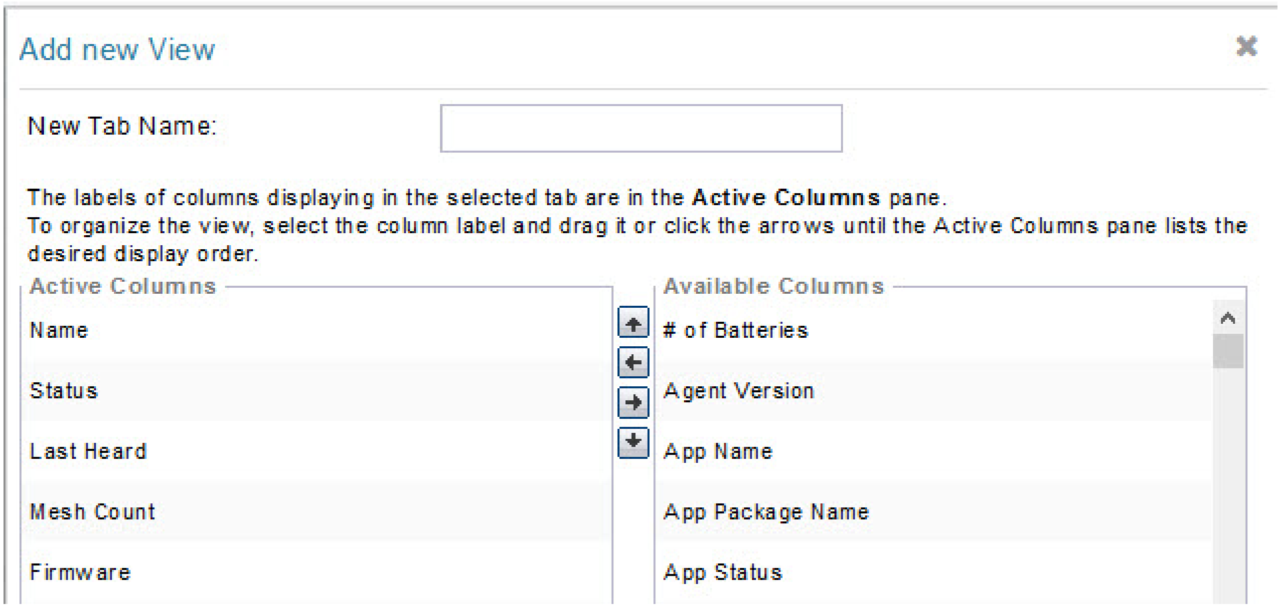
- Add and delete tabs
- Specify the properties to display in the columns for each view (see Device Properties by Category, on page 237 for available properties)
- Change the order of columns

# Adding Device Views

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




**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.

- Use up and down arrow buttons or drag the properties to the desired position to change the column order.
- Click the right arrow button or drag properties out of the **Active Columns** list to remove them.

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

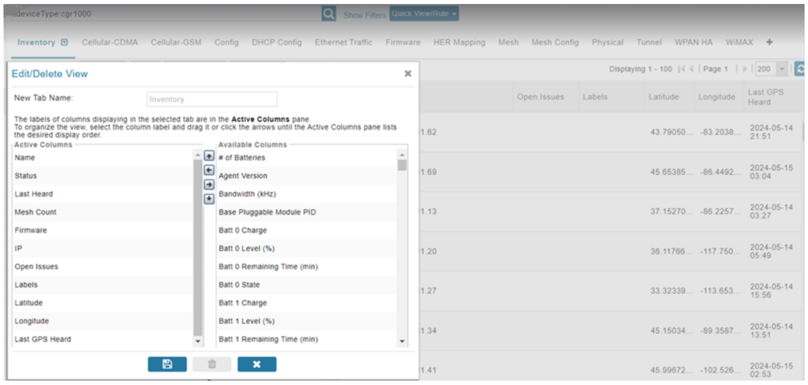
**Step 4** Click **Save View**.

# Editing Device Views

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

**Step 2** 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.



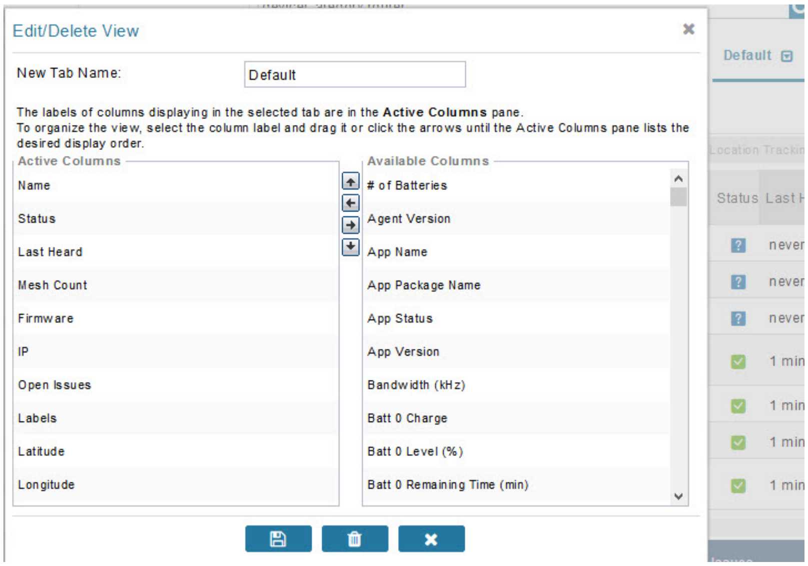

e) Click the **X** icon to close this view without saving changes.

**Step 3** Click the disk icon to save the view.

# Deleting a Device View

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

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



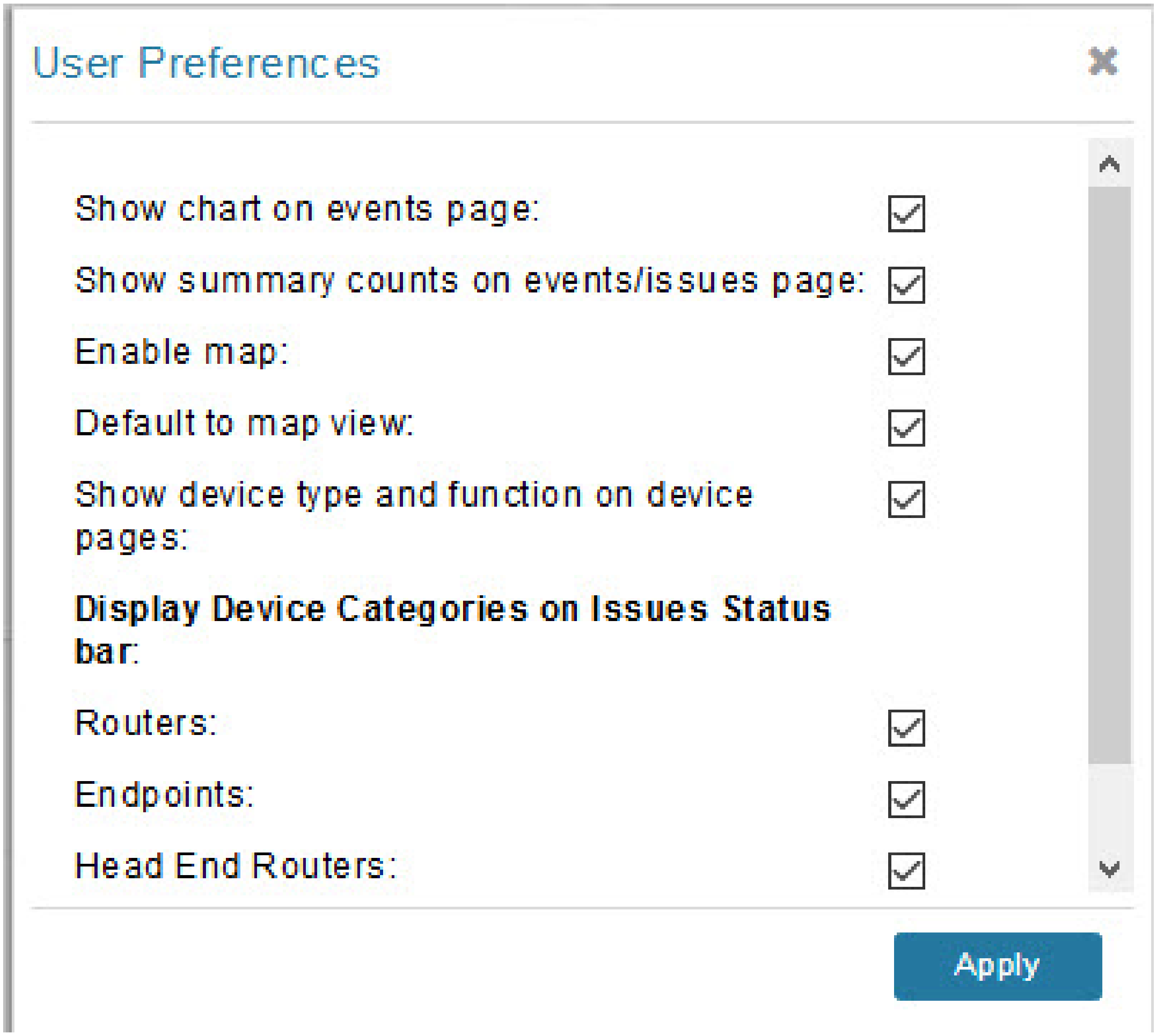

# Viewing Devices in Map View

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

To view devices in Map view:

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

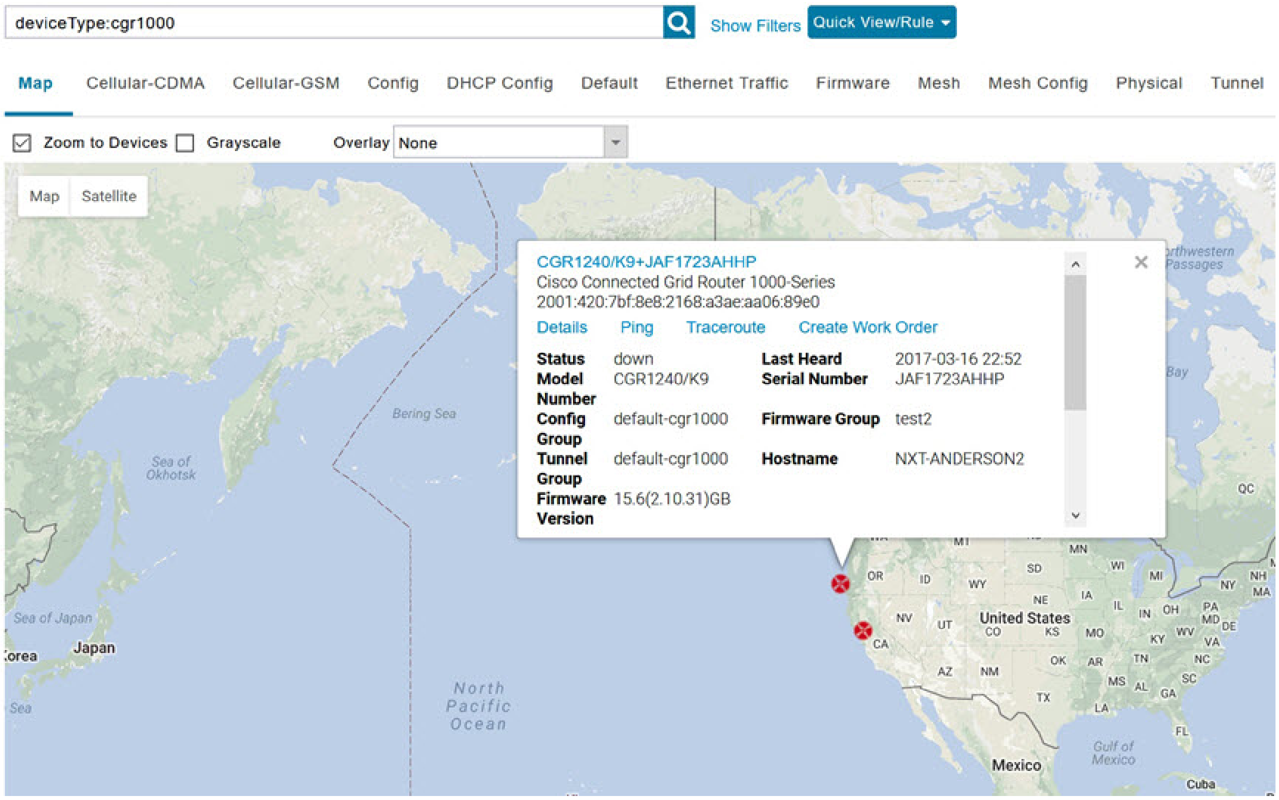
**Step 2** Select the **Enable map** check box, and click **Apply**.




**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 Creating a Quick View Filter, on page 159.

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 Configuring RPL Tree Polling, on page 83 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:

**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:<br>• For Routers you can overlay: None, All, or Associated Endpoints on the map.<br>• 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:

**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:

**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.

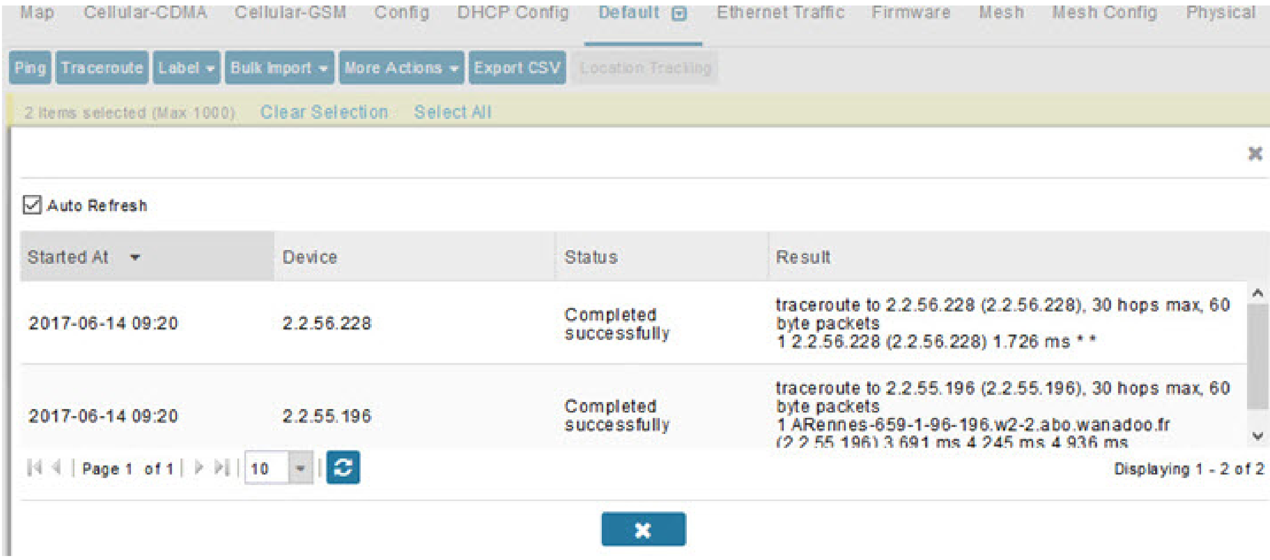
To trace routes to selected devices, in List view:

**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

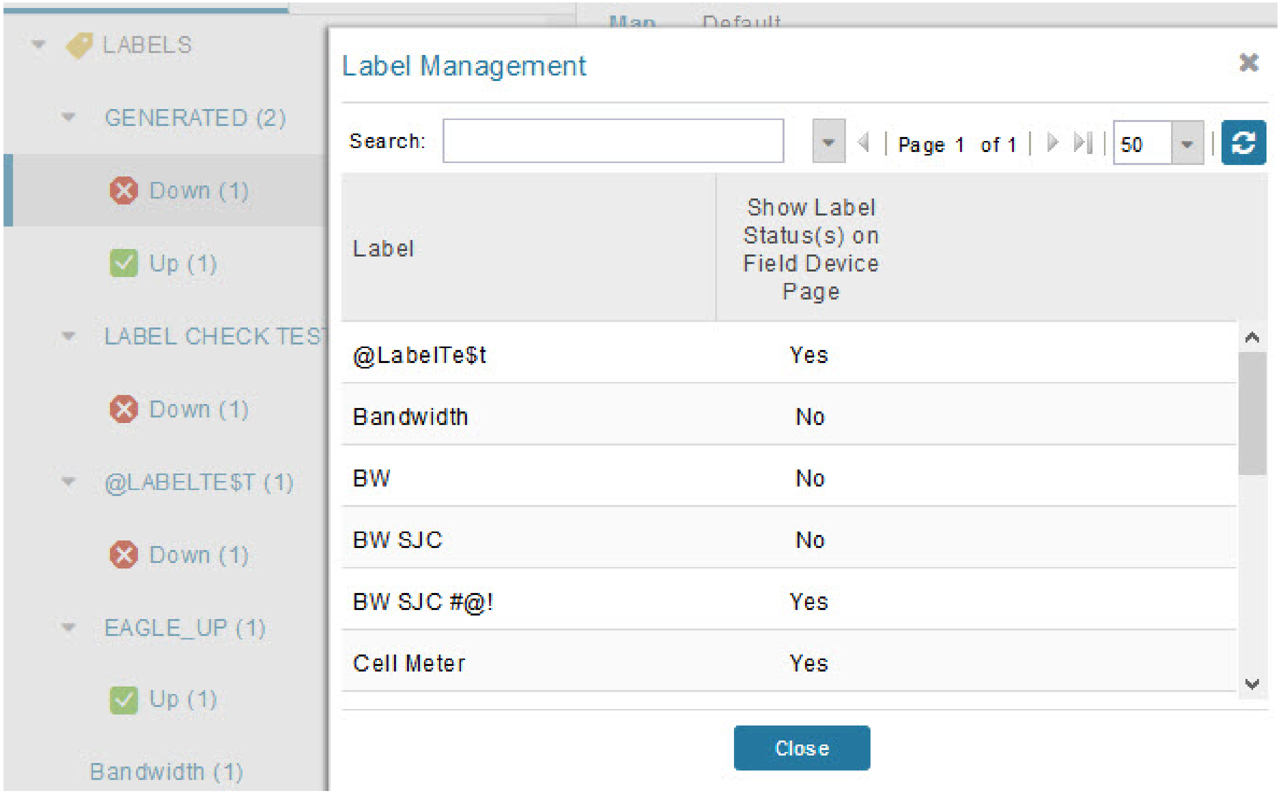
You use labels to create logical groups of devices to facilitate locating devices and device management.

## 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:

**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.

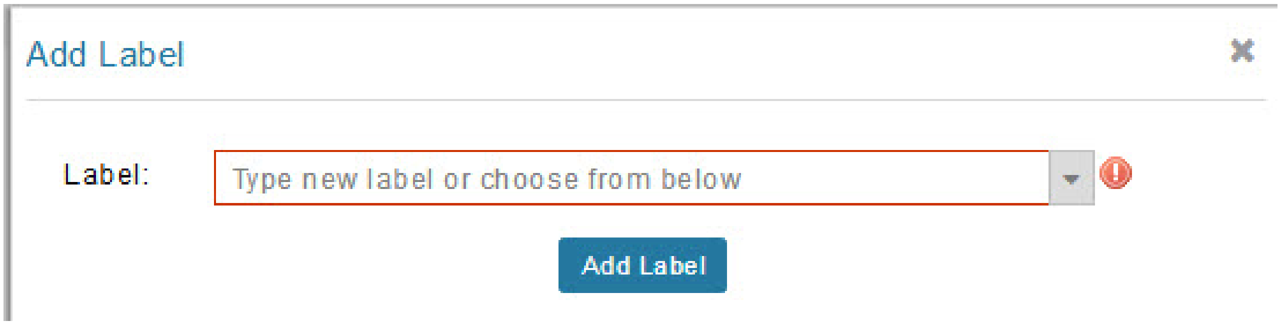
**Step 3** Click **Close**.

## Adding Labels

To add labels to selected devices, in List view:

**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 166.

## Removing Labels

To remove labels from selected devices, in List view:

**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**.

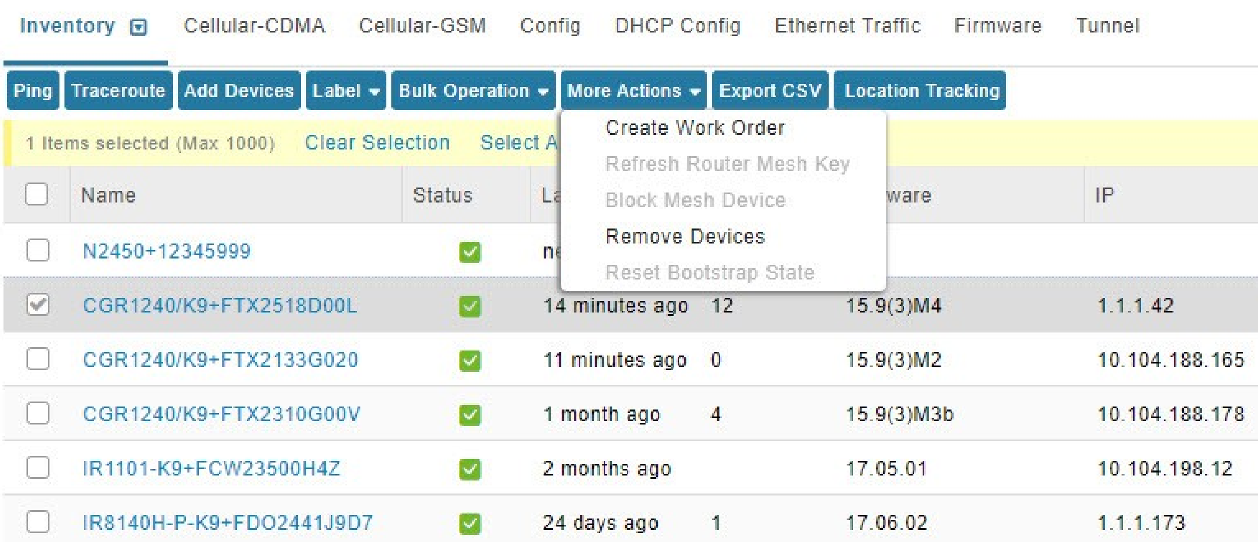
To remove labels in bulk, see Removing Labels in Bulk, on page 166.

# 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:

**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 155
- Head-end Router, Router, and Endpoint Information, on page 156

**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 21: NMS Server Pane Areas*

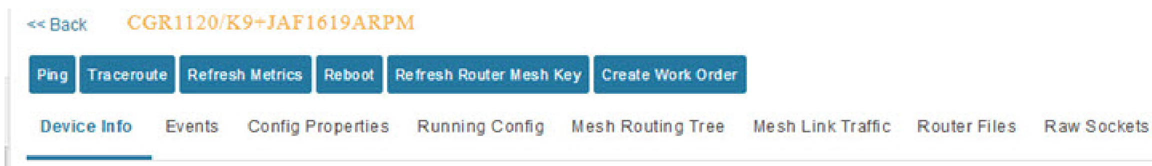
| Area and Field Name | Description |
|---|---|
| **Host System Information** | |

| Area and Field Name | Description |
|---|---|
| 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.<br>For more information on viewing the chart for default or custom-defined time intervals, refer to Setting Time Filters To View Charts, on page 335 |
| Memory Usage | Memory usage plotted in MB. |
| CSMP | CoAP Simple Management Protocol (CSMP) message statistics. |

## Head-end Router, Router, and Endpoint Information

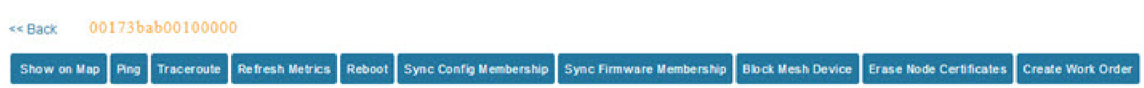
Select **DEVICES** > **Field Devices** and then select a device type (router, head-end router or endpoint) from the Browse Devices pane. Then, click on the Name of a specific system from the device list to see the available information (such as Device Info, Events, Config Properties, etc.) for that system 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 236).<br>For routers and endpoints, IoT FND also displays charts (see Viewing Device Charts, on page 358 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 236).<br>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 175. |
| Running Config (routers) | Displays the running configuration on the device. |
| Routing Tree (CGR1000, endpoints: gateway-IR500, meter-cgmesh, meter-OW Riva) | Displays the routing tree. For routers, the pane displays all the possible routers from the endpoints to the router. For endpoints, the Routing Tree pane displays the mesh route to the router. |
| Link Traffic (routers) | Displays the type of link traffic over time in bits per second. |
| Router Files (routers) | Lists files uploaded to the .../managed/files/ directory. |
| Raw Sockets (routers) | Lists metrics and session data for the TCP Raw Sockets (see table in the Raw Sockets Metrics and Sessions). |
| Embedded AP (IR829 only) | Lists inventory (configuration) details and metrics for the attached access point. |
| AP Running Config (C800 and IR8829 only) | Lists the running configuration file for the attached access point. |

# Actions You Can Perform from the Detailed Device Information Page




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

| Action | Description |
| --- | --- |
| **Show on Map** (C800, endpoints) | Displays a popup window with a map location of the device. This is the equivalent of entering **eid:***Device_EID* in the search field in Map View. |
| **Ping** | Sends a ping to the device to determine its network connectivity. See Pinging Devices, on page 151. |
| **Traceroute** | Traces the route to the device. See Tracing Routes to Devices, on page 151. |
| **Refresh Metrics**<br>(Head-end routers and routers only) | Instructs the device to send metrics to IoT FND.<br>**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**<br>(Mesh endpoints only) | Synchronizes the configuration membership for this device. See Synchronizing Endpoint Membership, on page 182. |
| **Sync Firmware Membership**<br>(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**<br>(Mesh endpoints only) | Blocks the mesh endpoint device.<br>**Caution** This is a disruptive operation.<br>**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**<br>(Routers and DA Gateway only) | Creates a work order. See Demo and Bandwidth Operation Modes, on page 232. |

# Using Filters to Control the Display of Devices

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

## Browse Devices Filters

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

## Creating and Editing Quick View Filters

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

## Creating a Quick View Filter

To create a Quick View filter:

---

**Step 1** On any device page, click **Show Filters** and add filters to the Search field

For more information about adding filters, see Adding a Filter, on page 159.

**Step 2** From the **Quick View/Rule** drop-down menu, choose **Create Quick View**.

**Step 3** In the Create Quick View dialog box that opens, enter a Name for the view.

**Step 4** Click the disk icon to save the view. To close without saving, click the X.

---

## Editing a Quick View Filter

To edit or delete a Quick View filter:

---

**Step 1** Click the Quick View tab and select the filter to edit.

**Step 2** From the **Quick View/Rule** drop-down menu, choose **Edit Quick View**

**Step 3** In the **Update Quick View** dialog box, make the necessary modifications, and then click **Save**

**Step 4** To delete the Quick View, click the **Delete** button.

---

## Adding a Filter

To add a filter to the Search field:

---

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

**Step 2** From the **Label** drop-down menu, choose a filter.

The drop-down menu defines filters for all device information categories. For more information about these categories, see Working with Router Views, on page 92.

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

For more information about operators, see Filter Operators, on page 160. If you choose a numeric metric from the Label menu (for example, **Transmit Speed**), you can specify a range of values in the filter you are adding. For date/time filters, “between” is the operator. Use the calendar buttons to specify the date range for the filter.

**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.

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

## Filter Operators

Filter Operators describes the operators you can use to create filters.

*Table 22: Filter Operators*

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

## Search Syntax

IoT FND supports this simple query language syntax:

Search := filter [filter ...]

Filter := fieldname operator value

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

Note the following when creating filters to search fields:

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

*Table 23: Filter Examples*

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

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

# Performing Bulk Import Actions

In IoT FND, you can perform 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:

**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 161

For more information about adding HERs, see Adding HERs to IoT FND, on page 162

For more information about adding routers, see Adding Routers to IoT FND, on page 163

**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/
EgDOdSb5dqw0u31OeVrEtPY0xBHraYgPv+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 like the following example that consists of a header line followed by one or more lines, each representing an HER:

```
eid,deviceType,lat,lng,ip,netconfUsername,netconfPassword
ASR1001+JAE1546007O,asr1000,40.0,-132.0,172.27.166.57,admin,cisco
ASR1001+JAE15460071,asr1000,40.0,-132.0,172.27.166.58,admin,cisco
```

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

**Note** For device configuration field descriptions, see Device Properties, on page 236

*Table 24: 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. |

| Field | Description |
|---|---|
| lat | (Optional) The location (latitude and longitude) of the HER. |
| lng | |
| ip | The IP address of the HER. The address must be reachable from the IoT FND server. |
| netconfAddress | |
| netconfUsername | The SSH username and password that IoT FND uses to connect to the HER. |
| netconfPassword | |

When you add an HER, IoT FND displays its status as Unheard. IoT FND changes the status to Up after it polls the HER. IoT FND polls HERs in the background every 15 minutes to collect device metrics, so it should take no more than 15 minutes for the status of HERs to change to Up after you add them to IoT FND. However, you can trigger the polling of HERs by clicking Actions You Can Perform from the Detailed Device Information Page.

## 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 236.

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

*Table 25: Router Import Fields*

| Field | Description |
|---|---|
| PID | The product ID, as supplied by Cisco. This is not printed on the product. |

| Field | Description |
|---|---|
| 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

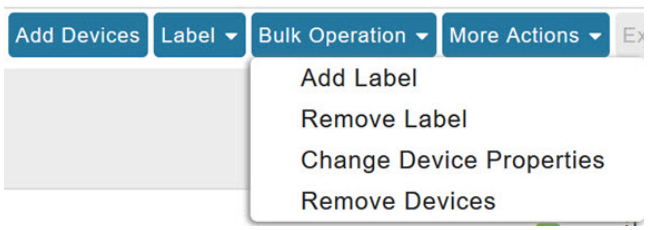
You can remove devices in bulk using a CSV file listing the EIDs of the devices to remove.

> **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.

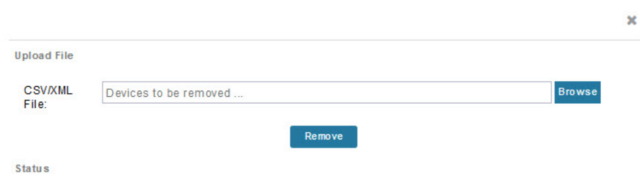
To remove devices in bulk:

**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:

**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:

**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:

**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:

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

IoT FND displays the list of rules stored in its database. Rule Fields 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. |

| Field | Description |
|---|---|
| Rule definition | The syntax of the rule. Some examples are listed below.<br>• IoT FND executes this rule when a device battery 0 level drops below 50%: `battery0Level<50`<br>• `deviceType:cgmesh eventName:up`<br>• `deviceType:ir500 eventName:outage` |
| Rule Actions | The actions performed by the rule. For example:<br>`Log Event With: CA-Registered, Add Label: CA-Registered`<br>In this example, the actions:<br>• Set the eventMessage property of the Rule Event generated by this rule to CA-Registered.<br>• 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 168

# Creating a Rule

To add a rule:

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

**Step 2** Click **Add**.

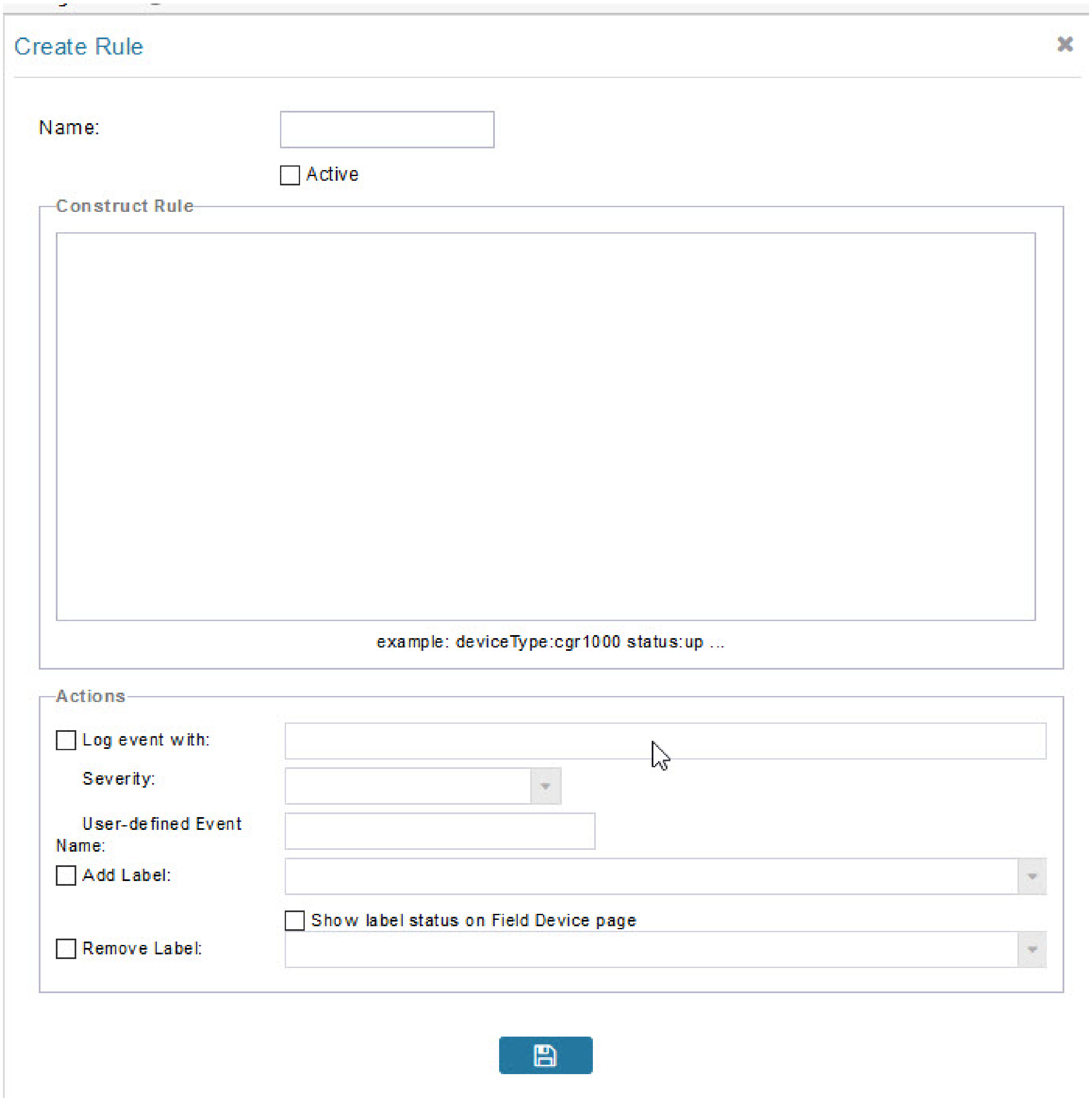
**Step 3** Enter a name for the rule.

**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, on page 160.




**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.<br>• **Severity** — Select the severity level to assign to the event.<br>• **User-defined Event** — Assign a name to the event Searching By Event Name, on page 344.<br><br>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):<br><br>`16494287: NMS-200-5: May 02 2017 22:32:41.964 +0000: %CGMS-7`<br>`-UNSPECIFIED: %`<br>`[ch=EventProducer][sev=DEBUG][tid=com.espertech.esper.Outbound-`<br>`CgmsEventProvider-1]: Event Object`<br>` which is send = EventObject`<br>`[netElementId=50071, eventTime=1335997961962, eventSeverity=0,`<br>` eventSource=cgr1000, eventType=UserEventType,`<br>` **eventMessage=Red Alert**`<br>`, **eventName=CHECK ROUTER**`<br>`, lat=36.319324, lng=-129.920815,`<br>`geoHash=9n7weedx3sdydv1b6ycjw, eventTypeId=1045,`<br>` 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:

**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:

**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:

**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 171
- Editing the ROUTER Configuration Template, on page 183
- Editing the ENDPOINT Configuration Template, on page 206
- Pushing Configurations to Routers, on page 207
- Pushing Configurations to Endpoints, on page 210


## Configuring Device Group Settings

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

# Creating Device Groups

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

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

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

**Note** You cannot delete the default groups, but you can change their names, although we do not recommend it. Also, the default ROUTER and ENDPOINT groups use the same icon, while custom groups use a different icon.


- Creating ROUTER Groups, on page 173
- Creating Endpoint Groups, on page 174


## Creating ROUTER Groups

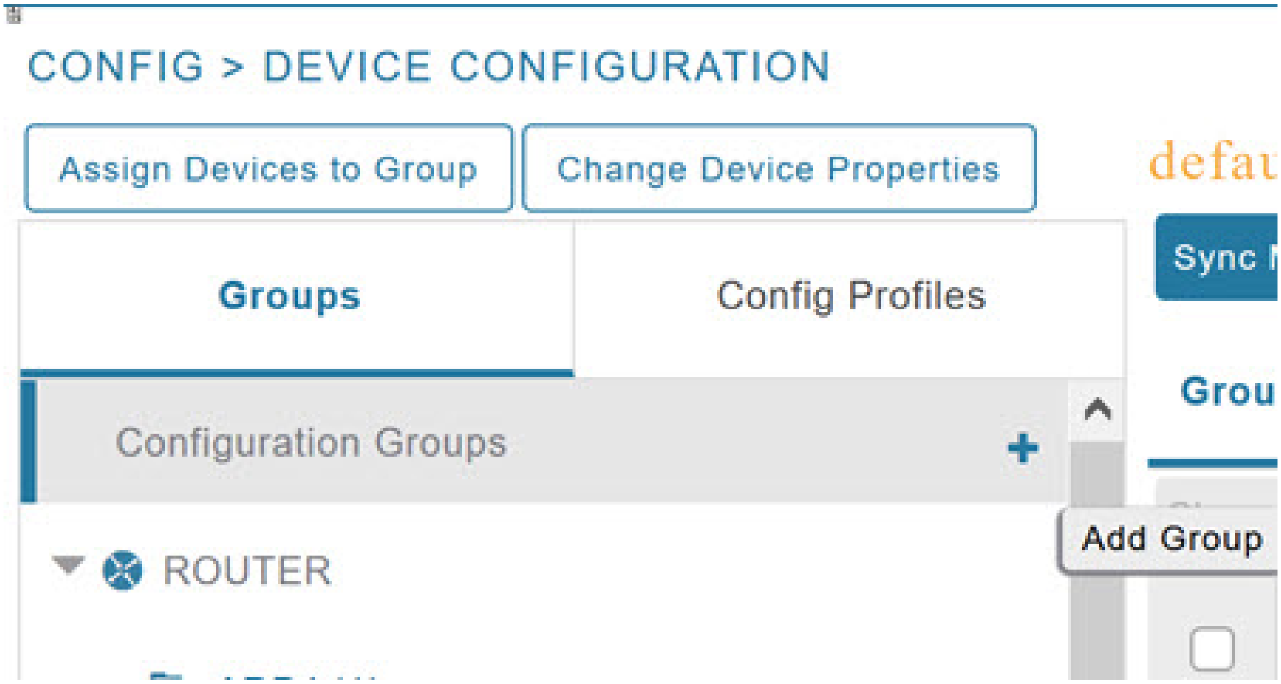
**Note** CGRs, IR800s, C800s, and C5921s (SBR) can coexist on a network; however, you must create custom templates that include all router types.

To create a router configuration group:

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

**Step 2** Select the default configuration group: **Default-cgr1000**, **Default-ir800**, **Default-c800**, **Default-ir1100**, **Default-ir8100**, **Default-ir1800**, **Default-sbr**, 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 178
- To remove a group, see Deleting Device Groups, on page 180

## Creating Endpoint Groups

To create an endpoint configuration group:

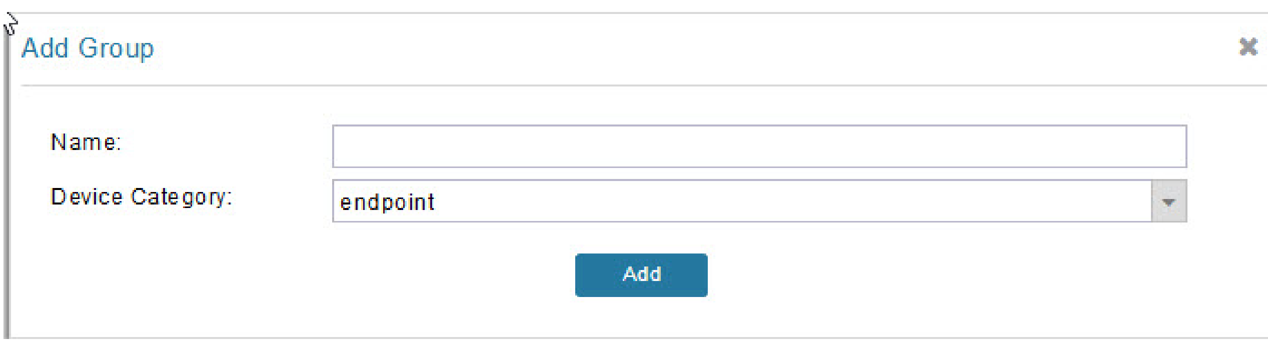
**Step 1** Choose **CONFIG** > **Device Configuration**.

**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 178
- To remove a group, see Deleting Device Groups, on page 180

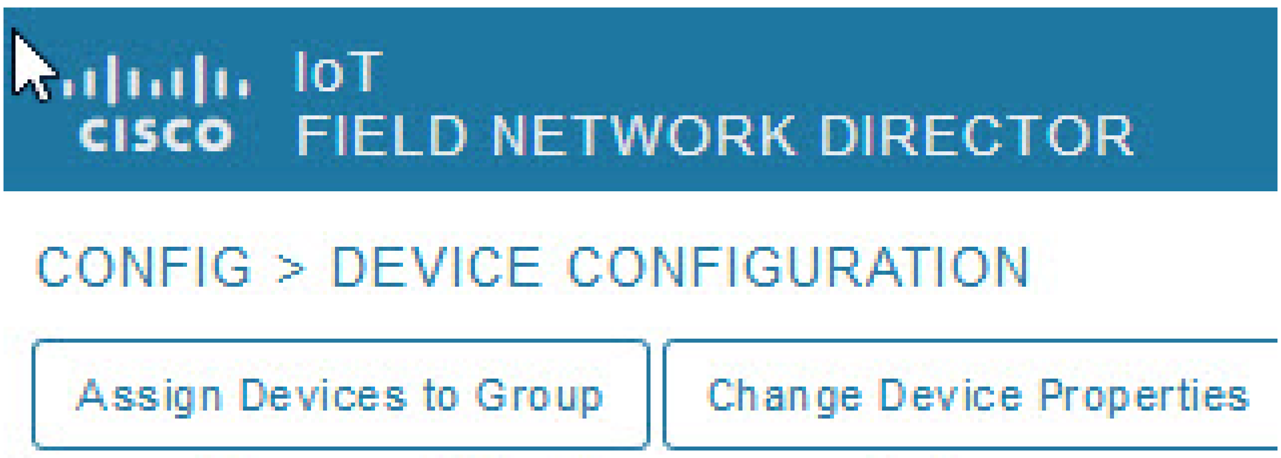
## Changing Device Configuration Properties

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:

**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 236.

## 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 Mark-Down Timer

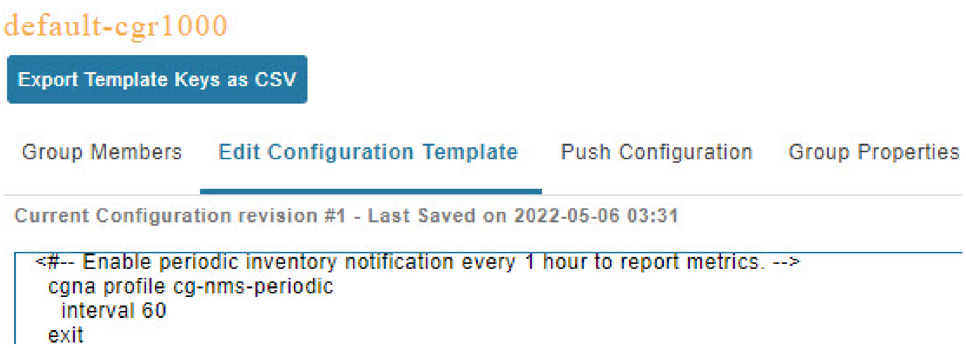
# Configuring Periodic Inventory Timer

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

**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.

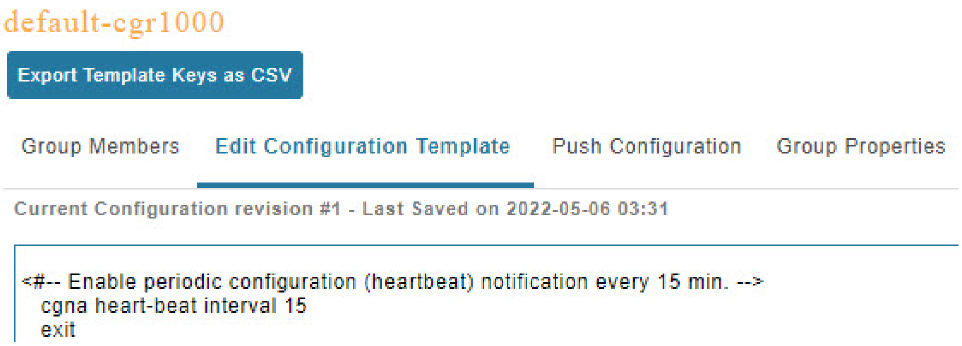
# Configuring Heartbeat Notification

To configure the heartbeat notification for a ROUTER configuration group:

**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 177.

**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 Configuring Heartbeat Notification .

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**).

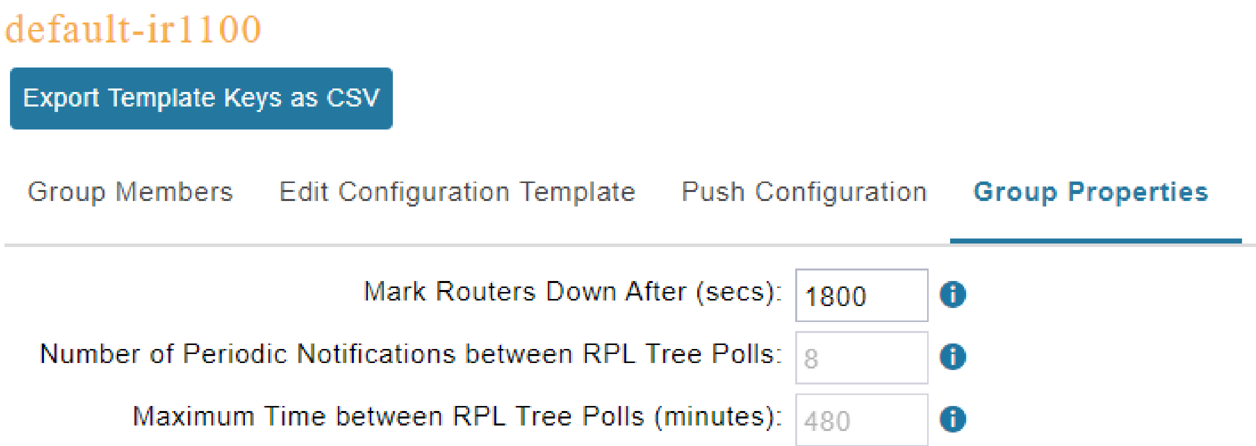
If the last heard value is greater than the device mark-down value, then IoT FND marks the device state as *Down* in the IoT FND GUI. However, before marking the device *Down*, IoT FND must check the status of the tunnel interface that is associated with the device. If the tunnel interface is *Down*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

**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 176.

**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:

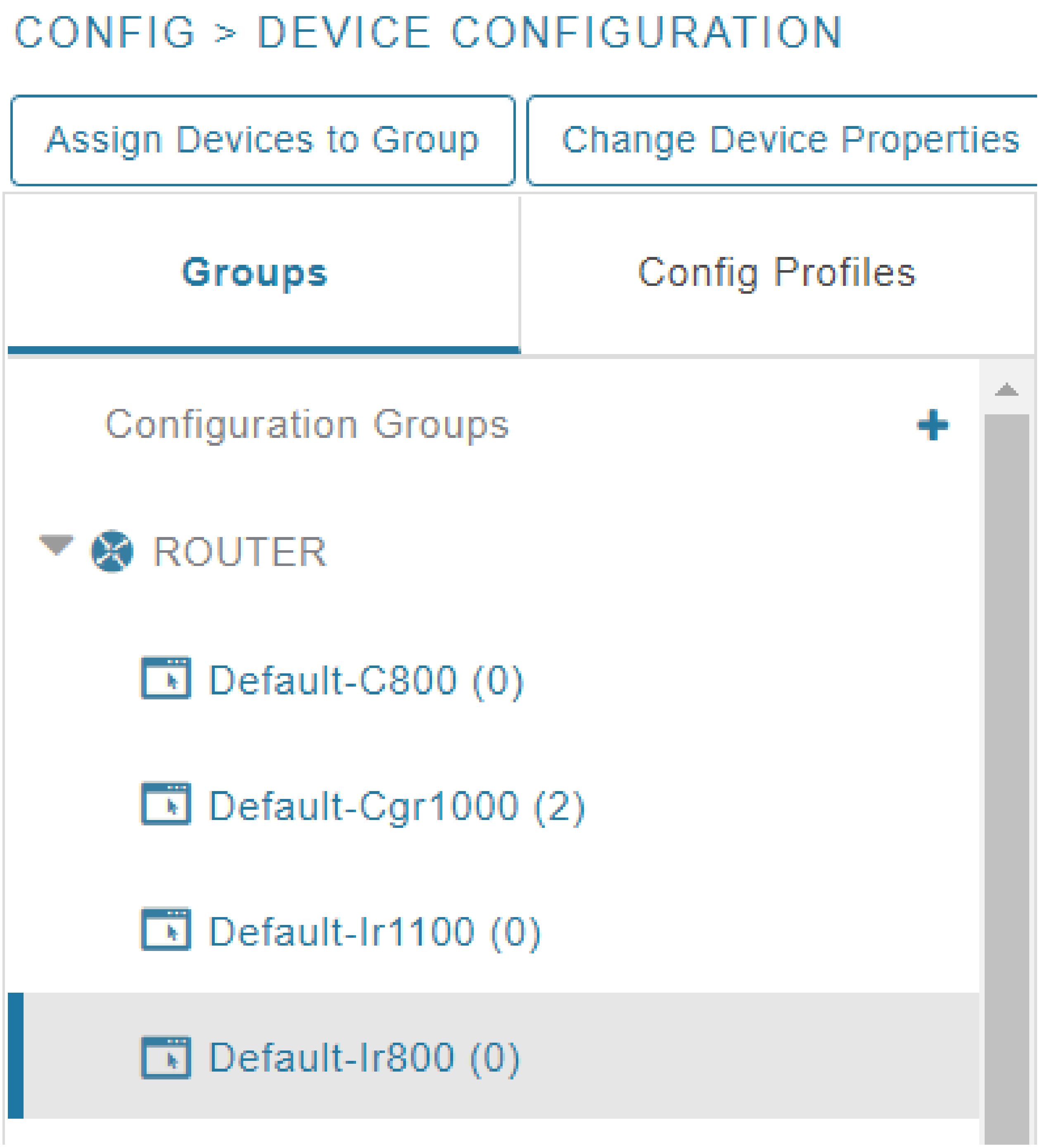
**Step 1** Choose **CONFIG** > **Device Configuration**.

**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:

**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

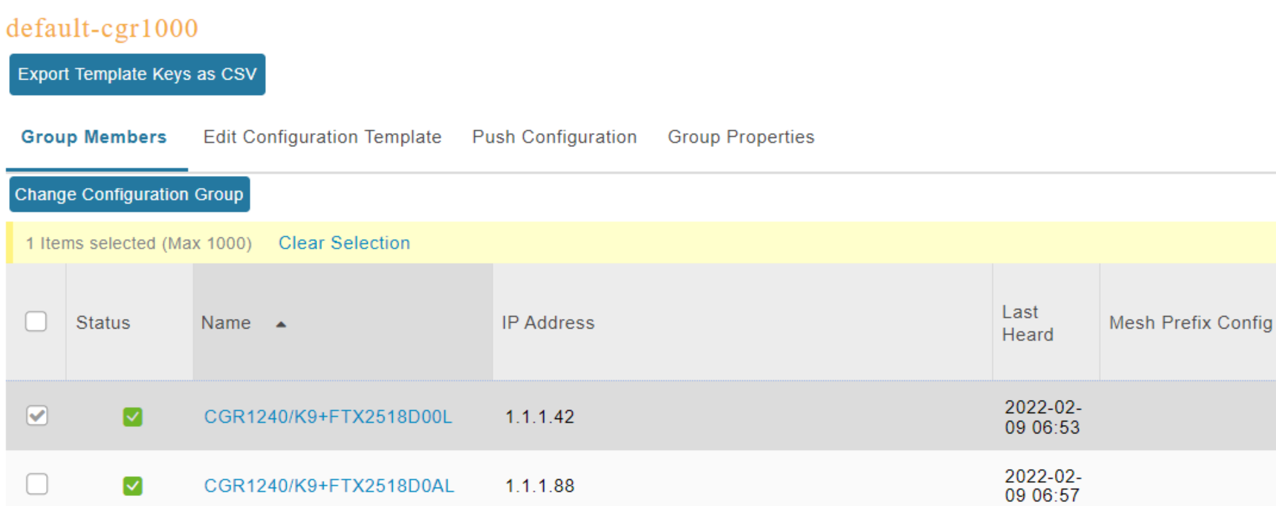
To move devices to another configuration group:

**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.

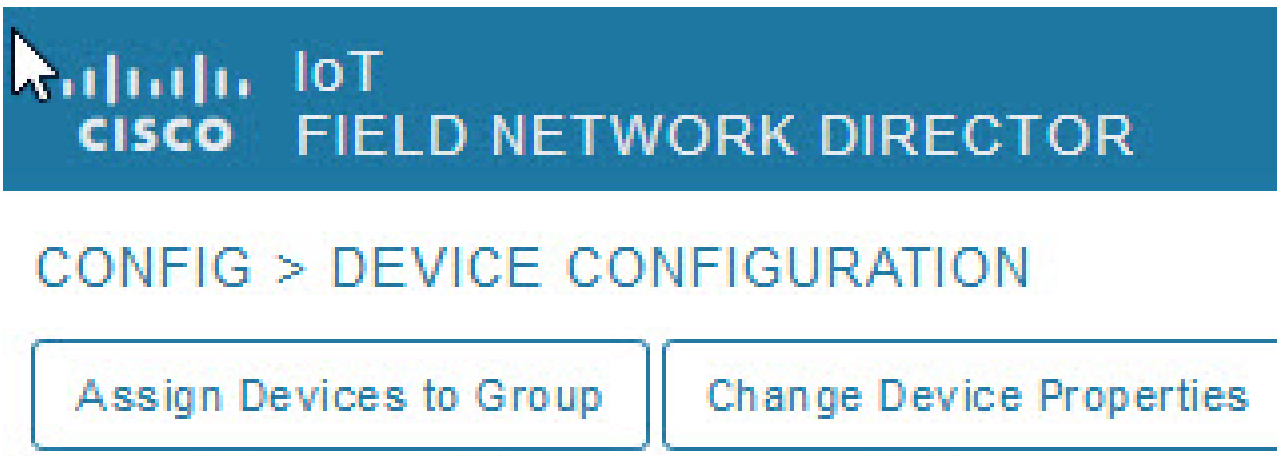
For example, this CSV file specifies the EIDs of three CGRs to move:

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

To move devices to another configuration group in bulk:

**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:

**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:

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

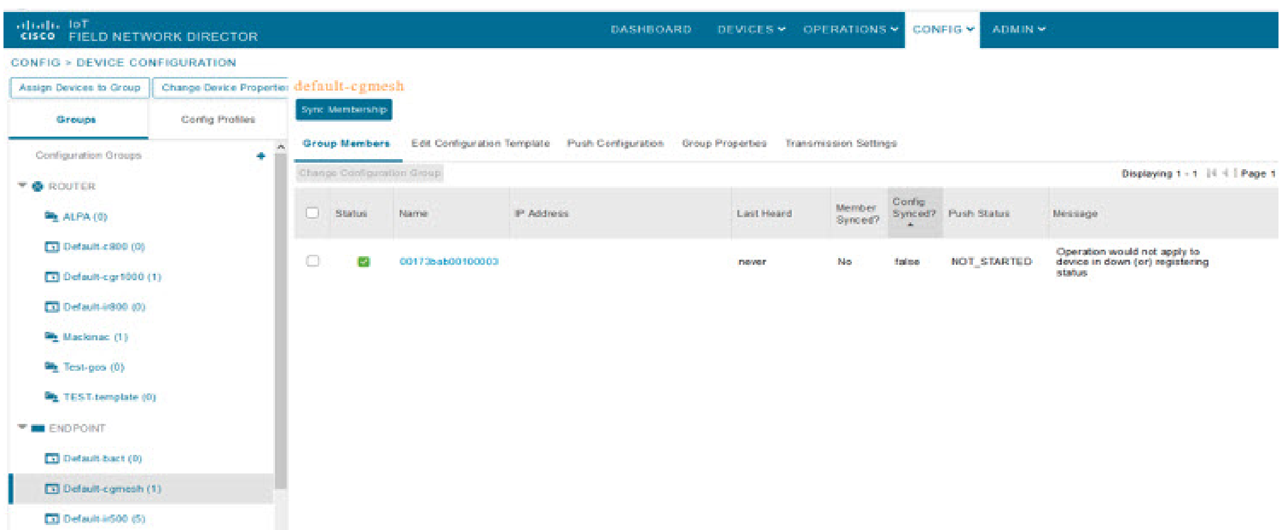
**Step 2** Select an ENDPOINT group (left pane) such as Default-cgmesh.

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

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

**Step 5** When prompted, click Yes to confirm synchronization.

**Step 6** Click **OK**.



# Editing the ROUTER Configuration Template

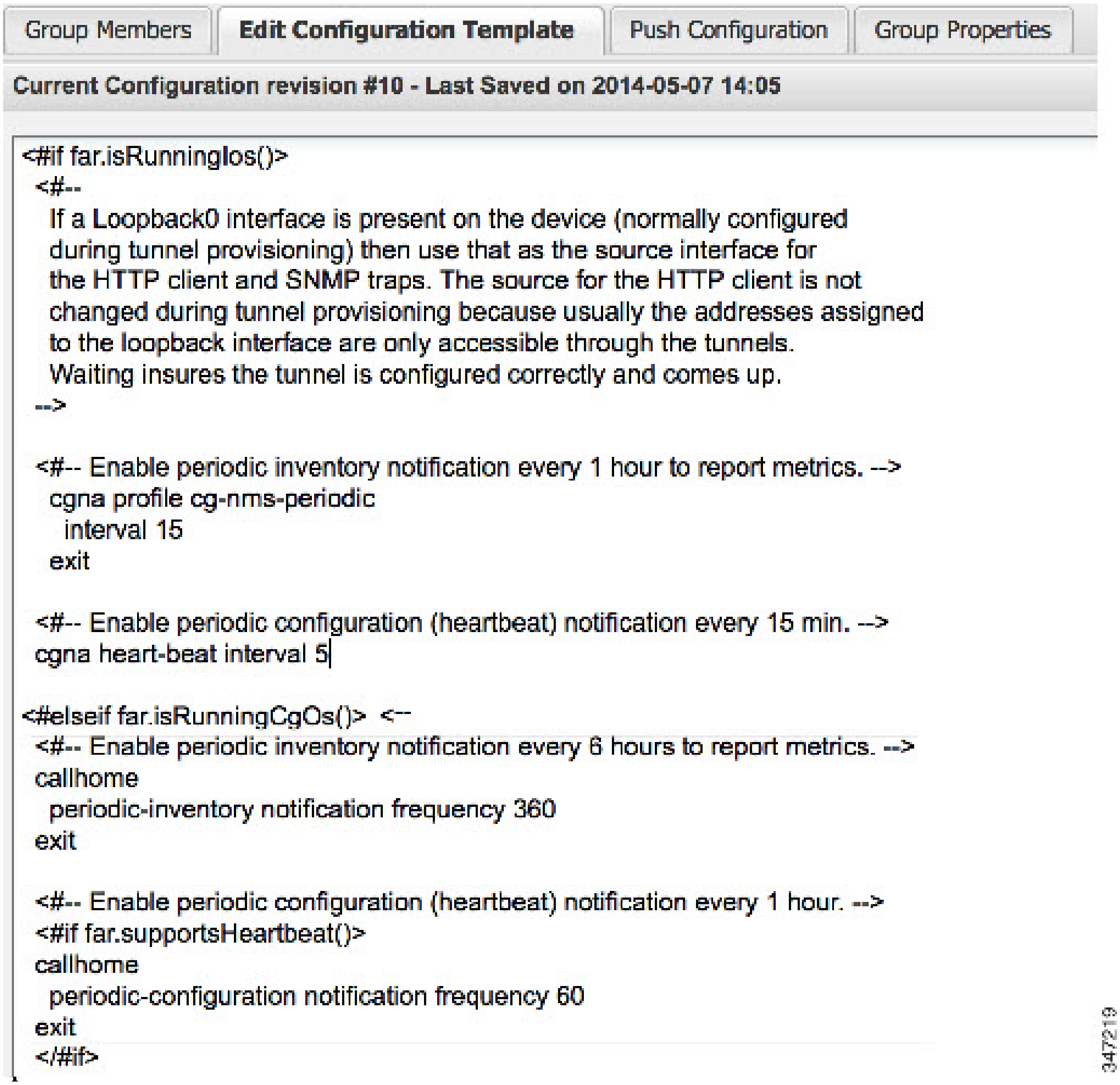
IoT FND lets you configure routers in bulk using a configuration template. When a router registers with IoT FND, IoT Field Network Director pushes the configuration defined in the default template to the device and commits the changes to the router startup configuration. IoT FND then retrieves the running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

To edit a ROUTER group configuration template:

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

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

**Step 3** Click **Edit Configuration**




**Step 4** Edit the template.

The template is expressed in FreeMarker syntax

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

**Step 5** Click **Save Changes**.

### What to do next

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

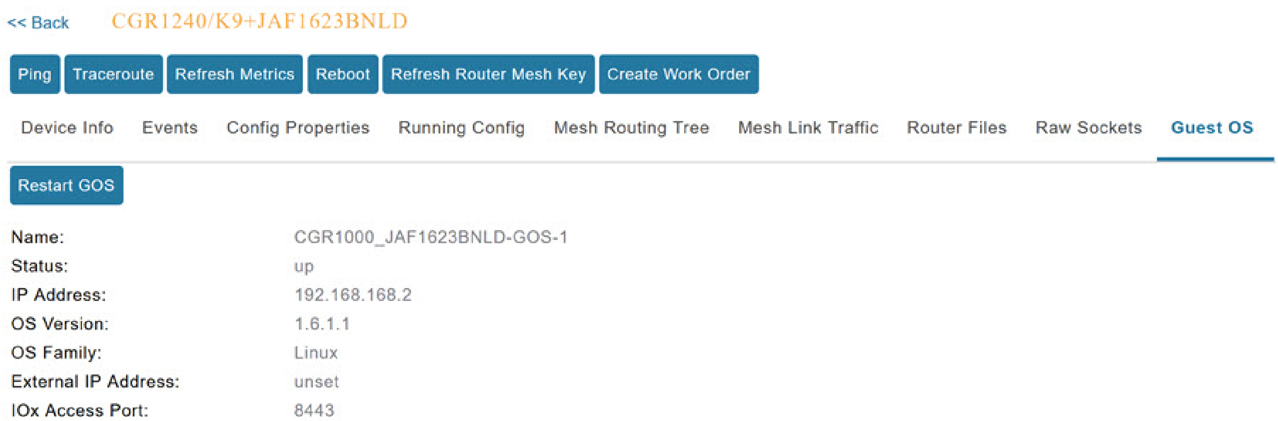
# Editing the AP Configuration Template

To edit an AP group configuration template:

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

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

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




**Step 4** Edit the template.

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

*AP TEMPLATE EXAMPLE*

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

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

.

**Step 5** Click **Save Changes**.

### What to do next

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

# Configuration Details for WPAN Devices

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

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

```
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A03
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A07
            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1806
            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1807
            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1808
            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1809
            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:180A
            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:180B
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A01
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C05
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C06
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C07
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A02
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A04
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A05
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C03
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C08
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C09
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C0A
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A06
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C02
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C04
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A08
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A09
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A0A
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C00
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C01
                            \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C0B
                    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A0B
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E00    // CY PLC nodes
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E01
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E02
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E03
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E04
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E05
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E06
            \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E07
RPL SLOT TREE: Num.DataEntries 44, Num.GraphNodes 45 (external 0) (RF 36) (PLC 8)
cisco-FAR5#ping
 2001:RTE:RTE:64:217:3BCD:26:4E01
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:RTE:RTE:64:217:3BCD:26:4E01, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 254/266/294 ms
cisco-FAR5#ping
 2001:RTE:RTE:64:207:8108:3C:1C00
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:RTE:RTE:64:207:8108:3C:1C00, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 272/441/636 ms
cisco-FAR5#
cisco-FAR5#show wpan 4/1 rpl stable

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

# Enabling Router GPS Tracking

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

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

```
<#--
Enable the following configurations to generate events that track if the router
moves by a certain distance (unit configurable) or within a certain time (in minutes)
-->
```

```
<#-- cgna geo-fence interval 10 -->
<#-- cgna geo-fence distance-threshold 100 -->
<#-- cgna geo-fence threshold-unit foot -->
<#-- cgna geo-fence active -->
```

**Note** Because GPS traps only generate Informational logs, we recommend that you create a rule-based event with high severity (such as CRITICAL) to inform the administrator of router movement. An example of this type of rule definition is: configGroup:name eventName:deviceLocChanged (see Creating a Rule, on page 168)

## Configuring 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 that the trap was received by IoT FND. To enable SNMP v3 Informational Events, uncomment the following lines in the default configuration file and push the new configuration file to all router(s) in the group:

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

# Support of Dual WPAN for IR8100

Cisco IoT FND supports dual Wireless Personal Area Network (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. IoT FND uses the slot number in which the module is inserted for mapping the inventory details of the respective WPAN interface. In 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. For example, the Tx speed of the WPAN inserted in slot 1 is Mesh Tx, Tx speed of the WPAN inserted in slot 2 is Mesh Tx2, and the Tx speed of the WPAN inserted in slot 3 is Mesh Tx3.

**Note** All the parameters related to WPAN are displayed based on the slot number whereas user configurable parameters are displayed based on the number of the interface.

The 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).

**Note** We recommend you to reregister the device after WPAN addition or removal.

**Note** Cisco IoT FND 4.8.1 supports dual WPAN feature for IR8100 with firmware version greater than or equal to 17.08.01. IoT FND maps the properties or metrics of WPAN based on the slot number in which it is inserted. However, if the firmware version of registered IR8100 is less than 17.08.01, IoT FND processes the properties or metrics the same way as it does for single WPAN i.e., the mapping is not based on slot number. For example, though the WPAN is inserted in slot 2 of the IR8100 with firmware version <17.08.01, the related properties or metrics always point to a set of attributes without the slot number suffix.

This leads to the following scenarios:

- With IoT FND 4.8.1, the firmware upgrade of IR8100 from version < 17.08.01 to a version >=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 IR8100 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 IoT FND 4.8.1 upgrade process, the already registered IR8100 device with firmware version >= 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 IR8100 is already mapped to existing set of mesh properties or metrics (without the slot number suffix).

**Limitations**

High Availability feature in WPAN is not supported by IR8100 and so it is not supported for dual WPAN.

*Table 26: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Support of Dual WPAN for IR8100 | IoT FND 4.8.1 | 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. |

# Prerequisites for Dual WPAN

The following are the prerequisites to support dual WPAN in IR8100:

- 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.

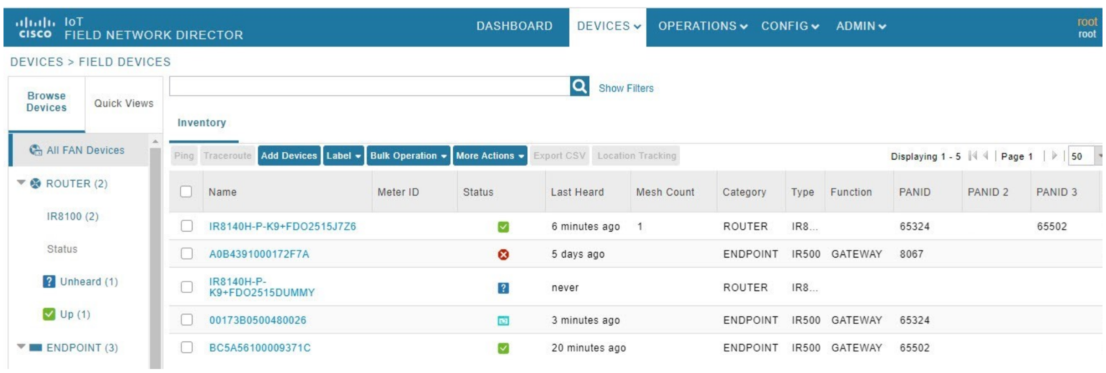
# Support of Dual WPAN in Field Device Page

Select **DEVICES** > **FIELD DEVICES**. The FAN view is visible where all the devices are listed. You can view WPAN related information in this Field Device page.

**Note** If WPAN is not inserted in slot 1, then all the columns appear empty. If the WPAN is inserted in either slot 2 or slot 3, you can view WPAN related parameters by adding them. For more information, see Adding Device Views, on page 145. This displays the respective parameters related to WPAN inserted in either slot 2 or slot 3.

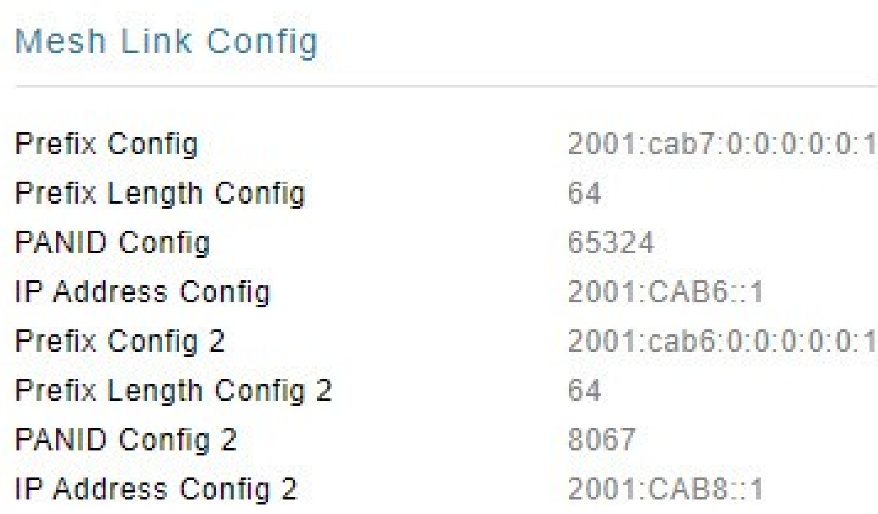
- In the FAN device view, you can view PANID 2 and PANID 3 columns in the Inventory tab that indicates the meshPanID parameter of WPAN that is inserted in either slot 2 or slot 3.

**Note** If the WPAN module is not inserted in the respective slot, the corresponding column appears empty. The PANID 2 and PANID 3 columns appear empty for other devices.



- To add user configurable parameters for both the WPAN interfaces:
  - Upload a csv file from the device list page. For more information on uploading csv, see Changing Device Properties in Bulk, on page 165.
  - After uploading, navigate to **DEVICES** > **FIELD DEVICES** > **Browse Devices tab** > **IR8100**. Click Mesh Config tab to view the uploaded values. or

Navigate to **DEVICES** > **FIELD DEVICES** > **Browse Devices tab** > **IR8100**. Click the device on the right pane to view the device information. Go to Config Properties tab to view the Mesh Link Config details displayed for both the WPANs with the parameters suffixed according to the slot number.



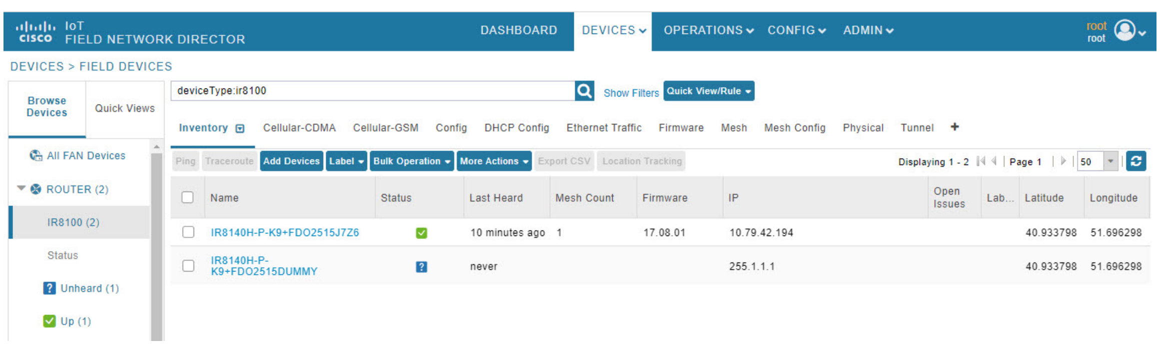

# Support of Dual WPAN in Router Device View

In the **DEVICES** > **FIELD DEVICES** page, select Router group in the Browse Devices tab.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 145.

# Support of Dual WPAN in IR8100 Device View

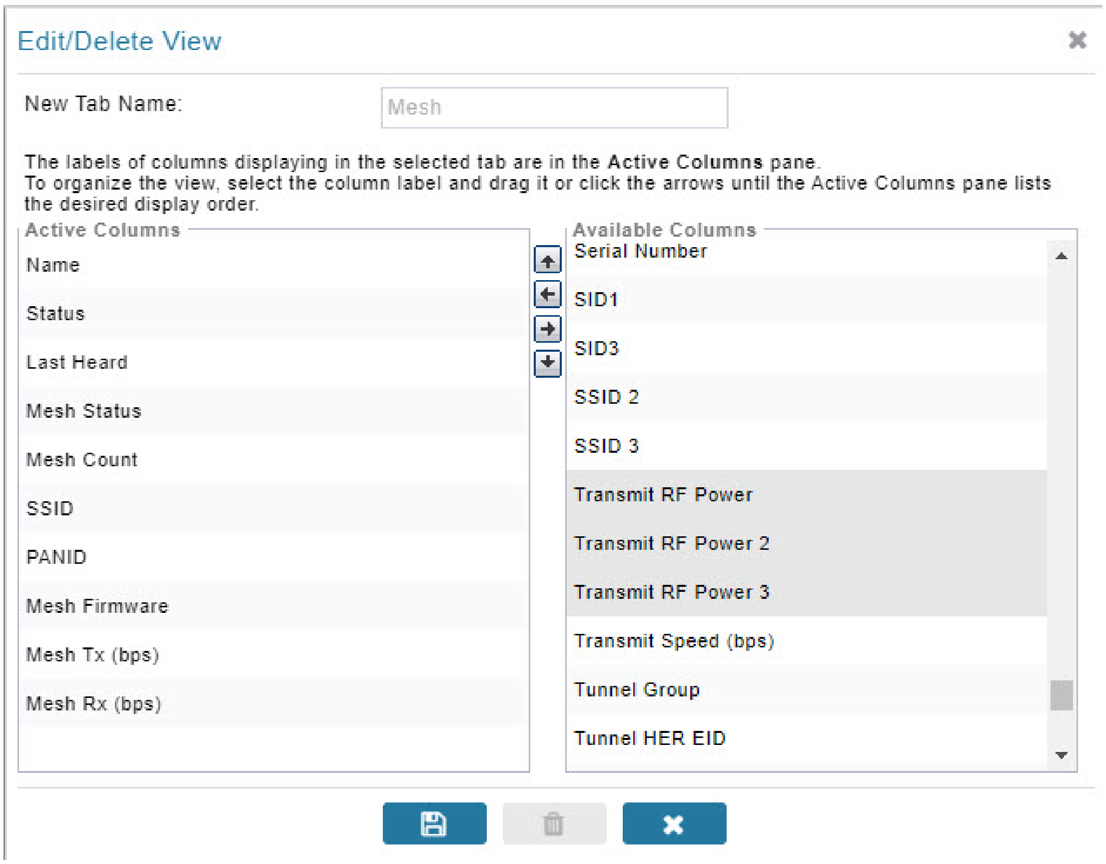
In the **DEVICES** > **FIELD DEVICES** page, select IR8100 under Router category in the Browse Devices tab.

In the Inventory tab, the IR8100 device view displays the parameters for the WPAN inserted in slot 1 by default. The Mesh tab and Mesh Config tab show the existing properties related to WPAN inserted in slot 1.



Additional WPAN parameters are included for the WPANs that are inserted in other slots. You can view the additional attributes by customizing your default view. To add a new tab or edit the existing default view:

- Click + to create a new tab and add WPAN related fields. or
- 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, on page 144.

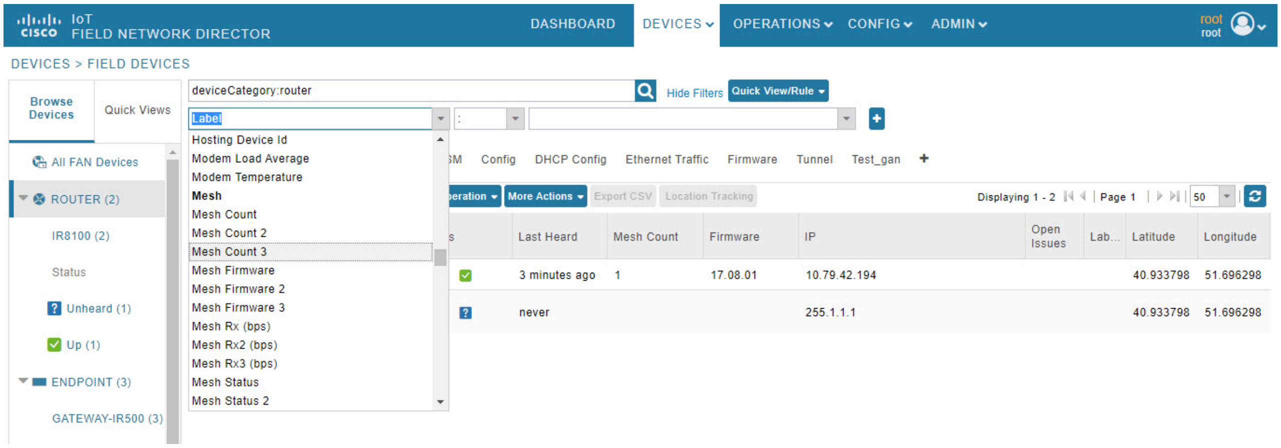



## Using Filters to View Additional Dual WPAN Fields

The newly added WPAN parameters are available in the show filter. You can choose the show filter based on the slot number in which the WPAN is inserted.

**Step 1** Click **Show Filters** in the default view.

**Step 2** Select the WPAN parameters from the drop-down list and enter the search criteria. The search results are displayed in the page accordingly. For more information on filters, see Using Router Filters, on page 97.

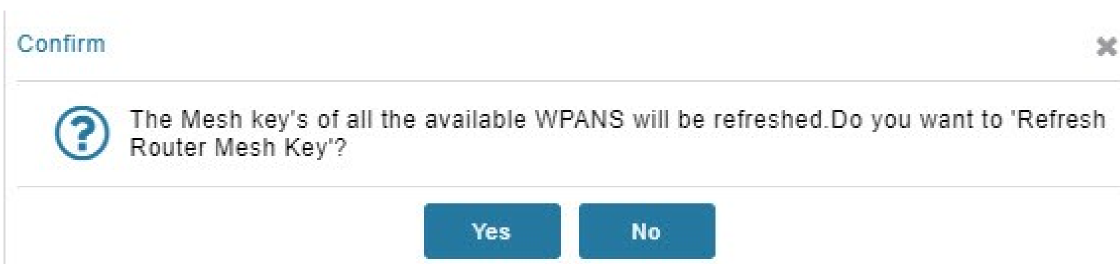



# Refreshing the Router Mesh Key for Dual WPAN

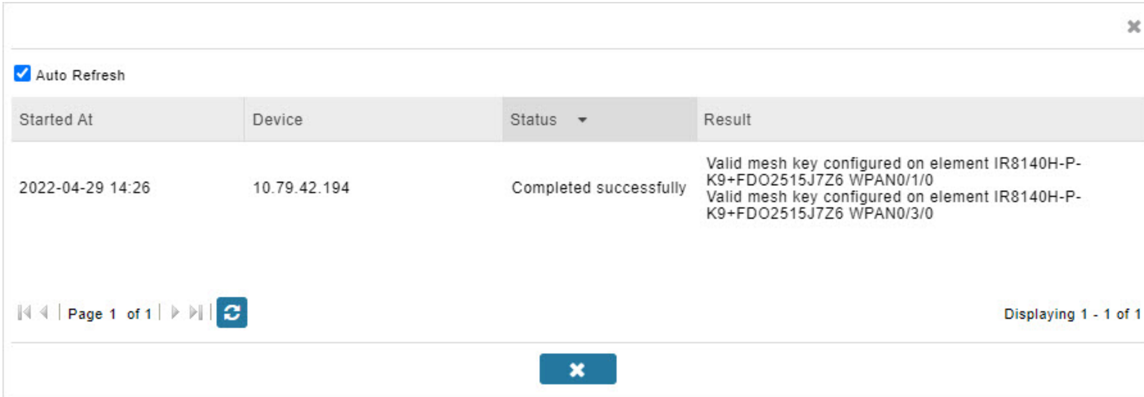
Refreshing the router mesh key helps to avoid the downtime of devices once they are expired.

- Navigate to **DEVICES** > **FIELD DEVICES** > **Browse Devices tab** > **IR8100**. Select the IR8100 devices for which you want to refresh the router mesh key. Go to **More Actions** > **Refresh Router Mesh Key**. For more information, see Refreshing the Router Mesh Key. or
- Navigate to **DEVICES** > **FIELD DEVICES** > **Browse Devices tab** > **IR8100**. Click the IR8100 device for which you want to refresh the router mesh key. In the device details page, click **Refresh Router Mesh Key** button.

FND triggers the refresh of mesh key for both the WPANs (with different expiration periods) that are inserted in any of the three available slots. A confirmation message appears.



Click **Yes** to continue. The following window displays the status of the router refresh.




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

# Support of Dual WPAN on Device Details Page

To view dual WPAN related information associated with IR8100,

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

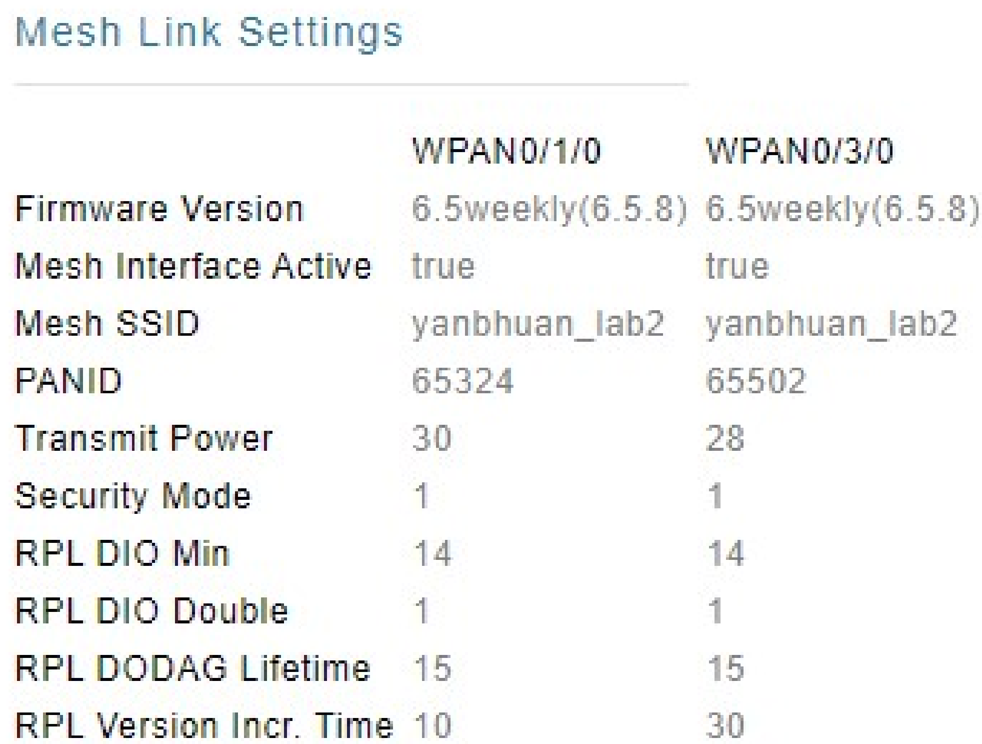
**Step 2** Select IR8100 router group on the left pane.

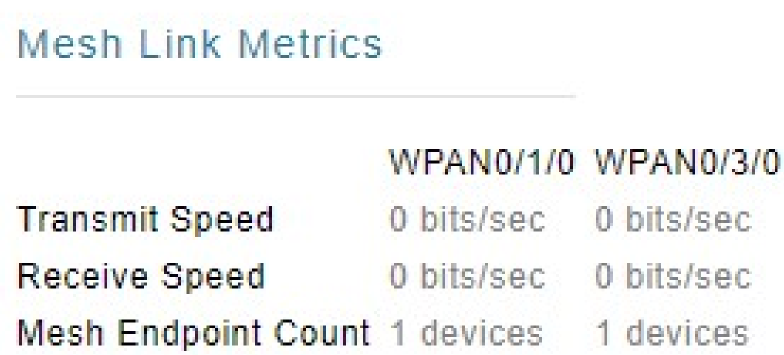
**Step 3** Click the IR8100 device on the right pane.

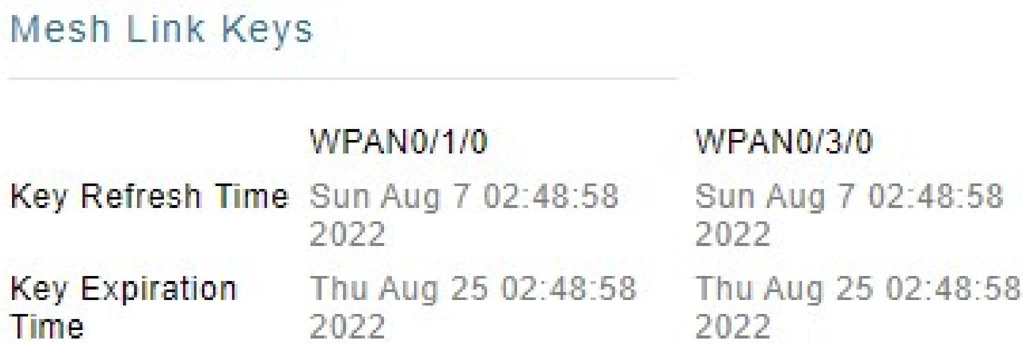
The device details page displays information for the selected device.

## Viewing Device Info Tab

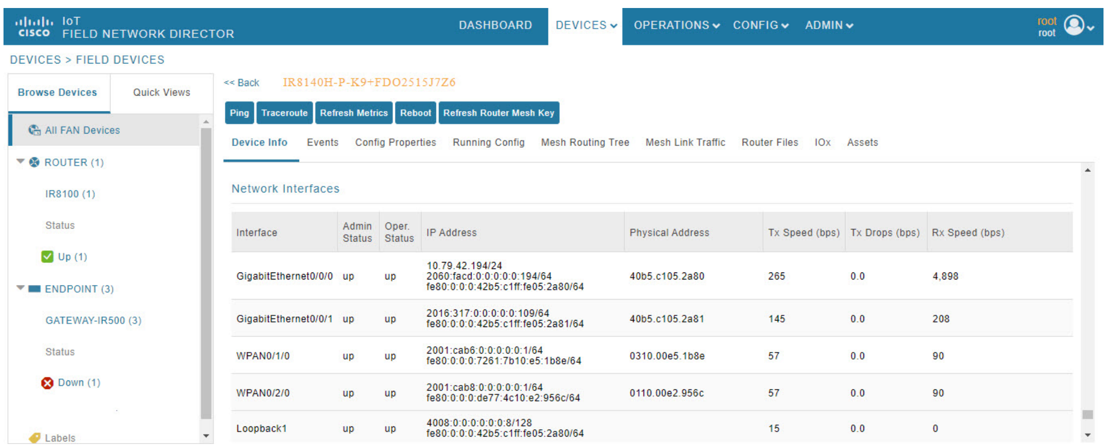
- The Mesh Link Settings, Mesh Link Metrics, and Mesh Link Keys section displays the values of the various parameters which are retrieved from both the WPANs. Under each section, the columns with WPAN interface name are displayed and the respective value of the parameters is listed under the respective column. The following view displays the parameter values of the WPANs inserted in slot 1 and 3. For more information on Mesh Link Settings, see Link Settings, on page 246. For more information on Mesh Link Metrics, see Link Metrics, on page 245. For more information on Mesh Link Keys, see Mesh Link Keys, on page 247.


Mesh Link Settings
WPAN0/1/0
WPAN0/3/0
Firmware Version
6.5weekly(6.5.8)
6.5weekly(6.5.8)
Mesh Interface Active
true
true
Mesh SSID
yanbhuan_lab2
yanbhuan_lab2
PANID
65324
65502
Transmit Power
30
28
Security Mode
1
1
RPL DIO Min
14
14
RPL DIO Double
1
1
RPL DODAG Lifetime
15
15
RPL Version Incr. Time
10
30


Mesh Link Metrics
WPAN0/1/0
WPAN0/3/0
Transmit Speed
0 bits/sec
0 bits/sec
Receive Speed
0 bits/sec
0 bits/sec
Mesh Endpoint Count
1 devices
1 devices




- 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.

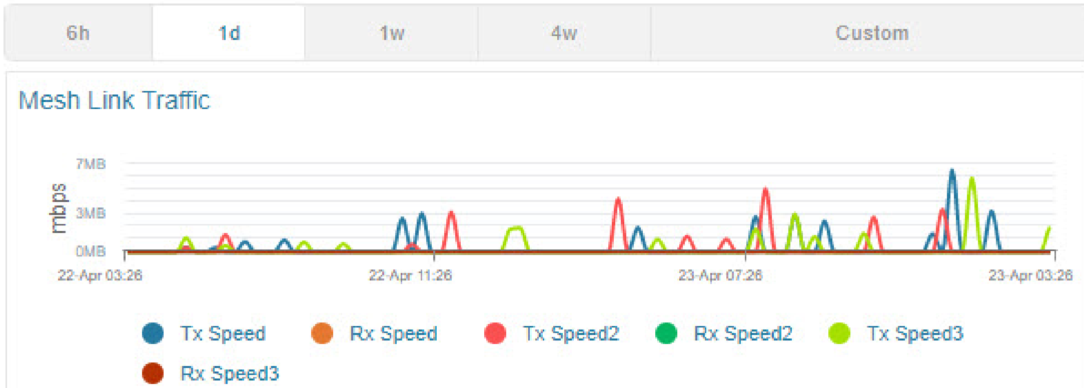



The following table describes the Network Interface fields in the Device Info page.

| 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 |

- The Device Info tab displays 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 colour coded to distinguish the slot in which the

WPAN is inserted. For example, the colour used for Tx or Rx speed of WPAN in slot 1 is different from that of WPAN in slot 2.

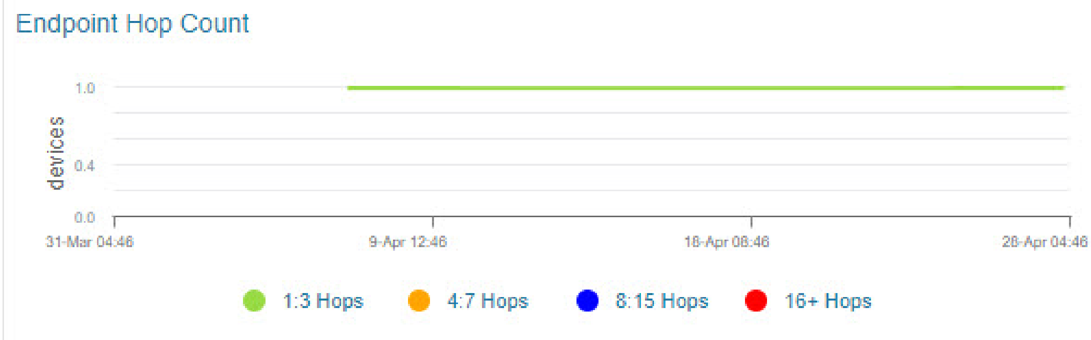



**Note** Click on colour code and the respective line in the chart is removed from the graph. This applies for all the charts.

- The endpoint count chart shows the aggregated endpoint count which is connected to both the WPAN interfaces as well as individual endpoint count from each WPAN interface. Three new colour codes are added to indicate the WPANs connected in slot one, two, and three. The Total Endpoint Count shows the sum of endpoints connected in both the WPANs whereas Endpoint Count shows the number of endpoints connected in the WPAN that is inserted in slot 1. Endpoint Count 2 and Endpoint Count 3 represent the number of endpoints connected in WPAN 0/2/0 and WPAN 0/3/0.

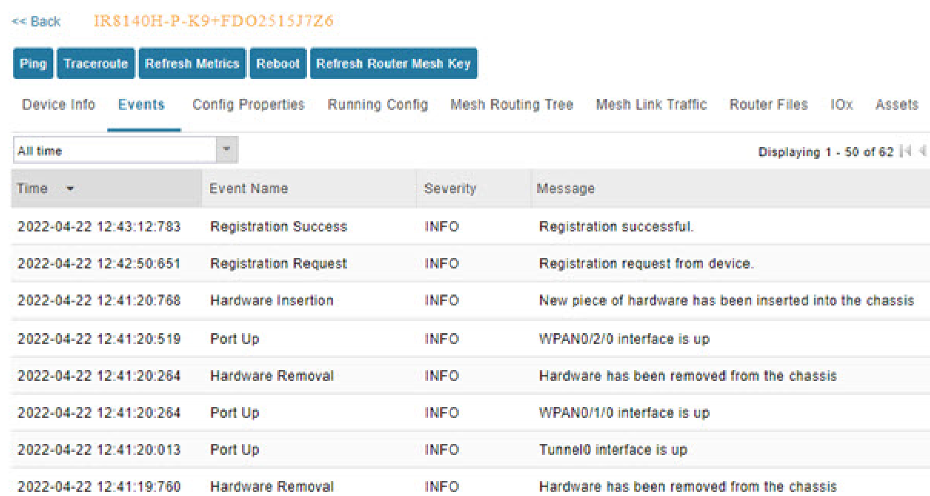
**Note** If two WPANs have the same endpoint count, the endpoint count line of the WPAN inserted in higher slot number overlaps the endpoint count line of the WPAN inserted in lower slot number. For example, when two WPANs are connected in slot 3 and slot 1, then the endpoint count line indicating the WPAN inserted in slot 3 overlaps the endpoint count line indicating the WPAN inserted in slot 1. To see the individual endpoint count, click on colour code and the respective line in the chart is removed from the graph.

- The endpoint hop count chart shows an aggregated endpoint count between the hops connected to both the WPAN interfaces.




## Viewing Dual WPAN Events

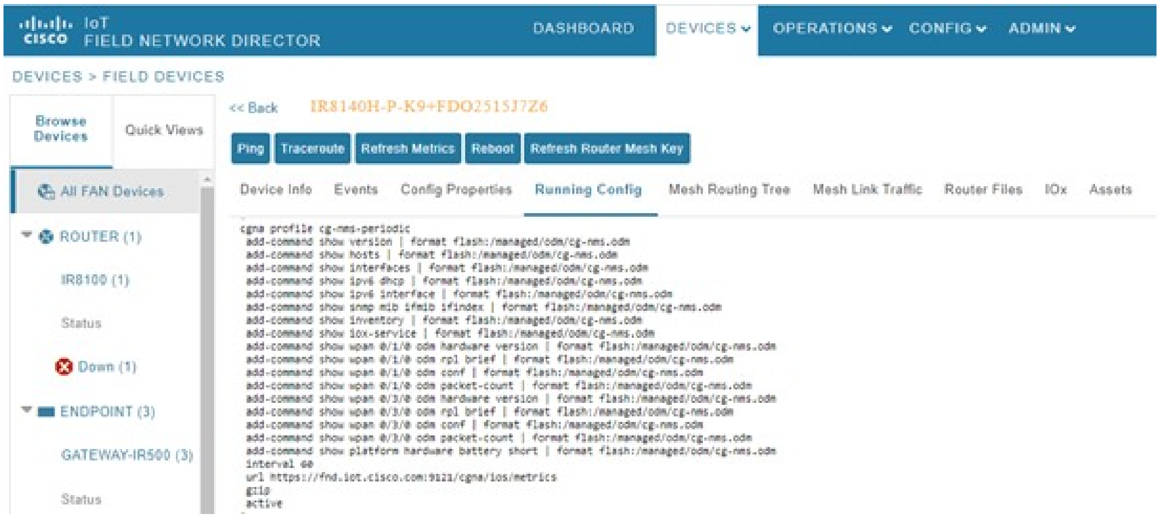
In the device details page, navigate to Events tab. This tab displays the events and alerts for both WPANs.




For more information on this, see Viewing Events.

## Viewing Running Config Tab

In the Running Config tab, both the WPAN related show commands are displayed.




## Viewing Mesh Routing Tree

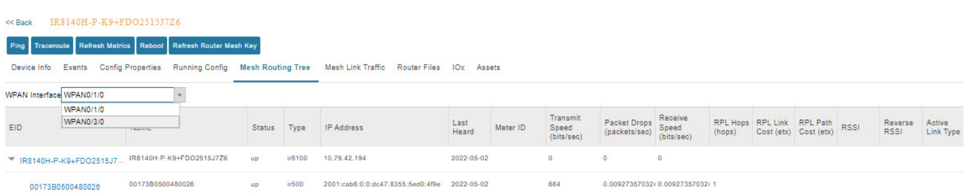
The Mesh Routing Tree tab allows you to select the available WPAN interface for which you want to see the mesh routing table information. For example, if you want to see the mesh routing tree information of WPAN inserted in slot number one, then you must select WPAN0/1/0.

**Note** By default, the 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.

**Step 1** Click **Mesh Routing Tree** tab in the device details page.

**Step 2** Select the required WPAN slot number from the WPAN Interface drop-down list.

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



The following 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. |

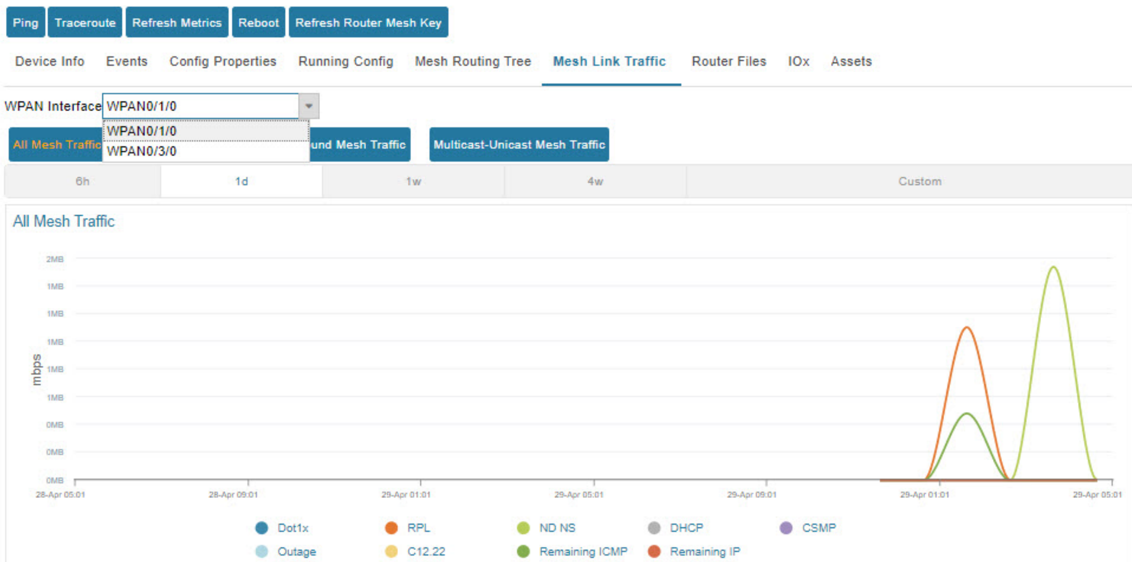
| Field | Description |
|---|---|
| IP Address | Indicates the IP address of the device. |
| Last Heard | Last date and time the device contacted IoT FND. |
| Meter ID | Meter ID of the device. |
| Transmit Speed (bits/sec) | Indicates the speed (bits/sec) of data transmitted by the interface. |
| Packet 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. |
| 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. |

**Note** During RPL tree polling, the information is fetched from both WPAN interfaces and processed by FND. For more information on polling, refer to Configuring RPL Tree Polling, on page 83.

## Viewing Mesh Link Traffic Chart for Dual WPAN

Click Mesh Link Traffic tab in the device details page. Select the WPAN interface from the drop-down list. The chart displays the mesh link metrics per interface based on the selection of all mesh, inbound mesh, outbound mesh, or multicast-unicast mesh traffic button. Click the default or custom-defined time intervals to view charts based on the selection. For more information, see Setting Time Filters To View Charts, on page 335.

**Note** By default, the 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.




# Support of Dual WPAN in Device Configuration Page

Choose **CONFIG** > **Device Configuration** > **ROUTER** > **Default-Ir8100**.

- 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.

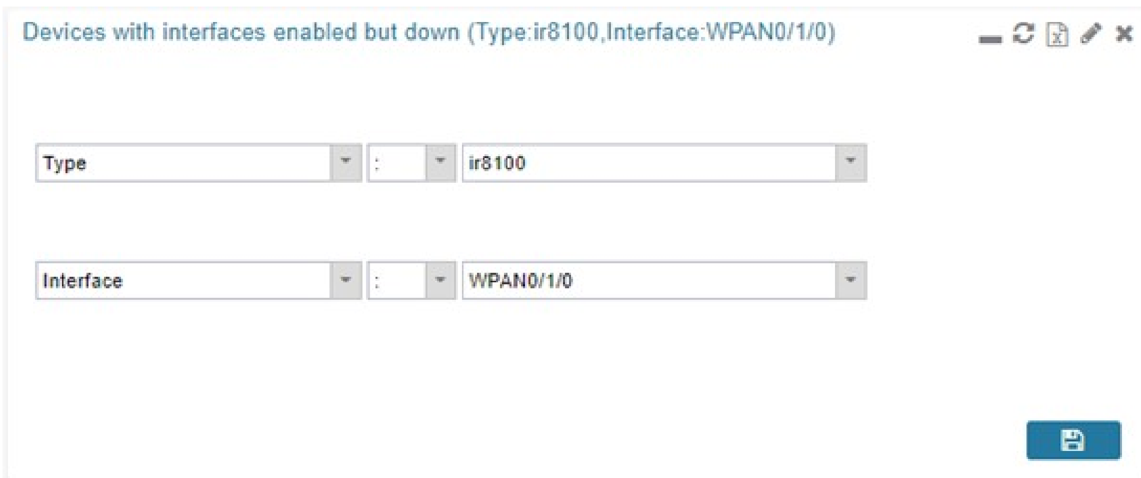

- Edit Configuration Template tab—The page allows you to define user configurable parameters in the template. FND maps the defined parameters to the WPAN parameter value configured through CSV. To configure the user configurable parameters:
  - Navigate to Edit Configuration Template tab.
  - Enter the parameter values in the template and click the disk icon. The WPAN specific user configurable parameters are displayed in the Running Config tab in the device details page as well.

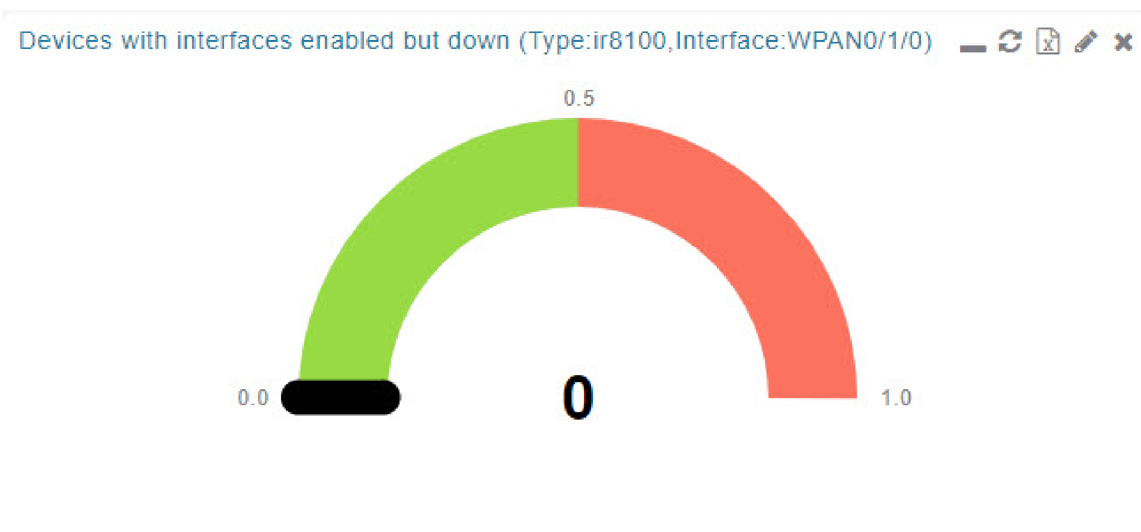
> **Note** You can change device properties by clicking the **Change Device Properties** button above the devices pane.

- Export Templates Keys CSV—In the Device Configuration page, click **Export Template Keys as CSV** button. The WPAN related user configurable parameters are exported in a csv file.

# Support of Dual WPAN in Dashboard page

In the dashboard, scroll down to view the Devices with interfaces enabled but down dashlet. Under the interface filter option, both the WPANs are listed. Set the filter with Type as ir8100 and Interface as WPAN x|y|z. FND displays the status of the respective interface. Click on the needle of the gauge chart to show the devices for which the selected interfaces are enabled but down in the Field Devices page. For more information, see Pre-defined Dashlets, on page 326.



# Editing the ENDPOINT Configuration Template

To edit an ENDPOINT configuration template:

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

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

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

**Step 4** Edit the template.

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

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

| | |
|---|---|
| • **Report Interval**: The number of seconds between data updates. | |
| • **BBU Settings**: Enable this option to configure BBU Settings for range extenders with a battery backup unit. | |
| • **Enable Ethernet**: Check this check box to enable Ethernet for selected devices or configure NAT 44 settings on selected DA Gateway devices. | |
| **Note** | For NAT 44 configuration, you must specify values for all three fields in a CSV file. The default values are 127.0.0.1, 0, 0, respectively. You do not need to configure any other settings for a particular map index. If these settings are invalid for that map index, they are ignored during a configuration push. |
| • **MAP-T Settings**: The IPv6 and IPv4 settings for the device. | |
| **Note** | For Cisco IOS CGRs, MAP-T rules are set by indicating the MAP-T IPv6 basic mapping rule (BMR), IPv4 BMR, and IPv6 default mapping rule (DMR). On Cisco IR509 devices, the MAP-T IPv6 is an IPv6 prefix that integrates the MAP-T BMR IPv6 rules, IPv4 suffix value, and length being based on the BMR EA length value. |
| • **Serial Interface 0 (DCE)Settings**: The data communications equipment (DCE) communication settings for the selected device. | |
| **Note** | There can be only one session per serial interface. You must configure the following parameters for all TCP Raw Socket sessions (for each virtual line and serial port) for the selected DA Gateway device(s): |
| • Initiator – Designates the device as the client/server | |
| • TCP idle timeout (min) – Sets the time to maintain an idle connection. | |
| • Local port – Sets the port number of the device | |
| • Peer port – Sets the port number of the client/server connected to the device. | |
| • Peer IP address – Sets the IP address of the host connected to the device. | |

| |
|---|
| • Connect timeout – Sets the TCP client connect timeout for Initiator DA Gateway devices. |
| • Packet length – Sets the maximum length of serial data to convert into the TCP packet. |
| • Packet timer (ms) – Sets the time interval between each TCP packet creation. |
| • – Special Character – Sets the delimiter for TCP packet creation. |
| • **Serial Interface 1 (DTE) Settings**: The data terminal equipment (DTE) communication settings for the selected device. |
| **Note** The IPv6 prefix must valid. Maximum prefix lengths are: |
| • IPv6: 0–128 |
| • IPv4: 0–32 |

**Step 5** Click **Save Changes**.

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

.

# Pushing Configurations to Routers

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

To push the configuration to routers:

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

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

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

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

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

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

**Step 6** Click **Start**.

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

In the Status column, one of these values appears:

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

### What to do next

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

# Enabling CGR SD Card Password Protection

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

**Note** This does not apply to C800s or IR800s

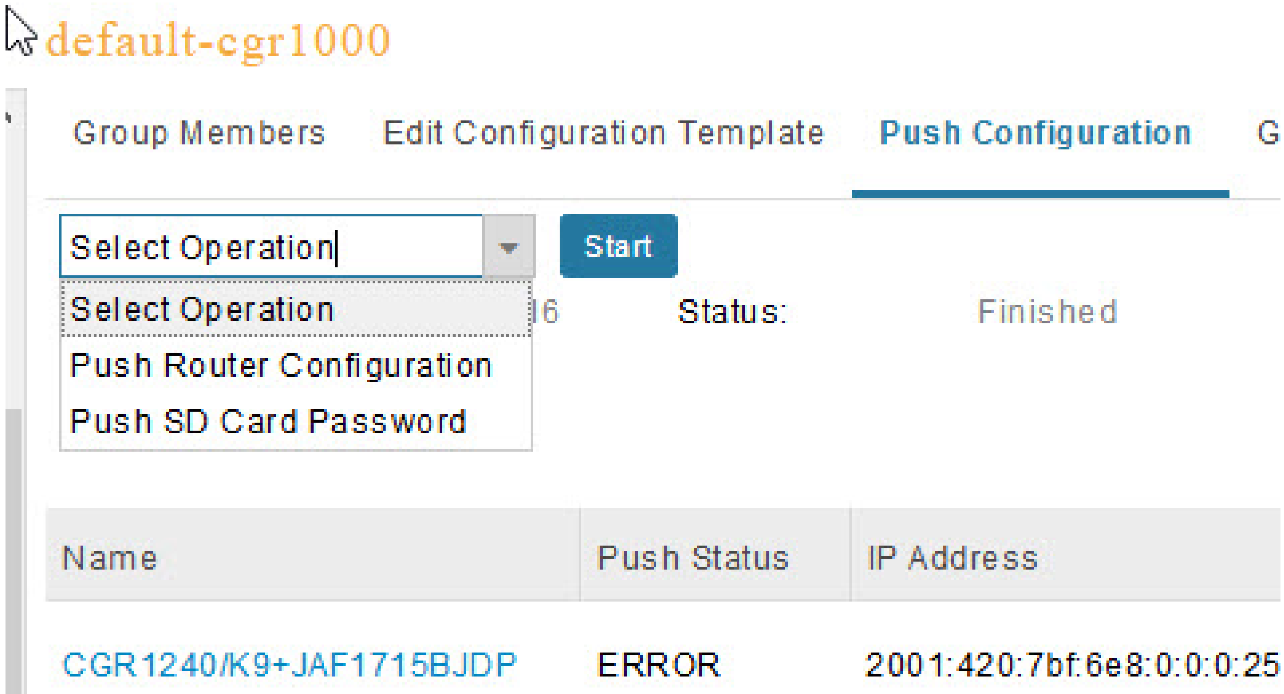
The Device Info pane displays CGR SD card password protection status in the Inventory section. The Config Properties tab displays the SD card password in the Router Credentials section

To enable CGR SD card password protection

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

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

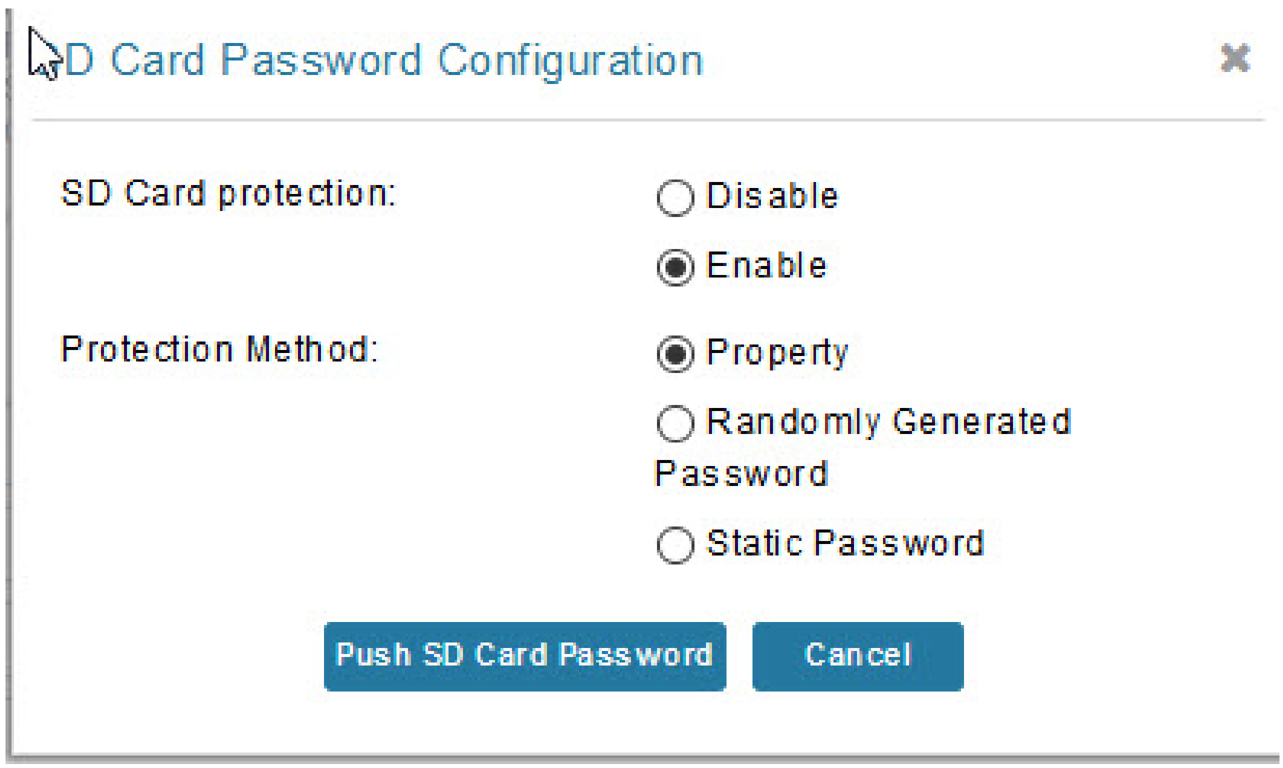
**Step 3** Select the **Push Configuration** tab.




**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:

**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 11: DEVICES > FIELD DEVICES > Endpoint Re-Enrollment (1 of 2), on page 212
- Device Configuration page — Figure 13: CONFIG > DEVICE CONFIGURATION > Endpoint Certificate Re-enrollment, on page 213
- DTLS Relay Settings — Figure 14: Support for DTLS Relay Settings and Cert Auto-Renew Settings for ITRON30 and IR500 Devices, on page 213

- Additionally, Certificate Information is provided for IR500s — Figure 15: Certificate Information for IR500, on page 213

*Figure 11: DEVICES > FIELD DEVICES > Endpoint Re-Enrollment (1 of 2)*

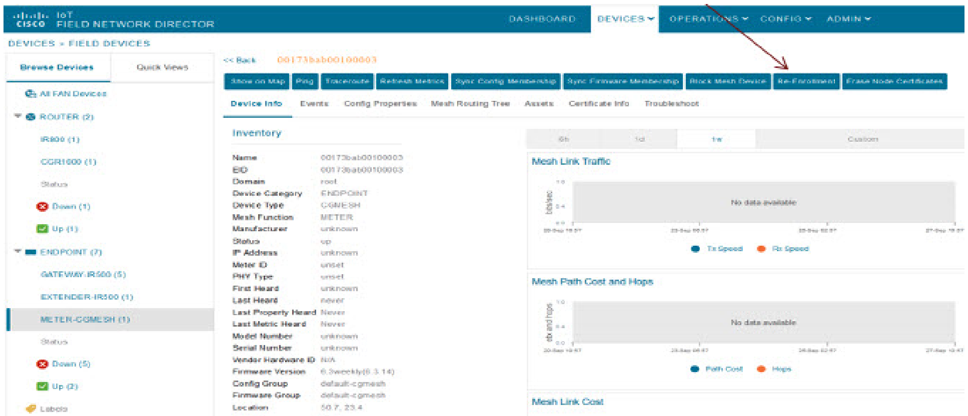



*Figure 12: DEVICES > FIELD DEVICES > Endpoint Re-Enrollment (2 of 2)*

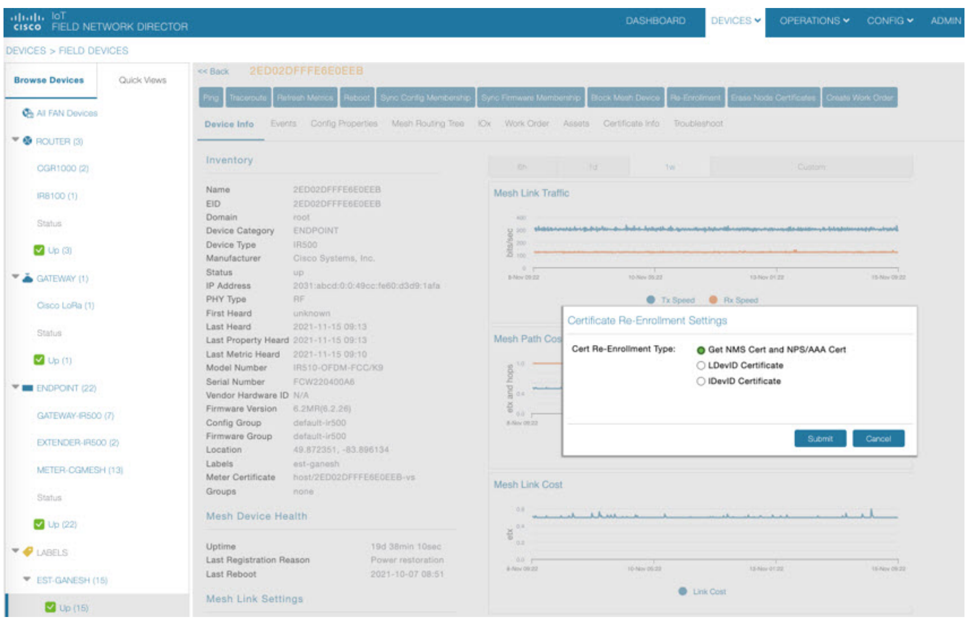


*Figure 13: CONFIG > DEVICE CONFIGURATION > Endpoint Certificate Re-enrollment*

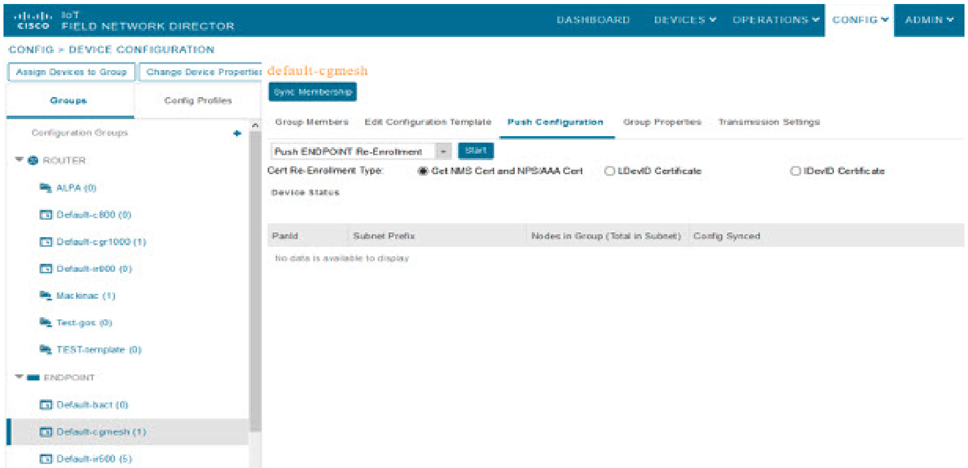
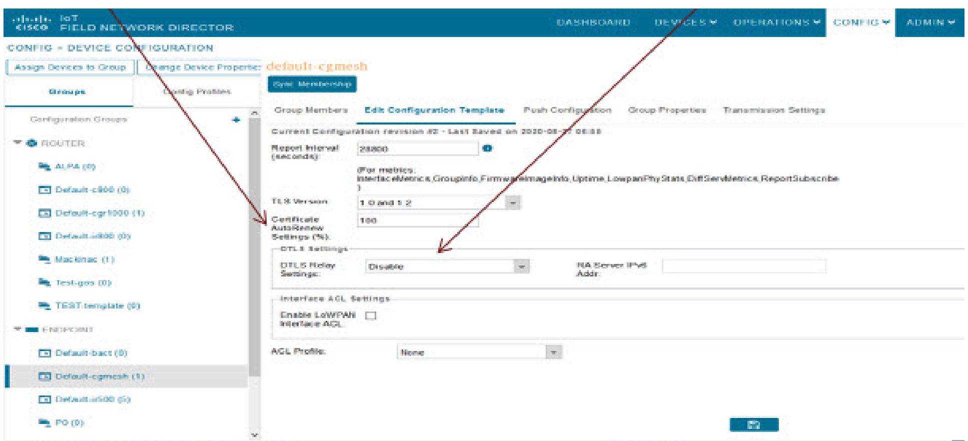
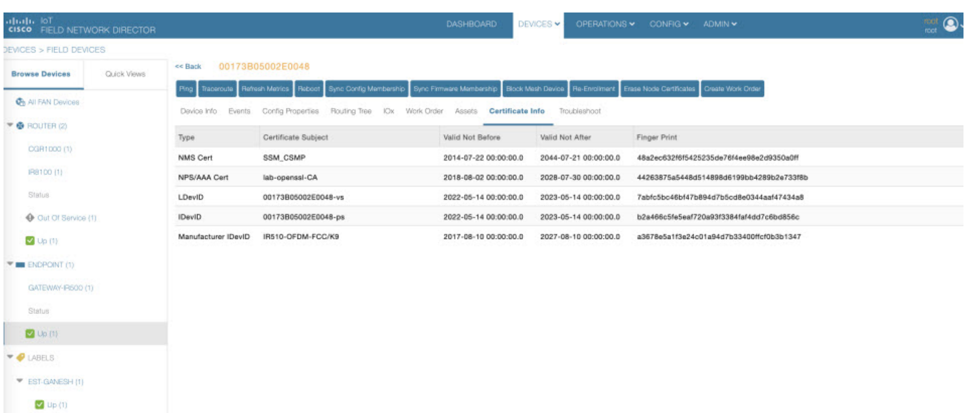



*Figure 14: Support for DTLS Relay Settings and Cert Auto-Renew Settings for ITRON30 and IR500 Devices*




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.

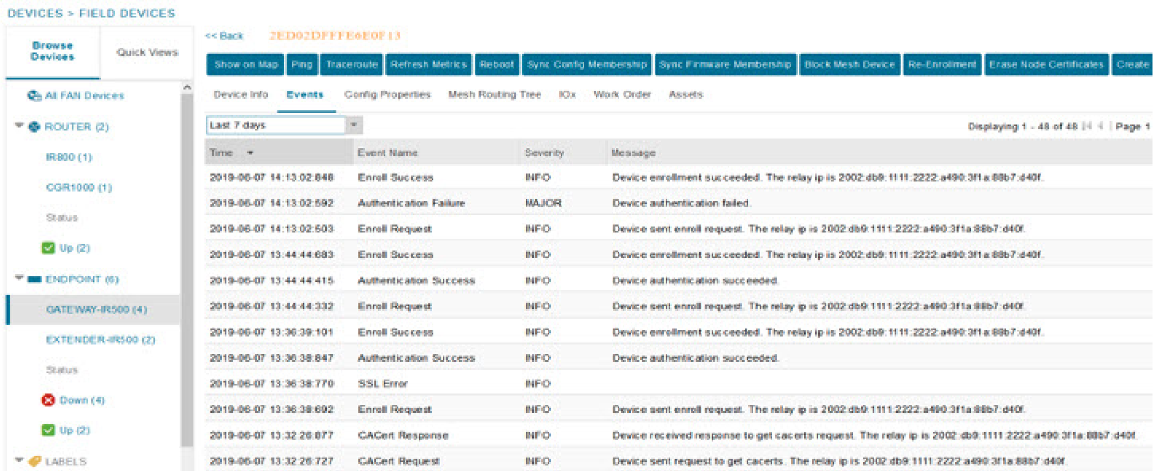
*Figure 15: Certificate Information for IR500*



# New Events for IR500

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

***Figure 16: 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:**

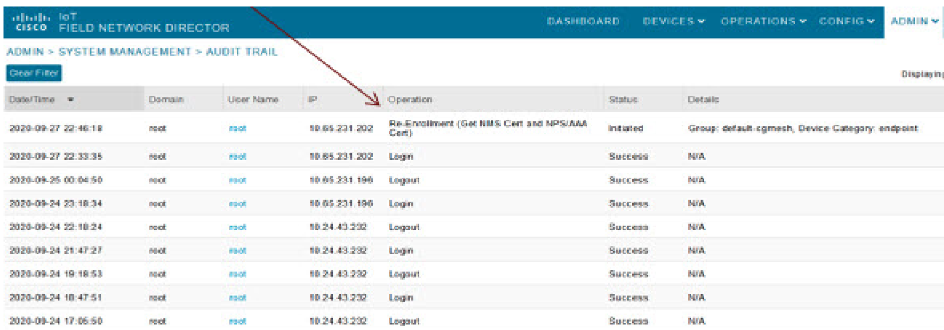
Operation: Re-enrollment (Get NMS Cert and NPS/AAA Cert)

Status: Initiated

Details: Group default-cg-mesh

Device category: endpoint

***Figure 17: 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, on page 257). The GOS, Hypervisor, and Cisco IOS all upgrade when you perform a Cisco IOS image bundle installation or update.

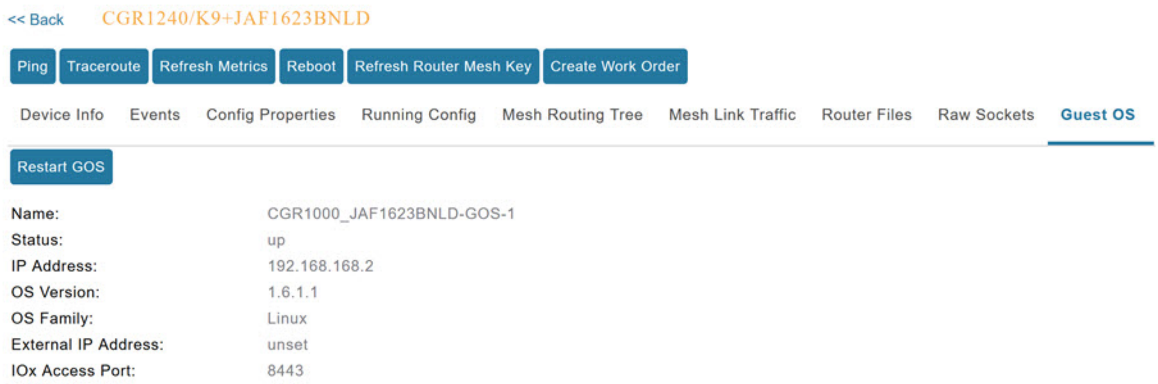
After any Cisco IOS install or upgrade, when IoT FND discovers a GOS, it checks if the initial communications setup is complete before it performs the required setup. The CGR must have a DHCP pool and Gigabit Ethernet 0/1 interface configured to provide an IP address and act as the gateway for the Guest 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 18: DEVICES Field Devices Information Page Showing Guest OS tab and Restart GOS Button*




This section includes the following topics:



## Pushing GOS Configurations

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

# Application Management Support in IoT FND

## Prerequisites

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

## Registering IR1100 Devices with IoT FND through CSV

To register the device:

**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:

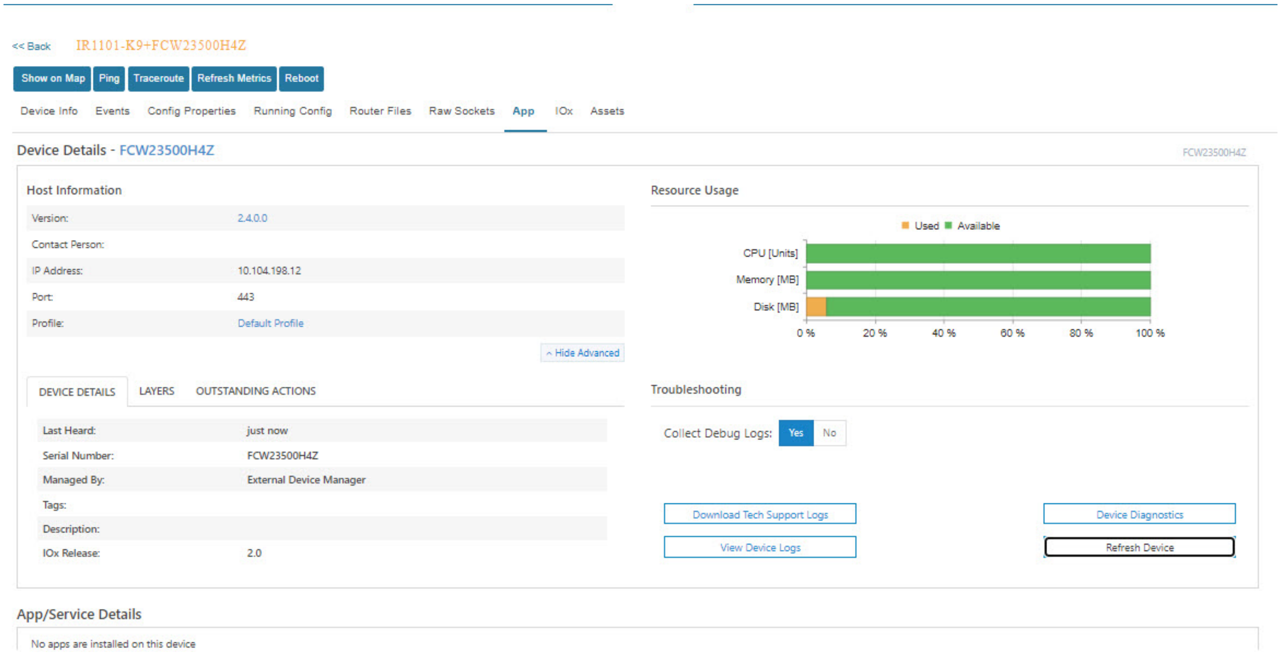
**Step 1** Navigate to IOx tab check whether IOx is started.

**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.



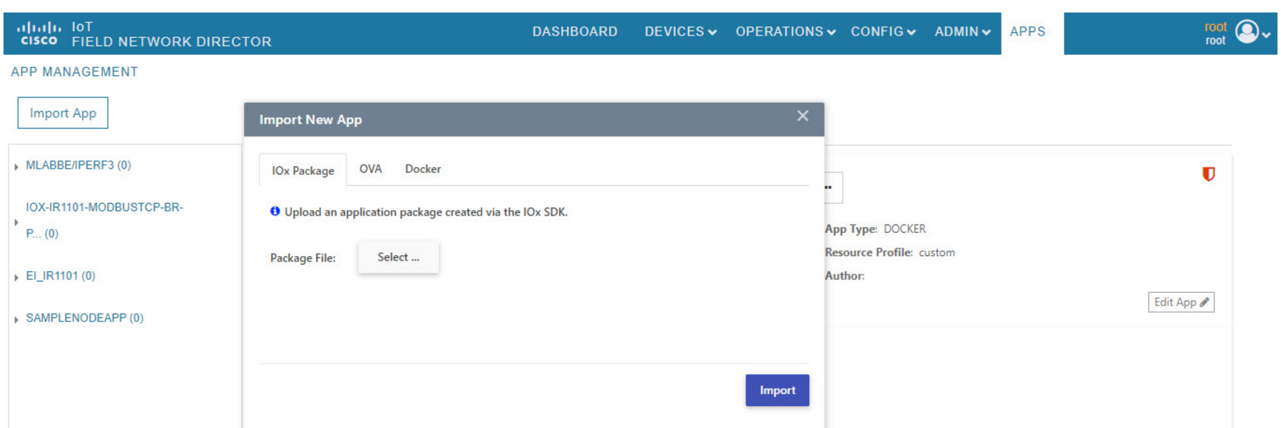

**Note** If the last heard state of the device is Just now, then it confirms that the device is properly registered and started with IOx service.

# 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.

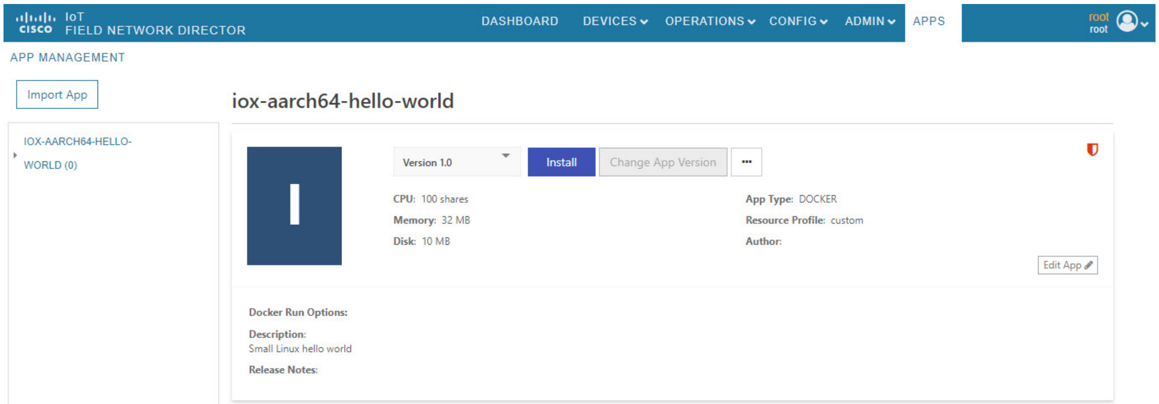
**Step 1** Click **Import App**.

**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**.



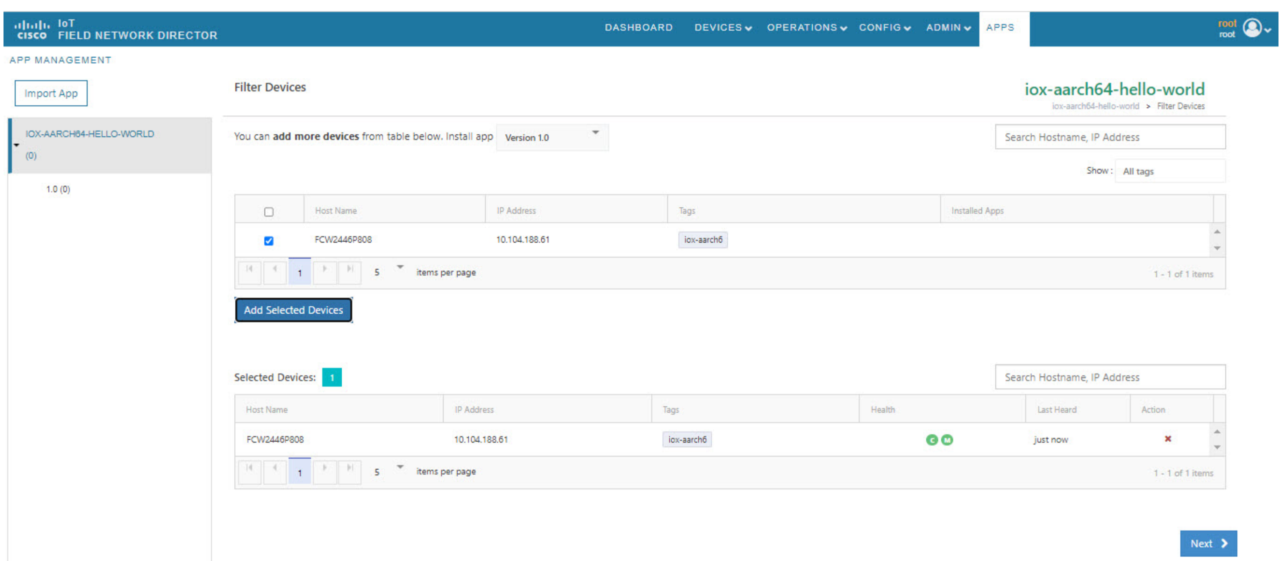
**Note** If you install the application without configuring the interface or enabling the IOx, you will get the following error "No networks have been configured on this device” and the application installation will fail.

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

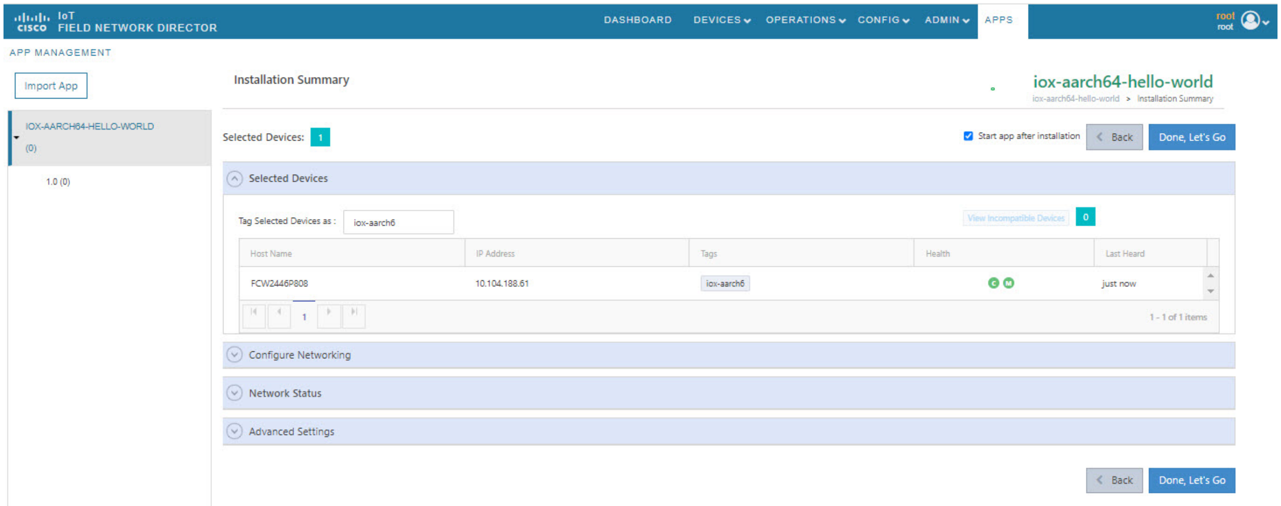
**Step 2** Click **Add Selected Devices**. The device is added to the Selected Devices section where the Last Heard status of the device can be seen.

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

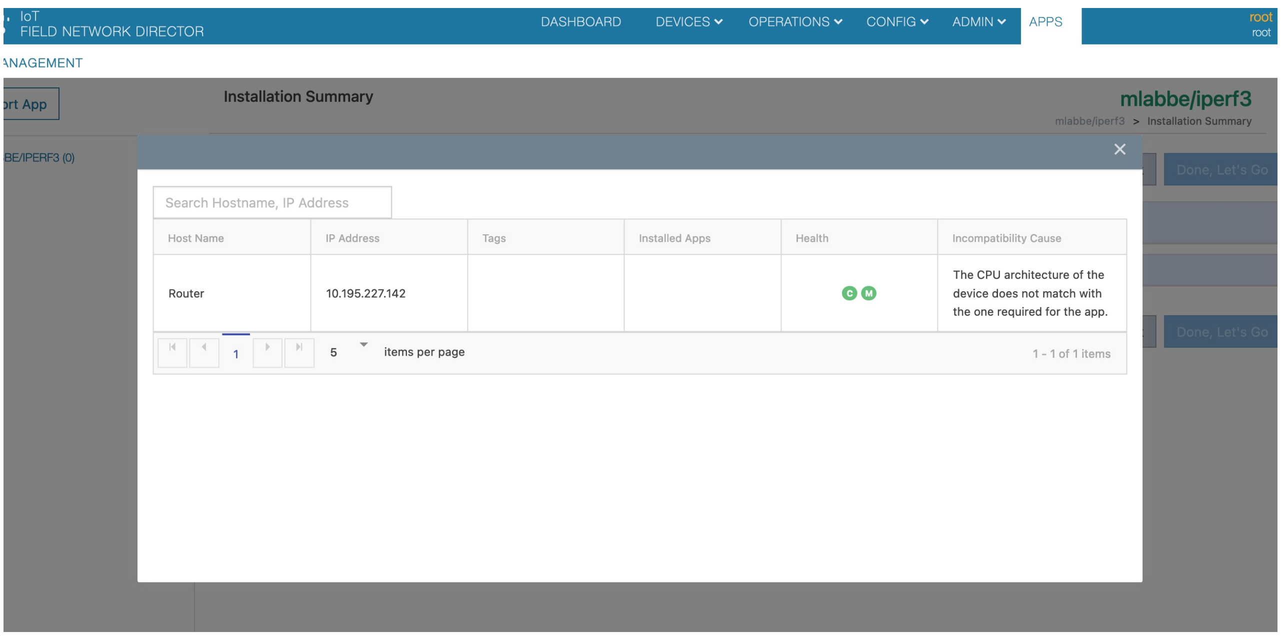
**Step 3** Click **Next**.



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

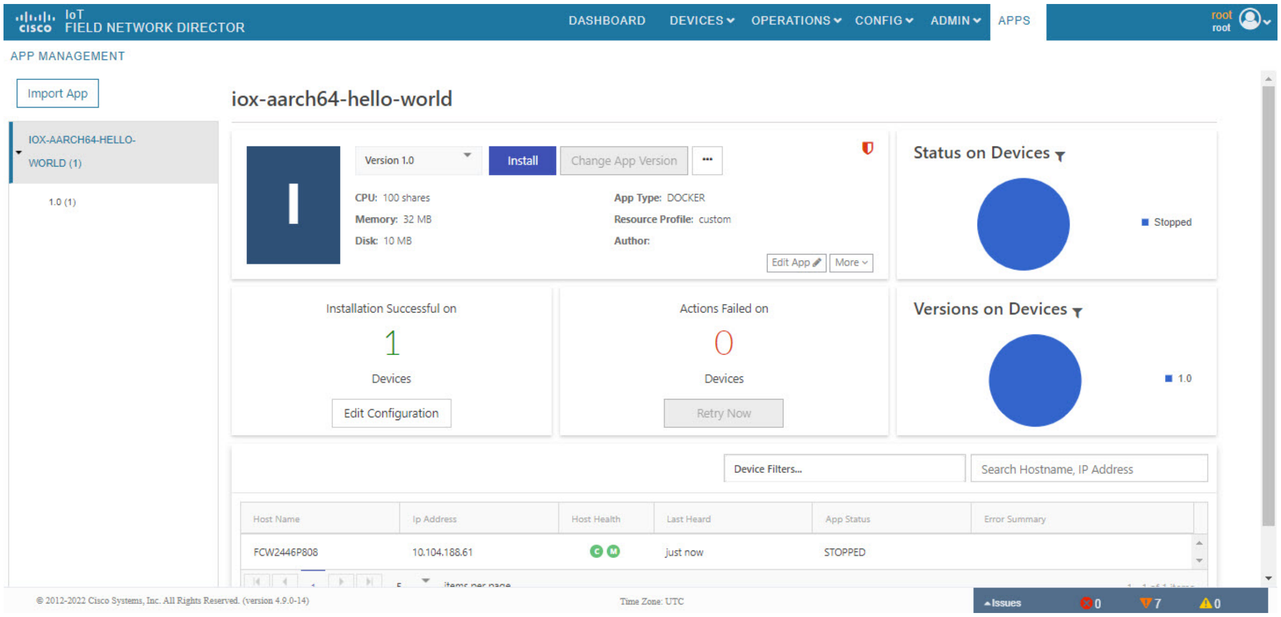



**Note** If you install incompatible application, then you will get the following CPU architecture error.




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

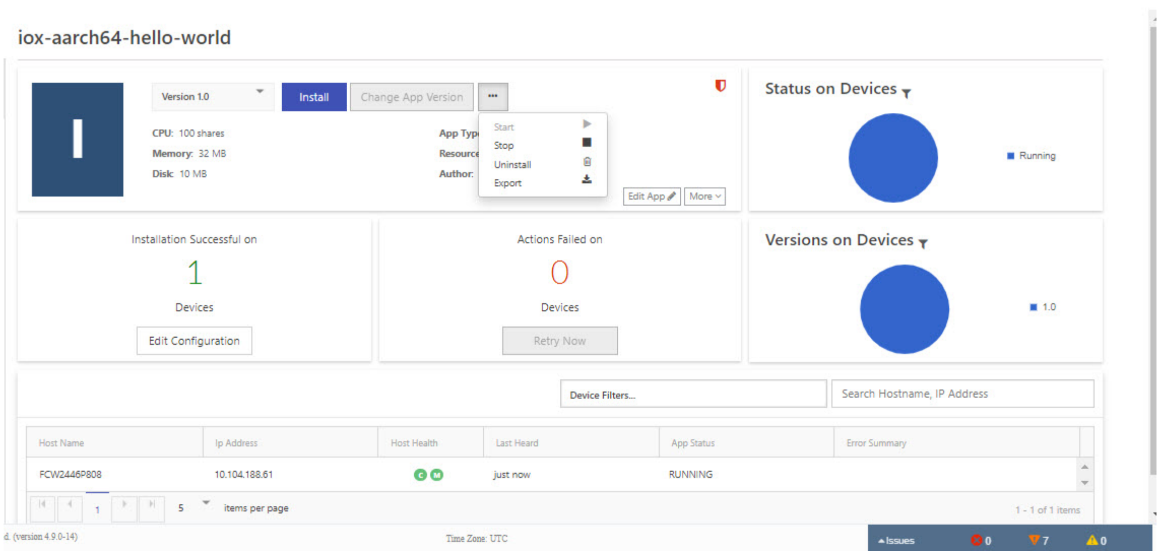
"Installation Successful on device" message appears once installation is complete. The device that is capable of IOx is discovered automatically and the Host Name, Ip Address are properly populated in IoT FND.




# Managing the Application

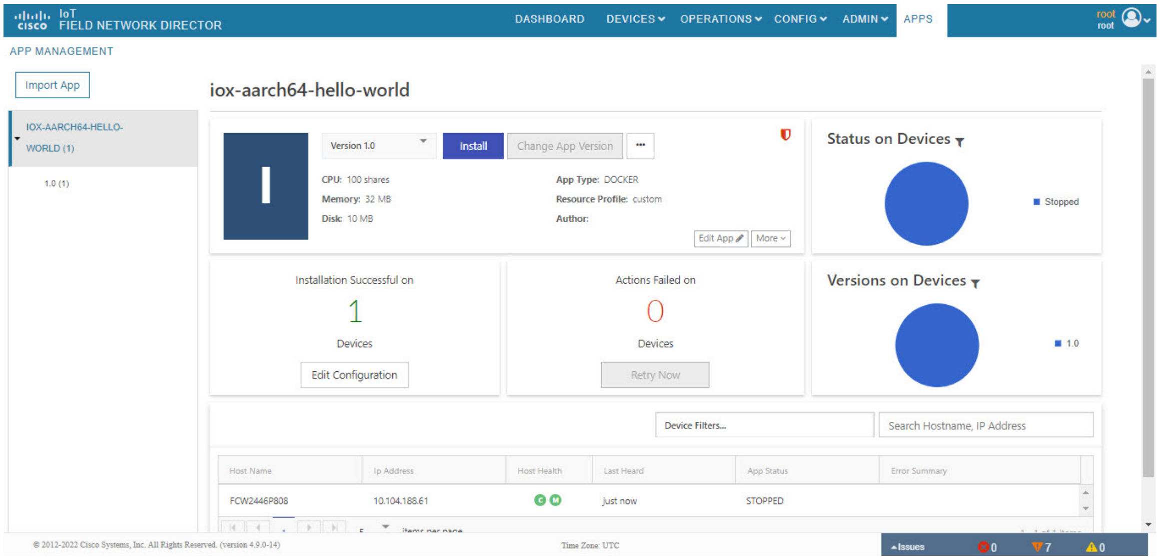
This section describes how to start, stop, and uninstall the application from the APPS menu.

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.

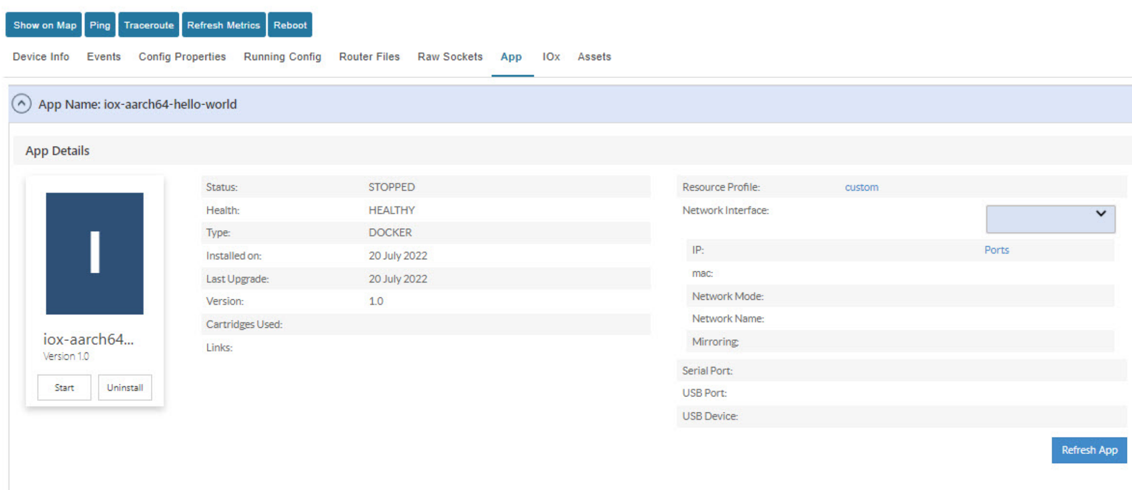


# Stopping the Application

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.



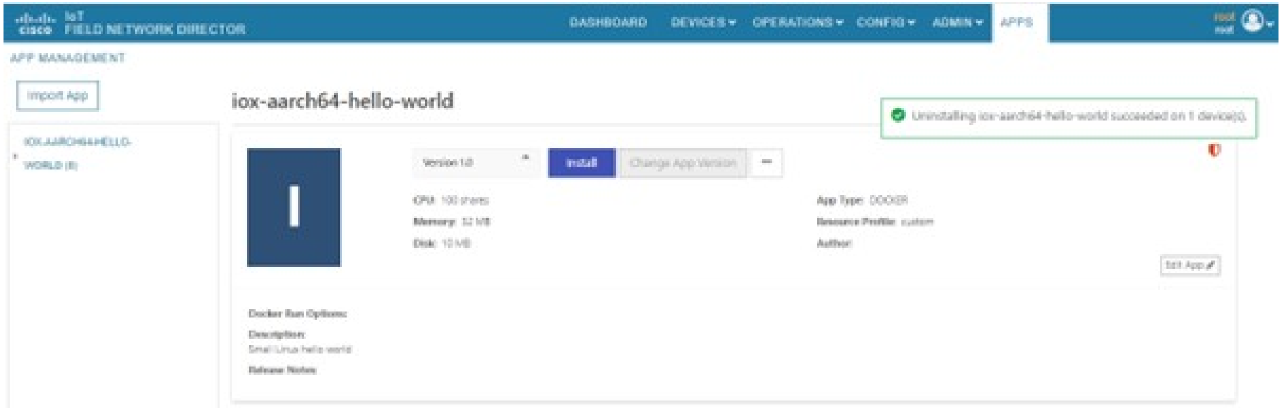

You can either start or uninstall the application from this page or from the APPS main menu. If you click **Uninstall**, the operation is complete and the following message is displayed “Successfully performed undeploy action on iox-aarch64-hello-world app.”

## Uninstalling the Application

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

**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.

# 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:



**Note** File management is role-dependent and may not be available to all users. See Managing Roles and Permissions, on page 57 in the Managing User Access chapter.

# File Types and Attributes

Two types of EEM scripts are used on the router: an embedded applet, and Tool Command Language (TCL) scripts that execute on the router individually. You can upload and run new EEM TCL scripts on the router without doing a firmware upgrade. EEM files upload to the *eem* directory in router flash memory. These scripts display in the **Import File** page File Type column as *eem script* . You must edit the configuration template file to activate the EEM TCL scripts (see Editing the ROUTER Configuration Template, on page 183). 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 19: Search for a Specific CGR Device File Name and Upload to FND Router Page, on page 225). 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 20: Upload Multiple CGR Files Within a Given String Search Range to the FND Router Page, on page 225).

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 19: Search for a Specific CGR Device File Name and Upload to FND Router Page*

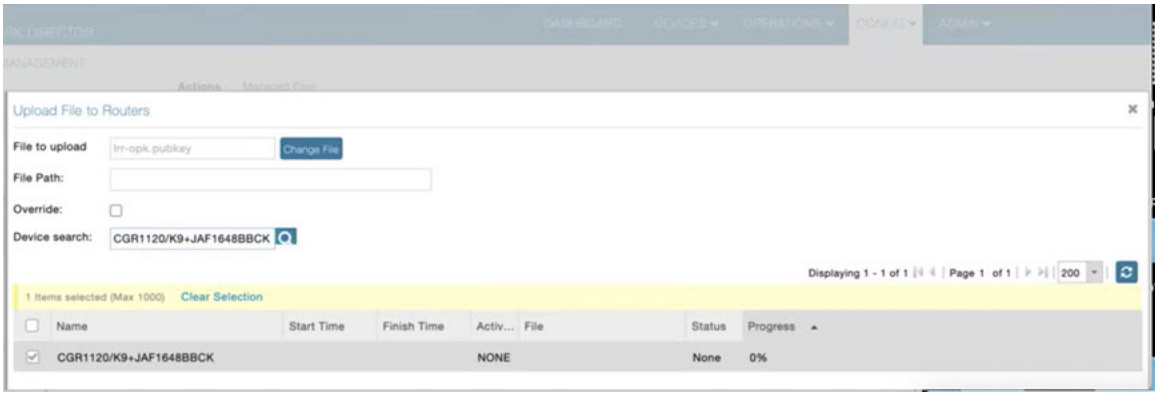
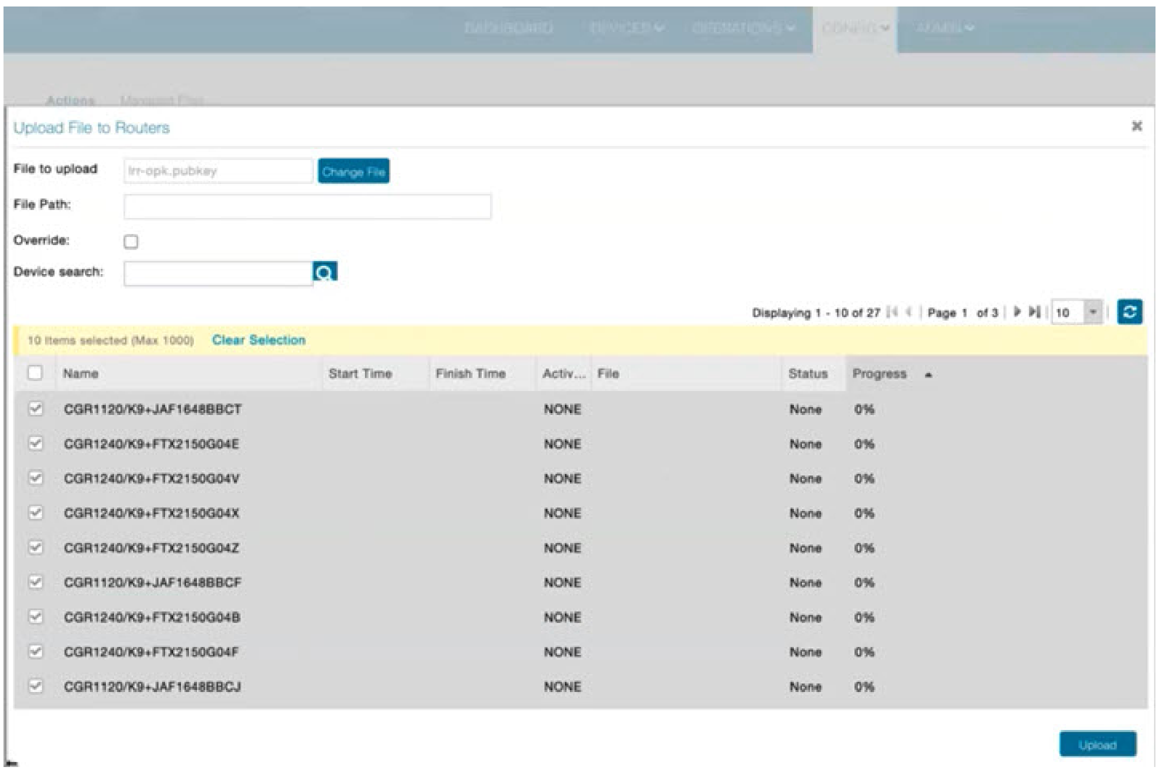



*Figure 20: Upload Multiple CGR Files Within a Given String Search Range to the FND Router Page*




# 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:

---

**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:

**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:

**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:

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

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

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

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

**Step 4** Click **Delete File**.

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

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

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

**Step 6** Click **Delete**.

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

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

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

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

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

# Hardware Security Module

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

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

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

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

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

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

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

# Verification of FND and HSM Integration After FND and HSM Upgrade

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

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

**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:

3059301306072a8648ce3d020106082a8648ce3d030107034200004d914167514ec0a110f3170eef74

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 27: 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:

**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:

**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:

**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:

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

**Step 2** In the Provisioning Process panel:

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


# Device Properties

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

## Types of Device Properties

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

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

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

# Device Properties by Category

This section presents IoT FND device properties by category.

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

## Cellular Link Metrics for CGRs

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

***Table 28: 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.<br>The LED states on the cellular interface and corresponding RSSI values are:<br>• Off: RSSI < = -110<br>• Solid amber: -100 < RSSI <= -90<br>• Fast green blink: -90 < RSSI <= -75<br>• Slow green blink: -75 < RSSI <= -60<br>• Solid green: RSSI > -60 |
| Bandwidth Usage (Current Billing Cycle) | CellBwPerCycle (bytes) | Displays current bandwidth usage (in bytes) of a particular route for the current billing cycle. |
| Cell Module Temperature | cellModuleTemp | Internal temperature of 3G module. |
| Cell ECIO | cellularEcio | Signal strength of CDMA at the individual sector level. |

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

## Cellular Link Settings

Table 29: Cellular Link Settings Fields lists the fields in the Cellular Link area of the Device Detail page for all Cellular interfaces.

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

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

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

| Cellular Link Settings | Interface 0 and Interface 1 | Interface 2 and Interface 3 |
|---|---|---|
| — | — | — |

Additionally, the 4G LTE dual-active radio module does not support or display all fields summarized in Table 29: Cellular Link Settings Fields

*Table 29: Cellular Link Settings Fields*

| Field | Key | Configurable | Description |
|---|---|---|---|
| Cellular Network Type | N/A | Yes | Defines the type of cellular network for example, GSM or CDMA. |
| Module Status | cellularStatus | No | Displays whether the cellular interface module is active in the network. There is also an unknown state for the module. |
| Network Name | N/A | Yes | Defines the service provider name, for example, AT&T or Verizon. |
| Cell ID | cellularID | No | Displays the cell ID for the cellular interface. This value must exist to activate the interface. |

| Field | Key | Configurable | Description |
|---|---|---|---|
| Cellular SID | cellularSID | No | Displays the System Identification Number for the CDMA cellular area. |
| Cellular NID | cellularNID | No | Displays the Network Identification Number for the CDMA cellular area. |
| Cellular Roaming Status | cellularRoamingStatus | No | Indicates whether the modem is in the Home network or Roaming. |
| Cellular Modem Serial Number | N/A | No | Displays the serial number of the connected modem. |
| Cellular Modem Firmware Version | cellularModemFirmwareVersion | No | Displays the version of the modem firmware on the module installed within the CGR. |
| Connection Type | connectionType | No | Displays the connection type as:<br>• Packet switched<br>• Circuit switched<br>• 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:<br>• Packet switched<br>• Circuit switched |
| IMSI | cellularIMSI | No | The International Mobile Subscriber Identity (IMSI) identifies an individual network user as a 10-digit decimal value within a GSM and CDMA network.<br>Possible values are:<br>• 10-digit decimal value<br>• Unknown |
| IMEI | cellularIMEI | No | Displays the International Mobile Equipment Identity (IMEI) for the cellular interface within a GSM network only. The IMEI value is a unique number for the cellular interface. |

| Field | Key | Configurable | Description |
|---|---|---|---|
| Cellular Module Temperature | cellularModemTemp | — | Displays the modem temperature. |
| ICCID | cellularICCID | — | The Integrated Circuit Card Identification Number is a unique 18-22 digit code that includes a SIM card's country, home network, and identification number. |

## DA Gateway Properties

Table 30: DA Gateway Metrics Area Fields describe the fields in the DA Gateway area of the Device Info view.

*Table 30: 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:<br>• 0 indicates no security mode set<br>• 1 indicates 802.1x with 802.11i key management |
| Meter Certificate | meterCert | The subject name of the meter certificate. |
| Mesh Tone Map Forward Modulation | toneMapForwardModulation | Mesh tone map forward modulation:<br>• 0 = Robo<br>• 1 = DBPSK<br>• 2 = DQPSK<br>• 3 = D8PSK |
| Mesh Tone Map Reverse Modulation | N/A | Mesh tone map reverse modulation:<br>• 0 = Robo<br>• 1 = DBPSK<br>• 2 = DQPSK<br>• 3 = D8PSK |
| Mesh Device Type | N/A | The primary function of the mesh device (for example, meter, range extender, or DA gateway). |
| Manufacturer of the Mesh Devices | N/A | Manufacturer of the mesh device as reported by the device. |

| Field | Key | Description |
|---|---|---|
| Basic Mapping Rule End User IPv6 Prefix | N/A | End-user IPv6 address for basic rule mapping for the device. |
| Basic Mapping Rule End User IPv6 Prefix Length | N/A | Specified prefix length for the end-user IPv6 address. |
| Map-T IPv6 Address | N/A | IPv6 address for MAP-T settings. |
| Map-T IPv4 Address | N/A | IPv4 address for MAP-T settings. |
| Map-T PSID | N/A | MAP-T PSID. |
| Active Link Type | N/A | Link type of the physical link over which device communicates with other devices including IoT FND. |

## Device Health

The Table 31: Device Health Fields describes the fields in the Device Health area of the Device Info view.

***Table 31: 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

Table 32: Embedded Access Point Credentials Fields describes the fields in the Embedded Access Point Credentials area of the Device Info view.

***Table 32: 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

Table 33: Embedded AP Properties describes the fields on the Embedded AP tab of the C800 or IR800 Device Info view.

***Table 33: Embedded AP Properties***

| Field | Key | Description |
|---|---|---|
| Inventory | NA | Summary of name, EID, domain, status, IP address, hostname, domain name, first heard, last heard, last property heard, last metric heard, model number, serial number, firmware version, and uptime details. |

| Field | Key | Description |
|---|---|---|
| Wi-Fi Clients | N/A | Provides client MAC address, SSID, IPv4 address, IPv6 address, device type, state, name, and parent. |
| Dot11Radio 0 Traffic | N/A | Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps), and Rx speed (bps). |
| Dot11Radio 1 Traffic | N/A | Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps,) and Rx speed (bps). |
| Tunnel3 | N/A | Provides admin status (up/down), operational status (up/down), Tx speed (bps), Tx drops (bps), and Rx speed (bps). |
| BVI1 | N/A | Provides admin status (up/down), operational status (up/down), IP address, physical address, Tx speed (bps), Tx drops (bps) and Rx speed (bps). |
| GigabitEthernet0 | N/A | Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps), and Rx speed (bps). |

## Ethernet Link Metrics

Table 34: Ethernet Link Metrics Area Fields describes the fields in the Ethernet link traffic area of the Device Info view.

*Table 34: Ethernet Link Metrics Area Fields*

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

## IOx Node Properties

Table 35: IOx Node Properties Fields describe the fields in the Iox Node Properties area of the Config Properties page.

*Table 35: 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 |

| Field | Key | Description |
|---|---|---|
| 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

Table 36: Head-End Routers Netconf Config Client Fields describes the fields in the Netconf Client area of the **Head-End Routers** > **Config Properties** page.

*Table 36: Head-End Routers Netconf Config Client Fields*

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

## Head-End Routers Tunnel 1 Config

Table 37: 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 37: Head-End Routers Tunnel 1 Config Fields*

| Field | Key | Configurable | Description |
|---|---|---|---|
| IPsec Tunnel Source 1 | ipsecTunnelSrc1 | Yes | Identifies the source interface or IP address of IPsec tunnel 1. |
| IPsec Tunnel Dest Addr 1 | ipsecTunnelDestAddr1 | Yes | Identifies the destination interface or IP address of IPsec tunnel 1. |
| GRE Tunnel Source 1 | greTunnelSrc1 | Yes | Identifies the source interface or IP address of GRE tunnel 1. |
| GRE Tunnel Dest Addr 1 | greTunnelDestAddr1 | Yes | Identifies the destination interface or IP address of GRE tunnel 1. |

## Head-End Routers Tunnel 2 Config

Table 38: 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 38: Head-End Routers Tunnel 2 Config Device Fields*

| Field | Key | Configurable | Description |
|---|---|---|---|
| IPsec Tunnel Source 2 | ipsecTunnelSrc2 | Yes | Identifies the source interface or IP address of IPsec tunnel 2. |

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

## Inventory

The table describes the fields in the Inventory area of the Device Info page for CGR1000.

***Table 39: Inventory Fields***

| Field | Key | Configurable | Description |
|---|---|---|---|
| Config Group | configGroup | Yes | Name of the configuration group to which the device belongs. |
| Device Category | deviceCategory | No | Category of the device. |
| Device Type | deviceType | No | Device type that determines other fields, the way the device communicates, and the way it appears in IoT FND. |
| Domain Name | domainName | Yes | Domain name configured for this device. |
| EID | eid | No | Primary element ID of the device, which is used as the primary unique key for device queries. |
| Firmware Group | firmwareGroup | Yes | Name of the firmware group to which the device belongs. |
| Firmware Version | runningFirmwareVersion | No | Firmware version running on the device. |
| Hardware Version | vid | No | Hardware version of the device. |
| Hypervisor Version | hypervisor | No | (Cisco IOS CGRs running Guest OS only) The version of the Hypervisor. |
| Hostname | hostname | No | Hostname of the device. |
| IP Address | ip | Yes | IP address of the device. Use this address for the IoT FND connection through a tunnel. |
| Labels | label | Yes | Custom label assigned to the device. A device can have multiple labels. Labels are assigned through the UI or API, but not through an XML or CSV file. |
| Last Heard | lastHeard | No | Last date and time the device contacted IoT FND. |
| Last Metric Heard | N/A | No | Time of last polling (periodic notification). |
| Last Property Heard | N/A | No | The time of last property update for the router. |
| Last RPL Tree Update | N/A | No | The time of last Routing Protocol for Low power and Lossy Networks (RPL) tree poll update (periodic notification). |

| Field | Key | Configurable | Description |
|---|---|---|---|
| Location | N/A | No | Latitude and longitude of the device. |
| Manufacturer | N/A | No | Manufacturer of the endpoint device. |
| Function | crmesh | No | Function of the mesh device. Valid values are Range Extender and Meter. |
| Meter Certificate | meterCert | No | Global or unique certificate reported by the meter. |
| Meter ID | meterId | No | Meter ID of the mesh endpoint (ME). |
| Model Number | pid | No | Product ID of the device. |
| Name | name | Yes | Unique name assigned to the device. |
| SD Card Password Lock | N/A | Yes | (CGRs only) State of the SD card password lock (on/off). |
| Serial Number | sn | No | Serial number of the device. |
| Status | status | No | Status of the device. |
| Tunnel Group | tunnelGroup | Yes | Name of the tunnel group to which the device belongs. |

## Link Metrics

Table 40: Link Metrics Fields describes the fields in the Link Metrics area of the Device Info page.

*Table 40: Link Metrics Fields*

| Field | Key | Description |
|---|---|---|
| Active Link Type | activeLinkType | Determines the most recent active RF or PLC link of a meter. |
| Meter ID | meterId | Meter ID of the device. |
| PANID | meshPanid | PAN ID of the endpoint. |
| Mesh Endpoints | meshEndpointCount | Number of RMEs. |
| Mesh Link Transmit Speed | meshTxSpeed | Current speed of data transmission over the uplink network interface (bits/sec) averaged over a short element-specific time period (for example, an hour). |
| Mesh Link Receive Speed | meshRxSpeed | Rate of data received by the uplink network interface (bits/sec) averaged over a short element-specific time period (for example, an hour). |
| Mesh Link Transmit Packet Drops | N/A | Number of data packets dropped in the uplink. |
| Route RPL Hops | meshHops | Number of hops that the element is from the root of its RPL routing tree. |
| Route RPL Link Cost | linkCost | RPL cost value for the link between the element and its uplink neighbor. |
| Route RPL Path Cost | pathCost | RPL path cost value between the element and the root of the routing tree. |

| Field | Key | Description |
|---|---|---|
| Transmit PLC Level | tx_level dBuV | Supported on the PLC and the Itron OpenWay RIVA Electric devices and the Itron OpenWay RIVA G-W (Gas-Water) devices only (u within dBuV = micro) |

## Link Settings

Table 41: Link Settings Fields describes the fields in the Link Settings area of the Device Info view.

***Table 41: 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 42: 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

Table 43: Mesh Link Config Fields describes the fields in the Mesh Link Config area of the **Routers** > **Config Properties** page.

*Table 43: 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

Table 44: Mesh Link Keys Fields describes the fields in the Mesh Link Keys area of the Device Info view.

*Table 44: 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

Table 45: NAT44 Metrics Fields describes the fields in the NAT44 area of the Device Info page.

*Table 45: NAT44 Metrics Fields*

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

## PLC Mesh Info

Table 46: PLC Mesh Info Fields describes the fields in the PLC Mesh Info area of the Device Info view.

*Table 46: PLC Mesh Info Fields*

| Field | Key | Description |
|---|---|---|
| Mesh Tone Map Forward Modulation | toneMapForwardModulation | Mesh tone map forward modulation:<br>• 0 = Robo<br>• 1 = DBPSK<br>• 2 = DQPSK<br>• 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:<br>• 0 = Robo<br>• 1 = DBPSK<br>• 2 = DQPSK<br>• 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

Table 47: PLC Mesh Info Fields describes the fields in the PLC Mesh Info area of the Device Info view.

*Table 47: PLC Mesh Info Fields*

| Field | Key | Description |
|---|---|---|
| Mesh Tone Map Forward Modulation | toneMapForwardModulation | Mesh tone map forward modulation:<br>• 0 = Robo<br>• 1 = DBPSK<br>• 2 = DQPSK<br>• 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:<br>• 0 = Robo<br>• 1 = DBPSK<br>• 2 = DQPSK<br>• 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

Table 48: Raw Sockets Metrics and Sessions View describes the fields in the TCP Raw Sockets area of the **Field Devices** > **Config Properties** page.

*Table 48: 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 Table 49: Router Battery Device View describes the fields in the Router Battery (Battery Backup Unit (BBU) area of the Device Info page.

*Table 49: 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. |

## Router Config

Table 50: Router Config Device View describes the fields in the Router Config area of the **Field Devices** > **Config Properties** page.

*Table 50: Router Config Device View*

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

## Router Credentials

Table 51: Router Credentials Fields describes the fields in the Router Credentials area of the **Field Devices** > **Config Properties** page.

*Table 51: 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. |

| Field | Key | Configurable | Description |
|---|---|---|---|
| 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

Table 52: DHCP Proxy Config Fields describes the fields in the DHCP Proxy Config area of the **Field Devices** > **Config Properties** page.

*Table 52: DHCP Proxy Config Fields*

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

## Router Health

Table 53: Router Health Device View describes the Router Health fields in the Device Info view.

*Table 53: Router Health Device View*

| Field | Key | Configurable | Description |
|---|---|---|---|
| Uptime | uptime | No | Indicates the length of time (in seconds) that the router has been up and operating since its last reset. |
| Door Status | doorStatus | No | Options for this field are:<br>• “Open” when the door of the router is open<br>• “Closed” after the door is closed |

| Field | Key | Configurable | Description |
|---|---|---|---|
| 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

Table 54: Router Tunnel 1 Config Device View describes the fields in the Router Tunnel 1 Config area of the **Field Devices** > **Config Properties** page.

***Table 54: 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

Table 55: Router Tunnel 2 Config Device View describes the fields in the Router Tunnel 2 Config area of the **Field Devices** > **Config Properties** page.

***Table 55: Router Tunnel 2 Config Device View***

| Field | Key | Configurable | Description |
|---|---|---|---|
| Tunnel Source Interface 2 | tunnelSrcInterface2 | Yes | Defines the interface over which the second tunnel is built to provide WAN redundancy. |
| OSPF Area 2 | ospfArea2 | Yes | Defines the OSPFv2 Area 2 in which the router (running IPv4) is a member. |
| OSPFv3 Area 2 | ospfV3Area2 | Yes | Defines OSPFv3 Area 2 in which the router (running IPv6) is a member. |
| IPsec Dest Addr 2 | ipsecTunnelDestAddr2 | Yes | Defines the destination IP address for IPsec tunnel 2. |

| Field | Key | Configurable | Description |
|---|---|---|---|
| GRE Dest Addr 2 | greTunnelDestAddr2 | Yes | Defines the destination IP address for GRE tunnel 2. |

## Router Tunnel Config

Table 56: Router Tunnel Config Device View describes the fields in the Router Tunnel Config area of the **Field Devices** > **Config Properties** page.

*Table 56: 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

Table 57: SCADA Metrics View describes the fields on the SCADA tab of the Device Info page.

*Table 57: SCADA Metrics View*

| Field | Key | Configurable | Description |
|---|---|---|---|
| Channel Name | channel_name | No | Identifies the channel on which the serial port of the router communicates to the RTU. |
| Protocol Type | protocol | No | Identifies the Protocol Translation type. |
| Messages Sent | N/A | No | The number of messages sent by the router. |
| Messages Received | N/A | No | The number of messages received by the router. |
| Timeouts | N/A | No | Displays the timeout value for connection establishment. |
| Aborts | N/A | No | Displays the number of aborted connection attempts. |
| Rejections | N/A | No | Displays the number of connection attempts rejected by IoT FND. |
| Protocol Errors | N/A | No | Displays the number of protocol errors generated by the router. |
| Link Errors | N/A | No | Displays the number of link errors generated by the router. |
| Address Errors | N/A | No | Displays the number of address errors generated by the router. |

| Field | Key | Configurable | Description |
|---|---|---|---|
| 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

Table 58: WiFi Interface Config Fields describe the fields in the WiFi Interface Config area of the **Field Devices** > **Config Properties** page.

***Table 58: WiFi Interface Config Fields***

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

## WiMAX Config

Table 59: 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 59: WiMAX Config Fields***

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

## WiMAX Link Metrics

Table 60: WiMAX Link Health Fields describe the fields in the WiMAX Link Health area of the Device Info page.

*Table 60: WiMAX Link Health Fields*

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

## WiMAX Link Settings

Table 61: WiMAX Link Settings Fields describe the fields in the WiMAX Link Settings area of the Device Info page.

*Table 61: 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. |

CHAPTER 6

# Managing Firmware Upgrades

This section describes managing firmware upgrade settings in IoT FND, and includes the following sections:

Use IoT FND to upgrade the firmware running on routers (CGR1000s, C800s, IR800s), AP800s and Cisco Resilient Mesh Endpoints (RMEs) such as meters and range extenders. IoT FND stores the firmware binaries in its database for later transfer to routers in a firmware group through an IoT FND and IoT-DM file transfer, and to RMEs using IoT FND.

Cisco provides the firmware bundles as a zip file. For Cisco IOS, software bundles include hypervisor, system image and IOx images (for example, Guest-OS, Host-OS).

Firmware system images are large (approximately 130 MB); kickstart images are approximately 30 MB. Every firmware bundle includes a manifest file with metadata about the images in the bundle. You can pause, stop, or resume the upload process.



## Router Firmware Updates

IoT FND updates router firmware in two steps:

**Step 1** Uploads the firmware image from IoT FND to the router. Firmware images upload to the flash:/managed/images directory on the router.

**Note** In some cases the router might be in a Firmware Group. Refer to Configuring Firmware Group Settings, on page 269.

Because of their large size, firmware-image uploads to routers take approximately 30 minutes, depending on interface speeds

**Note** If you set the property, collect-cellular-link-metrics, to ‘true’ in cgms.properties, then the following Cellular link quality metrics are collected for CGR1000, IR800 and IR1100, each time you initiate a firmware upload from IoT FND:

- RSRP: Reference Signal Received Power which is the power of the reference signal
- RSRQ: Reference Signal Received Quality or the quality of the reference signal which is the a ratio of RSSI to RSRP
- SINR: Signal-to-Noise Ratio which compares the strength of the signal to the background noise.
- RSSI: Received Signal Strength Indicator or the strength of the reference signal

Additionally, the following cgna profile is created on the CGR1240 and activated when the firmware upload is triggered.

```
cgna profile cg-nms-cellularlinkmetrics
add-command show cellular 3/1 all | format
flash:/managed/odm/cg-nms.odm
interval 5
url https://<FND IP address>:9121/cgna/ios/metrics
gzip
active
```

**Note** On execution of the cgna profile above, the metrics data is persisted in the Metrics_History table in the database and can be collected by using the getMetricHistory NBAPI.

**Step 2** Installs the firmware on the device and reloads it.

During the firmware install the boot parameters on the routers are updated according to the new image file and the router is reloaded after enabling the *cg-nms-register* cgna profile.

**Note** You must initiate the firmware installation process. IoT FND does not automatically start the upload after the image upload.

When a router contacts IoT FND for the first time to register and request tunnel provisioning, IoT FND rolls the router back to the default factory configuration (ps-start-config) before uploading and installing the new firmware image.

**Note** This rollback requires a second reload to update the boot parameters in ps-start-config and apply the latest configuration. This second reload adds an additional 10–15 minutes to the installation and reloading operation.

# Upgrading Guest OS Images

Depending on CGR factory configuration, a Guest OS (GOS) may be present in the VM instance. You can install or upgrade Cisco IOS on the **CONFIG** > **FIRMWARE UPDATE** page (see Router Firmware Updates, on page 257). 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 GigabitEthernet 0/1 interface configured to provide an IP address and act as the gateway for the GOS. The new GOS image overwrites existing configurations. IoT FND has an internal backup and restore mechanism that ports existing apps to the upgraded Guest OS. See Monitoring a Guest OS for more information.

See Cisco 1000 Series Connected Grid Routers Configuration Guides for information on configuring the CGR.

**Note:** If IoT FND detects a non-Cisco OS installed on the VM, the firmware bundle will not upload and the Cisco reference GOS will not install.

# Upgrading WPAN Images

At the **CONFIG** > **FIRMWARE UPDATE** page, you can upload the independent WPAN images (IOS-WPAN-RF, IOS-WPAN-PLC, IOS-WPAN-OFDM, IOS-WPAN-IXM) to IoT FND using the Images sub-tab (left-hand side) and Upload Image button like other image upgrades. This process is known as a non-integrated WPAN firmware upgrade.

**Note:** The WPAN firmware image integrated with the IOS CGR image option is still supported.

Also, if only the WPAN firmware upgrade from the image bundled with IOS image is desired (for example, when the WPAN firmware upgrade option was not checked during IOS upgrade), the "Install from Router" option is also provided under respective WPAN image types (IOS-WPAN-RF or IOS-WPAN-PLC).

For detailed steps, go to Working with Router Firmware Images, on page 274.

# Changing Action Expiration Timer

You can use the cgnms_preferences.sh script to set or retrieve the action expiration timer value in the IoT FND database:

```
/opt/cgms
/bin/cgnms_preferences setCgrActionExpirationTimeout 50
```

Valid options are:

**Step 1** set *<pkg>actionExpirationTimeoutMins<value>*

where:

- *<pkg>* is the preference package (required for *set* and *get* operations).
- *actionExpirationTimeoutMins* is the preference key (required for *set* and *get* operations).
- *<value>* is the preferred value, in minutes (required for *set* and *setCgrActionExpirationTimeout* operations).

**Step 2** setCgrActionExpirationTimeout <value>

**Step 3** get *<pkg>actionExpirationTimeoutMins*

**Step 4** *getCgrActionExpirationTimeout*

**Example**

In the following example, the action timer value is retrieved, set, the current value retrieved again, the value removed, and a null value retrieved:

```
[root@userID-lnx2 cgms]#./dist/cgms-1.x/bin/cgnms_preferences.sh
getCgrActionExpirationTimeout
2013-08-12 22:38:42,004:INFO:main:CgmsConnectionProvider: registered
the database url for CG-NMS: [jdbc:oracle:thin:@localhost:1522:cgms]
5
[root@userID-lnx2 cgms]#./dist/cgms-1.x/bin/cgnms_preferences.sh
setCgrActionExpirationTimeout 50
2013-08-12 22:38:51,907:INFO:main:CgmsConnectionProvider: registered
the database url for CG-NMS: [jdbc:oracle:thin:@localhost:1522:cgms]
Successfully set the preferences.
[root@userID-lnx2 cgms]#./dist/cgms-1.x/bin/cgnms_preferences.sh
getCgrActionExpirationTimeout
2013-08-12 22:38:58,591:INFO:main:CgmsConnectionProvider: registered
```

```
the database url for CG-NMS: [jdbc:oracle:thin:@localhost:1522:cgms]
50
[root@userID-lnx2 cgms]#./dist/cgms-1.x/bin/cgnms_preferences.sh
get com.cisco.cgms.elements.ciscocgr actionExpirationTimeoutMins
2013-08-12 22:39:12,921:INFO:main:CgmsConnectionProvider: registered
the database url for CG-NMS: [jdbc:oracle:thin:@localhost:1522:cgms]
50
[root@userID-lnx2 cgms]#./dist/cgms-1.x/bin/cgnms_preferences.sh
set com.cisco.cgms.elements.ciscocgr actionExpirationTimeoutMins 15
2013-08-12 22:39:23,594:INFO:main:CgmsConnectionProvider: registered
the database url for CG-NMS: [jdbc:oracle:thin:@localhost:1522:cgms]
Successfully set the preferences.
[root@userID-lnx2 cgms]#./dist/cgms-1.x/bin/cgnms_preferences.sh
get com.cisco.cgms.elements.ciscocgr actionExpirationTimeoutMins
2013-08-12 22:39:29,231:INFO:main:CgmsConnectionProvider: registered
the database url for CG-NMS: [jdbc:oracle:thin:@localhost:1522:cgms]
15
```

# Working with Resilient Mesh Endpoint Firmware Images

This section describes how to add Resilient Mesh Endpoint (RME) firmware images to IoT FND, and how to upload and install the images on routers.

## Overview

When you instruct IoT FND to upload a firmware image to the members of an RME firmware group or subnet, IoT FND pushes the image to the group members in the background and tracks the upload progress to ensure that the devices receive the image.

A Resilient Mesh Endpoint (RME) stores three firmware images:

- Uploaded image: Image most recently uploaded.
- Running image: Image that is currently operational.
- Backup image: It serves as a golden (fallback) image for the RME if there is an issue with the running image.

**Note** You can initiate up to 3 firmware downloads simultaneously.

**Note** IR500s and other RME devices can coexist on a network; however, for firmware management they cannot belong to the same group.

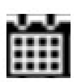
**Note** RME devices can report BL/Boot Loader image types to IoT FND, but IoT FND cannot upload boot loader images to devices.

# Actions Supported and Information Displayed at the Firmware Management Pane

At the Firmware Management pane, you can filter the display by Subnet, PanID or Group when you are in the Devices tab.

For every image in the list, IoT FND displays the information as noted in the table:

***Table 62: Image Information Displayed by IoT FND***

| Item | Description |
|---|---|
| Image | Image name. |
| Uploaded | Specifies the number of devices that uploaded the image. Click the number to display a list of these devices. |
| Running | Specifies the number of devices running this image. Click the number to display a list of these devices. |
| Backup | Specifies the number of devices using this image as a backup. Click the number to display a list of these devices. |
| Boot Loader | Specifies the boot loader image version. |
| LMAC | Specifies the LMAC image version. |
| BBU | Specifies the BBU image version. |
| Status | Specifies the status of the upload process. |
| Scheduled Reload | Specifies the scheduled reload time. |
| Actions | Provides two actions:<br>• Schedule Install and Reload —Schedule the installation date and time of the loaded image and the reboot of the endpoint by selecting the Calendar icon.<br><br>• Set as Backup —Set the firmware backup image by selecting the clock icon with reverse arrow.<br><br>See Setting the Installation Schedule, on page 262 for complete steps. |

# Set a Firmware Backup Image

To set an image as a firmware image backup:

**Step 1** Click the Set as Backup button. (See the icon in the Actions summary in Table 62: Image Information Displayed by IoT FND, on page 261).

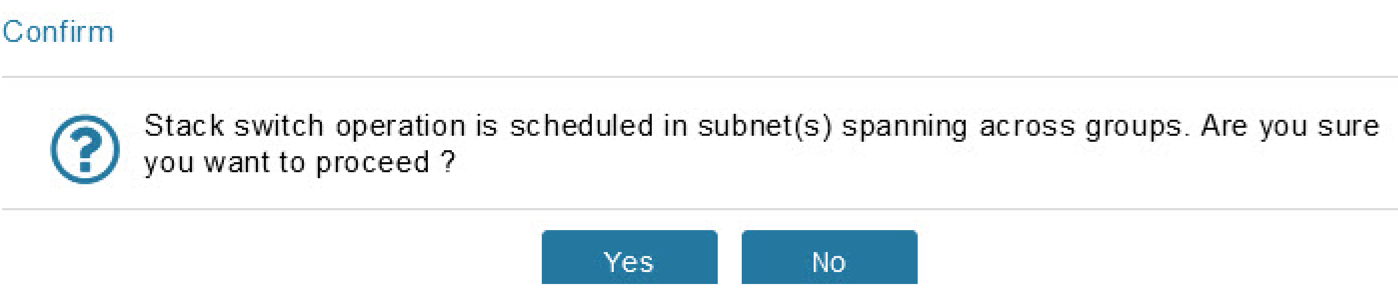
**Step 2** Click **Yes** to confirm backup.

## Setting the Installation Schedule

To set the installation schedule for an image:

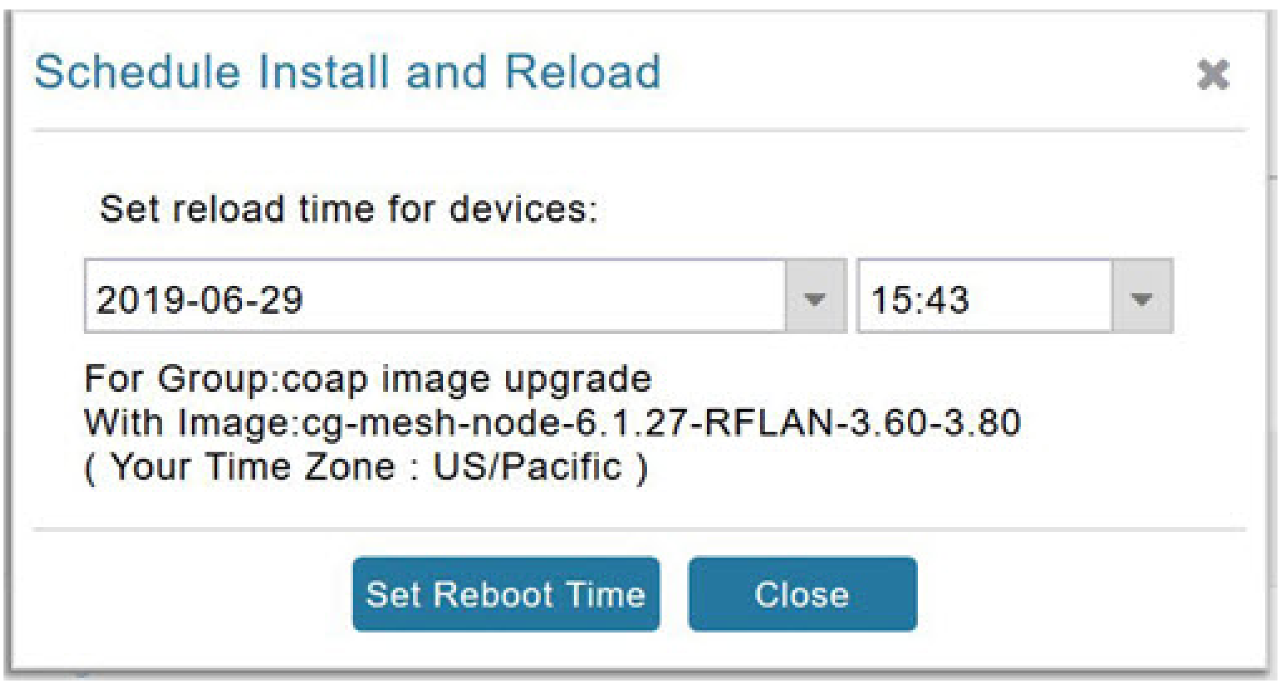
**Step 1** Click the **Schedule Install and Reload** button (Calendar icon). For more information, see Table 62: Image Information Displayed by IoT FND, on page 261.

The following message appears if you try to schedule a reload operation for the node that is scheduled for stack switch operation.




**Step 2** In the page that appears, specify the date and time for the installation of the image and rebooting of device.

***Figure 21: Schedule and Install and Reload Page***




**Step 3** Click the **Set Reboot Time** button.

# Firmware Update Transmission Settings

You can configure the Transmission Speed for pacing mesh firmware downloads at the Transmission Settings tab (See CONFIG > FIRMWARE UPDATE page).

**Step 1** Select the Transmission Speed. Options are Slow (default), Medium, Fast or Custom.

The Slow setting is recommended as the initial setting. You can increase the Slow setting to Medium (or even Fast) if the following conditions exist:

- The slow setting does not cause any issues in the database and it is able to handle the workload presented without raising any alarms.
- There is a need to improve on the time taken to do the firmware download.

**Step 2** Configure the minimum number of nodes necessary to enable the Multicast firmware upload.

**Note** For Custom Transmission Speed, you will have to specify Multicast Threshold, Unicast Delay and Minimum Multicast Delay values. Refer to the table below for the definitions of the terms on the **CONFIG** > **FIRMWARE UPDATE** > **Transmissions Settings** page.

*Figure 22: CONFIG > FIRMWARE UPDATE*

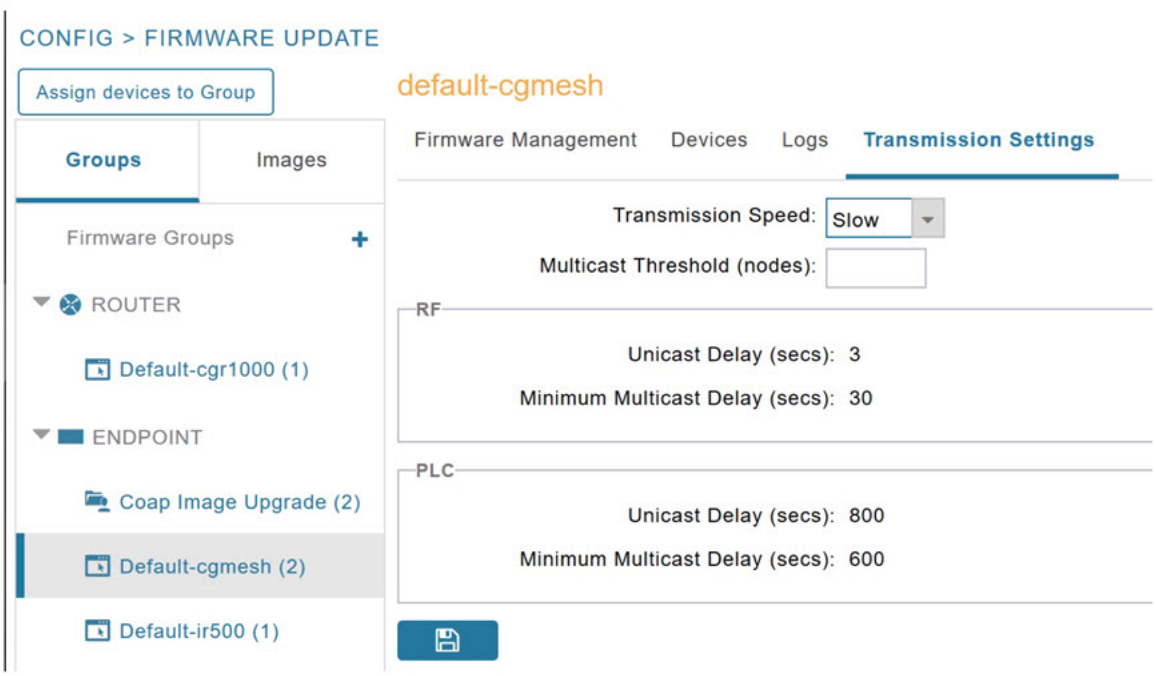



*Table 63: Definitions of variables seen on CONFIG > FIRMWARE UPDATE Transmissions Settings page*

| Item | Description |
|---|---|
| Minimum Multicast Delay (seconds) | Time between subsequent blocks when sending multi-cast messages/blocks/packets to a node. |

| Item | Description |
| --- | --- |
| Multicast Threshold (nodes) | Minimum number of nodes needed to ensure that a multicast transmission can happen in a subnet, if the number of elements requiring a specific image block is greater than or equal to the multicast-threshold value. |
| Transmission Speed | Options are Slow (default), Medium, Fast or Custom. |
| Unicast Delay (seconds) | Time between subsequent blocks when sending unicast messages, blocks or packets to a node. |

# Uploading a Firmware Image to a Resilient Mesh Endpoint (RME) Group

To upload a firmware image to mesh endpoint group members:

**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE**.

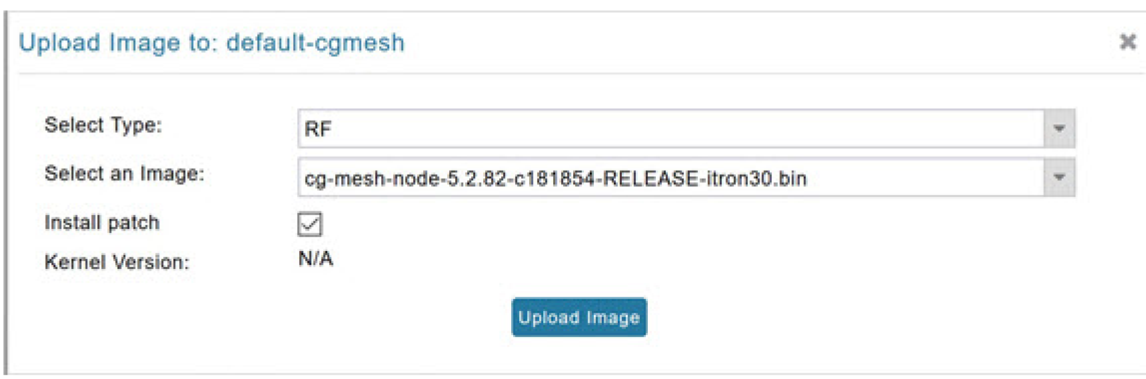
**Step 2** Click the **Groups** tab (left-pane).

**Step 3** Select the Endpoint firmware group to update.

**Step 4** In the right panel, select Firmware Management and then click the Upload Image button. In the entry panel that appears, do the following:

a) From the Select Type drop-down menu, choose the firmware type for your device.
b) From the Select an Image drop-down menu, choose the firmware bundle to upload.
c) Click **Upload Image**.
d) (Optional) Check the Install patch box, if you choose *to install only the patch* of the new image (For more information, see Figure 23: Check Install Patch Item to ONLY Install the Patch Rather than the Full Image, on page 264).

***Figure 23: Check Install Patch Item to ONLY Install the Patch Rather than the Full Image***




e) Click **OK**.

IoT FND adds the image to the list of images in the Firmware Management pane and starts the upload process in the background. A bar chart displays the upload progress (percentage complete). See Figure 24: Firmware Update - Percentage Complete (top-portion of screen), on page 265 and Figure 25: Firmware Update - Upload Summary (bottom-portion of screen), on page 265.

**Note** Click the Sync Membership button to ensure that FND and the member endpoint firmware group information are the same.

*Figure 24: Firmware Update - Percentage Complete (top-portion of screen)*

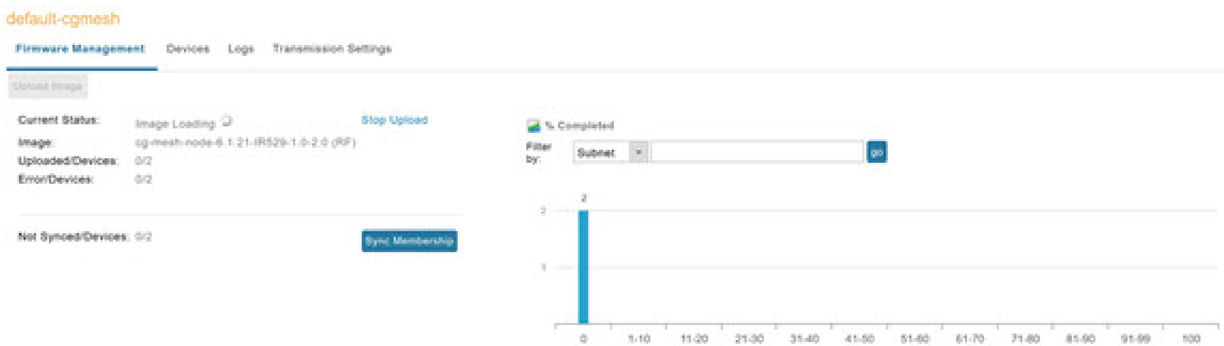
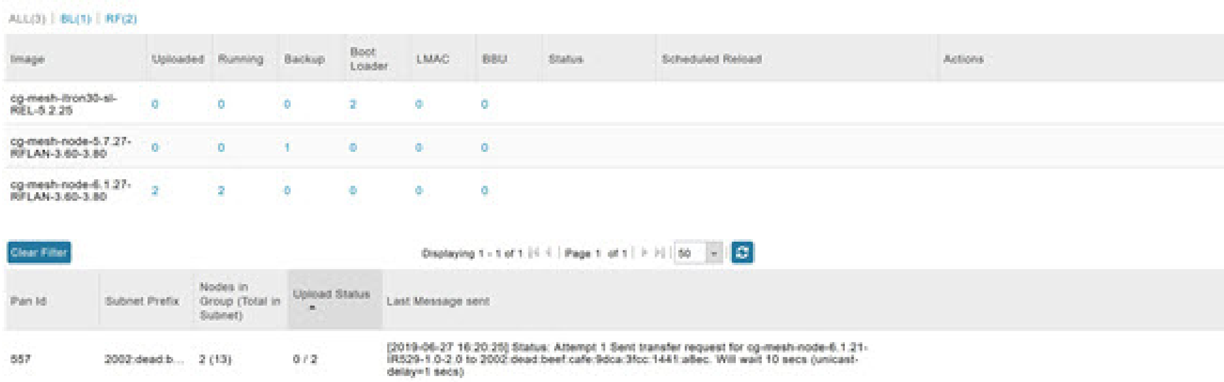


*Figure 25: Firmware Update - Upload Summary (bottom-portion of screen)*



# Uploading a Firmware Image to FND

To upload a firmware image to mesh endpoint group members:

**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE**.

**Step 2** Select the **Images** tab (left-pane).

**Step 3** Select the Endpoint Image type (such as BBU, IOx-IR500 LMAC) to be uploaded.

**Step 4** Click on + (plus icon) next to the FIRMWARE IMAGES heading to browse the firmware from your local system.

**Step 5** Browse and click on **Add file**.

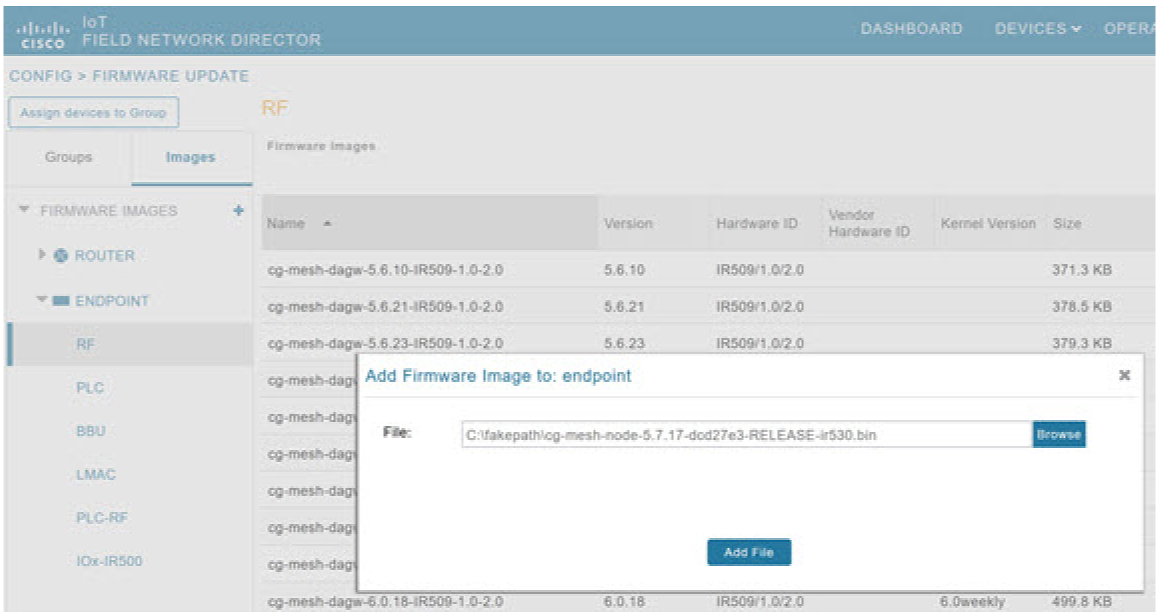
IoT FND can upload the following image types to ENDPOINT devices as shown in the table below:

*Table 64: Firmware Images for Endpoints*

| Image Type | Description |
|---|---|
| RF | For endpoints with RF radio only. |

| Image Type | Description |
|---|---|
| PLC | For endpoints with Power line communication (PLC) radio only. |
| BBU | For Battery back up (BBU) units. |
| LMAC | For Local MAC connected devices. |
| IOx-IR500 | For IR500 devices running Cisco IOx software. |

*Figure 26: Using IoT FND to Upload Images to an Endpoint*




## Modifying Display of Firmware Management Page

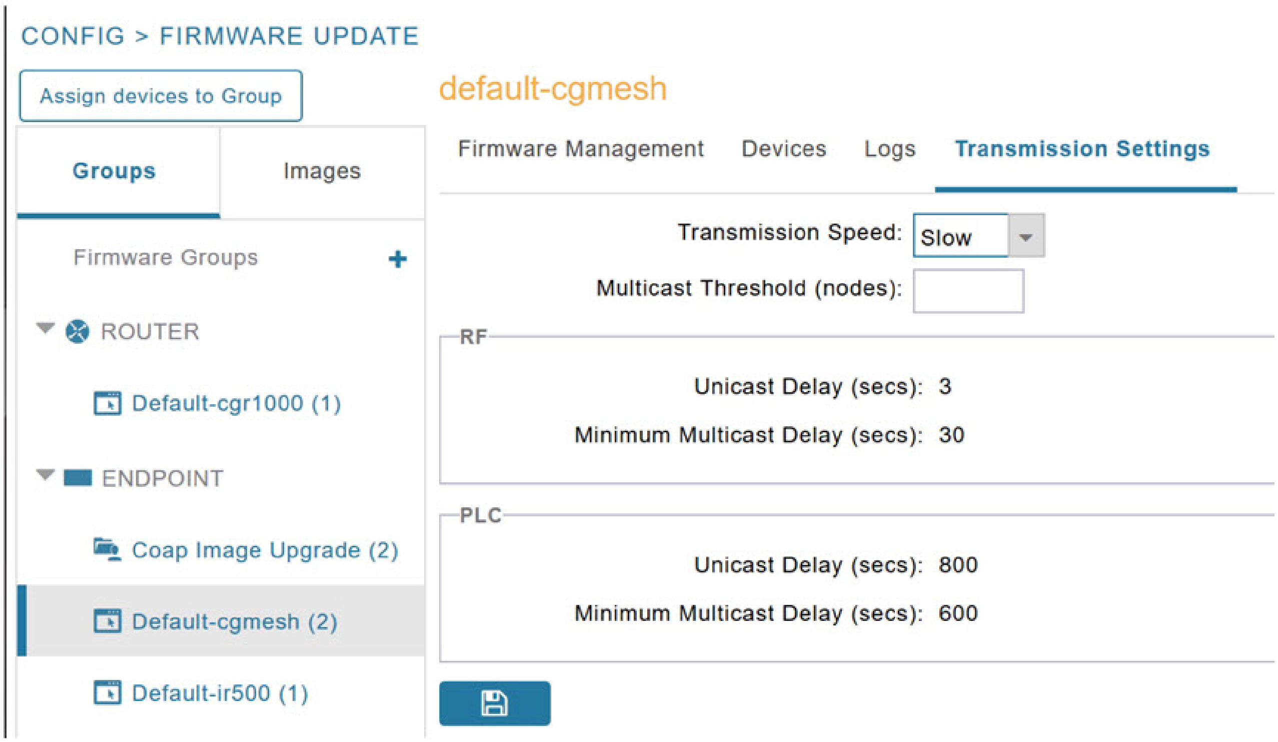
You can filter the Firmware Management page display by Subnet, PanId or Group in the Devices tab.

To modify the display of firmware management page:

**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE**.

**Step 2** Click the **Sync Membership** button to ensure that the information for FND and the member endpoint firmware group is the same.

*Figure 27: CONFIG > FIRMWARE UPDATE*




## Viewing Mesh Device Firmware Image Upload Logs

To view the mesh device firmware image upload logs:

**Step 1** Click the **Sync Membership** button to sync the group members in the same firmware group.

**Step 2** Click the **Devices** tab to view member's devices.

**Step 3** Click the **Logs** tab to view log files for the group.

For more information, refer to Figure 24: Firmware Update - Percentage Complete (top-portion of screen), on page 265
.

# AP800 Firmware Upgrade During Zero Touch Deployment

During the PnP bootstrapping, whenever an access point (AP) or router sends the firmware request, FND will need to make the choice as to whether Unified Firmware or Autonomous Firmware is updated on the AP to make it accessible to the Cisco Wireless LAN Controller (WLC) after a firmware upgrade.

**Note** Once you set up the DHCP server on a Cisco IOS router, WLC generally handles the software updates for the AP.

Allows you to set the desired firmware that will update an IR829 or C800 router during ZTD.

There are two possible firmware options:

- **Option 1**: Set the ‘unified’ version (k9w8: the factory-shipped version) as the desired firmware.
- **Option 2** : Set the autonomous firmware as the desired firmware version.

During the ZTD process, the firmware upgrade of an access point (AP) or embedded AP on an IR829 or C800 router will upgrade using the firmware version you define as the autonomous firmware.

To define the Autonomous Firmware for an IR829 or C800 router:

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

**Step 2** Select the desired router: Default-ir800 or C800 (left-pane).

**Step 3** Check the installed firmware version, BEFORE upload. if equal to the latest version, skip firmware upgrade.

**Step 4** Before you upload the software to the router, check the image and version:

- If the router image version is equal to the latest version, skip upgrade.
- If router image has the latest

**Step 5** Select Edit AP Configuration Template tab (right-pane).

**Step 6** Enter the following text in the 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 (Note: Enter a single WLC IP
address(10.10.10.15) in hex format)
ip address <router_ip> 255.255.255.0
! {Note the symbol in this line is an exclamation point}
service-module wlan-ap 0 bootimage unified
```

**Step 7** Click disk icon (bottom of page) to save the commands in the configuration template.

# Image Diff Files for IR809 and IR829

To reduce the file size that transfers across network for IR809 and IR829, you can send a partial image:

- At the Upload Image page, select type: IOS-IR800.
- Check box for option: “install patch for IOS and hypervisor from this bundle.”

# Gateway Firmware Updates

IC3000 Firmware Updates:

- At the **CONFIG** > **FIRMWARE UPDATE** page, you can add or delete the IC3000 firmware image.

**Note** Firmware image upload depends on interface speeds. You can set the timeout duration (in minutes) for firmware upload in cgms.properties file using "igma-idle-timeout" key. If you don’t set this duration, then default timeout duration will be 15 minutes.

- At the **Images** tab page, expand the Gateway icon and click on IC3000 to see a list of available IC3000 images.

# Configuring Firmware Group Settings

This section describes how to add, delete, and configure firmware groups, and includes the following topics:



**Note** Upload operations only begin when you click the **Resume** button.

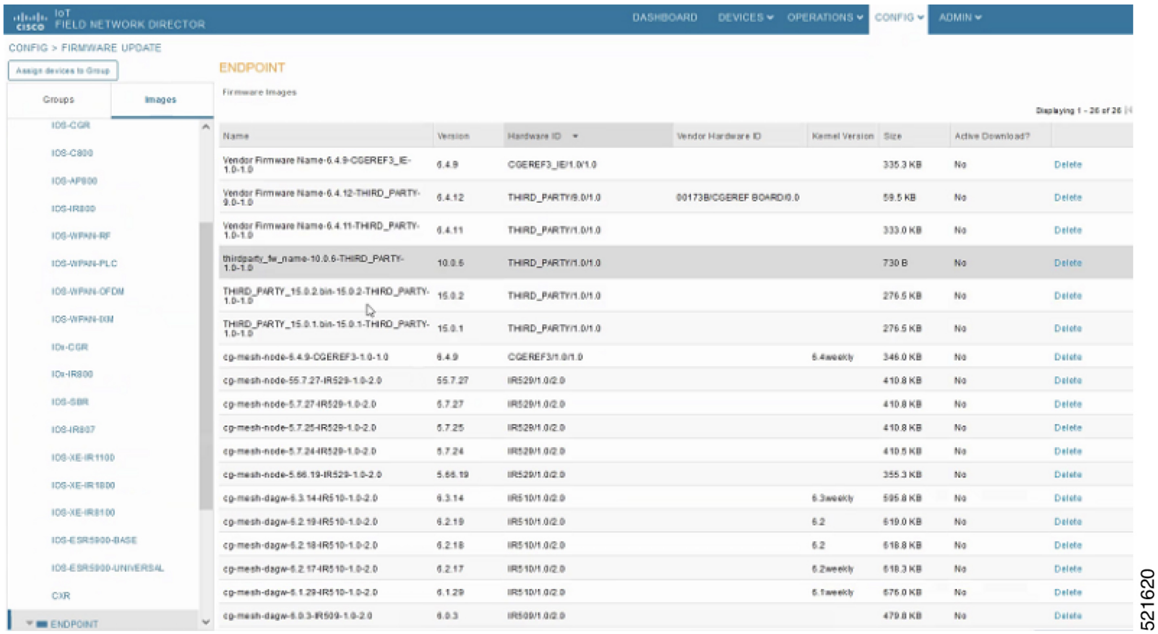
When you add routers or RMEs to IoT FND, the application sorts the devices into the corresponding default firmware group: default-<*router*> or default-cgmesh. Use these groups to upload and install firmware images on member devices. Add firmware groups to manage custom sets of devices. You can assign devices to firmware groups manually or in bulk. Before deleting a firmware group, you must move all devices in the group to another group. You cannot delete non-empty groups.

When creating firmware groups note the guidelines:

- CGRs, IR800s, and C800s can coexist on a network; however, for firmware management, they cannot belong to the same firmware group.
- IR500s and other RMEs devices can coexist on a network; however, for firmware management, they cannot belong to the same group.

The Groups tab on the **CONFIG** > **FIRMWARE UPDATE** page displays various device metrics.

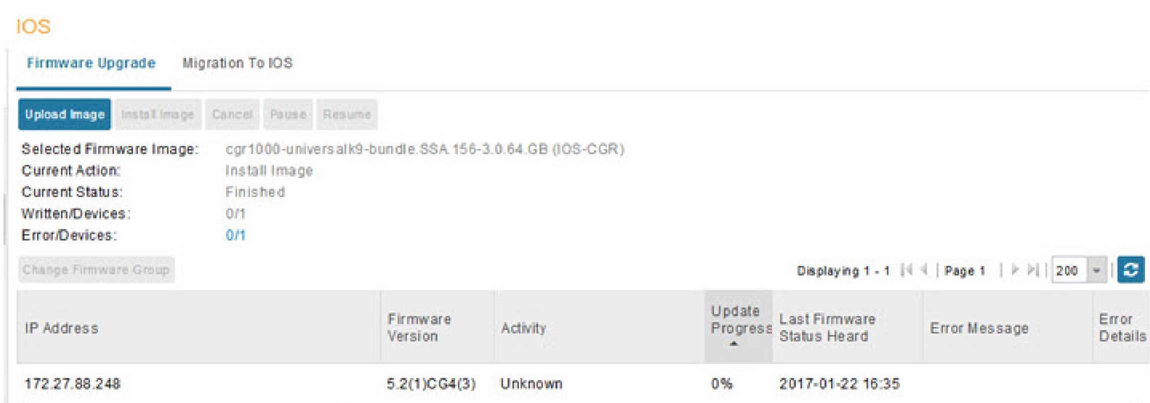
*Figure 28: CONFIG > FIRMWARE UPDATE*




**Tip** At the Firmware Update page, click the Error/Devices link (not shown) in Figure 29: Firmware Upgrade Page – Viewing Errored Devices, on page 270 to apply a filter.

Click **Clear Filter** to revert to an unfiltered view of the selected device group.

*Figure 29: Firmware Upgrade Page – Viewing Errored Devices*

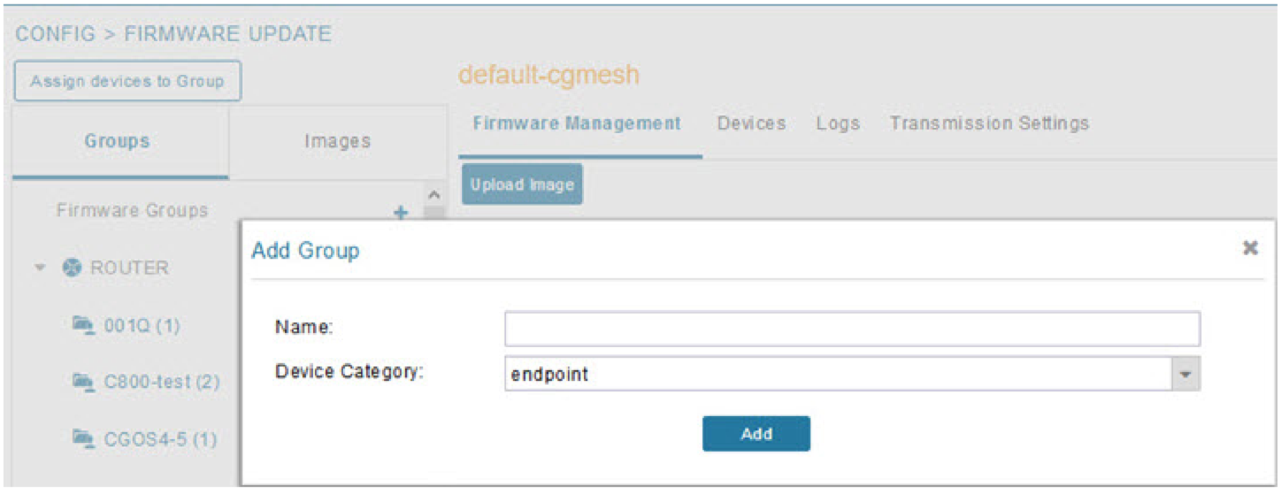



# Adding Firmware Groups

To add a firmware group:

**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE**.

**Step 2** Click the **Groups** tab.




**Step 3** In the Groups pane, select one of the following:

- Default-cgr1000
- Default-c800
- Default-ir500
- Default-ir800
- Default-cgmesh
- Default-sbr

**Step 4** Click + next to Firmware Groups heading in the Groups pane to Add Group.

**Step 5** In the **Add Group** dialog box, enter the name of the firmware group. Device Category options depend on the device type you select in Step 3.

**Step 6** Click **Add**.

The new group label appears under the corresponding device type in the Firmware Groups pane.

**Note** To assign devices to the new group, see Assigning Devices to a Firmware Group, on page 271.

# Assigning Devices to a Firmware Group

This section explains moving devices to another firmware group in bulk or manually.

## Moving Devices to Another Group In Bulk

To move devices from one group to another in bulk:

**Step 1** Create a CSV or XML file listing devices that you want to move using the format shown in the following examples:

| *DeviceType/EID* for CGRs: | *EID* only for mesh endpoints: | *EID* only for IR800s |
|---|---|---|
| `eid`<br>`CGR1120/k9+JS1`<br>`CGR1120/k9+JS2`<br>`CGR1120/k9+JS3` | `eid`<br>`00078108003c1e07`<br>`00078108003C210b` | `eid`<br>`ir800` |
| ***EID* only for ISR 800s:** | ***EID* only for IR500s:** | ***EID* only for IC3000** |
| `eid`<br>`C819HGW-S-A-K9+FTX174685V0`<br>`C819HGW-S-A-K9+FTX174686V0`<br>`C819HGW-S-A-K9+FTX174687V0` | `eid`<br>`da1`<br>`da2`<br>da3 | `eidIC3000+FOC2219Y47Z` |

**Note** Each file can only list one device type.

**Step 2** Choose **CONFIG** > **FIRMWARE UPDATE**.

**Step 3** Click the **Groups** tab.

**Step 4** Click the **Assign devices to Firmware Group** button (found above the Groups tab).

**Step 5** In the window that appears, click **Browse** and locate the device list CSV or XML file.

**Step 6** From the **Group** drop-down menu, choose the destination group.

**Step 7** Click **Assign to Group**.

**Note** IoT FND moves the devices listed in the file from their current group to the destination group.

**Step 8** Click **Close**.

## Moving Devices to Another Group Manually

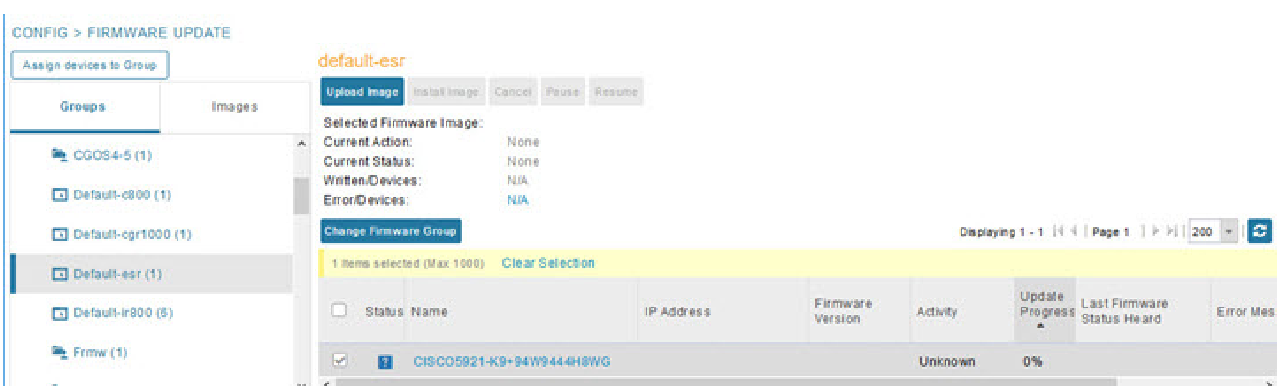
To manually move devices to a group:

**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE**.

**Step 2** Click the **Groups** tab.

**Step 3** In the Firmware Groups pane, select the desired firmware group based on device type.

**Note** If this is an ENDPOINT firmware group, click the **Devices** tab above the main pane.



**Step 4** Check the check boxes of the devices that you want to move.

**Step 5** Click **Change Firmware Group** to open a pop up window.

**Step 6** From the **Firmware Group** drop-down menu, choose the firmware group to which you want to move the devices or enter a new group name.

**Step 7** Click **Change Firmware Group**.

**Step 8** Click **Close**.

# Renaming a Firmware Group

In the **Firmware Update** page, there are two firmware groups available, namely user-created groups and default groups of router, endpoint, or gateway. IoT FND allows you to rename the user-created firmware groups only. You cannot rename the default firmware groups.

To rename a firmware group:

**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE**.

**Step 2** Click the **Groups** tab.

**Step 3** In the Firmware Groups pane, select the firmware group to rename.

**Step 4** Move the cursor over the firmware group and click the **Edit Group Name** pencil icon.


**Note** Starting with IoT FND, you can only rename the user-created firmware groups and you cannot rename the default firmware groups. The pencil icon does not appear for the default firmware groups.

**Step 5** In the **Rename Group** window, enter the new name and then click **OK**.

**Note** When you enter an invalid character entry (such as, @, #, !, or +) within the Rename Group field, IoT FND displays a red alert icon, highlights the field in red, and disables the **OK** button.

# Deleting Firmware Groups

**Note** Before deleting a firmware group, you must move all devices in the group to another group. You cannot delete non-empty groups.

To delete a firmware group:

**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE**.

**Step 2** Click the **Groups** tab.

**Step 3** In the Firmware Groups pane, select a firmware group to display a list of all possible firmware images for that group in the right pane.

**Step 4** Check the box next to the firmware group that you want to delete.

**Step 5** Click Clear Selection that appears above the entry (yellow bar).

**Step 6** To confirm deletion, click **Yes**.

**Step 7** Click **OK**.

# Working with Router Firmware Images

This section describes how to work with router firmware images in IoT FND.

## Installing a Firmware Image

To install an image on devices in a router firmware group:

**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE**.

**Step 2** Click the **Groups** tab.

**Step 3** In the Groups pane, select the firmware group.

**Note** IoT FND recognizes devices as firmware-specific, and uploads the proper image to selected devices.

**Step 4** In the Images pane, select a device subgroup (such as IOS-CGR, IOS-WPAN-RF, CDMA) to refine the display to those device types.

This step above is necessary because IoT FND recognizes devices as firmware-specific and ensures the system uploads the proper image to selected devices.

**Step 5** At the **CONFIG > FIRMWARE UPDATE** page, click the Groups tab; and, then **Install Image** on the Firmware Upgrade tab.

IoT FND sends commands to install the uploaded image and make it operational.

**Step 6** Click **Yes**.

IoT FND starts the installation or reloading process.

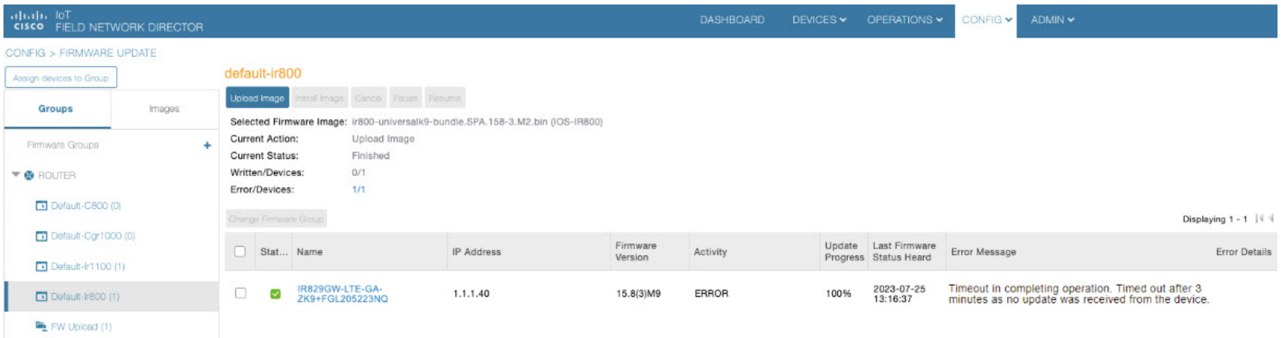
**Note** If you restart IoT FND during the image installation process, IoT FND restarts the firmware installation operations that were running prior to IoT FND going offline.

You can pause or stop the installation operation as described in:


- Stopping Firmware Image Installation, on page 279
- Pausing and Resuming Router Firmware Image Installation, on page 278

**Note** The firmware installation operation can time out on some routers. During firmware install, the job scheduler that runs every two hours times out the stuck firmware install jobs that has progressed upto 35%. The default time of the job scheduler of two hours can be modified in the "firmware-install-timeout-schedule-cron-hour" key in the cgms.properties file. Provide values within the range of greater than 0 and less than 24. This job scheduler is applicable only for install at 35%.

**Note** When a firmware install or image upload operation for routers take extended run time, it can result in prolonged wait times for the other jobs in the queue. You can configure timeout duration for the stuck firmware jobs in the “router-firmware-upload-timeout-minutes” and “router-firmware-install-timeout-minutes” keys in cgms.properties file. The default value is set to 8 hours (480 minutes). The timeout is accounted after the device stops responding and the following error message is displayed.




# Adding a Firmware Image to IoT FND

Before you can upload and install a firmware image on a device, add the image file (as a zip archive) to IoT FND. IoT FND stores the image in its database.

**Note** Do not unzip the image file. IoT FND unzips the file.

To add a firmware image to IoT FND:

**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE**.

**Step 2** Click the **Images** tab ( CONFIG > FIRMWARE UPDATE > Image).

**Step 3** In the Images pane, select **ROUTER**, **ENDPOINT**, or **GATEWAY** and the type of device group.

**Step 4** Click the + icon to select an image found to the right of the Firmware Images heading.

**Step 5** Click **Browse** to locate the firmware image. Select the image, then click **Add File**.

**Step 6** Click **Upload**.

The image appears in the Firmware Images panel ( CONFIG > FIRMWARE UPDATE > Image).

- To delete an image, click the **Delete link** shown at far-right of entry. Click **Yes** to confirm.

  Firmware images with a download in progress (with Yes in the Active Download? column) cannot be deleted.

- To upload the firmware image to devices in a group, select the group (from Groups listing on CONFIG > FIRMWARE UPDATE page) and then click **Upload Image**. See Uploading a Firmware Image to a Router Group, on page 276.

# Uploading a Firmware Image to a Router Group

When you upload a firmware image to router firmware group members, IoT FND pushes the image to the group members in the background and tracks the upload progress to ensure that the devices receive the image.

On routers, firmware image upload and installation requires 200 MB of free disk space. IoT FND stores image files in the .../managed/images directory on the router.

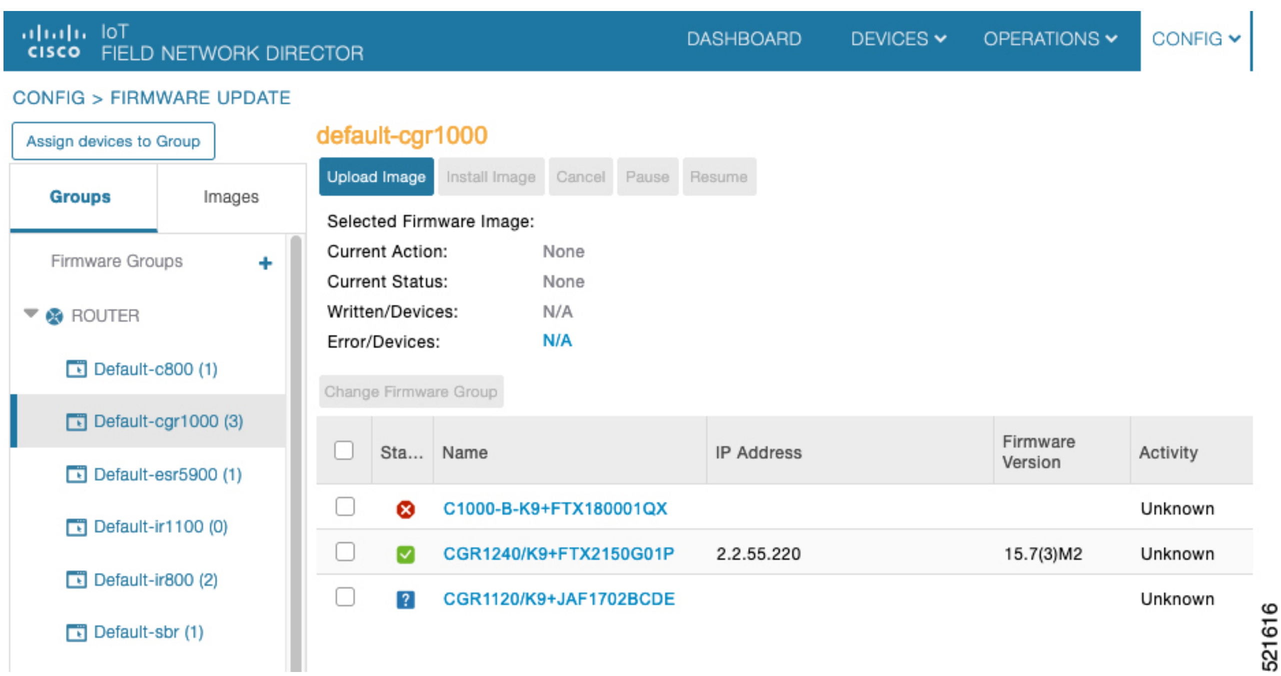
**Note** If there is not enough disk space on the router for the firmware image, the IoT FND initiates disk cleanup process on the router and removes unused files in the .../managed/images directory that is not currently running or referenced in the before-tunnel-config, before-registration-config, express-setup-config, and factory-config files for IOS CGRs, sequentially, until there is enough disk space to upload the new image.

If there is still not enough space, you must manually delete unused files on the router.

To upload a firmware image to router group members:

**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE**.

*Figure 30: Updating Firmware for a CGR1000*




**Step 2** Click the **Groups** tab.

**Step 3** In the Groups pane, select the router firmware group that you want to update.

IoT FND displays the firmware image type applicable to the router:

| Image | Type | Applicable Devices |
|---|---|---|
| CDMA | All | Cisco IOS CGRs, IR800s, and ISR800s. |
| GSM | All | Cisco IOS CGRs, IR800s, and ISR800s. |
| IOS-CGR | CGR1000 | Cisco IOS CGRs (CGR1240 and CGR1120) . |
| IOS-C800 | C800 | Cisco 800 Series ISR connected devices. |
| IOS-AP800 | AP800 | Cisco 800 Series Access Points. |
| IOS-IR800 | IR800 | Cisco 800 Series ISRs. |
| LORAWAN | lorawan | Cisco IR829-GW |
| IOS-WPAN-RF | CGR1000 | Cisco IOS-CGR |
| IOS-WPAN-PLC | CGR1000 | Cisco IOS-CGR |
| IOS-WPAN-OFDM | CGR1000 | Cisco IOS-CGR |
| IOS-WPAN-IXM | IR800 | LoRaWAN IXM module when operating as an interface for Cisco IR809. |
| IOx-CGR | cgr1000-ioxvm | Cisco IOS-CGR |
| IOx-IR800 | IR800 | Cisco 800 Series ISRs. |
| IOS-SBR | C5921 | Cisco 5921 Embedded Services Router |
| IOS-IR807 | IR800 | Image (Cisco IOS only) loads to IR807 within the IR800 firmware group. |
| IOS-XE-IR1100 | IR1100 | Cisco 1101 Series Industrial Integrated Services Routers |
| IOS-XE-IR1800 | IR1800 | Cisco Catalyst IR1800 Rugged Series Routers (IR1821, IR1831, IR1833, and IR1835) |
| IOS-XE-IR8100 | IR8100 | Cisco IR8140 Heavy-Duty Series Routers |
| IOS-ESR5900-BASE | C5921 | Cisco 5921 ESR (C5921) |
| IOS-ESR5900-UNIVERSAL | C5921 | Cisco 5921 ESR (C5921) |
| IOT-FND-IC3000 | IC3000 | Cisco IC3000 Gateway |

**Step 4** Click **Upload Image** to open the entry panel.

**Step 5** From the **Select Type:** drop-down menu, choose the firmware type for your device.

**Step 6** From the **Select an Image:** drop-down menu, choose the firmware bundle to upload.

For some software bundles, you also have the option to select one or more of the following options (as noted in parenthesis next to the options listed below):

- Install Guest OS from this bundle (IOS-CGR, IOS-IR800).

- Clean LoRaWAN application data on the install (LORAWAN).
- Install WPAN firmware from this bundle (IOS-CGR).

**Step 7** Click **Upload Image**.

**Step 8** Click **OK**.

IoT FND starts the upload process. After the image uploads, install the image as described in Installing a Firmware Image , on page 274.

# Pausing and Resuming Router Firmware Image Installation

You can pause the firmware image installation process at any time.

**Note** Pausing the installation pauses all queued tasks. Currently running tasks complete.

To pause firmware image installation to devices in a firmware group:

**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE**.

**Step 2** In the Groups pane, select the firmware group.

**Step 3** In the Firmware Upgrade window, click the **Pause** button.

**Step 4** Click **Yes** to confirm the action.

You can resume the installation process by clicking **Resume**.

# Pausing and Resuming Router Firmware Image Uploads

You can pause the image upload process to router firmware groups at any time, and resume it later.

**Note** The image upload process does not immediately pause; all queued (but not running) operations pause, but currently running tasks complete. The status changes to PAUSING until the active operations complete.

To pause firmware image upload:

**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE**.

**Step 2** Click the **Groups** tab.

**Step 3** In the Groups pane, select the firmware group.

**Step 4** Click **Pause**.

The Status column displays PAUSING until the active upload operations complete. No new upload operations start until you click the **Resume** button.

**Step 5** Click **Yes**.

To resume the upload process, click **Resume**.

**Note** If a IoT FND server goes down while the firmware image is being uploaded to devices, the server resumes the upload process for the scheduled devices after the server comes up. For IoT FND server clusters, if one server goes down during the upload process, another server in the cluster resumes the process.

# Stopping Firmware Image Installation

You can stop firmware image installation at any time. When you stop image installation, the running version of the firmware remains in place.

**Note** Stopping the installation cancels all queued tasks. Currently running tasks complete.

To stop firmware image installation to devices in a firmware group:

**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE**.

**Step 2** Click **Groups**.

**Step 3** In the Groups pane, select the firmware group.

**Step 4** In the Firmware Upgrade window, click **Cancel** button.

**Step 5** Click **Yes** to confirm the action.

# Canceling Router Firmware Image Upload

You can stop the image upload process to firmware router groups at any time. Stopping the upload can take a few minutes. When you cancel the image upload, the image upload process immediately stops currently running tasks, and blocks all queued tasks.

**Note** Running tasks do not complete, leaving partial files on the disk and sets the firmware group status to CANCELING until you complete the upload operation.

To stop firmware image uploading to a group:

**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE**.

**Step 2** Click the **Groups** tab.

**Step 3** In the Groups pane, select the firmware group.

**Step 4** Click **Cancel**.

**Step 5** Click **Yes**.

---

# Viewing Firmware Image Files in IoT FND

To view the firmware image files in IoT FND:

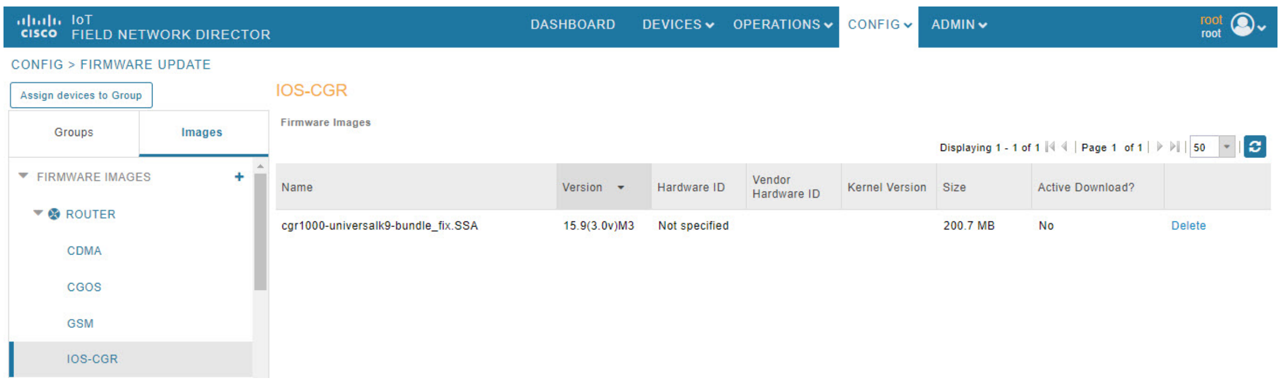
---

**Step 1** Go to **Images** pane in the **CONFIG** > **FIRMWARE UPDATE** page.

**Step 2** Select ROUTER or ENDPOINT to display all firmware images for those devices in the IoT FND database.

**Step 3** Select the firmware image type to refine the display (see CONFIG > FIRMWARE UPDATE > Image).

***Figure 31: CONFIG > FIRMWARE UPDATE > Image***




---

# Support for Wi-SUN Stack Switch

Starting with Cisco IoT FND 4.8.1 release, you can switch devices from CG-Mesh to Wi-SUN (Wireless and Smart Utility Networks) stack. User with administrative privilege or firmware upgrade permission can only perform this switch operation. During the switching process, a single or multiple PAN nodes are grouped and scheduled for switching devices from CG-Mesh to Wi-SUN stack. Wi-SUN stack supports both unicast and multicast transmissions. For more information on the switching process, refer to Switching Devices from CG-Mesh to Wi-SUN Stack, on page 281.

### Supported Platforms

IoT FND supports the following platforms for switching devices from CG-Mesh to Wi-SUN stack:

- ITRON30
- IR510
- IR530

### Prerequisites

- Firmware version must be 6.2 MR.

- CGR version must be greater than Cisco IOS 15.9(3)M1.

**Note** On successful switching of devices from CG-Mesh to Wi-SUN stack mode, ensure to update the WPAN OFDM/FSK stack mode to Wi-SUN stack. If the WPAN OFDM/FSK is not updated, the node cannot join back the network and will move to *Down* state in FND.

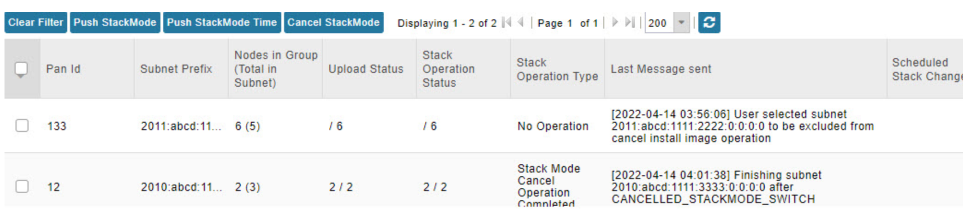
*Table 65: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Support For Wi-SUN Stack Switch | IoT FND 4.8.1 | This feature allows you to switch devices from CG-Mesh to Wi-SUN stack. |

# Switching Devices from CG-Mesh to Wi-SUN Stack

The process of switching devices from CG-Mesh to Wi-SUN stack involves the following tasks:

1. Pushing Devices to Wi-SUN Stack Mode, on page 281
2. Scheduling Devices for Wi-SUN Stack Switch




**Note** If the selected PAN ID spans across multiple groups, then all the devices in that PAN get pushed with new stack mode and time or get cancelled.

## Pushing Devices to Wi-SUN Stack Mode

To push devices to Wi-SUN stack mode:

**Step 1** Choose **CONFIG** > **Firmware Update**.

**Step 2** Click the **Groups** tab in the left pane.

**Step 3** Select the default or user-defined firmware group from the **ENDPOINT**.

**Step 4** Check the **PAN ID** check box in the **Stack Mode Switch** table for which you want to push the stack mode.

**Step 5** Click **Push StackMode**.

Based on the status of the push stack mode process, the following states are displayed for the selected PAN ID in the **Stack Mode Switch** table.

*Table 66: PAN ID Status*

| Field | Description |
|---|---|
| Stack Operation Type Column | Displays the following states for the push stack mode operation:<br>• **Stack Mode Push Initiated** — Denotes the initiation of the stack mode operation.<br>• **Stack Mode Push Completed** — Denotes the completion of the stack mode operation. |
| Stack Operation Status Column | Displays the overall success and failure status of the devices for the selected PAN during the stack mode operation. |

**Note** The **Devices** tab displays the status of the stack mode operation at the device level. For more information, refer to Viewing Stack Mode Information for Devices, on page 286

a) In the **Stack Mode Push Initiated** state, the devices in the selected PAN ID are validated based on the following scenarios:

*Table 67: Push Stack Mode Validation*

<table>
<tr><th>Scenarios</th><th>System Validation</th><th>User Action</th></tr>
<tr><td rowspan="2">Firmware version 6.2 MR.</td><td>Checks if the devices in the selected PAN ID are running firmware version 6.2 MR.<br>• If the firmware version is lower than 6.2 MR, then an error message appears.<br>Note Go to the Devices tab, for more information on the devices that are running a lower version.</td><td>• You must upgrade the devices to firmware version 6.2 MR.<br>• After upgrading the devices, you must again push new stack mode for the selected PAN ID.</td></tr>
<tr><td colspan="2">• If the firmware version is greater than 6.2 MR, then the devices are already in Wi-SUN stack.</td></tr>
</table>

| Scenarios | System Validation | User Action |
|---|---|---|
| Stack mode configuration. | Checks if all devices in the selected PAN ID received the stack mode configuration.<br>• Some devices in the selected PAN ID fail to receive the configuration. | • Push stack mode again for the selected PAN ID.<br>or<br>• Remove the devices that are in Down state from FND and again push stack mode for the remaining devices in the PAN ID. |
| | • If all the devices in the selected PAN ID received the stack mode configuration, then you can schedule the devices for stack switch operation initiation. | Scheduling Devices for Wi-SUN Stack Switch, on page 283<br>**Note** You can schedule the devices for Wi-SUN stack switch only on successful completion of pushing stack mode configuration to all devices in the selected PAN. |

b) On successful completion of the validation, the stack operation state for the selected PAN ID changes to **Stack Mode Push Completed**.

## Scheduling Devices for Wi-SUN Stack Switch

**Note** You can schedule devices for the Wi-SUN stack switching process only on successful completion of pushing devices to stack mode. For more information on pushing devices to Wi-SUN stack mode, see Pushing Devices to Wi-SUN Stack Mode, on page 281

To schedule devices for Wi-SUN stack switch:

**Step 1** Choose **CONFIG** > **Firmware Update**.

**Step 2** From the **Stack Mode Switch** table, check the **PAN ID** check box.

**Note** You can select only the PAN ID that has successfully completed the push stack mode configuration.

**Step 3** Click **Push StackMode Time**.

A **Confirm** dialog box appears to schedule the switching initiation process for moving CG-Mesh devices to Wi-SUN stack.

Based on the status of the stack mode time process, the following states are displayed for the selected PAN ID in the **Stack Mode Switch** table.

*Table 68: PAN ID Status*

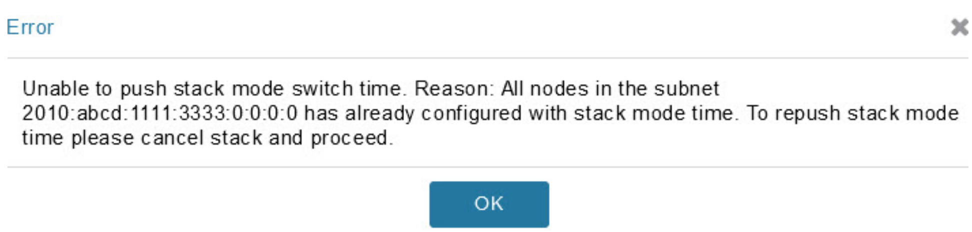
| Field | Description |
|---|---|
| Stack Operation Type Column | Displays the following states for the stack mode time operation:<br>• **Stack Switch Time Push Initiated** — Denotes the scheduling of the stack switch time operation.<br>• **Stack Switch Time Push Completed** — Denotes the completion of the stack switch time operation. |
| Stack Operation Status Column | Displays the overall success and failure status of the devices for the selected PAN during the stack mode time operation. |

**Note** The **Devices** tab displays the status of the stack mode time operation at the device level. For more information, refer to Viewing Stack Mode Information for Devices, on page 286.

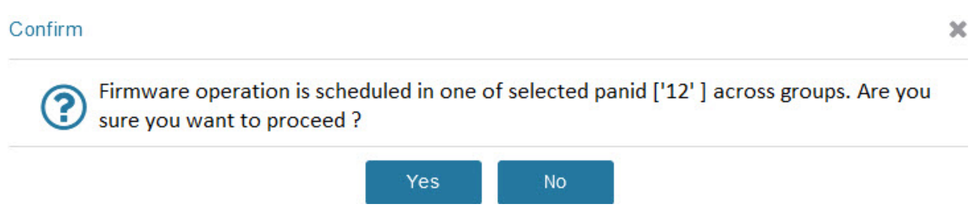
**Step 4** Click **Yes** to confirm the stack switching operation.

On confirming the stack switching process, the stack operation type gets updated to **Stack Switch Time Push Initiated** state for the selected PAN ID.

**Note** The following message appears if you push stack mode time to the node that is already configured with stack mode time.




The following message appears if you push stack mode time for the node that is already scheduled for firmware operation.




**Step 5** In the **Schedule Switch Wi-SUN Stack** dialog box, select the time and click **Schedule**.

**Note** Ensure that the scheduled time is not more than 49 days from the current date.

**Note** If the scheduled time is in the past, an error message appears.

**Step 6** Click **OK** in the **Success** dialog box.

On successful completion of the stack switch process, the stack operation type column in the table gets updated to **Stack Switch Time Push Completed** state for the selected PAN ID.

**Note** We recommend that you wait until all the devices in the selected PAN get switched to Wi-SUN stack, as there is a possibility of some devices failing to switch in the scheduled time. However, the failed devices automatically switch to Wi-SUN stack mode after a one-day time period.

**Note** If you want to reschedule the stack time for some reason, then you have to cancel the current stack switch operation, push the stack mode again, and reinitiate the scheduling stack switch process.

## Cancelling Wi-SUN Stack Switch Operation

You can cancel the Wi-SUN stack switch operation only on successful completion of the previously configured or scheduled stack mode operation.

To cancel Wi-SUN stack switch operation:

**Step 1** Choose **CONFIG** > **Firmware Update**.

**Step 2** In the **Firmware Management** page, check the **PAN ID** check box for which you have completed either configuration or scheduling operation.

**Step 3** Click **Cancel StackMode**.

Based on the status of the stack mode cancellation process, the following states are displayed for the selected PAN ID in the **Stack Mode Switch** table.

*Table 69: PAN ID Status*

| Field | Description |
|---|---|
| Stack Operation Type Column | Displays the following states for the cancel stack mode operation:<br>• **Stack Mode Cancel Initiated** — Denotes the initiation of the stack mode cancellation process.<br>• **Stack Mode Cancel Push Completed** — Denotes the completion of the stack mode cancellation process. |
| Stack Operation Status Column | Displays the overall success and failure status of the devices for the selected PAN during the cancel operation. |

**Note** The **Devices** tab displays the status of the cancel stack mode operation at the device level. For more information, refer to Viewing Stack Mode Information for Devices, on page 286.

**Step 4** Click **Yes** to cancel the stack switch operation.

A **Success** dialog box appears to indicate the successful cancellation of the Wi-SUN stack switch operation.

# Viewing Stack Mode Information for Devices

From the **Devices** tab, you can view the stack mode status and stack mode time of each device for the following processes:

- Pushing Devices to Wi-SUN Stack Mode
- Scheduling Devices for Wi-SUN Stack Switch
- Canceling Wi-SUN Stack Switch Operation

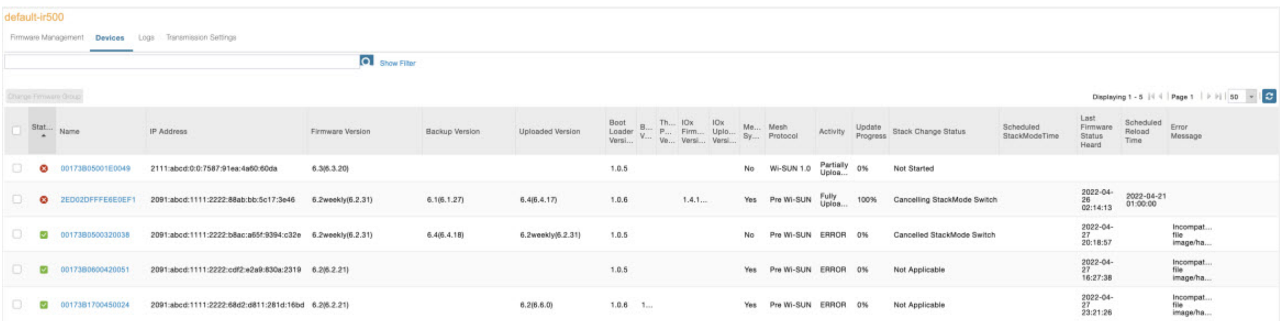
**Step 1** Choose **CONFIG** > **FIRMWARE UPDATE** > **Groups** tab.

**Step 2** Select the default or user-defined firmware group from the **ENDPOINT**.

**Step 3** Select the **PAN ID** from the Stack Mode Switch table.

**Step 4** Click the **Devices** tab.

The table displays stack mode configuration status and stack mode time at the device level.




The **Stack Change Status** column displays the following states:

***Table 70: Device State***

| Device State | Description |
|---|---|
| Not Started | Indicates the supported devices that are not initiated for Wi-SUN stack switch. |
| Not Applicable | Indicates the devices that are not supported for Wi-SUN stack switch. |
| Configuring StackMode | Indicates the devices that are pushed for stack mode operation. |
| Configured Stackmode | Indicates the devices that are successfully configured with stack mode. |
| Scheduling Stackmode time | Indicates the devices that are scheduled for stack mode switch. |
| Success | Indicates the devices that are successfully switched from CG-Mesh to Wi-SUN stack. |

| Device State | Description |
|---|---|
| Canceling stackmode switch | Indicates the devices that are scheduled for canceling stack mode switch. |
| Cancelled stackmode switch | Indicates the devices that are successfully cancelled from switching to Wi-SUN stack. |

**Filtering Options**

a) Click **Show Filter**. The page displays three drop-down lists.
b) Select the search option from the first drop-down list. For example, if you select Status from the first drop-down list, the available list of states appears in the third drop-down list.
c) Select the required option in the third drop-down list and click +.

   Your selection is displayed in the text box above the drop-down lists.

d) Click the search icon.

   The table displays information based on the search criteria set by you.

# Viewing Logs for Wi-SUN Stack Switch

To view logs for Wi-SUN stack switch:

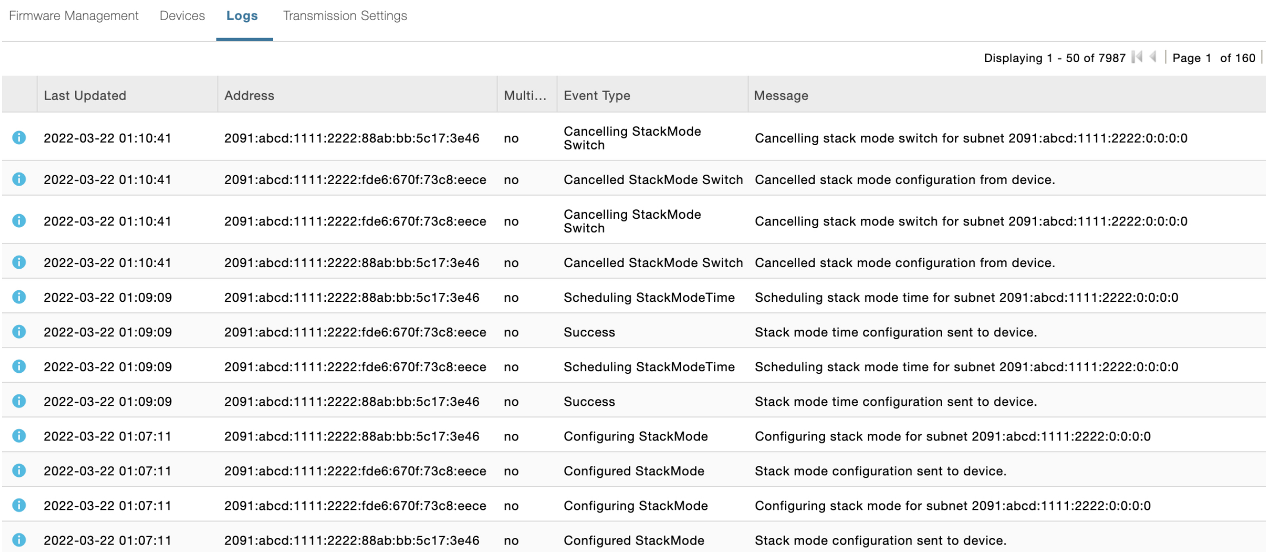
**Step 1** Choose **CONFIG** > **Firmware Update**.

**Step 2** Select the firmware group from the **ENDPOINT** in the left pane.

**Step 3** In the **Firmware Management** page, select the **PAN ID** for which you want to see the logs.

**Step 4** Click the **Logs** tab.

In the **Logs** page, you can view the events that are recorded for the selected PAN ID.





| | Last Updated | Address | Multi... | Event Type | Message |
|---|---|---|---|---|---|
| | 2022-03-22 01:10:41 | 2091:abcd:1111:2222:88ab:bb:5c17:3e46 | no | Cancelling StackMode Switch | Cancelling stack mode switch for subnet 2091:abcd:1111:2222:0:0:0:0 |
| | 2022-03-22 01:10:41 | 2091:abcd:1111:2222:fde6:670f:73c8:eece | no | Cancelled StackMode Switch | Cancelled stack mode configuration from device. |
| | 2022-03-22 01:10:41 | 2091:abcd:1111:2222:fde6:670f:73c8:eece | no | Cancelling StackMode Switch | Cancelling stack mode switch for subnet 2091:abcd:1111:2222:0:0:0:0 |
| | 2022-03-22 01:10:41 | 2091:abcd:1111:2222:88ab:bb:5c17:3e46 | no | Cancelled StackMode Switch | Cancelled stack mode configuration from device. |
| | 2022-03-22 01:09:09 | 2091:abcd:1111:2222:88ab:bb:5c17:3e46 | no | Scheduling StackModeTime | Scheduling stack mode time for subnet 2091:abcd:1111:2222:0:0:0:0 |
| | 2022-03-22 01:09:09 | 2091:abcd:1111:2222:fde6:670f:73c8:eece | no | Success | Stack mode time configuration sent to device. |
| | 2022-03-22 01:09:09 | 2091:abcd:1111:2222:fde6:670f:73c8:eece | no | Scheduling StackModeTime | Scheduling stack mode time for subnet 2091:abcd:1111:2222:0:0:0:0 |
| | 2022-03-22 01:09:09 | 2091:abcd:1111:2222:88ab:bb:5c17:3e46 | no | Success | Stack mode time configuration sent to device. |
| | 2022-03-22 01:07:11 | 2091:abcd:1111:2222:88ab:bb:5c17:3e46 | no | Configuring StackMode | Configuring stack mode for subnet 2091:abcd:1111:2222:0:0:0:0 |
| | 2022-03-22 01:07:11 | 2091:abcd:1111:2222:fde6:670f:73c8:eece | no | Configured StackMode | Stack mode configuration sent to device. |
| | 2022-03-22 01:07:11 | 2091:abcd:1111:2222:fde6:670f:73c8:eece | no | Configuring StackMode | Configuring stack mode for subnet 2091:abcd:1111:2222:0:0:0:0 |
| | 2022-03-22 01:07:11 | 2091:abcd:1111:2222:88ab:bb:5c17:3e46 | no | Configured StackMode | Stack mode configuration sent to device. |

# Viewing Audit Trail for Wi-SUN Stack Switch

To view audit trail for Wi-SUN stack switch :

**Step 1** Choose **ADMIN** > **System Management** > **Audit Trail**.

**Step 2** In the Audit Trail page, click the **Date/Time** drop-down arrow to filter the audit trail based on the date and time.

You can view the audit trail of the stack operations that were performed on the selected PAN ID.

| | | | | | | |
|---|---|---|---|---|---|---|
| 2022-02-24 11:34:59 | root | root | 10.65.78.18 | Stack Mode Push | Initiated | Stack Mode Push Operation , Device Category: endpoint, For PANID ['7'] |
| 2022-02-24 11:26:12 | root | root | 10.65.78.18 | Cancel Stack | Initiated | Cancel stack mode push operation , Device Category: endpoint, For PANID ['7'] |
| 2022-02-24 11:22:25 | root | root | 10.65.78.18 | Scheduled Stack Switch Time | Initiated | Stack switch time push operation , Device Category: endpoint, for PANID ['7'] |
| 2022-02-24 11:18:28 | root | root | 10.65.78.18 | Cancel Stack | Initiated | Cancel stack mode push operation , Device Category: endpoint, For PANID ['7'] |
| 2022-02-24 10:49:04 | root | root | 10.65.78.18 | Stack Mode Push | Initiated | Stack Mode Push Operation , Device Category: endpoint, For PANID ['12'] |

CHAPTER 7

# Managing Tunnel Provisioning

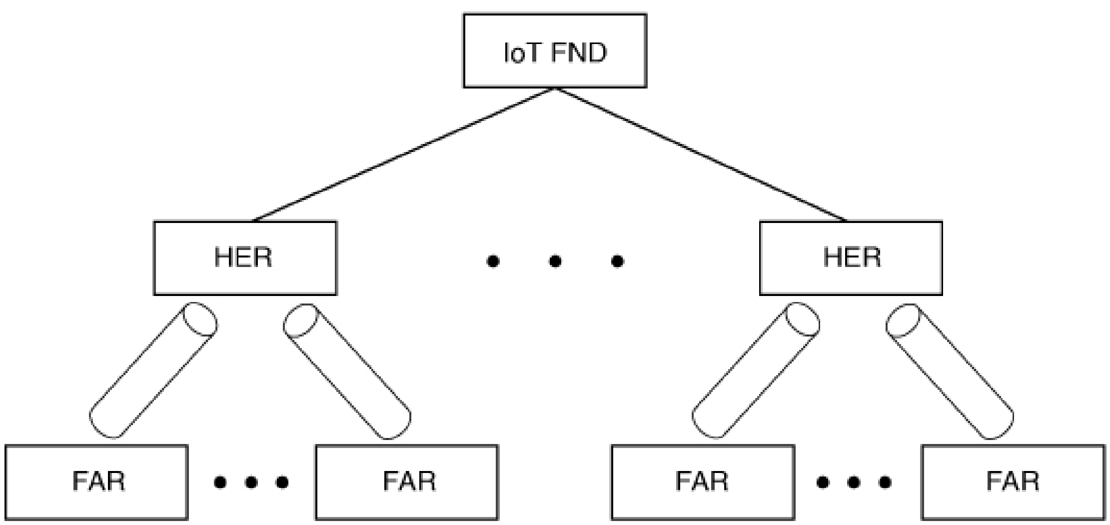
This section describes how to configure IoT FND for tunnel provisioning and how to manage and monitor tunnels connecting FARs (CGRs and C800s) and HERs.



# Overview

IoT FND sends the commands generated from processing the tunnel provisioning templates to FARs and HERs to provision secure tunnels between them. The default IoT FND templates contain CLI commands to set up and configure GRE and IPsec tunnels. One HER can serve up to 500 FARs, which may include multiple tunnels with the same HER EID and name.

***Figure 32: Tunnels Connect FARs and their Corresponding HERs***



To provision tunnels between HERs and FARs, IoT FND executes CLI tunnel configuration commands on these devices. By default, IoT FND provides basic tunnel configuration templates containing the CLI tunnel configuration commands. You can also use your own templates. Although the tunnel provisioning process is automatic, you must first complete the configuration steps outlined in Tunnel Provisioning Configuration Process. After that, whenever a FAR comes online, IoT FND automatically provisions it with a tunnel. Before you configure IoT FND for tunnel provisioning, ensure that the IoT FND TPS Proxy is installed and running.

# ZTD without IPSec

Beginning with IoT FND Release 3.1.x, you have the option to initiate ZTD with no IPSec configured by ensuring that the Tunnel Provisioning Template is empty of any CLI. This initial approach of bringing up your network without a factory configuration does not preclude subsequent use of IPSec in your network

# Tunnel Provisioning Configuration Process

To configure IoT FND for tunnel provisioning:

| | | |
|---|---|---|
| 1 | Configure the DHCP servers.<br><br>Configure DHCP servers to provide unique IP addresses to IoT FND. The default IoT FND tunnel provisioning templates configure a loopback interface and the IP addresses required to create the tunnels.<br><br>Cisco IOS CGRs/FARs use FlexVPN. Ensures that the template only contains addresses for the loopback interface. | Configuring the DHCP Server for Tunnel Provisioning, on page 293<br><br>**Note** In IoT FND 4.6.1 release and greater you can use the “Tunnel Provisioning Optimization” feature that allows the following:<br><br>When using a FlexVPN/DMVPN for a FAR, a new property ‘optimizeTunnelProv=true’ is used to tell FND to avoid HER configuration during the Tunnel Provisioning of the device (router). This property is uploaded for each router using the CSV file. |
| 2 | Configure the tunnel settings.<br><br>Configure the NMS URL and the DHCP proxy client settings on the Provisioning Settings page in IoT FND (**ADMIN** > **System Management** > **Provisioning Settings**). | See the Configuring Provisioning Settings in Managing System Settings chapter. |
| 3 | Cisco IOS CGRs use the CGNA service | See Managing Devices chapter. |
| 4 | Configure HER management.<br><br>Configure HERs to allow management by IoT FND using NETCONF over SSH. | Configuring HERs before adding them to IoT FND. |

| | | |
|---|---|---|
| 5 | Add HERs to IoT FND. | Adding HERs to IoT FND.<br><br>See Adding HERs to IoT FND in Managing Devices chapter. |
| 6 | Review the IoT FND tunnel provisioning templates to ensure that they create the correct type of tunnel. | See Configuring Tunnel Provisioning Templates in Managing Tunnel Provisioning chapter. |
| 7 | (Optional) If you plan to use your own templates for tunnel provisioning, create one or more tunnel provisioning groups and modify the default tunnel provisioning templates. | Configuring Tunnel Provisioning Templates, on page 300 |
| 8 | Configure FARs to contact IoT FND over HTTPS through the IoT FND TPS proxy. | This step is typically performed at the factory where the FARs are configured to contact the TPS Proxy. |
| 9 | Add FARs to IoT FND.<br><br>Import the FARs into IoT FND using the Notice-of-Shipment XML file. | See Adding Routers to IoT FND in the Managing Devices chapter. |
| 10 | Map FARs to their corresponding HER. | Tunnel Provisioning Configuration Process, on page 290 |

After completing the previous steps, deploy the FARs and power them on. Tunnel provisioning happens automatically.

This is the sequence of events after a FAR is turned on:

### Before you begin

You must generate the keystore files on the IoT FND and TPS Proxy before configuring tunnel provisioning. Then, you configure IoT FND and the TPS Proxy to talk to one another (refer to Setting Up TPS Proxy, Configuring IoT FND to Use the TPS Proxy, and Starting the IoT FND TPS Proxy). Use the `systemctl` command for TPS proxy if the OS version is RHEL 8.x or greater.

| RHEL Version | Command |
|---|---|
| 8.x | `systemctl <start/stop/status/restart> tpsproxy` |
| 7.x | `service tpsproxy <start/stop/status/restart>` |

**Step 1** Upon joining the uplink network after being turned on, the FAR sends a request for certificate enrollment.

**Step 2** The FAR then requests tunnel provisioning to IoT FND through the IoT FND TPS Proxy.

**Step 3** IoT FND looks up the FAR record in the IoT FND database and determines which tunnel provisioning templates to use. IoT FND also looks up which HERs to which to establish a tunnel.

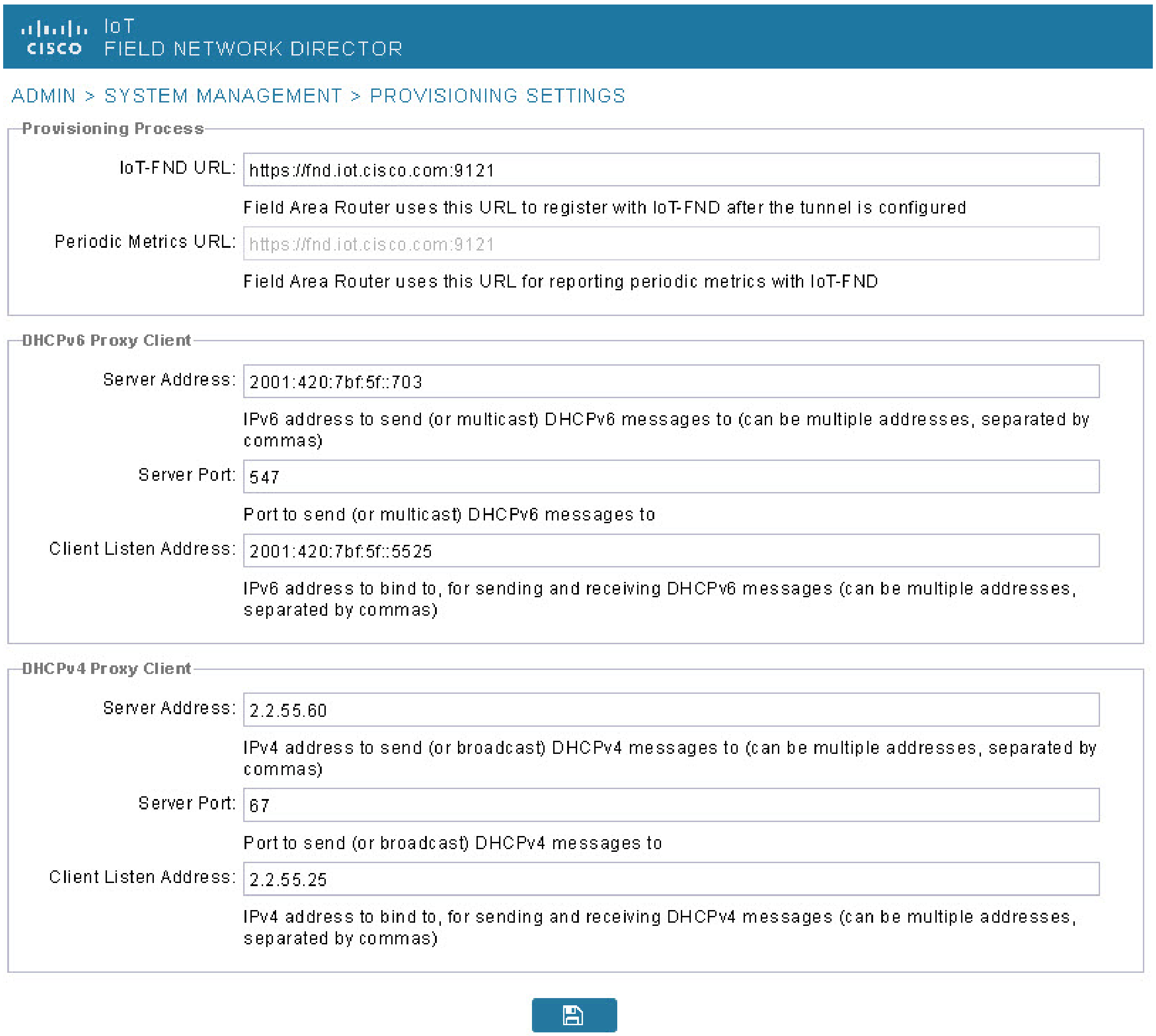
**Step 4** For Cisco IOS CGRs, the default templates configure the CGR to use FlexVPN. The FlexVPN client is configured on the CGR that will contact the HER and ask for a FlexVPN tunnel to be dynamically constructed. This is how the HER dynamically adds a new tunnel endpoint interface for the CGR.

**Step 5** Before processing FAR templates, IoT FND processes the HER Tunnel Deletion template and sends the resulting commands to the HERs. This is done for each HER to remove existing tunnel configuration that may be associated with the FAR.

**Step 6** IoT FND uses the FreeMarker template engine to process the FAR Tunnel Addition template. The engine converts the templates to text, which IoT FND assumes to be CLI configuration commands (Cisco IOS per the CGR). IoT FND uses these commands to configure and bring up one end of the tunnel on the FAR.

**Step 7** IoT FND uses the FreeMarker template engine to process the HER Tunnel Addition template. The engine converts the templates to text, which IoT FND assumes to be commands for configuring the tunnel on the HERs.

**Step 8** For Cisco IOS CGRs, if no errors occurred applying the commands generated by the templates to the FAR and HERs, IoT FND configures a new active CGNA profile “cg-nms-register,” and deactivates the cg-nms-tunnel profile. That cg-nms-register profile uses the IoT FND URL.



The specified URL uses the IoT FND registration port (default 9121) instead of the tunnel provisioning port. The Fully Qualified Domain Name (FQDN) in that URL is different and resolves to an IP address that is only reachable through the tunnels.

# Configuring Tunnel Provisioning

This section describes how to configure IoT FND for tunnel provisioning.

## Configuring the DHCP Server for Tunnel Provisioning

For tunnel provisioning to succeed, configure the DHCP server used by IoT FND to supply addresses to create tunnels between the FARs and HERs. For example, configure the DHCP server to provide IP addresses for tunnel provisioning on a permanent-lease basis.

IoT FND makes the DHCP requests based on the settings defined in the tunnel provisioning templates. During tunnel provisioning, the IoT FND templates can make two kinds of DHCP requests:

- Request an IP address, and then make it available to the template.
- Request a subnet with two IP addresses, and then make both addresses available to the template.

IoT FND can make these requests for IPv4 addresses and IPv6 addresses.

The ability to request DHCP addresses from the template gives you maximum flexibility when defining tunnel configurations because you allocate the exact address needed for each FAR and corresponding interface on the HER. The default tunnel provisioning templates provided address the most common use case: one IPsec tunnel between the FAR and its corresponding HER. Each end of this IPsec tunnel gets a dynamically allocated IPv4 address:

- If your DHCP server supports subnet allocation, use it to obtain two addresses that belong to the same subnet.
- If your DHCP server only supports address allocation, configure it so that the two DHCP address requests return addresses that can be used as ends of an IPsec tunnel.
- If your routing plan calls for allocating unique IPv4 addresses for each FAR and assigning it to a loopback interface above the IPsec tunnel, allocate this address using the IoT FND template.

If you choose to build IPv6 GRE tunnels, allocate the IPv6 addresses for each end of the tunnel using DHCP prefix delegation or individual address requests.

This section describes example DHCP settings for tunnel provisioning. How you configure these settings depends on your installation. This section provides general guidelines for configuring the DHCP server for tunnel provisioning using the Cisco Network Registrar (CNR).

## Configuring DHCP for Tunnel Provisioning Using CNR

The CNR CLI script in the following example configures the CNR DHCP server to service requests made by the default tunnel provisioning templates in IoT FND. When using this script, ensure that the subnets are appropriate for your DHCP server environment.

### Example CNR DHCP Server Tunnel Provisioning Script

```
# These commented out commands support re-applying the configuration by first
# removing any previously applied configuration, in reverse order. This should
# not be done in a production environment, but may be useful when initially
# developing and testing a configuration.

# scope v4address-perm delete
# dhcp-address-block v4subnet-perm delete
# prefix v6subnet-perm delete
# prefix v6address-perm delete
# policy permanent delete

# Configure the server to automatically map any IPv4 or IPv6 user class
# option values to selection tags. By default CG-NMS includes a value of
# "CG-NMS" for the user class in its requests. The tag is used to insure
# prefixes and scopes configured to satisfy requests from CG-NMS are only
# used for that purpose.

dhcp set map-user-class-id=append-to-tags

# Since CG-NMS uses the leased addresses and subnets in router
# configuration the addresses and subnets must be permanently allocated
# for that purpose. Create a policy that instructs the DHCP server to
# offer a permanent lease.

policy permanent create
policy permanent set permanent-leases=enabled

# Configure DHCPv6.

# The default CG-NMS tunnel template will request IPv6 addresses for
# use with CGR loopback interfaces.

prefix v6address-perm create 2001:DB8:0:0:1::/80 dhcp-type=dhcp
prefix v6address-perm set description="Pool for leasing addresses for loopback
interfaces."
prefix v6address-perm set policy=permanent
prefix v6address-perm set selection-tags=CG-NMS

# The default CG-NMS tunnel template will request IPv6 prefixes for
# use with GRE tunnels. Force use of a /127 prefix.

prefix v6subnet-perm create 2001:DB8:0:0:2::/80 dhcp-type=prefix-delegation
prefix v6subnet-perm set description="Pool for leasing prefixes for GRE tunnels."
prefix v6subnet-perm set policy=permanent
prefix v6subnet-perm set selection-tags=CG-NMS
prefix-policy v6subnet-perm set default-prefix-length=127
prefix-policy v6subnet-perm set shortest-prefix-length=127

# Configure DHCPv4.

# The default CG-NMS tunnel template will request IPv4 subnets for
# use with IPsec tunnels. Note that currently address pools for
# IPv4 subnet allocation can only be configured using the CLI as the
# CNR Web UI does not currently support them.

# If CNR allowed you to set a description on DHCP address blocks it would be:
# "Pool for leasing subnets for IPsec tunnels."

dhcp-address-block v4subnet-perm create 192.0.2.0/24
dhcp-address-block v4subnet-perm set default-subnet-size=31
dhcp-address-block v4subnet-perm set policy=permanent
dhcp-address-block v4subnet-perm set selection-tags=CG-NMS
```

```
# The default CG-NMS tunnel template will request IPv4 addresses for
# use with loopback interfaces.

scope v4address-perm create 198.51.100.0 255.255.255.0
scope v4address-perm set description="Pool for leasing addresses for
loopback interfaces."
scope v4address-perm set policy=permanent
scope v4address-perm addRange 198.51.100.2 198.51.100.254
scope v4address-perm set selection-tag-list=CG-NMS

# Configure detailed logging of incoming and outgoing packets. This is useful when
# debugging issues involving DHCP, however this level of logging will lower the
# performance of the DHCP server. If this is a production server under heavy load
# it may be necessary to forgo detailed packet logging.

dhcp set log-settings=missing-options,incoming-packet-detail,
outgoing-packet-detail,unknown-criteria,client-detail,
client-criteria-processing,dropped-waiting-packets,v6-lease-detail

# Save the changes and reload the server to have them take effect.
save
dhcp reload

# List the current configuration.

policy list
prefix list
dhcp-address-block list
scope list
dhcp show
```

# Configuring Tunnel Group Settings

You use groups in IoT FND to bulk configure tunnel provisioning. By default, all FARs are added to the appropriate default group (default-cgr, default-c800). Default groups contain the templates used for tunnel provisioning.

## Creating Tunnel Groups

If you plan to use one set of templates for all FARs, whether using the default templates, modified default templates or custom templates, do not create additional groups. To define multiple sets of templates, create groups and customize the templates for these groups.

**Note** CGRs and C800s can be in the same tunnel provisioning group if your custom templates are applicable to both router types.

To create a tunnel group:

**Step 1** Choose **CONFIG** > **Tunnel Provisioning**.

**Step 2** Click + icon in left pane to add a group.

**Step 3** Enter a name of the new group, and then click **OK**.

The group appears in the Tunnel Groups pane.

After creating a tunnel group, the next step is to move FARs from other groups to it, as described in Moving FARs to Another Group, on page 298.

## Deleting Tunnel Groups

Only empty groups can be deleted. Before you can delete a tunnel group, you must move the devices it contains to another group.

To delete an empty tunnel group:

**Step 1** Choose **CONFIG** > **Tunnel Provisioning**.

**Step 2** In the TUNNEL GROUPS left pane, select the tunnel group to delete.

**Step 3** Click (-) to delete the group.

**Step 4** Click **Yes** to confirm deletion.

## Viewing Tunnel Groups

The Tunnel Provisioning page lists information about existing tunnel groups.

Follow these steps to view the tunnel groups defined in IoT FND:

**Step 1** Choose **CONFIG** > **Tunnel Provisioning**.

**Step 2** Click **Group Members** tab.

**Step 3** In the TUNNEL GROUPS pane (left), select a group.

IoT FND displays the following Tunnel Group information for each router in the group. Not all routers support all fields.

***Table 71: Tunnel Group Fields***

| Field | Description |
|---|---|
| Name | Router EID (device identifier). |
| Status | Status of the router:<br>• Unheard—The router has not contacted IoT FND yet.<br>• Unsupported—The router is not supported by IoT FND.<br>• Up—The router is in operation.<br>• Down—The router is turned off. |
| Last Heard | Last time the router contacted or sent metrics to IoT FND. If the router never contacted IoT FND, **never** appears in this field. Otherwise, IoT FND displays the date and time of the last contact, for example,**4/10 19:06**. |

| | |
|---|---|
| Tunnel Source Interface 1Tunnel Source Interface 2 | Router interface used by the tunnel. |
| OSPF Area 1<br>OSPF Area 2 | Open shortest path first (OSPF) areas 1 and 2. |
| OSPFv3 Area 1<br>OSPFv3 Area 1 | OSPFv3 area 1<br>OSPFv3 area 2. |
| IPsec Dest Addr 1<br>IPsec Dest Addr 2 | IPv4 destination address of the tunnel. |
| GRE Tunnel Dest Addr 1<br>GRE Tunnel Dest Addr 2 | IPv6 destination address of the tunnel. |
| Certificate Issuer Common Name | Name of the CA that issued the certificate. |

## Renaming a Tunnel Group

In the Tunnel Provisioning page, there are two tunnel provisioning groups available, namely user-created group and default group. IoT FND allows you to rename the user-created Tunnel Provisioning Groups only. You cannot rename the default Tunnel Provisioning Groups.

**Note** You can rename the user-created tunnel group at any time. Cisco recommends using short, meaningful names. Names cannot be more than 250 characters long.

To rename a tunnel group:

**Step 1** Choose **CONFIG** > **Tunnel Provisioning**.

**Step 2** In the TUNNEL GROUPS pane, mouse over the tunnel group to rename and click the **Edit** pencil icon.

**Note** The pencil icon does not appear for Default Tunnel Provisioning groups.

**Step 3** Enter the new Group Name and then click **OK**.

### What to do next

**Note** When you enter an invalid character entry (such as, @, #, !, or +) in the entry field, the field is highlighted in red and disables the **OK** button.

## Moving FARs to Another Group

You can move FARs to another group either in bulk or manually.

### *Moving FARs to Another Group Manually*

To move FARs to another group manually:

**Step 1** Choose **CONFIG** > **Tunnel Provisioning**.

**Step 2** Click the **Group Members** tab.

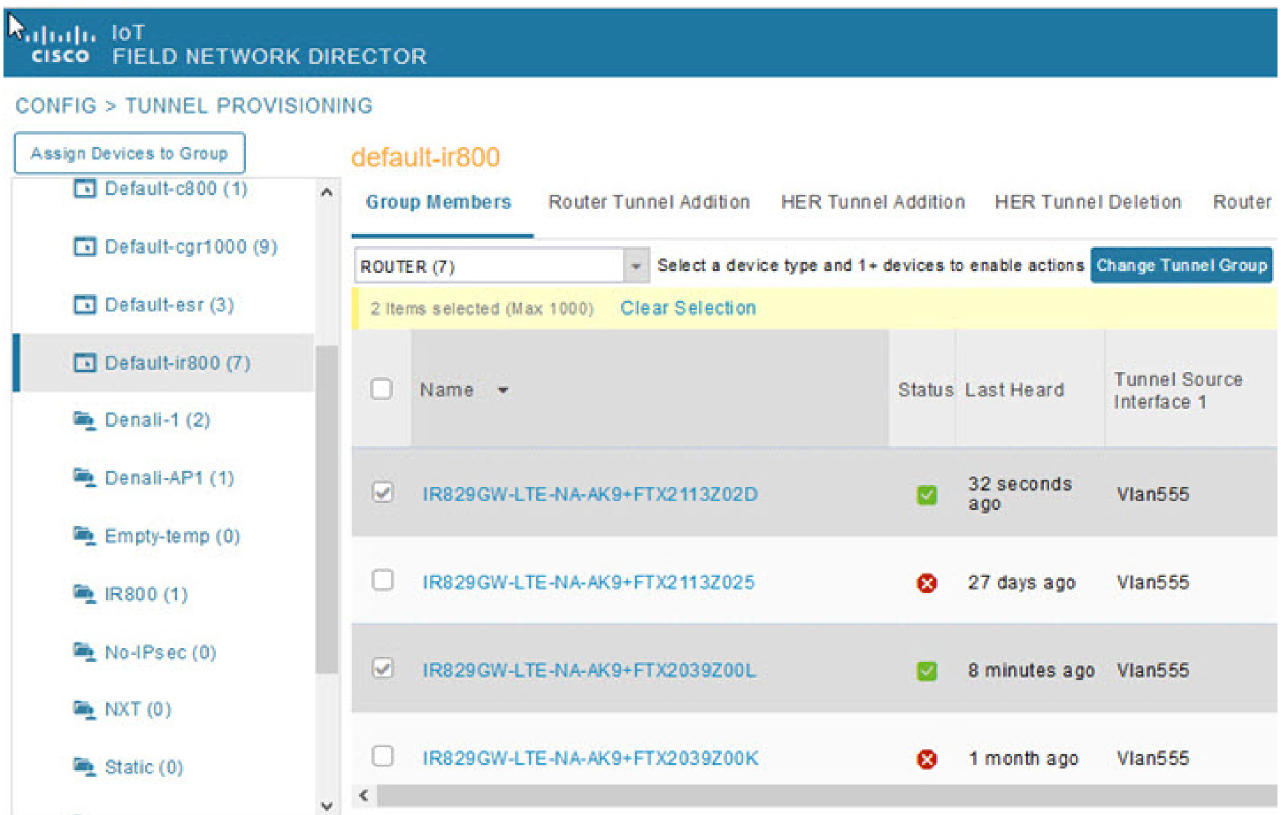
**Step 3** In the TUNNEL GROUPS pane, select the tunnel group with the routers to move.

**Step 4** Choose the device type from the **Select a device type** drop-down menu.

**Step 5** Check the check boxes of the FARs to move.

To select all FARs in a group, click the check box at the top of the column. When you select devices, a yellow bar displays that maintains a count of selected devices and has the Clear Selection and Select All commands. The maximum number of devices you can select is 1000.

**Step 6** Click the **Change Tunnel Group** button.




**Step 7** From the drop-down menu, choose the tunnel group to which you want to move the FARs.

**Step 8** Click **Change Tunnel Group**.

**Step 9** Click **OK** to close the dialog box.

### *Moving FARs to Another Group in Bulk*

You can move FARs in bulk to another group by importing a CSV or XML file containing the names of the FARs to move. Ensure that the file contains entries in the format shown the following example:

```
eid
CGR1120/k9+JSM1
CGR1120/k9+JSM2
CGR1120/k9+JSM3
CGR1120/k9+JSM4
C819HGW-S-A-K9+FTX174685V0
```

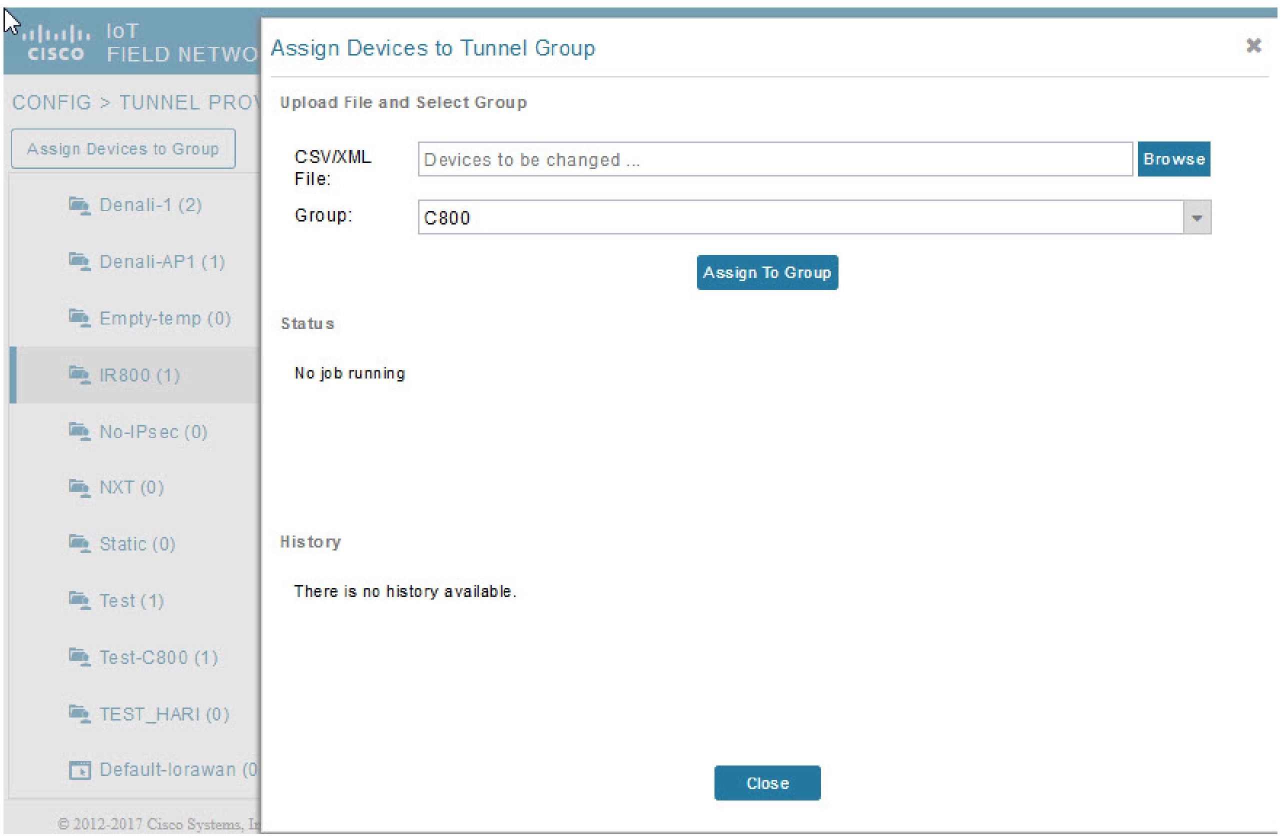
The first line is the header, which tells IoT FND to expect FAR EIDs in the remaining lines (one FAR EID per line).

To move FARs to another group in bulk:

**Step 1** Create a CSV or XML file with the EIDs of the devices to move to a different group.

**Step 2** Choose **CONFIG** > **Tunnel Provisioning**

**Step 3** Click **Assign Devices to Tunnel Group** to open an entry panel.




**Step 4** Click **Browse** and locate the file that contains the FARs that you want to move.

**Step 5** From the **Group** drop-down menu, choose the destination tunnel group.

**Step 6** Click **Assign To Group**.

**Step 7** Click **Close**.

# Configuring Tunnel Provisioning Templates

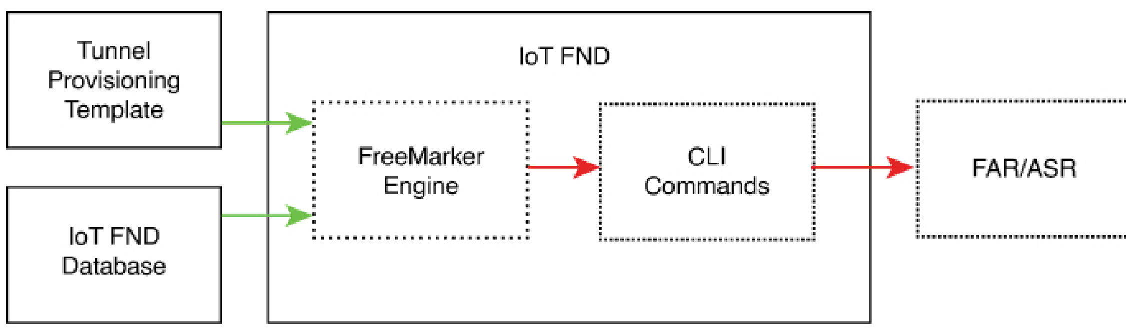
IoT FND has three default tunnel provisioning templates:

- Field Area Router Tunnel Addition—IoT FND uses this template to generate the CLI configuration commands for creating one end of an IPsec tunnel on the FAR.
- Head-End Router Tunnel Addition—IoT FND uses this template to generate the CLI configuration commands for creating the other end of the IPsec tunnel on the HER.
- Head-End Router Tunnel Deletion—IoT FND uses this template to generate the CLI configuration commands for deleting any existing tunnel to the FAR at the other end of the tunnel.

## Tunnel Provisioning Template Syntax

The IoT FND tunnel provisioning templates are expressed with the FreeMarker syntax. FreeMarker is an open-source Java-based engine for processing templates and is built into IoT FND. As shown in CLI Command Generation from Templates in IoT FND, FreeMarker takes as input the tunnel provisioning template and data supplied by IoT FND, and generates CLI commands that IoT FND runs on the FARs and HERs in the “configure terminal” context.

*Figure 33: CLI Command Generation from Templates in IoT FND*




In IoT FND, the tunnel provisioning templates consist of router CLI commands and FreeMarker variables and directives. The use of FreeMarker syntax allows IoT FND to define one template to provision multiple routers.

This section describes the basic FreeMarker syntax in the tunnel provisioning templates. For information about FreeMarker visit http://freemarker.sourceforge.net/.

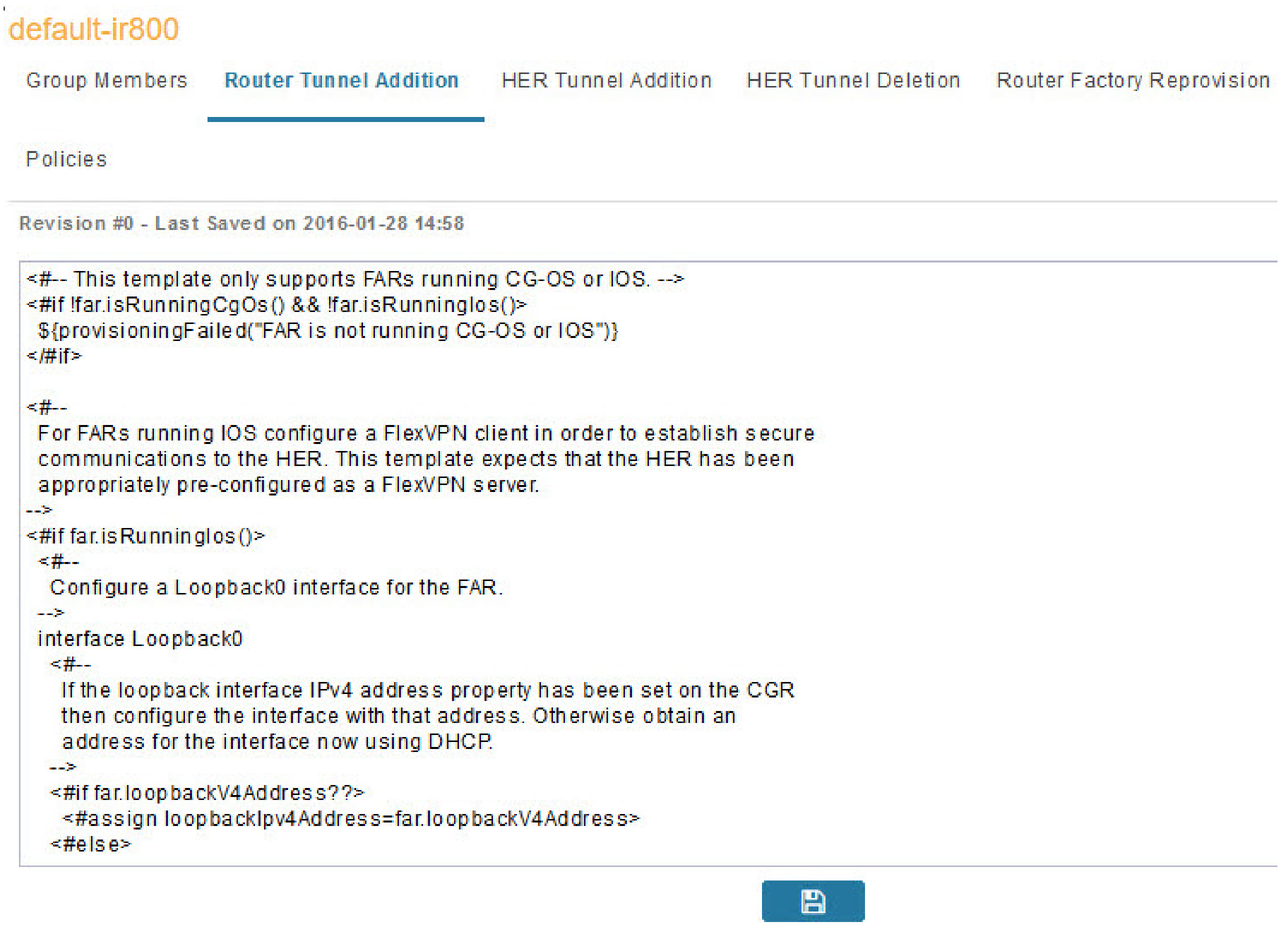
## Configuring the Field Area Router Tunnel Addition Template

To edit the FAR Tunnel Addition template to provide one end of an IPsec tunnel on FARs in the group:

**Step 1** Choose **CONFIG** > **Tunnel Provisioning**.

**Step 2** In the **TUNNEL GROUPS** pane, select the tunnel group with the template to edit.

**Step 3** Click the **Router Tunnel Addition** tab.




**Step 4** Modify the default template.

**Tip** Use a text editor to modify templates and copy the text into the template field in IoT FND.

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

**Step 6** Click **OK** to confirm the changes.

See also, Tunnel Provisioning Template Syntax, on page 300.

## Configuring the Head-End Router Tunnel Addition Template

**Note** To ensure that both endpoints are in a matching subnet, this template must use the same Identity Association Identifier (IAID) as the FAR template.

To edit the HER Tunnel Addition template to create the other end of the IPsec tunnel on HERs in the group:

**Step 1** Choose **CONFIG** > **Tunnel Provisioning**.

**Step 2** In the TUNNEL GROUPS pane, select a tunnel group.

**Step 3** Click the **HER Tunnel Addition** tab.

**Step 4** Modify the default HER addition template.

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

**Step 6** Click **OK** to confirm the changes.

### Configuring the HER Tunnel Deletion Template

To edit the HER tunnel deletion template to delete existing tunnels to FARs at the other end of the tunnel:

**Step 1** Choose **CONFIG** > **Tunnel Provisioning**.

**Step 2** In the TUNNEL GROUPS pane, select the tunnel group whose template to edit.

**Step 3** Click the **HER Tunnel Deletion** tab.

**Step 4** Modify the default HER deletion template.

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

**Step 6** Click **OK** to confirm the changes.

# Configuring FND for IXM

Cisco IoT FND supports the following configurations for the Cisco Wireless Gateway for LoRaWAN:

- Firmware upgrade
- Hardware monitoring and events reporting
- IP networking configuration and operations (for example, IP address and IPsec)
- Zero Touch provisioning that includes either installing Thingpark LRR software or configuring Common Packet Forwarder (CPF)

## PNP Support for IXM

By default, PNP (Plug and Play) automatic discovery mode for Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS) and Cisco Connection Online (CCO) is enabled. When using DHCP server with option 43, for example, on boot-up, the IXM device gets the IP address from the DHCP server. The device gets the PNP Server IP address (TPS or FND IP) through option 43. The PNP request is sent to IoT FND. IoT FND applies the config to the running config and configures the startup config by executing the **copy running-config startup-config** command. IoT FND terminates the PNP profile when IoT FND pushes the configuration to IXM.

For CCO redirection, associate the root certificate with the PNP profile. For this, export the FND root certificate using the below command under **/opt/cgms/server/cgms/conf**.

**keytool -export -alias root -file mydomain.der -keystore cgms_keystore && openssl x509 -inform der -in mydomain.der -out certificate_root.pem**

Upload the root certificate in the PNP redirection page or along PNP profile.

**Step 1** Set the following property in cgms.properties to true in order to trust the (IXM) server.

trust-ixm-server-cert=true //Default value is false

**Step 2** Restart FND service.

**Note** To clean the startup config and trigger PNP, enter the following command.

```
archive download-sw firmware /factory /
force-reload <image file path>
```

# Gateway Bootstrap Configuration Template

In the **Config** > **Tunnel Provisioning** page, choose Default-Lorawan. In the Gateway Bootstrap Configuration tab, enter the commands to LoRaWAN before triggering PnP on the device.

The sample config is given below.

```
hostname <hostname>
!crypto ipsec profile primary
   ipaddr <ipaddr> iketime 86000 keytime 86000 aes 256
  subnet <subnet> ip>/24
  exit
ip domain lookup
ip domain name cisco.com
ip host fnd.iot.cisco.com <fnd ip address>
!
interface Fast Ethernet 0/1
  ipaddress dhcp
  exit
!
ip default-gateway <default gateway ip>
!
username <username> password <password>
!
ip ssh authenticaton-retires 3
radio off
ip ssh admin-access
ip ssh port 22
!
ntp server ip <ntp server ip>
ipsec isakmp admin <password> group 19 <password>
ipsec enable
!
igma secure enable
!
igms event destination <FND IP> 5683
!
igma profile iot-fnd-register
  active
  add-command show fpga
  add-command show inventory
  add-command show ip interface FastEthernet 0/1
  add-command show ipsec status info
  add-command show platform status
```

```
  add-command show radio
  add-command show version
  interval 2
  url https://fnd.iot.cisco.com:9121/igma/register
  exit
!
igma local-trustpoint sudi
```

# Preparing IoT FND for IXM Zero Touch Deployment

Follow these steps to prepare IoT FND for IXM Zero Touch Deployment (ZTD)

- Using Thingpark LRR Software
- Enabling CPF (Common Packet Forwarder)

**Note** To enable CPF, set enable-cpf=true flag in cgms.properties file.

**Step 1** If you are using Pre-Shared Key (PSK) authentication for tunneling, add the **userPropertyTypes.xml** file to the IoT FND server under `/opt/cgms/server/cgms/conf`.

**Step 2** Restart the IoT FND service after adding the following.

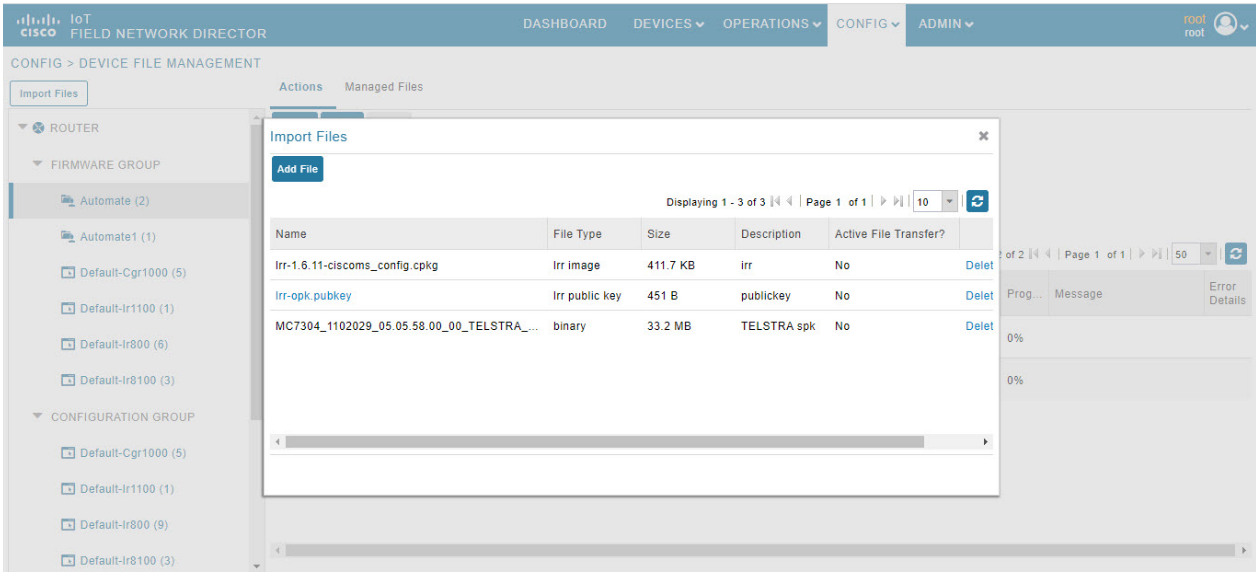
**Note** If you are using Rivest-Shamir-Adleman (RSA), ignore this step.

The userPropertyTypes.xml is shown below.

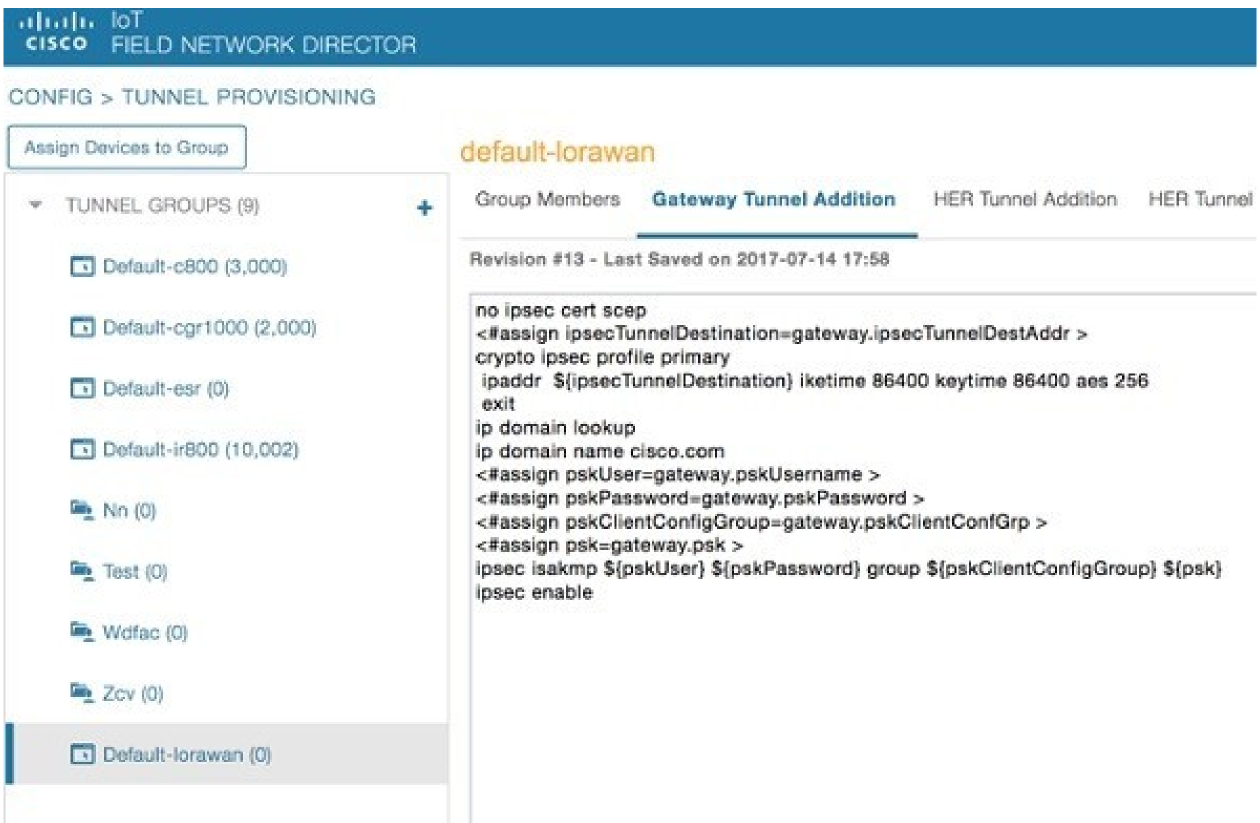
```xml
<?xml version="1.0" encoding="UTF-8"?>
<cgms xmlns="http://www.w3schools.com"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://www.w3schools.com propertyTypes.xsd">
  <propertyTypes kind="lorawan">
  <!--Psk Properties -->
   <propertyType>
      <name>pskUsername</name>
      <displayName>XAUTH Username</displayName>
      <description>Username for PSK IPsec XAUTH</description>
   </propertyType>
   <propertyType>
      <name>pskPassword</name>
      <issecure>1</issecure>
      <displayName>XAUTH Password</displayName>
      <description>Password for PSK IPsec XAUTH</description>
   </propertyType>
   <propertyType>
      <name>pskClientConfGrp</name>
      <displayName>PSK Client Configuration Group</displayName>
      <description>PSK Client Configuration Group</description>
   </propertyType>
   <propertyType>
      <name>psk</name>
      <issecure>1</issecure>
      <displayName>Pre Shared Key</displayName>
      <description>Pre Shared Key</description>
   </propertyType>
  </propertyTypes>
</cgms>
```

**Step 3** In the **Config** > **Device File Management** page, click **Import Files**.

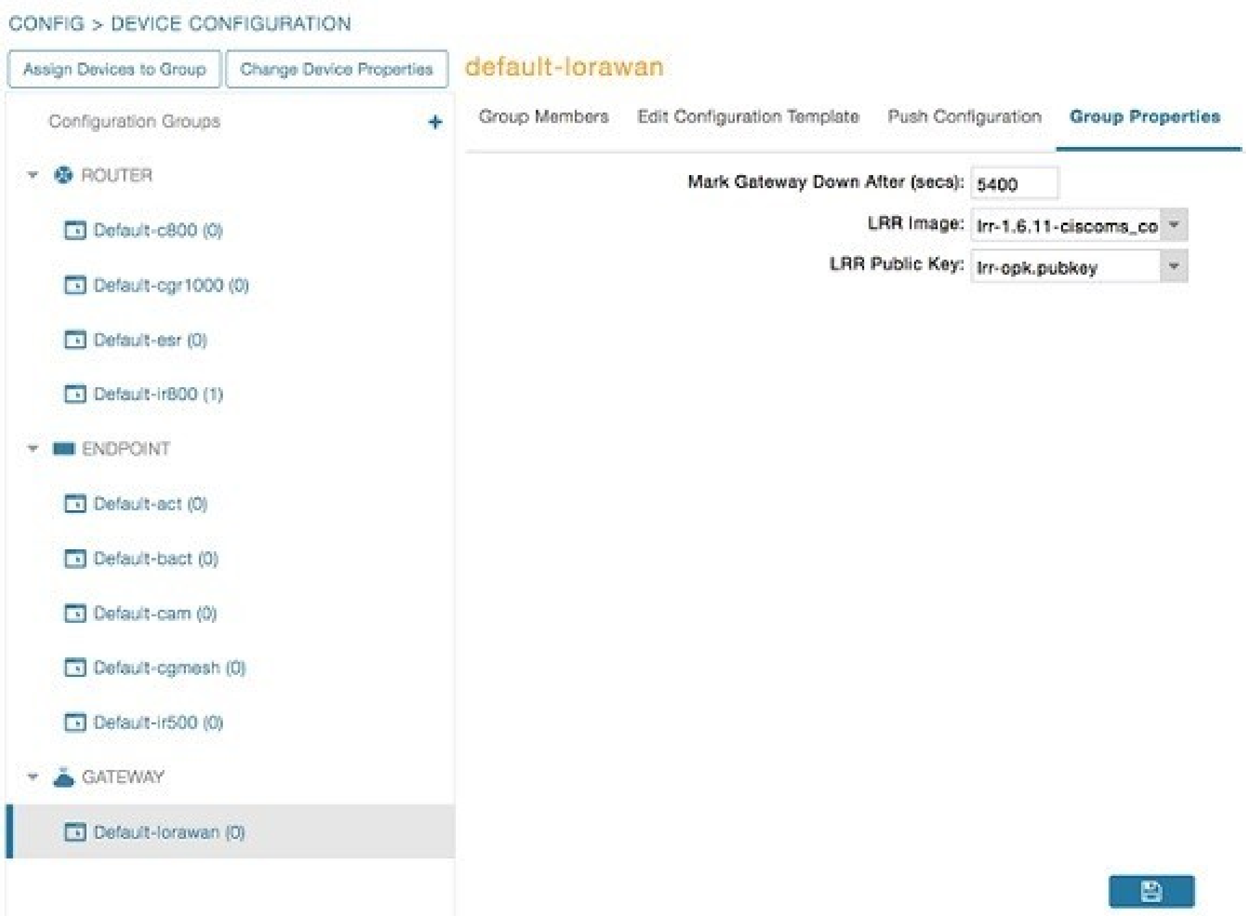
**Step 4** Click **Add File** to add the Actility LRR and public key to IoT FND.



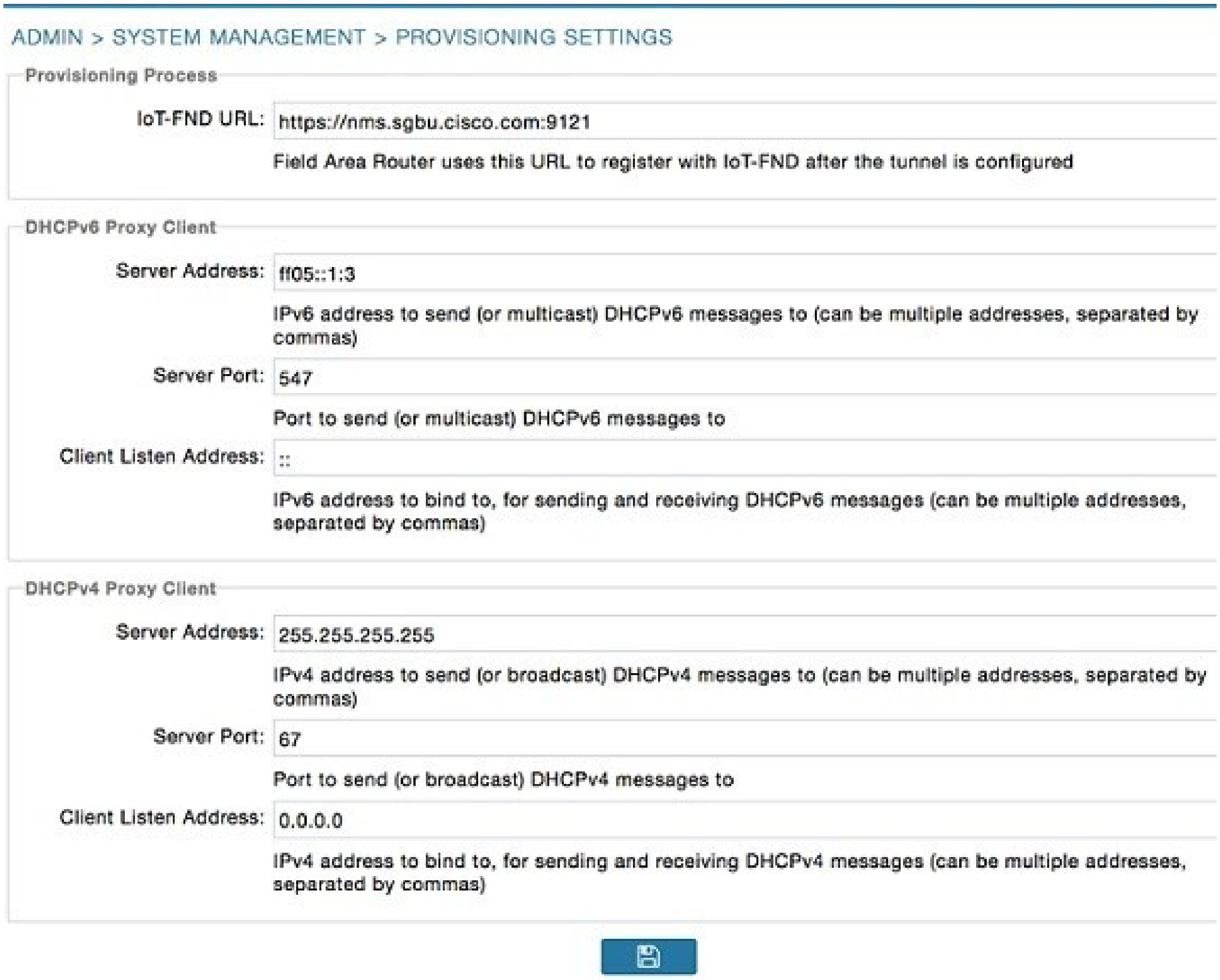

**Step 5** In the **Config** > **Tunnel Provisioning** page, update the tunnel configuration group with the following parameters in the Gateway Tunnel Addition tab and click **Save**.




**Step 6** In **Config** > **Device Configuration** page, click the Group Properties tab. Update the device configuration group properties with the following parameters for Default–lorawan and click **Save**.




**Step 7** Go to **Admin** > **System Management** > **Provisioning Settings** page. The common name is populated in IoT-FND URL field.




**Step 8** Make sure you have obtained certificates from the Certificate Authority (CA). Execute the **show ipsec certs** command to verify that the LDevID certs are enrolled by the device. Make sure the firewall allows ports 9120, 9121, 9122, and all the SSH, telnet, and DHCP ports. Make sure the TPS name is pingable and execute the **copy running express-setup-config** command.

```
Hostname IXM
!
ip domain lookup
ip domain name cisco.com
!
ip name-server 55.55.0.15
!
interface FastEthernet 0/1 description interface
ip address 4.4.4.2 255.255.255.0 exit
!
ip default-gateway 4.4.4.1
!
ntp server ip 55.55.0.1
!
clock timezone America/Los_Angeles
!
igma profile iot-fnd-tunnel
```

```
active
add-command show fpga interval 5
url https://ps.sgbu.cisco.com:9120/igma/tunnel exit

ipsec cert scep https://55.55.0.15/csertsrv/msecp.dll us ca mil
cisco iot test true ndes true 2048
```

**Note** You need to add the HER configuration manually, for example, the tunnel crypto profiles and transform sets. The following is a sample template, where VPN uses PSK as authentication.

```
username cisco password 0 cisco

crypto isakmp policy 1
    encr aes 256
    hash sha256
    authentication pre-share
    group 19
crypto isakmp keepalive 10
!
crypto isakmp client configuration group 19
    key cisco
    domain cisco.com
    pool POOL
    acl split
    save-password
    netmask 255.255.255.128
crypto isakmp profile test
    match identity group 19
    client authentication list AUTH
    isakmp authorization list NET
    client configuration address respond
    client configuration group 19
    virtual-template 1
!
!
crypto ipsec transform-set test esp-aes 256 esp-sha256-hmac
 mode tunnel
!
!
crypto ipsec profile ipsecprof
    set security-association lifetime kilobytes disable
    set transform-set test
    set isakmp-profile test

interface Virtual-Template1 type tunnel
    tunnel protection ipsec profile ipsecprof
    ip unnumbered GigabitEthernet0/1
    tunnel source GigabitEthernet 0/1
    tunnel mode ipsec ipv4

ip local pool POOL 20.20.0.0 20.20.255.255
```

**Step 9** Encrypt the PSK passwords using the signature-tool under `/opt/cgms-tools/bin`.

**Step 10** Add the encrypted passwords in the CSV file and prepare it for upload.

**Step 11** Add the modem to IoT FND and add ISR4K using the sample CSV shown below.

```
eid,netconfUsername,netconfPassword,ip,deviceType,lat,domain,lng,
ipsecTunnelDestAddr,tunnelHerEid, pskUsername,pskPassword,pskClientConfGrp,psk

IXM-LPWA-900-16-K9+FOC21028RAK,,,,lorawan,10,root,10,4.4.4.1,
C3900-SPE250/K9+FOC172417YT,cisco,ki8OjEO5Pr+
krJTtUooUMD0GoqmOAznc2JObiUUr4ismXyP0uXs8JRuSPOfojMDavGIHiO8unUUJm3zdxv0LP8b6fe5G+
```

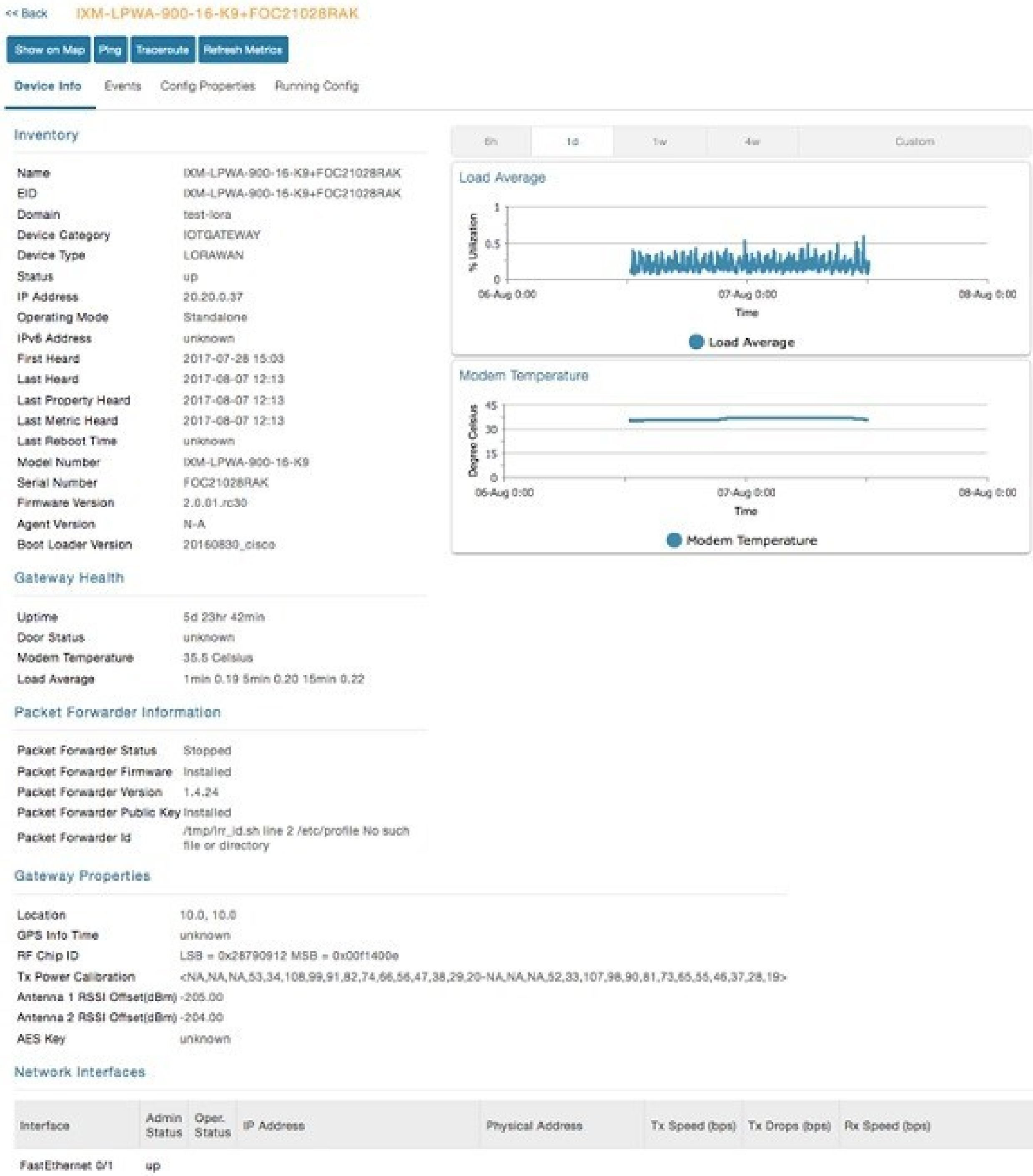
```
oshy76A6IqX1jk7ymSFOaVPQBT8fUS6onjsuSThiLERS0B6Brn2gRx/
KpQMk9IdYQMOSsHh4khvtxbqBZy6j++pIjeG4+ dPz/v52DmJR+DOrE7ZQpfvS9PSHkJoaqC2o6PrKN5YZ50G9+
Tm+diPmbyv/PdHKtXn1ny3qBAdbfDwOjlA+NtJPld3/ 06vq6WhHsgujYwMJWs7Cuu3rR0/FVHF/
5wFxarakJsfo/zd69EpzrI8Hsic/QmMzA==,19, ki8OjEO5Pr+
krJTtUooUMD0GoqmOAznc2JObiUUr4ismXyP0uXs8JRuSPOfojMDavGIHiO8unUUJm3zdxv0LP8b6fe5G+
oshy76A6IqX1jk7ymSFOaVPQBT8fUS6onjsuSThiLERS0B6Brn2gRx/KpQMk9IdYQMOSsHh4khvtxbqBZy6j++pIjeG4+
dPz/v52DmJR+DOrE7ZQpfvS9PSHkJoaqC2o6PrKN5YZ50G9+Tm+diPmbyv/PdHKtXn1ny3qBAdbfDwOjlA+NtJPld3/
06vq6WhHsgujYwMJWs7Cuu3rR0/FVHF/5wFxarakJsfo/zd69EpzrI8Hsic/QmMzA==C3900-SPE250/K9+FOC172417YT,
nms,sgbu123!,55.55.0.18,isr3900,,,,,,,,
```

**Note** The sample CSV for CPF is shown below.

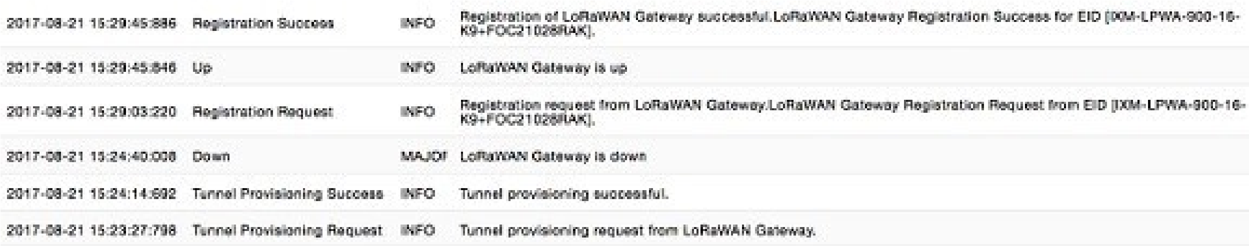
```
eid,netconfUsername,netconfPassword,ip,deviceType,lat,domain,lng,
ipsecTunnelDestAddr,tunnelHerEid, pskUsername,pskPassword,pskClientConfGrp,psk,
cpfNetworkServer,cpfServerPort,cpfAntOmniGain1,cpfAntLoss1,cpfAntOmniGain2,
cpfAntLoss2,cpfCountry,cpfGatewayId,cpfAuthMode
```

```
ki8OjEO5Pr+krJTtUooUMD0GoqmOAznc2JObiUUr4ismXyP0uXs8JRuSPOfo
jMDavGIHiO8unUUJm3zdxv0LP8b6fe5G+oshy76A6IqX1jk7ymSFOaVPQBT8fUS6onjsuSThi
LERS0B6Brn2gRx/KpQMk9IdYQMOSsHh4khvtxbqBZy6j++pIjeG4+
dPz/v52DmJR+DOrE7ZQpfvS9PSHkJoaqC2o6PrKN5YZ50G9+Tm+diPmbyv/
PdHKtXn1ny3qBAdbfDwOjlA+NtJPld3/
06vq6WhHsgujYwMJWs7Cuu3rR0/FVHF/5wFxarakJsfo/zd69EpzrI8Hsic/QmMzA==,19,
ki8OjEO5Pr+krJTtUooUMD0GoqmOAznc2JObiUUr4ismXyP0uX
s8JRuSPOfojMDavGIHiO8unUUJm3zdxv0LP8b6fe5G+
oshy76A6IqX1jk7ymSFOaVPQBT8fUS6onjsuSThiLERS0B6Brn2gRx/
KpQMk9IdYQMOSsHh4khvtxbqBZy6j++pIjeG4+dPz/v52DmJR+
DOrE7ZQpfvS9PSHkJoaqC2o6PrKN5YZ50G9+Tm+diPmbyv/PdHKtXn1ny3qBAdbfDwOjlA+NtJPld3/
06vq6WhHsgujYwMJWs7Cuu3rR0/FVHF/5wFxarakJsfo/zd69EpzrI8Hsic/
QmMzA==,19.19.19.2,5000,1,2,3,4,N/A,::1,none C3900-SPE250/K9+FOC172417YT,
nms,sgbu123!,55.55.0.18,isr3900,,,,,,,,,,,,,,,,
```

**Step 12** Once the modem is registered, the status of the IXM device is shown as up in IoT FND in the Device Info page. Click the modem link to view the detailed IXM modem information.

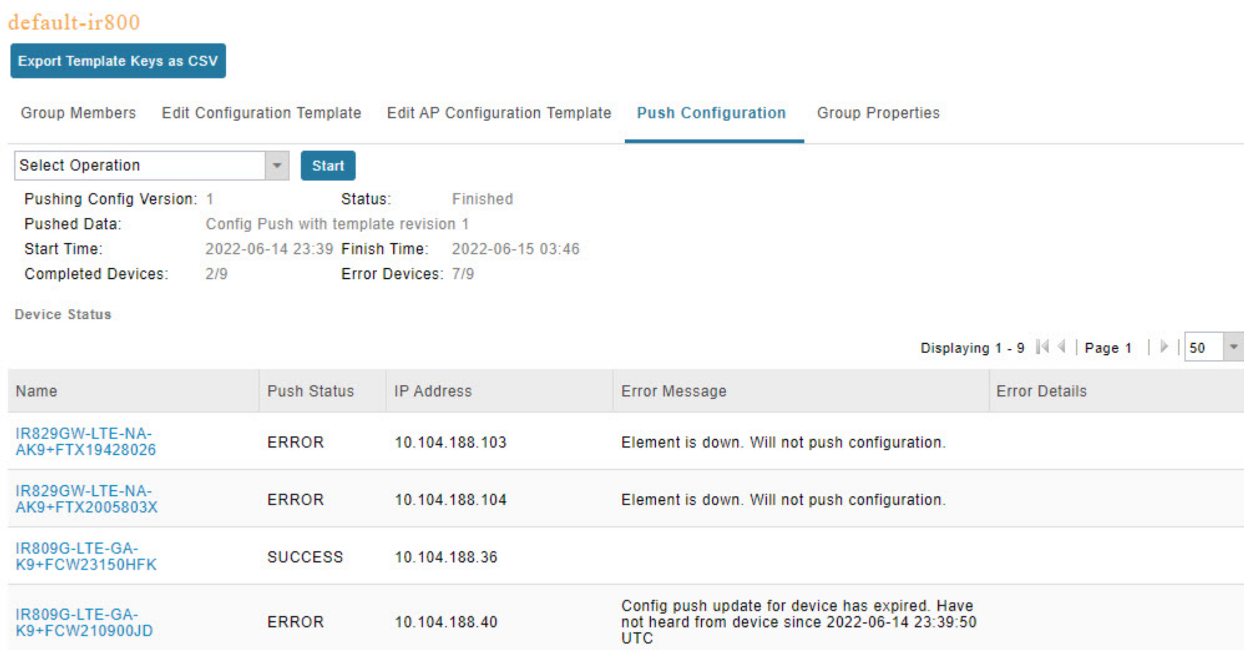



**Note** Please check the following events if there are issues with ZTD.




**Step 13** If configuration update is required or a new modem is added to the router, follow the steps from point 1 or you can invoke a configuration push.

In the **Config** > **Device Configuration** page, click Default-IR800 and go to Push Configuration tab to invoke a configuration push. Select Push ROUTER Configuration from the drop-down and click **Start**.

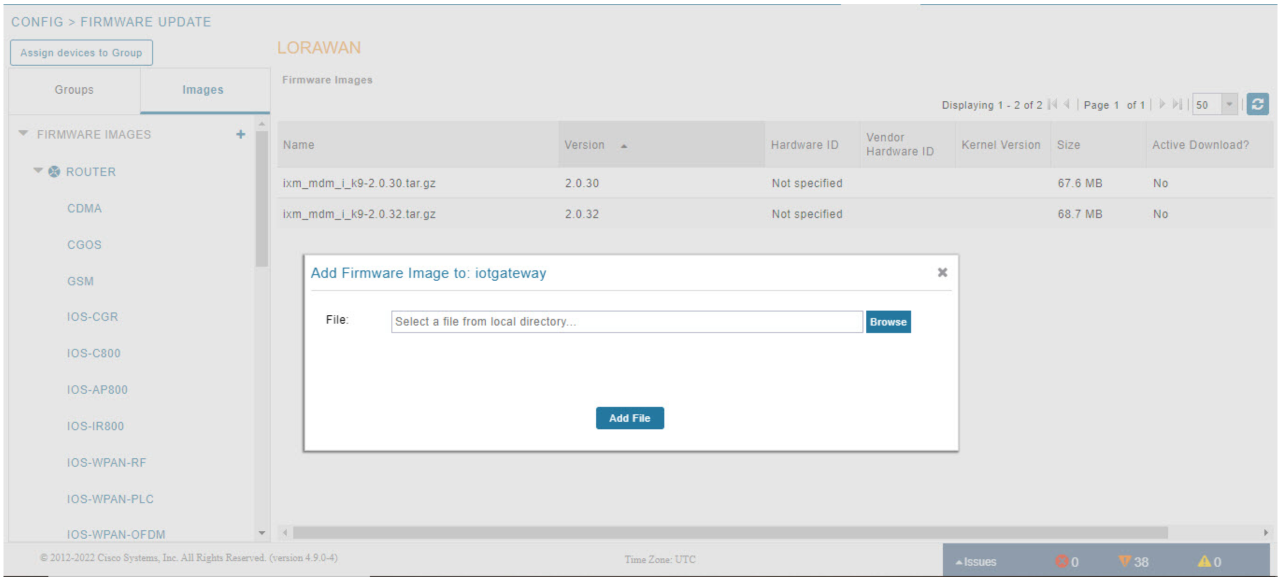



# IXM Firmware Update

Follow the steps for upgrading the firmware.

**Step 1** In **Config** > **Firmware Update** page, go to Images tab. Select Default-Lorawan under Gateway in the left pane and click + to open the entry panel.

**Step 2** Browse and select the firmware file from local directory. Click **Add File** to load the firmware file to IoT FND.

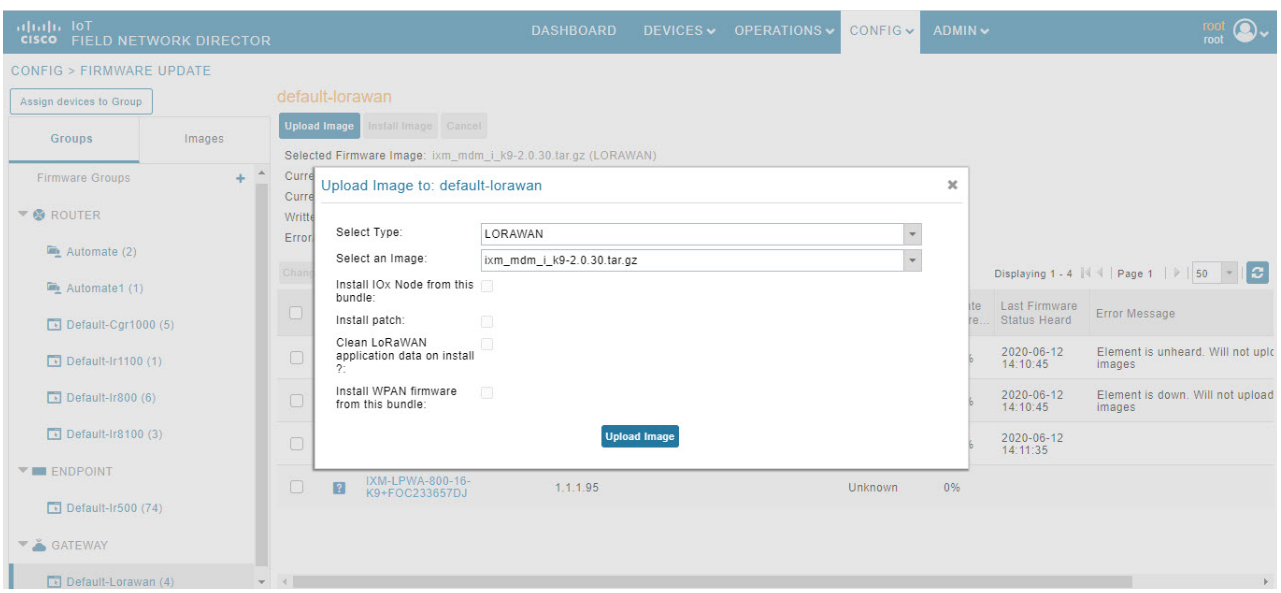



**Step 3** In the Firmware Update page, go to Groups tab. Select Default-Lorawan under Gateway in the left pane.

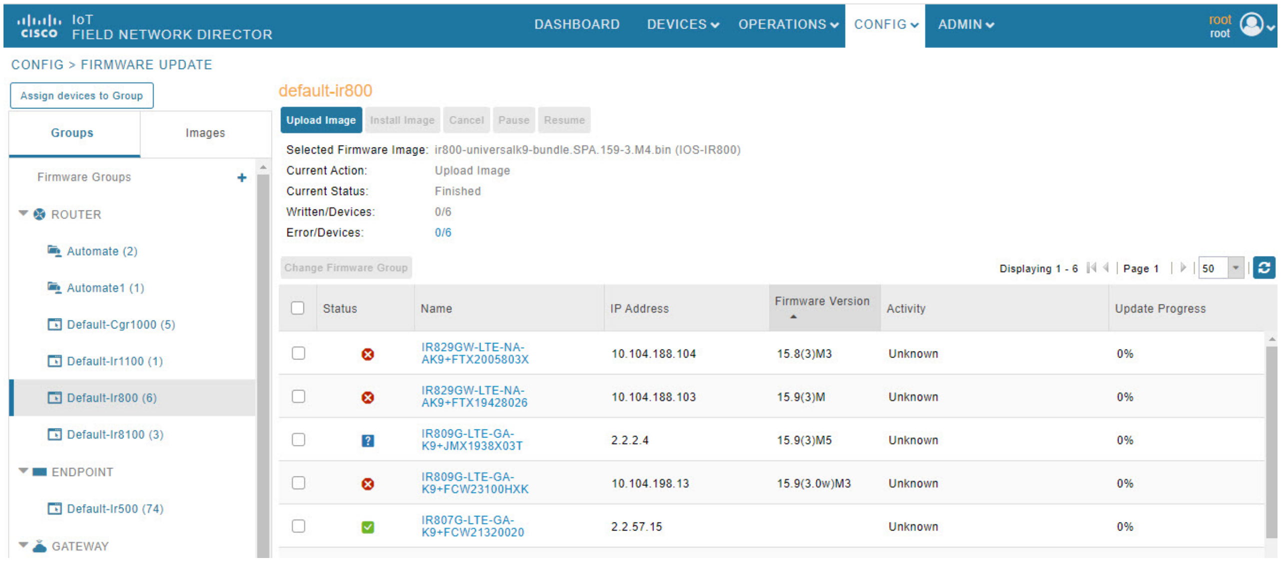
**Step 4** Click **Upload Image** to push the firmware to the IXM modem. For more information, see Uploading a Firmware Image to a Router Group, on page 276.

**Note** If you want to erase the LRR or public key, select **Clean LoRaWAN application data on install ?** option.

**Note** Firmware image upload depends on interface speeds. You can set the timeout duration (in minutes) for firmware upload in cgms.properties file using "igma-idle-timeout" key. If you don't set this duration, then default timeout duration will be 15 minutes.

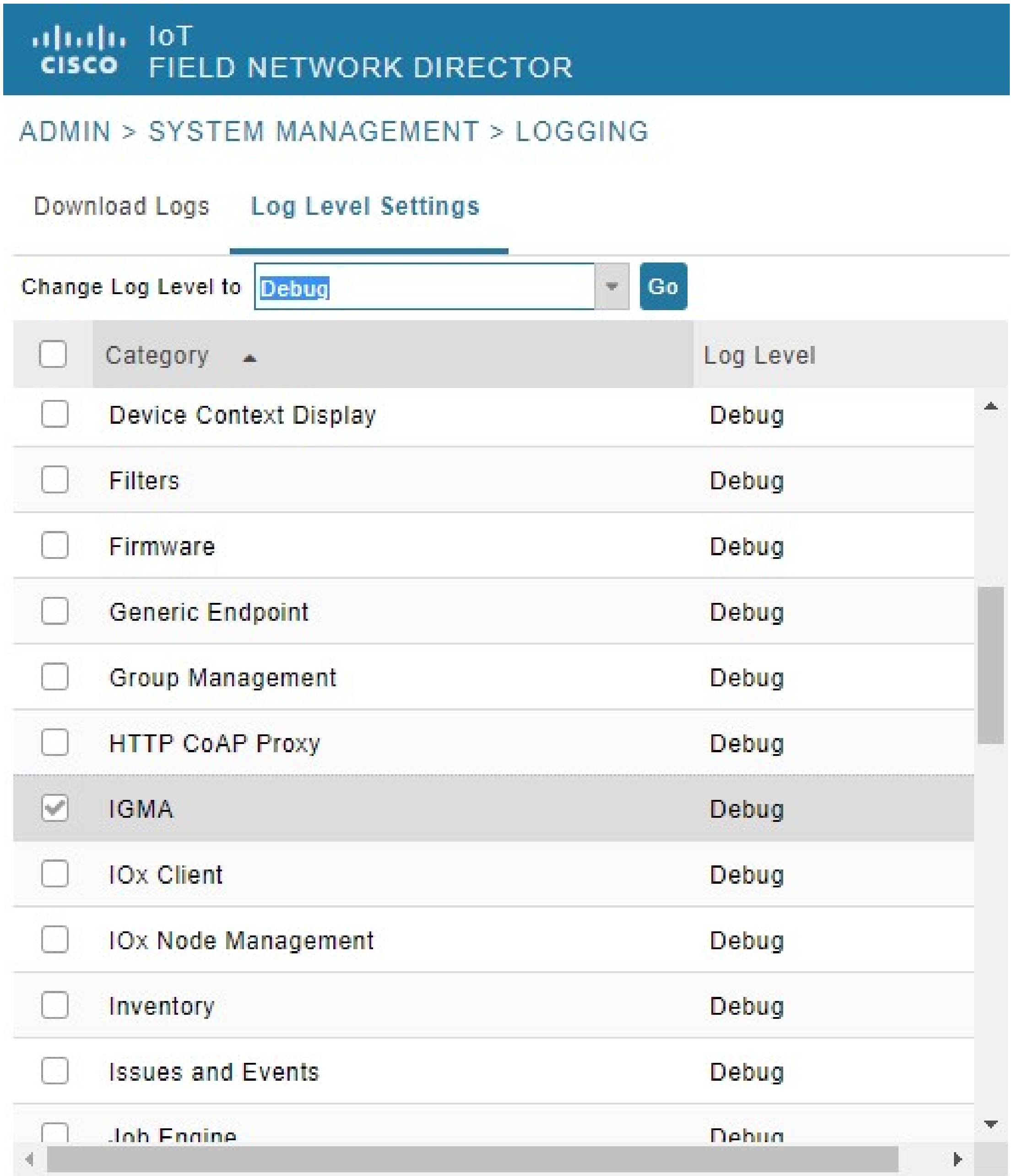



**Step 5** Click **Install Image** button to install the image once the upload is complete.




# Troubleshoot

- Click **Admin** > **System Management** > **Logging** to enable the following debug categories on IoT FND before troubleshooting.




- TPS does not have any messages from IXM.
  - Check if the certificates are installed correctly on IXM and from the same CA as the FND certs.
  - Make sure the IGMA profile is pointing to the correct tunnel profile and the proxy name resolution is correct.
  - Make sure the proxy can be pinged.
  - Make sure the IGMA profile has the correct commands.
- IoT FND does not have any messages from the IXM.

    - Check if the tunnel network is reachable from the FND cluster.
    - Make sure the IGMA profile is pointing to the correct FND profile and the name resolution is correct.
    - Make sure IoT FND can be pinged.

- Tunnel provisioning request failed.
    - Check IoT FND tunnel template for command accuracy.

- IoT FND registration failed.
    - Check IoT FND configuration template for command accuracy.
    - Tunnel issues (for example, flapping or disconnect).

# Monitoring Tunnel Status

To view tunnel status, choose **OPERATIONS** > **Tunnel Status**. The Tunnel Status page lists devices and their provisioned tunnels and displays relevant information about tunnels and their status. Tunnels are provisioned between HERs and FARs.

When you select Show Filter at the top of the page (when selected, replaced by Hide Filter), a number of search fields appear. You can filter by all the Field Names listed in Table 72: Tunnel Status Fields. The value entered in one search field will determine the available selections in the other fields. Select Hide Filter to remove the search fields.

Table 72: Tunnel Status Fields describes the tunnel status fields. To change the sort order of tunnels in the list by name, click the HER Name column heading. A small arrow next to the heading indicates the sort order.

**Note** It takes time for the status of the newly created tunnel to be reflected in IoT FND.

*Table 72: Tunnel Status Fields*

| Field | Description |
|---|---|
| HER Name | The EID of the HER at one end of the tunnel. To view the HER details, click its EID.<br>**Note** Because one HER can serve up to 500 FARs, there may be multiple tunnels in the list with the same HER EID.<br>The Network Interfaces area of the Device Info page displays a list of tunnels configured on the HER. The Config Properties and Running Config tabs also contain information about tunnels configured on this HER. |
| HER Interface | The name of the HER tunnel interface. These names are automatically generated when tunnels are created (Tunnel1, Tunnel2, Tunnel3, and so on) or Virtual-Interface1, Virtual-Interface 2 and so on). |

| Field | Description |
|---|---|
| Admin Status | The administrative status of the tunnel (up or down). This indicates if the administrator enabled or disabled the tunnel. |
| Oper. Status | The operational status of the tunnel (up or down). If the tunnel is down, traffic does not flow through the tunnel, which indicates a problem to troubleshoot. Ping the HER and FAR to determine if they are online, or log on to the routers over SSH to determine the cause of the problem. |
| Protocol | The protocol used by the tunnel (IPSEC, PIM, or GRE). |
| HER Tunnel IP Address | The IP address of the tunnel at the HER side. Depending on the protocol used, the IP address appears in dotted decimal (IPv4) or hexadecimal (IPv6) slash notation. |
| HER IP Address | The destination IP address of the tunnel on the HER side. |
| FAR IP Address | The destination IP address of the tunnel on the FAR side. |
| FAR Interface | The name of the interface on the FAR used by the tunnel. |
| FAR Tunnel IP Address | The IP address of the tunnel on the FAR side.<br>**Note** The IP addresses on both sides of the tunnel are on the same subnet. |
| FAR Name | The EID of the FAR. To view the FAR details, click its EID.<br>The Network Interfaces area of the Device Info page displays a list of tunnels configured on the FAR. The Config Properties and Running Config tabs also contain information about tunnels configured on this FAR. |

# Reprovisioning CGRs

In IoT FND, CGR reprovisioning is a process for modifying the configuration files on CGRs.

## CGR Reprovisioning Basics

This section explains CGR reprovisioning actions and sequence.

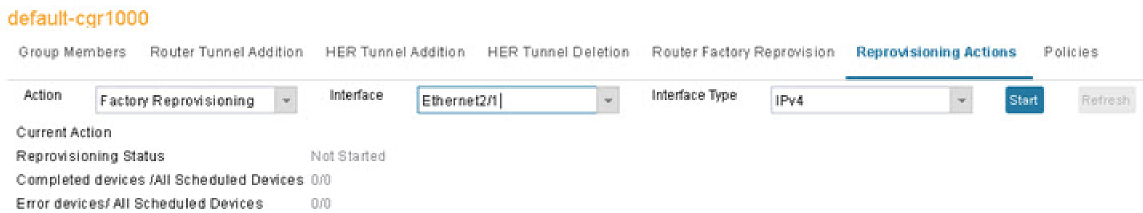
### CGR Reprovisioning Sequence

When you start tunnel or factory reprovisioning on a tunnel provisioning group, the reprovisioning algorithm sequentially goes through 12 CGRs at a time and reprovisions them.

After IoT FND reprovisions a router successfully or if an error is reported, IoT FND starts the reprovisioning process for the next router in the group. IoT FND repeats the process until all CGRs are reprovisioned.

There is a timeout of 4 hours when reprovisioning each CGR in the group. If the CGR does not report successful reprovisioning or an error within the timeout period, then IoT FND changes the Reprovisioning Status of the CGR to Error and displays a timeout error and any further information displays in the Error Details field.

# CGR Reprovisioning Actions




In IoT FND, you can perform the following two CGR reprovisioning actions at the Reprovisioning Actions pane of the Tunnel Provisioning page (**CONFIG** > **Tunnel Provisioning** > **Reprovisioning Actions**). You can also activate mesh firmware.

**Tip** You can also type in the interface instead of selecting the preloaded interface values.

***Table 73:***

| Reprovisioning Actions | Description |
|---|---|
| Factory Reprovisioning | Drop-down menu allows you to change the express-setup-config file loaded on the CGR during factory configuration.<br><br>This file contains a minimal set of information and is loaded on the CGR at the factory. This file provides the CGR with information to contact IoT FND (call home) through the TPS Proxy after the CGR is deployed and powered on. |
| Tunnel Reprovisioning | Drop-down menu allows you to change the golden-config file on a CGR. This file has the tunnel configuration defined on the CGR. |
| Mesh Firmware Activation | Drop-down menu allows you to select the Interface (such as cellular, Ethernet, etc.) and Interface Type (IPv6 or IPv4). |

Table 74: Reprovisioning Actions Pane Fields describes the fields on the Reprovisioning Actions pane.

***Table 74: Reprovisioning Actions Pane Fields***

| Field | Description |
|---|---|
| Current Action | The current reprovisioning action being performed and the associated interface. |
| Reprovisioning Status | The status of the reprovisioning action. |
| Completed devices /All Scheduled Devices | The number of CGRs that were processed relative to the number of all CGRs scheduled to be processed. |

| Field | Description |
|---|---|
| Error devices/ All Scheduled Devices | The number of CGRs that reported an error relative to the number of all CGRs scheduled to be processed. |
| Name | The EID of the CGR. |
| Reprovisioning Status | The status of the reprovisioning action for this CGR. |
| Last Updated | The last time the status of the reprovisioning action for this CGR was updated. |
| Template Version | The version of the Field Area Router Factory Reprovision template being applied. |
| Error Message | The error message reported by the CGR, if any. |
| Error Details | The error details. |

# Tunnel Reprovisioning

If you make changes to the Field Area Router Tunnel Addition template and want all CGRs already connected to IoT FND reprovisioned with new tunnels based on the modified template, use the tunnel reprovisioning feature of IoT FND.

Tunnel reprovisioning places the CGR in a state where no tunnels are configured, and then initiates a new tunnel provisioning request. To reprovision tunnels, IoT FND sequentially goes through the FARs (12 at a time) in a tunnel provisioning group. For every CGR, IoT FND rolls back the configuration of the CGR to that defined in the ps-start-config template file.

After a rollback to ps-start-config, the CGR contacts IoT FND to request tunnel provisioning. IoT FND processes the Field Area Router Tunnel Addition template and sends the resultant configuration commands for creating new tunnels to the CGR.

For Cisco IOS routers, the checkpoint files are before-tunnel-config, before-registration-config, and Express-setup-config. You perform a configuration replace for Cisco IOS based CGRs.

**Note** The Field Area Router Factory Reprovision template is not used when performing tunnel reprovisioning.

To configure and trigger tunnel reprovisioning:

**Step 1** Choose **CONFIG** > **Tunnel Provisioning**.

**Step 2** In the TUNNEL GROUPS pane, select the tunnel group whose template to provision.

**Step 3** Click the **Reprovisioning Actions** tab.

**Step 4** From the Action drop-down menu, choose **Tunnel Reprovisioning**.

**Step 5** Click **Start**.

IoT FND changes the Reprovisioning Status field to Initialized, and then to Running.

**Note** If you click **Stop** while tunnel reprovisioning is running, IoT FND stops the reprovisioning process only for the FARs in the queue that were not selected. However, for those CGRs in the queue that were selected for reprovisioning, the process completes (success or error) and cannot be stopped.

The reprovisioning process completes after IoT FND finishes attempting to reprovision each CGR in the tunnel provisioning group. If a CGR cannot be reprovisioned, IoT FND displays the error message reported by the CGR.

# Factory Reprovisioning

Use the Factory Reprovisioning feature in IoT FND to change the factory configuration of CGRs (express-setup-config).

Factory Reprovisioning involves these steps:

1. Sending the roll back command to the CGR.
2. Reloading the CGR.
3. Processing the Field Area Router Factory Reprovision template, and pushing the resultant commands to the CGR.
4. Saving the configuration in the express-setup-config file.

   After these steps complete successfully, IoT FND processes the Field Area Router Tunnel Addition, Head-End Router Tunnel Addition, and Head-End Router Tunnel Deletion templates and pushes the resultant commands to the CGR (see Tunnel Provisioning Configuration Process, on page 290).

To configure and trigger factory reprovisioning:

**Step 1** Choose **CONFIG** > **Tunnel Provisioning**.

**Step 2** In the TUNNEL GROUPS pane, select the tunnel group whose template you want to edit.

**Step 3** Click the **Router Factory Reprovision** tab and enter the template that contains the configuration commands to apply.

**Note** The Router Factory Reprovision template is processed twice during factory reprovisioning; once when pushing the configuration and again before saving the configuration in express-setup-config. Because of this, when making your own template, use the specific if/else condition model defined in the default template.

**Step 4** Click **Disk icon to Save**.

**Step 5** If needed, make the necessary modifications to the Field Area Router Tunnel Addition, Head-End Router Tunnel Addition, and Head-End Router Tunnel Deletion templates.

**Step 6** Click **Reprovisioning Actions** tab.

**Step 7** Select **Factory Reprovisioning**.


**Step 8** From the Interface drop-down menu, choose the CGR interface for IoT FND to use to contact the FARs for reprovisioning.

**Step 9** From the Interface Type drop-down menu, choose **IPv4** or **IPv6**.

**Step 10** Click the **Start** button.

IoT FND changes the Reprovisioning Status field to Initialized, and then to Running.

**Note** If you click **Stop** while factory reprovisioning is running, IoT FND stops the reprovisioning process only for the FARs in the queue that were not selected. However, for those CGRs in the queue that were selected for reprovisioning, the process completes and cannot be stopped.

The reprovisioning process completes after IoT FND has finished attempting to reprovision each CGR in the tunnel provisioning group. If a CGR cannot be reprovisioned, IoT FND displays the error message reported by the CGR.

### Sample Field Area Router Factory Reprovision Template

This sample template changes the WiFi SSID and passphrase in the factory configuration.

```
<#--IMPORTANT: This template is processed twice during factory
reprovisioning. The if/else condition described below is needed to
determine which part of the template is applied.
In this example, if no schedule name wimaxMigrationRebootTimer is found in
runningConfig, then the if part of the if/else section is applied. During
the second pass, this template runs the commands in the else section and
the no scheduler command is applied. If modifying this template, do not
remove the if/else condition or else the template fails. -->

<#if !far.runningConfig.text?contains("scheduler schedule name
wimaxMigrationRebootTimer")>

<#--Comment: This is a sample of generating wifi ssid and passphrase
randomly-->

wifi ssid ${far.randomSSID("PREFIX_")}
authentication key-management wpa2
wpa2-psk ascii ${far.randomPassword(10)}
exit

feature scheduler
scheduler job name wimaxMigration
reload
exit

scheduler schedule name wimaxMigrationRebootTimer
time start +02:00
job name wimaxMigration
exit

<#else>

no scheduler job name wimaxMigration
no scheduler schedule name wimaxMigrationRebootTimer
```

```
</#if>
```

CHAPTER 8

# Monitoring System Activity

This section describes how to monitor IoT FND system activity, including the following topics:



## Quick Start for New Installs

Quick Start for New Installs prompts you for information to determine the appropriate deployment. No Devices or licenses are added during the Quick Start Process. When you first open a new install of FND software, the DASHBOARD page appears and you select QUICK SETUP.

To quick start for new installs:

**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
- 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. 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.

**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
- Device Configuration and Device Groups
- Firmware Update

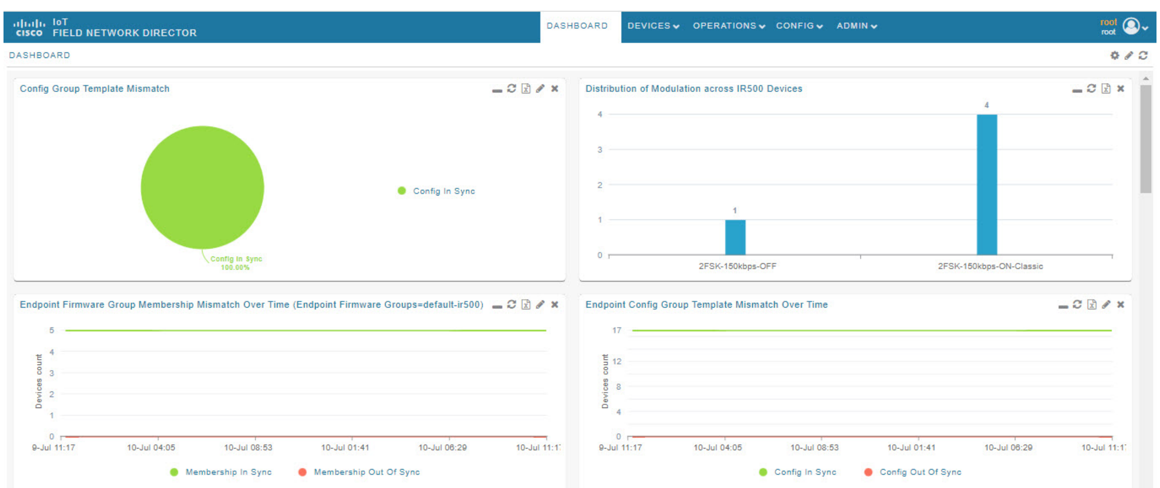
**Step 4** After you select one of the Guided Tours, you will be redirected to that configuration page and windows appear to step you through the configuration steps and let you Add or Update Values as necessary.

**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).

# Using the Dashboard

The IoT FND Dashboard displays *dashlets* to provide a visual overview of important network metrics for a device. You can select what you want to display.

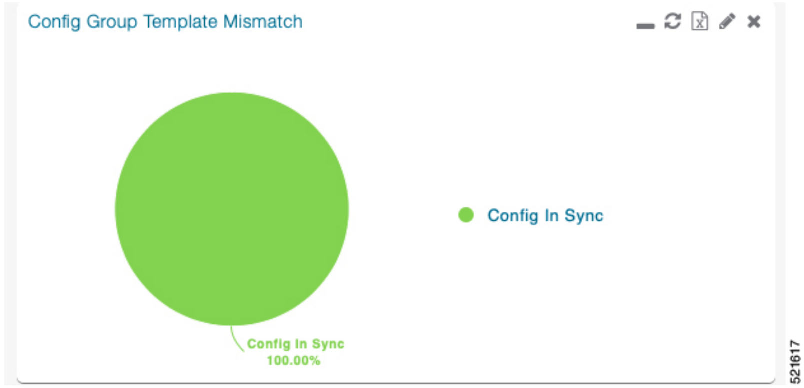
***Figure 34: DASHBOARD***



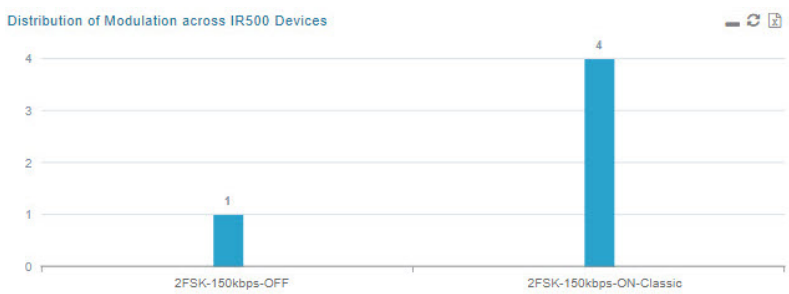

## Types of Dashlets

The Dashboard displays three types of dashlets for a selected device:

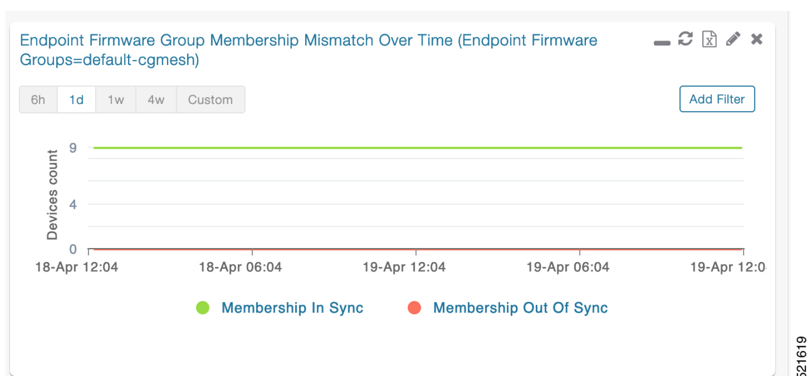
- Pie-chart dashlets display a ratio of the device properties as a pie chart.




- Bar-chart dashlets display device properties.




- Line-graph dashlets display graphs that show device variances over time.




**Tip** Graphs set to intervals longer than one day may not display the data at the last datapoint exactly as shown in the matching field on the Device Info page. This is because data aggregation is occurring less frequently than polling done to update the fields on the Device Info page. Set these graphs to the 6h or 1d intervals to update the data more frequently. Use intervals longer than one day to view data trends.

# Customize Dashboard Dashlets

At the DASHBOARD page use the three icons (Cog, Pencil, Refresh) in the upper-right hand-corner of the page to customize your Dashlets.

To customize the dashoard dashlets:

**Step 1** Click the Dashboard Settings Cog icon to Add Dashlets and Set Refresh Interval for all active dashlets.

**Step 2** Click the pencil icon to Add or Remove a Filter for a device.

**Step 3** Click the **Refresh** icon to refresh the dashlet.

At individual dashlets you can:

**Step 4** Click the dash (-) icon to minimize the dashlet.

**Step 5** Click the Refresh icon to refresh the dashlet.

**Step 6** Click the (+) icon to export data (.csv format) from the dashlet.

**Step 7** Click the filter icon (pencil icon) to: (Options vary by dashlet type):

| |
|---|
| Define reporting intervals by selecting defined periods such as (6h, 1d, 1w, 4w), Last Billing Period and Current Billing Period, or define your own Custom time period. |
| Define a Series Selector, which allows you to define different possible states for a chart. For example, the Endpoint Config Group Mismatch Over Time chart has the following Series Selector options: Config Out of Sync and Config in Sync. Clicking the Series Selector option names on the chart can cause the data to display or not display on the chart. When not selected, a name appears in a faded hue on the chart. |
| Use drop-down menus found in some table headings to display data in an ascending or descending order or display an additional heading option (such as Down Routers Over Time) in the table. |
| Define the number of entries that display on the chart by selecting a value from the Show drop-down menu. |
| Display data as either a bar chart or pie chart. |
| Define a custom line-graph chart. Select the number of devices to chart for line-graph chart displays. |
| Select a series to refine data in line-graph chart displays. |
| Filter line-graph chart displays by group. |
| Add a Filter. |

**Step 8** Click (**X**) to close the dashlet.

# Pre-defined Dashlets

| **Dashlet** | **Description** |
|---|---|
| Config Group Template Mismatch | This pie chart shows the number of devices with matched and mismatched configuration group templates. (Chart applies only to mesh endpoint configuration groups). |

| Dashlet | Description |
|---|---|
| Devices with interfaces enabled but down | This gauge chart displays the count of devices that have interfaces that are enabled but down and the count of interfaces. To display this dashlet, click add (Operation column) at the Dashboard Settings page, and then define the device type and interface (such as Type:cgr1000, Interface:Async 1/1) and save your entries. Once the dashlet is on the Dashboard, click the needle of the gauge chart to launch the Device Details list page that shows all devices that meet the criteria of having enabled, but down interfaces. |
| Distribution of modulations across meters | This line graph shows the distribution of modulations across meters. Modulations graphed: 8PSK, QPSK, BPSK, ROBO, OFDM600,OFDM200, FSK150, QPSK12.5. |
| Distribution of modulations across IR500 Devices | This line graph shows the distribution of modulations across IR500 devices. Modulations graphed: 8PSK, QPSK, BPSK, ROBO, OFDM600,OFDM200, FSK150, QPSK12.5. |
| Endpoint Config Groups Template Mismatch Over Time | This line graph shows the number of endpoints across all configuration groups and particular configuration groups that are out of sync for the configured time interval. |
| Endpoint Firmware Group Membership Mismatch Over Time | This line graph shows the number of endpoints across all firmware groups and particular firmware groups that are out of sync for the configured time interval. |
| Endpoint Inventory | This endpoint status displays the proportion (and count) of endpoints. For example, the count of devices with an Unheard status relative to the other states: Registering, Up, Down, and Outage. |
| Endpoint States Over Time | This line graph shows a count of endpoints and their states for the configured time interval. States shown: Registering, Down, Outage, Unheard, Up, Restored, Unmanaged. |
| Firmware Group Membership Mismatch | This pie chart shows the number of devices with mismatched firmware groups (applicable only to endpoint firmware groups). |
| Gateway Inventory | This pie chart shows the gateway count and its percentage of the whole by the following states: Unheard, Up, Down. |
| Hop Count Distribution | This pie chart shows the hop count distribution for mesh devices. |
| Router Inventory | This pie chart shows a router count and its percentage of the whole by the following states: Unheard, Up, Down. |
| Router States Over Time | This line graph shows the state of all routers over a configured time interval. States supported: Up, Down, Unmanaged, Unsupported and Unheard.<br>Use the Add Filter button to track:<br>• Specific router (Type)<br>• Router Configuration Groups<br>• Router Firmware Groups |

| Dashlet | Description |
|---|---|
| Routers With Top Cellular Bandwidth Usage | This bandwidth chart displays the following information for the top *n* routers: EID, Interface, Bandwidth Usage and Bandwidth Usage (in Bytes) for a router per the defined filter. The filter defines possible time periods (6h, 1d, 1w, 4w, Custom, Last Billing Period) to display. To define the filter, click the pencil icon.<br>**Note** You must define the Monthly Cellular Billing Period Start Day for the Last Billing Period option at the following page: **Admin** > **System Management** > **Server Settings** > **Billing Period Settings** . |
| Routers With Top Ethernet Bandwidth Usage | This bandwidth chart displays the following information for the top *n* routers: EID, Interface, Bandwidth Usage and Bandwidth in Usage (in Gigabits) for a router per the defined filter. The filter defines possible time periods (6h, 1d, 1w, 4w, Custom, Last Billing Period) to display. To define the filter, click the pencil icon.<br>**Note** You must define the Monthly Ethernet Billing Period Start Day for the Last Billing Period option at the following page: **Admin** > **System Management** > **Server Settings** > **Billing Period Settings** . |
| Routers With Least Cellular RSSI | This Cellular RSSI chart displays the following information for the top *n* routers: EID, Interface, Cellular RSSI and Cellular RSSI (in dBm) for a router. |
| Service Providers with Maximum Down Routers for Cellular 1 | This dashlet shows the service provider names, their associated cell IDs (if available), their associated total router count, the count of down routers, and a sparkline showing the down routers over time (when you select the option per Tip noted below).<br>This dashlet displays the aggregated maximum Down Routers for device types CGR1000, C800, and IR800 for single modem routers.<br>**Tip** Move your cursor over any column heading to display the Down Routers Over Time listings in either ascending or descending order. |
| Service Providers with Maximum Down Routers for Cellular 2 | This dashlet shows the service provider names, their associated cell IDs (if available), their associated total router count, the count of down routers, and a sparkline showing the down routers over time (when you select the option per Tip noted below).<br>This dashlet displays the aggregated maximum Down Routers for device types CGR1000, C800, and IR800 for dual modem routers.<br>**Tip** Move your cursor over any column heading to display listings in either ascending or descending order or to display the Down Routers Over Time column. |

# Repositioning Dashlets

You can configure the Dashboard to display charts in your preferred arrangement.

**Step 1** Click and drag the title bar of a chart to the desired position.

**Step 2** Click (x) within a chart to remove the chart from the page.

**Step 3** Collapse a dashlet to display only its title bar (such as Endpoint Inventory) by clicking the Minimize button (-).

**Step 4** To refresh a dashlet, click the **Refresh** button.

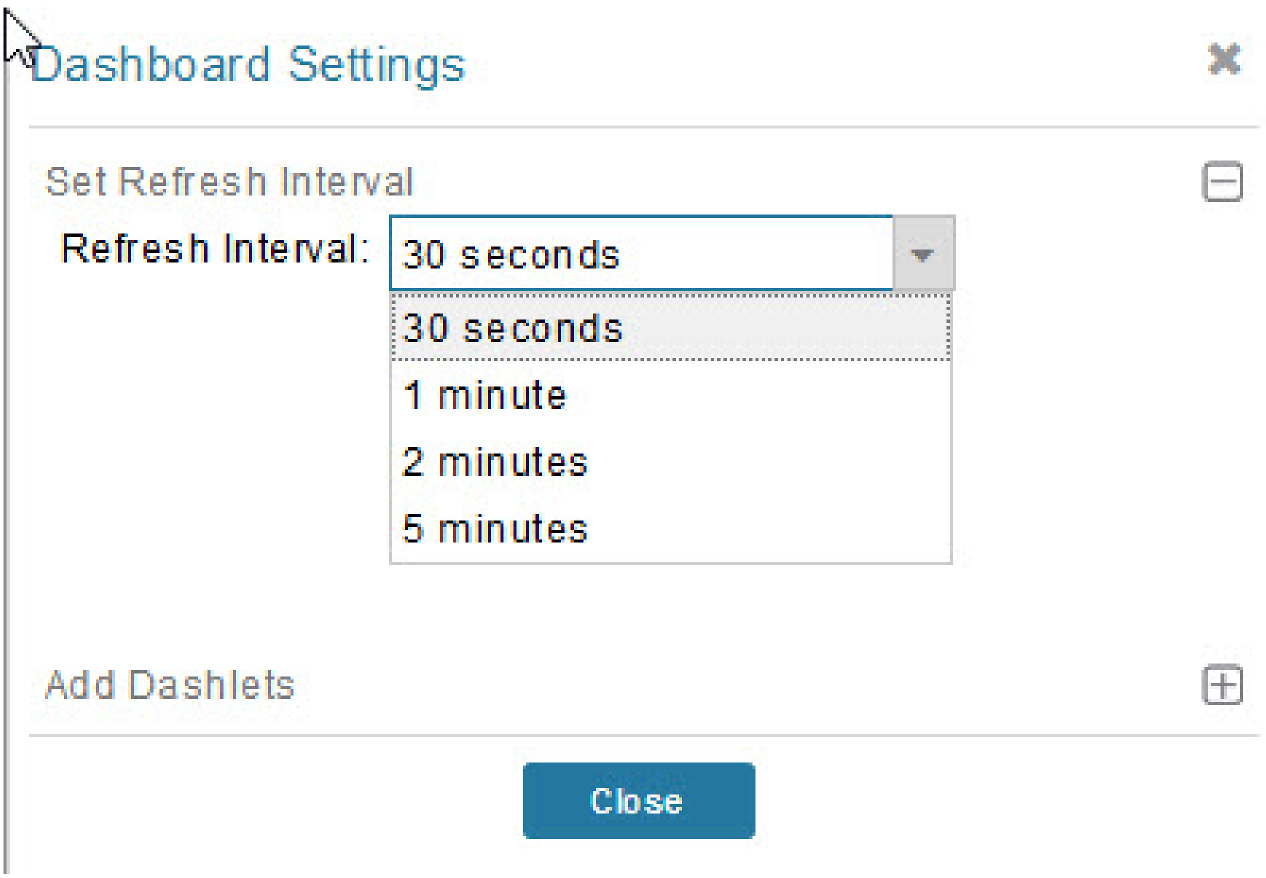
# Setting the Dashlet Refresh Interval

To set the refresh interval for dashlets:

**Step 1** Choose **DASHBOARD** menu.

**Step 2** Click the **Dashboard Settings** button (cog icon) in the upper-right corner of the page under the root <user> icon.

The Dashboard Settings panel appears.




**Step 3** From the drop-down menu, choose a refresh interval.

**Step 4** Close the Dashboard Settings dialog box when finished.

# Adding Dashlets

To add dashlets to the Dashboard:

**Step 1** Choose **DASHBOARD** menu.
**Step 2** Click the **Settings** button (cog icon) in the upper-right hand corner of the page.
**Step 3** Click **Add Dashlets (+)**.

**Note** No dashlets display in this dialog box if all are displaying on the Dashboard.

**Step 4** To add a listed dashlet to the Dashboard, select the name of dashlet.
**Step 5** Close the Dashboard Settings dialog box by clicking (x) in upper-right corner of panel when finished.

*Table 75: Router Metrics*

| Field Name | Key | Description |
|---|---|---|
| Bandwidth Usage | cellularBandwidth | The total accumulated amount of bytes sent and received over the cellular uplink backhaul. |
| Battery 0 Level | battery0Level | The percentage of charge remaining in battery 0. |
| Battery 0 Remaining Time | battery0Runtime | The runtime remaining on battery 0. |
| Battery 1 Level | battery1Level | The percentage of charge remaining in battery 1. |
| Battery 1 Remaining Time | battery1Runtime | The runtime remaining on battery 1. |
| Battery 2 Level | battery2Level | The percentage of charge remaining in battery 2. |
| Battery 2 Remaining Time | battery2Runtime | The runtime remaining on battery 2. |
| C1222 Multicast Incoming Traffic | c1222McastInTraffic | C1222 multicast receive traffic on the WPAN interface. |
| C1222 Multicast Outgoing Traffic | c1222McastOutTraffic | C1222 multicast transmit traffic on the WPAN interface. |
| C1222 Multicast Traffic | c1222McastTraffic | C1222 multicast traffic on the WPAN interface. |
| C1222 Total Incoming Traffic | c1222InTraffic | Total C1222 receive traffic on the WPAN interface. |
| C1222 Total Outgoing Traffic | c1222OutTraffic | Total C1222 transmit traffic on the WPAN interface. |
| C1222 Total Traffic | c1222Traffic | Total C1222 traffic on the WPAN interface. |
| C1222 Unicast Incoming Traffic | c1222UcastInTraffic | C1222 unicast receive traffic on the WPAN interface. |
| C1222 Unicast Outgoing Traffic | c1222UcastOutTraffic | C1222 unicast transmit traffic on the WPAN interface. |
| C1222 Unicast Traffic | c1222UcastTraffic | C1222 unicast traffic on the WPAN interface. |

| Field Name | Key | Description |
|---|---|---|
| Cellular Module Temperature | cellModuleTemp | The internal temperature of 3G module. |
| Chassis Temperature | chassisTemp | The internal temperature of the device. |
| CINR | wimaxCinr | The measured CINR value of the WiMAX RF uplink. |
| CSMP Incoming Traffic | csmpInTraffic | CSMP receive traffic on the WPAN interface. |
| CSMP Multicast Incoming Traffic | csmpMcastInTraffic | CSMP multicast receive traffic on the WPAN interface. |
| CSMP Multicast Outgoing Traffic | csmpMcastOutTraffic | CSMP multicast transmit traffic on the WPAN interface. |
| CSMP Multicast Traffic | csmpMcastTraffic | CSMP multicast traffic on the WPAN interface. |
| CSMP Outgoing Traffic | csmpOutTraffic | CSMP transmit traffic on the WPAN interface. |
| CSMP Traffic | csmpTraffic | Total CSMP traffic on the WPAN interface. |
| CSMP Unicast Incoming Traffic | csmpUcastInTraffic | CSMP unicast receive traffic on the WPAN interface. |
| CSMP Unicast Outgoing Traffic | csmpUcastOutTraffic | CSMP unicast transmit traffic on the WPAN interface. |
| CSMP Unicast Traffic | csmpUcastTraffic | Total CSMP unicast traffic on the WPAN interface. |
| Current Call Duration | cellConnectTime | The amount of time the current call lasted; applicable to CDMA only. |
| DHCP Incoming Traffic | dhcpInTraffic | DHCP receive traffic on the WPAN interface. |
| DHCP Outgoing Traffic | dhcpOutTraffic | DHCP transmit traffic on the WPAN interface. |
| DHCP Traffic | dhcpTraffic | Total DHCP traffic on the WPAN interface. |
| Dot 1x Traffic | dot1xTraffic | Total Dot 1x traffic on the WPAN interface. |
| Dot1x Incoming Traffic | dot1xInTraffic | Dot1x receive traffic on the WPAN interface. |
| Dot1x Outgoing Traffic | dot1xOutTraffic | Dot1x transmit traffic on the WPAN interface. |
| ECIO | cellularEcio | The signal strength of CDMA at individual sector level. |
| ICMP Incoming Traffic | icmpInTraffic | ICMP receive traffic on the WPAN interface. |
| ICMP Outgoing Traffic | icmpOutTraffic | ICMP transmit traffic on the WPAN interface. |
| Lowpan Incoming Traffic | lowpanInTraffic | Lo WPAN receive traffic on the WPAN interface. |
| Lowpan Outgoing Traffic | lowpanOutTraffic | Lo WPAN transmit traffic on the WPAN interface. |
| Mcast Incoming Traffic | mcastInTraffic | Multicast receive traffic on the WPAN interface. |
| Mcast Outgoing Traffic | mcastOutTraffic | Multicast transmit traffic on the WPAN interface. |
| Mesh Endpoint Count | meshEndpointCount | Number of active connected mesh endpoints. |

| Field Name | Key | Description |
|---|---|---|
| ND NS Incoming Traffic | ndnsInTraffic | ND NS receive traffic on the WPAN interface. |
| Outage Incoming Traffic | outageInTraffic | Outage on receive traffic on the WPAN interface. |
| Overall Battery Remaining Time | batteryRuntime | Battery runtime remaining (all batteries). |
| Raw Socket Rx (Frames) S0 | rawSocketRxFramesS0 | (C800 only) Raw socket receiving data rate in frames for serial interface 0. |
| Raw Socket Rx S0 | rawSocketRxSpeedS0 | (C800 only) raw socket receiving data rate for serial interface 0. |
| Raw Socket Rx S1 | rawSocketRxSpeedS1 | Raw socket receive data rate for serial interface 1. |
| Raw Socket Rx S2 | rawSocketRxSpeedS2 | Raw socket receive data rate for serial interface 2. |
| Raw Socket Rx(Frames) S1 | rawSocketRxFramesS1 | Raw socket receive data rate, in frames, for serial interface 1. |
| Raw Socket Rx(Frames) S2 | rawSocketRxFramesS2 | Raw socket receive data rate, in frames, for serial interface 2. |
| Raw Socket Tx (Frames) S0 | rawSocketTxFramesS0 | (C800 only) Raw socket transmit data rate, in frames, for serial interface 0. |
| Raw Socket Tx S0 | rawSocketTxSpeedS0 | (C800 only) Raw socket transmit data rate for serial interface 0. |
| Raw Socket Tx S1 | rawSocketTxSpeedS1 | Raw socket transmit data rate for serial interface 1. |
| Raw Socket Tx S2 | rawSocketTxSpeedS2 | Raw socket transmit data rate for serial interface 2. |
| Raw Socket Tx(Frames) S1 | rawSocketTxFramesS1 | Raw socket transmission data rate, in frames, for serial interface 1. |
| Raw Socket Tx(Frames) S2 | rawSocketTxFramesS2 | Raw socket transmission data rate, in frames, for serial interface 2. |
| Receive Packet Reassembly Drops | meshRxReassemblyDrops | The rate of receive packet fragments dropped because of no space in the reassembly buffer. |
| Receive Speed | ethernetRxSpeed | The rate of data received by the Ethernet uplink network interface, in bits per second, averaged over a short element-specific time period (for example, an hour). |
| Receive Speed | wimaxRxSpeed | The rate of data received by the WiMAX uplink network interface, in bits per second, averaged over a short element-specific time period (for example, one hour). |
| Receive Speed | cellularRxSpeed | The rate of data received by the cellular uplink network interface, in bits per second, averaged over a short element-specific time period (for example, one hour). |

| Field Name | 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 time period (for example, one hour). |
| Remaining ICMP Incoming Traffic | remainIcmpInTraffic | Remaining ICMP receive traffic on the WPAN interface. |
| Remaining ICMP Outgoing Traffic | remainIcmpOutTraffic | Remaining ICMP transmit traffic on the WPAN interface. |
| Remaining ICMP Traffic | remainIcmpTraffic | Total remaining ICMP traffic on the WPAN interface. |
| Remaining IP Incoming Traffic | remainIpInTraffic | Remaining IP receive traffic on the WPAN interface. |
| Remaining IP Outgoing Traffic | remainIpOutTraffic | Remaining IP transmit traffic on the WPAN interface. |
| Remaining IP Traffic | remainIpTraffic | Total remaining IP traffic on the WPAN interface. |
| RPL DAO Incoming Traffic | rplDaoInTraffic | DAO receive traffic on the WPAN interface. |
| RPL DIO Incoming Traffic | rplDioInTraffic | DIO receive traffic on the WPAN interface. |
| RPL Incoming Traffic | rplInTraffic | RPL receive traffic on the WPAN interface. |
| RPL RA Outgoing Traffic | rplRaOutTraffic | RA transmit traffic on the WPAN interface. |
| RPL Source Route Table Entries | meshRoutes | The number of entries a given router has in its source-route table. This provides a way to measure the number of elements in the PAN. |
| RPL Total Traffic | rplTraffic | Total RPL traffic on the WPAN interface. |
| RSSI | cellularRssi | The measured RSSI value of the cellular RF uplink. |
| RSSI | wimaxRssi | The measured RSSI value of the WiMAX RF uplink. |
| Total Incoming Traffic | totalInTraffic | Total receive traffic on the WPAN interface. |
| Total Outgoing Traffic | totalOutTraffic | Total transmit traffic on the WPAN interface. |
| Transmit Packet Drops | ethernetTxDrops | The rate of packets dropped because the outbound queue was full while trying to transmit on the Ethernet uplink interface. |
| Transmit Packet Drops | meshTxDrops | The rate of packets dropped because the outbound queue was full while trying to transmit on the mesh uplink interface. |
| Transmit Speed | ethernetTxSpeed | The current speed of data transmission over the Ethernet uplink network interface, in bits per second, averaged over a short element-specific time period (for example, one hour). |
| Transmit Speed | cellularTxSpeed | The current speed of data transmission over the cellular uplink network interface, in bits per second, averaged over a short element-specific time period (for example, one hour). |

| Field Name | Key | Description |
|---|---|---|
| Transmit Speed | wimaxTxSpeed | The current speed of data transmission over the WiMAX uplink network interface, in bits per second, averaged over a short element-specific time period (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 time period (for example, one hour). |
| Ucast Incoming Traffic | ucastInTraffic | Unicast receive traffic on the WPAN interface. |
| Ucast Outgoing Traffic | ucastOutTraffic | Unicast transmit traffic on the WPAN interface. |
| Uptime | uptime | The amount of time, in seconds, that the device has been running since last boot |
| Utilization Bytes (slots 1–8) | ethernetUtilBytes[slot number] | The data, in bytes, transmitted and received by the Ethernet on the uplink or downlink network interface at slot x. |
| Utilization Bytes (slot 9-11) | ethernetUtilBytes[9-11] | (Cisco IOS CGRs running GOS only) The data, in bytes, transmitted and received by the Ethernet on the uplink or downlink network interface at module/slot 0/0, 0/1, or 0/2, respectively. |

***Table 76: Router Properties***

| Field Name | Key | Description |
|---|---|---|
| Battery 0 State | battery0State | The state of battery 0 charge (combined attribute). |
| Battery 1 State | battery1State | The state of battery 1 charge (combined attribute). |
| Battery 2 State | battery2State | The state of battery 2 charge (combined attribute). |
| Cellular Roaming Status | cellRoamingStatus | The roaming status of the cellular module on the CGR. |
| Network Name | cellularNetworkName | The network that the cellular device is associated with. |
| Module Status | cellularStatus | The status and state of the cellular module. |
| Cellular Network Type | cellularType | The cellular network type (CDMA or GSM). |
| Door Status | doorStatus | The device door status (Open or Closed). |
| Power Source | powerSource | The device current power source. |
| Link State | wimaxLinkState | The device WiMAX link state. |

# Removing Dashlets

To remove dashlets from the Dashboard:

**Step 1** Choose **DASHBOARD** menu.

**Step 2** Close the dashlet by clicking (X) in the upper-right corner of the panel.

# Using Pie Charts to Get More Information

Roll over any segment of a pie chart to display a callout with information on that segment.

Click the Router Inventory and Mesh Endpoint Inventory pie charts to display the devices in List View.

# Setting Time Filters To View Charts

Use the **Filter** option to view charts for default or custom-defined time intervals. The chart provides statistical information on devices (such as device information, events, or issues) and FND servers.

- Default time intervals: The options available are **6h** (6 hours), **1d** (one day), **1w** (one week), or **4w** (four weeks). For example, **6h** collects the device data for the last 6 hours and **1d** collects the device data for the last 24 hours.

> **Note** You can hover over the chart to view the tooltip information. The tooltip appears by default in the charts for small data and displays information in the combination of data values, text, and/or tokens. For charts with a huge dataset, the tooltip doesn't appear by default. You have to select and expand the specific portion of the chart for which you need the information and then hover over to see the tooltip.

> **Note** You see only aggregated data for **1w**, **4w**, and **Custom** charts and not real-time data, to avoid performance impact on Cisco IoT FND. The processing of a huge amount of data and displaying them in real-time slows down Cisco IoT FND.

- Custom: This option allows you to customize the time frame for collecting the device data. The chart in the dashlets provides the device data specific to the time frame set by you.

> **Note** In some cases, the date and time displayed in the chart varies from the time frame customized by you. This time discrepancy is due to the time difference in the respective location of the Cisco IoT FND server and the Cisco IoT FND client. To rectify this time difference, you have to set the time zone in the Cisco IoT FND to your current location, using **User** > **Time Zone** (right top corner in the user interface).

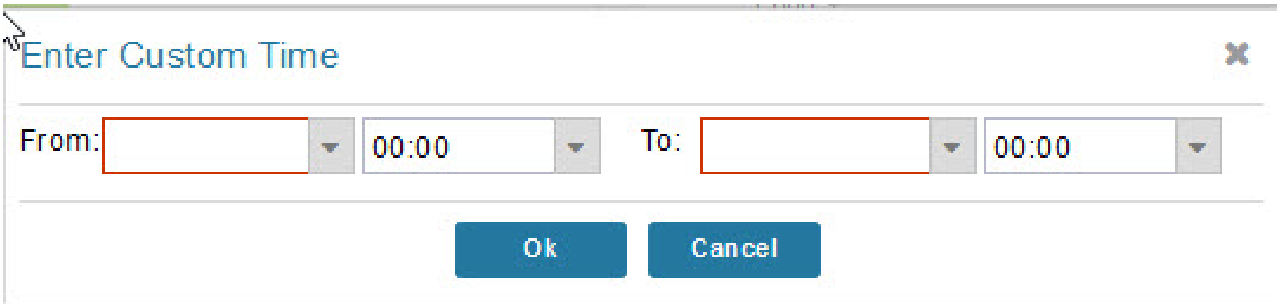
To set time filters to view charts:

**Step 1** Click **Filter** (pencil icon) in the right corner of the dashlet.

**Step 2** Click the **Custom** button.

**Step 3** In the **Enter Custom Time** window, select the time frame from the **From** and **To** fields.

**Step 4** Click **OK**.




**Note** The **From** and **To** fields are only enabled when the time range is set to Custom.

# Collapsing Dashlets

To collapse the dashlets:

**Step 1** Choose **DASHBOARD** menu.

**Step 2** Click the minimize icon **(-)** at the upper-right of the dashlet window to hide the window.

# Using the Series Selector

You use the Series Selector to refine line-graphs to display by device status. The device options are:

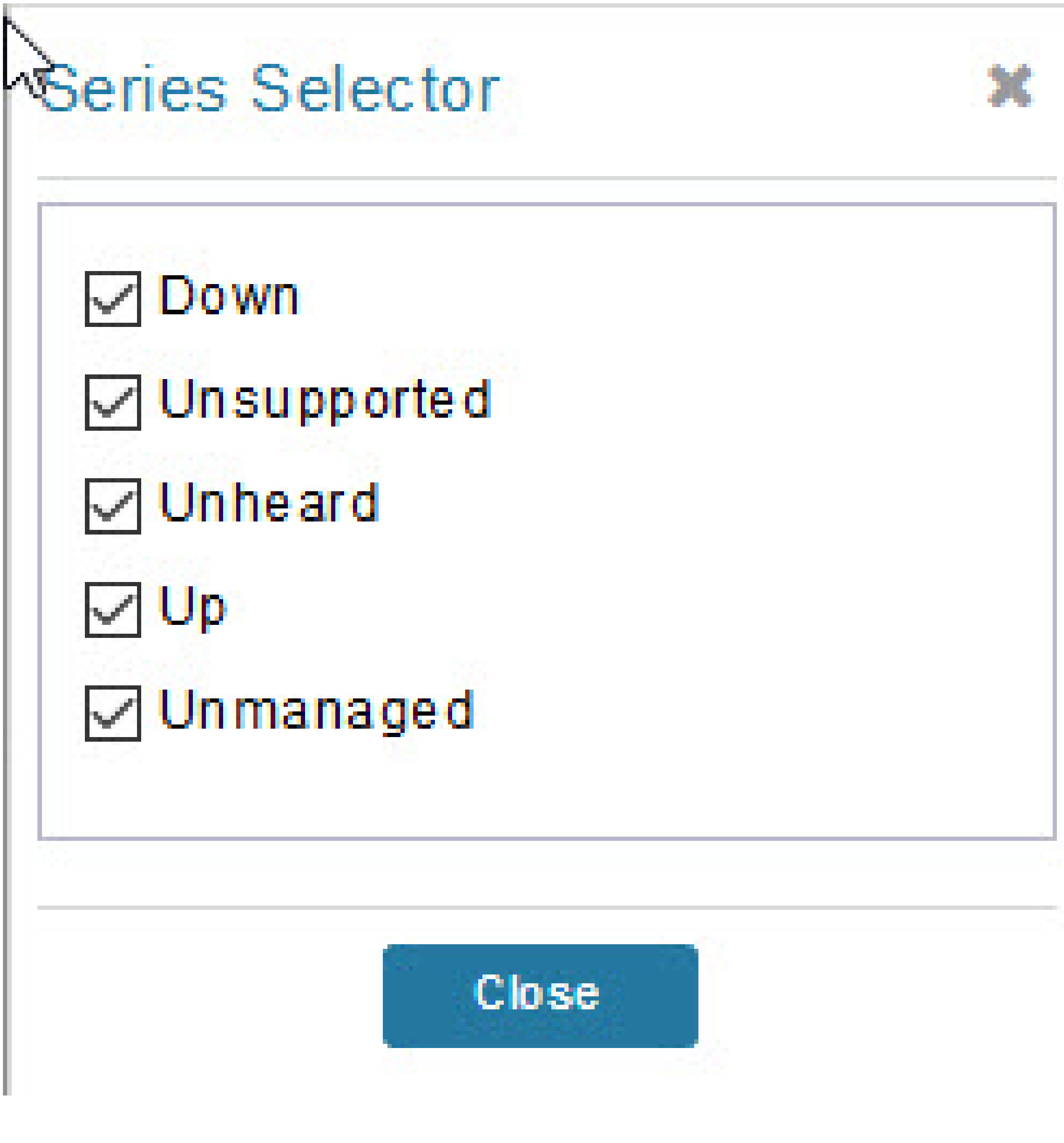
- Routers: Down, Outage, Unsupported, Unheard, and Up
- Mesh Endpoint Config Group: Config Out of Sync and Config In Sync
- Mesh Endpoint Firmware Group: Membership Out of Sync and Membership In Sync
- Mesh Endpoint States: Down, Outage, Unheard, and Up

To use the Series Selector:

**Step 1** Click **Series Selector**.

**Step 2** In the **Series Selector** dialog box, check the check boxes for the data series to show in the graph.

**Step 3** Click **Close**.




## Using Filters

You use filters to refine the displayed line-graph data by groups. Applied filters display after the dashlet title.

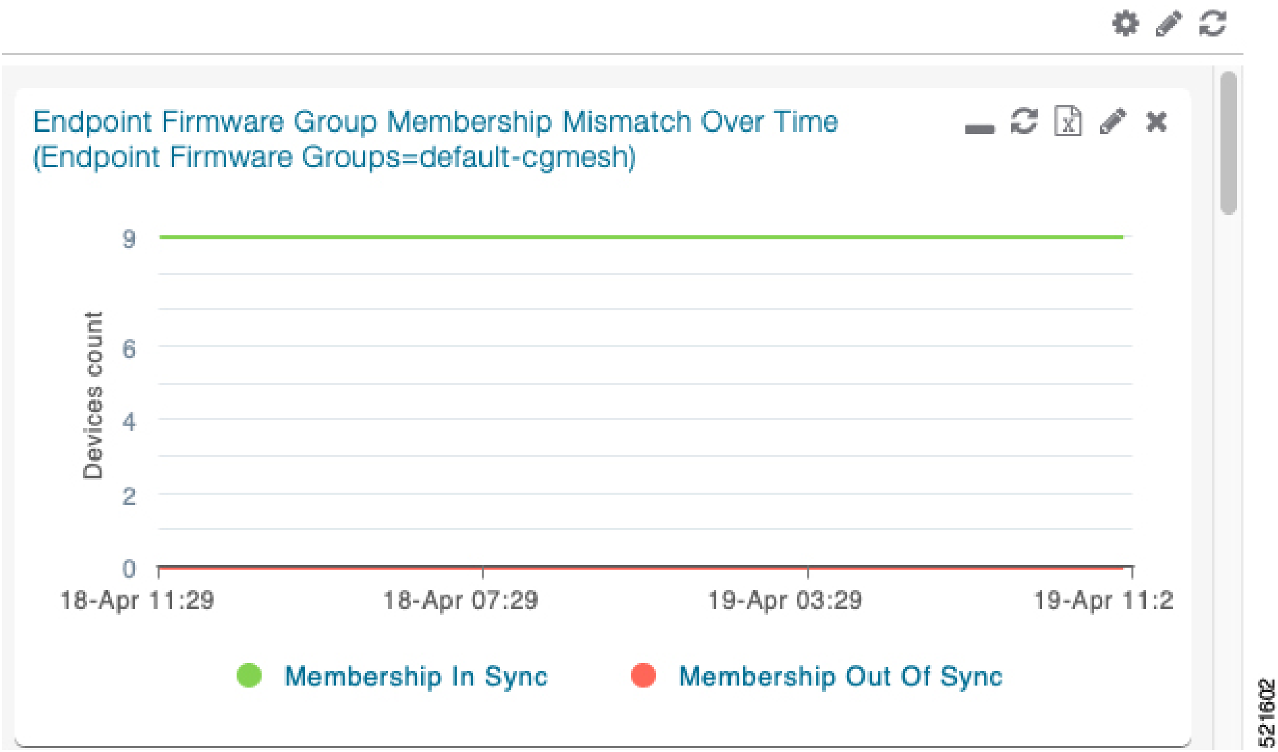
To use the filters:

**Step 1** Click the interval icon (pencil) in the upper-right corner of the panel to display the 2 filtering parameters on the chart: a time frame (such as 6h) and components (such as Endpoint Configuration Groups, Mesh Endpoints (MEs).

**Step 2** Click a time frame.

**Step 3** From the first drop-down menu, choose a group type.

*Figure 35: Endpoint Firmware Group Membership Mismatch Over Time*




**Step 4** From the first drop-down menu, choose a group type.

**Step 5** From the third drop-down menu, choose a group.

**Step 6** Click **Apply**.

The pencil icon is green and the filter displays next to the dashlet name to indicate that a filter is applied.

**Note** Click the **Remove Filter** button to remove the filter and close the filter options.

# Exporting Dashlet Data

You can export dashlet data to a CSV file.

To export dashlet data:

**Step 1** On the desired dashlet, click the export button (+).

A browser download session begins.

**Step 2** Navigate to your default download directory to view the export file.

**Note** The filename begins with the word "export-" and includes the dashlet name (for example, export-Node_State_Over_Time_chart-1392746225010.csv).

# Monitoring Events

This section provides an overview of events and how to search and sort events.

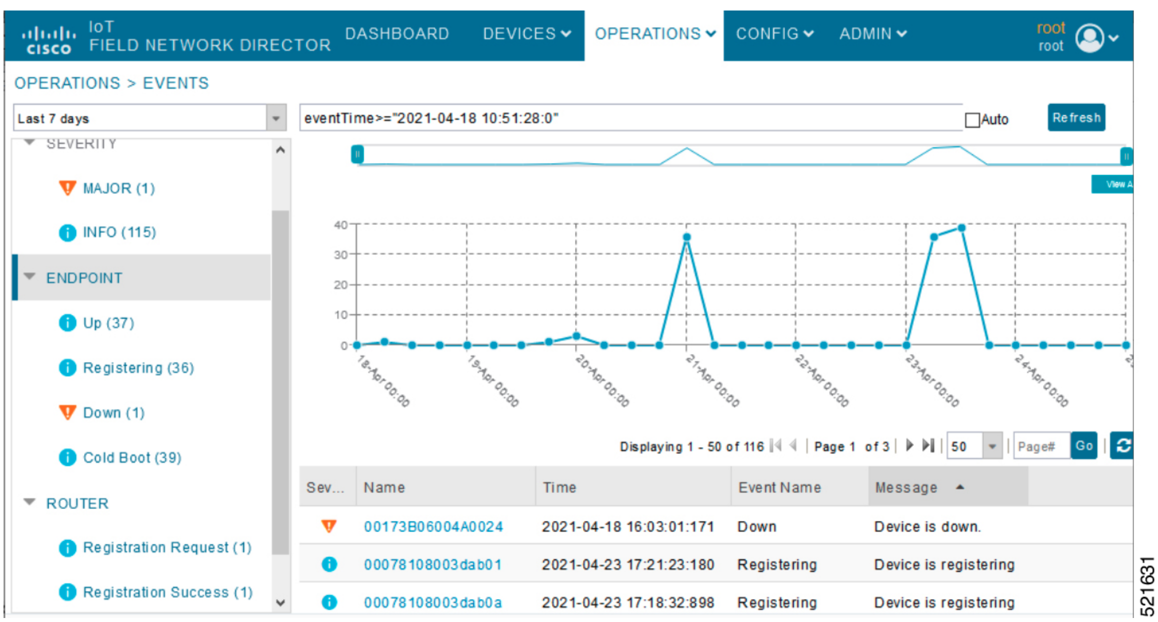
## Set Time Range and Page View Preferences for Operations > Events

In the Events tab of a device, you can define the following information:

- Relative time periods: 'Last 24 hours', 'Last 15 Minutes', 'Last 4 hours', 'Last 7 days', 'Last 30 days' and 'All Time' from the drop-down menu at the left-hand side of the page
- Absolute time periods reference a specific day such as Sunday, April 25, Saturday, April 24, Friday, April 24

You can also select the number of events to display on a page (such as '10', '50', '100', and '200') by selecting that value from the drop-down menu at the far-right side of the page.

*Figure 36: Set Time Range and Page View Preferences for Events for a Specific Period of Time for an Endpoint*



# Viewing Events

As shown in **Operation** > **Events** page, the Events page lists all events for those devices that IoT FND tracks. All events are stored in the IoT FND database server.

By default, the **Operations** > **Events** page displays the Events chart of which is a visual view of events in a time line.

From this page, you can also view the device information by clicking on one of the devices listed under router or endpoint on the left pane. The **Device Info** tab displays detailed information of the selected device along with the events chart. You can view the events chart of the device for default or custom-defined time intervals. For more information on viewing the chart for default or custom-defined time intervals, refer to Setting Time Filters To View Charts, on page 335.

However, depending on the number of devices the IoT FND server manages, this page can sometimes time out, especially when the system is fully loaded. In that case, open the Preferences window by choosing *username* > **Preferences** (top right), and uncheck the check boxes for options, ‘Show chart on events page’ and ‘Show summary counts on the events/issues page’, and then click **Apply**.

**Step 1** To limit the amount of event data displayed on this page, use the Filter drop-down menu (at the top of the left pane).

**Note** For example, you can show the events for the last 24 hours relative to the last 30 days, or events for a specific day within the last seven days.

**Step 2** To enable automatic refresh of event data to refresh every 14 seconds, check the checkbox next to the **Refresh** button. To immediately refresh event data click the **Refresh** button or the refresh icon.

**Note** The amount of event data displayed on the Events page is limited by the data retention setting for events at. **ADMIN** > **System Management** > **Data Retention**.

## All Events Pane Filters

Use the preset filters in the All Events pane to only view those event types.

## Device Events

In the left pane, IoT FND tracks events for the following devices:

- Routers
- Endpoints
- Head-end Devices
- CR Mesh Devices
- NMS Servers
- Database Servers

## Event Severity Level

In the left pane, select an event severity level to filter the list view to devices with that severity level:

- Critical
- Major
- Minor
- Info

Each event type has a preset severity level. For example, a Router Down event is a Major severity level event.

### Filtering by Severity Level

To filter by severity level, click the pencil icon:

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

**Step 2** Click the **SEVERITY** show/hide arrow (left-pane).

**Note** Only those severity levels (**CRITICAL**, **MAJOR**, **MINOR**, or **INFO**) that have occurred display in the left pane under the SEVERITY heading.

**Step 3** Click a severity level to display all events of that severity level in the Events pane (right-pane).

### Preset Events By Device

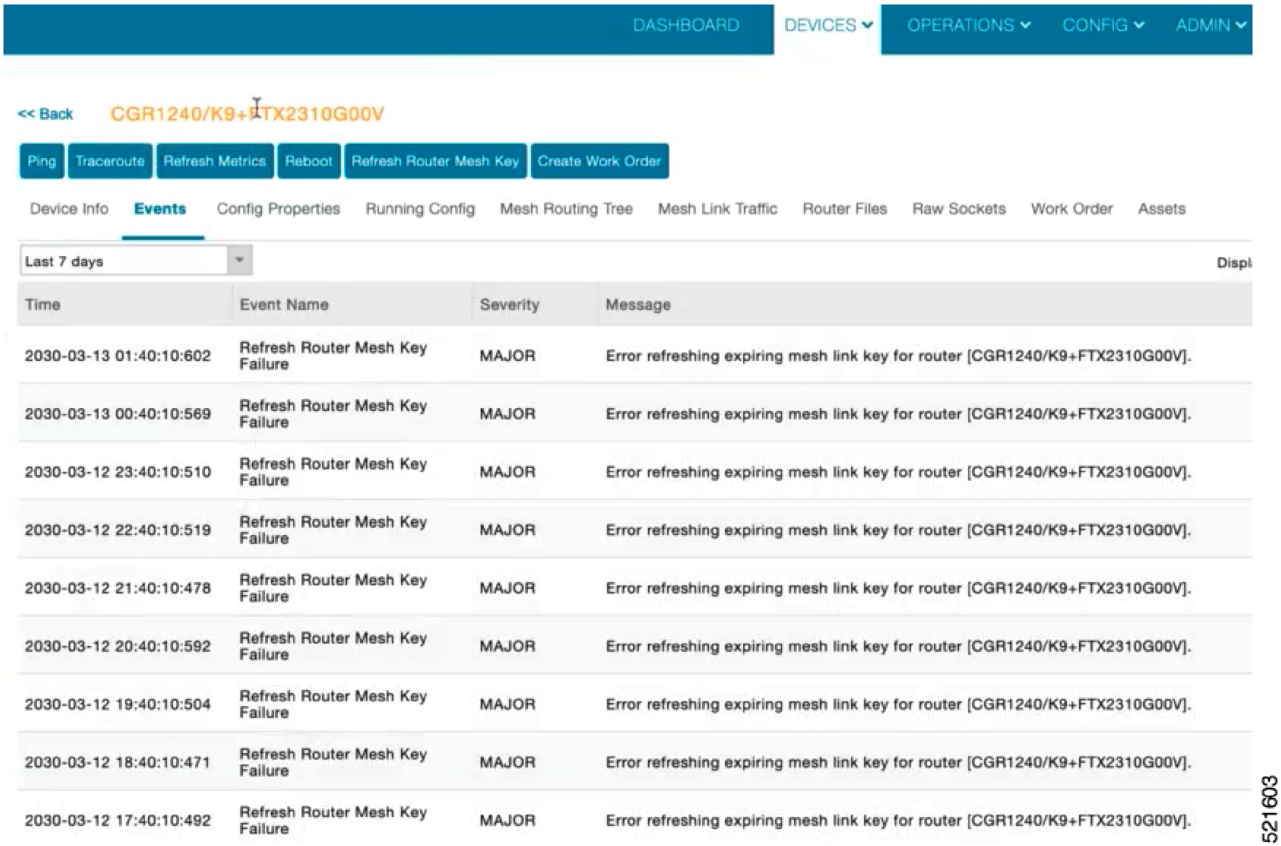
IoT FND has a preset list of events it reports for each device it tracks. A list of those events is summarized under each device in the left pane on the Events page. For example, in the left pane click the show/hide icon (  ) next to Routers to expand the list of all events for routers.

# Advanced Event Search

To use the filter to search for events:

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

*Figure 37: Searching for CGR1240 Events for the Past 7 Days*




**Step 2** Above the All Events heading (left pane), select a Relative (such as 7 days, 24 hours, 15 minutes) or Absolute (Day of the Week such as March 12) search time frame and an event category [SEVERITY | ROUTER or ENDPOINT} from the drop-down menu to narrow down your search. For example, you can select a SEVERITY option of MAJOR, MINOR or INFO and information for the chosen severity will display for all systems being managed by FND.

**Step 3** Click the **Show Filter** link at the top of the main pane.

**Step 4** Use the filter drop-down menus and fields to specify your search criteria.

**Step 5** Click the plus button (+) to add the search strings to the Search field.

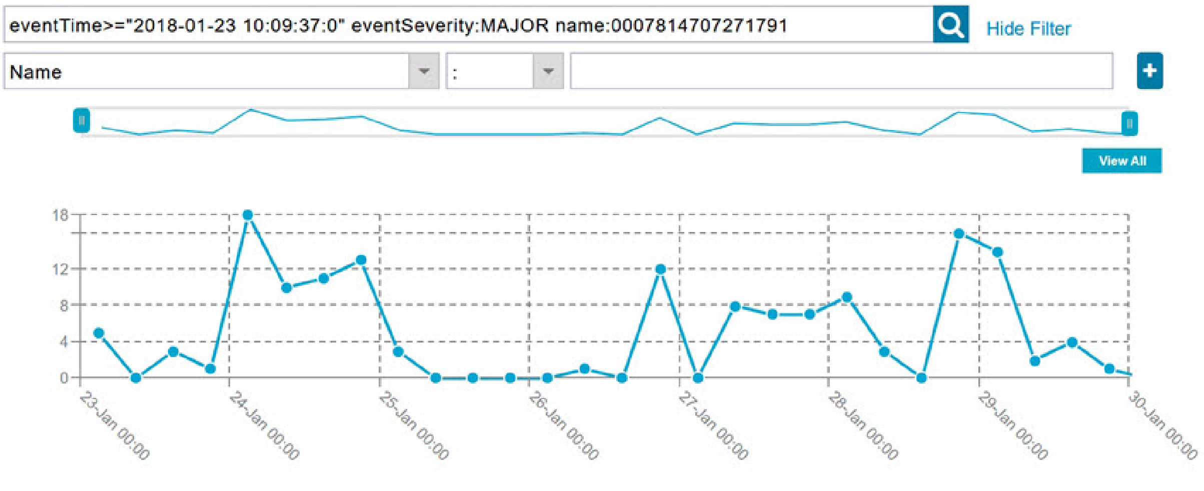
Repeat the process of adding search strings to the Search field as needed.

**Step 6** Click **Search Events** or press Enter.

The search results display in the Events pane.

You can also add search strings manually, as shown in the following examples:

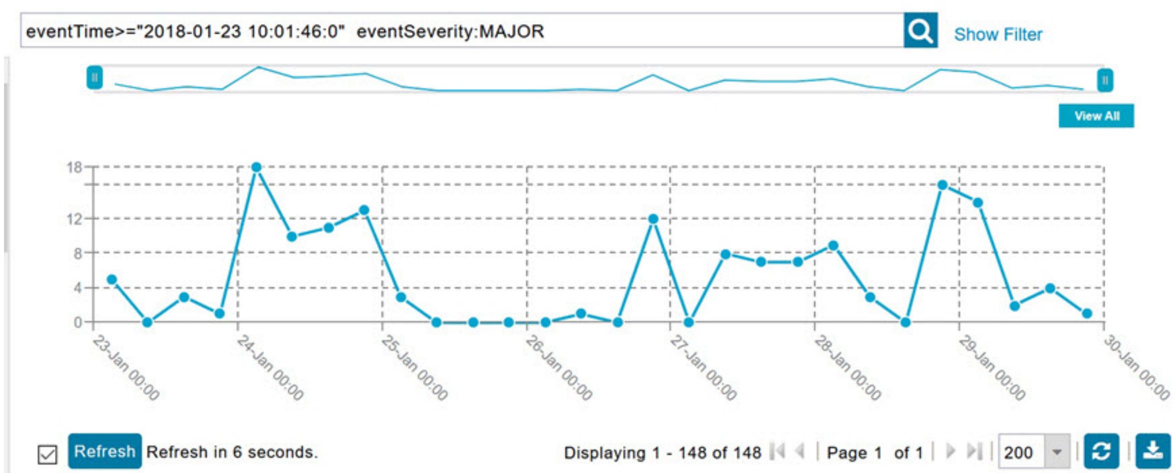
- To filter events by Name (EID), enter the following string in the Search Events field:
  - **name:** *router eid string*
  - Search Events by Name Filter




**Note** Note the use of the asterisk (*) wild card with this filter.

- To filter by event time period, enter the following string in the Search Events field, as shown in graph below:
  - **eventTime** *operator"YYYY-MM-DD HH:MM:SS:SSS"*
  - Supported operators are: <, >, >=, <=, :

  **Note** Do not enter a space between **eventTime** and the operator.




# Sorting Events

To sort events in ascending or descending order, roll over any column and select the appropriate option from the heading drop-down menu.

# Searching By Event Name

To search by event name (for example, Battery Low):

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

**Step 2** In the left pane, click the device type.

**Step 3** Click the **Show Filter** link at the top of the right pane to display the search fields.

**Step 4** Choose **Event Name** from the left drop-down menu.

**Step 5** Choose the event name from the options in the right drop-down menu.

**Step 6** Click the plus button (+) at the right to add the filter to the Search Events field.

The filter syntax appears in the Search Events field.

**Step 7** Click the **Search Events** button (magnifying glass icon).

The search results display in the Events pane.

# Searching by Labels

Allows you to search and filter events based on Label names tagged to Field Devices.

To search by labels:

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

**Step 2** Click **All Events** in the left pane.

**Step 3** Click the **Show Filter** link at the top of the right pane.

**Step 4** Choose **Label** from the left drop-down menu.

**Step 5** Choose the event name from the options in the right drop-down menu or create your own.

**Step 6** Click the plus button (+) at the right to add the filter to the Search Events field.

The filter syntax appears in the Search Events field.

**Step 7** Click the **Search Events** button (magnifying glass icon).

The search results display in the Events pane.

# Exporting Events

You can export events to a CSV file to examine as a log of event severity, time, name and event description by device.

To export events:

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

**Step 2** Click the desired severity level or device type in the left pane.

**Step 3** Click the **Export (+)** button .

A browser download session begins.

**Step 4** Navigate to your default download directory to access the CSV file.

# Events Reported

The table lists the events reported by IoT FND. Details include the event severity (Critical, Major, Minor, Information) and the devices that report those events.

*Table 77: Events Reported*

| Events | Devices | Severity |
|---|---|---|
| **CRITICAL EVENTS** | | |
| Certificate Expired | AP800, CGR1000, C800, FND, IR800 | Critical |
| DB FRA Space Critically Low | Database | Critical |
| DB Table Space Critically Low | Database | Critical |
| Invalid CSMP Signature | CGMESH, IR500 | Critical |
| Outage | Cellular, CGMESH, IR500 | Critical |
| RPL Tree Size Critical | CGR1000 | Critical |
| SD Card Removal Alarm | CGR1000 | Critical |
| **MAJOR EVENTS** | | |
| AAA Failure | C800, CGR1000, IR800 | Major |
| ACT2L Failure | C800, CGR1000, IR800 | Major |
| Archive Log Mode Disabled | Database | Major |
| Battery Failure | CGR1000 | Major |
| Battery Low | CGR1000, IR500 | Major |
| BBU Configuration Failed | IR500 | Major |
| BBU Firmware Download Failed | IR500 | Major |
| BBU Firmware Mismatch Found | CGR1000 | Major |
| BBU Firmware Upgrade Failed | IR500 | Major |
| BBU Lock Out | IR500 | Major |

| Events | Devices | Severity |
|---|---|---|
| BBU Power Off | IR500 | Major |
| Block Mesh Device Operation Failed | CGR1000 | Major |
| Certificate Expiration | AP800, C800, CGR1000, FND, IR800 | Major |
| DB FRA Space Very Low | Database | Major |
| Default Route Lost | CGMESH, IR500 | Major |
| Device Unknown | FND | Major |
| Door Open | C800, CGR1000, IR800, LORA | Major |
| Dot1X Authentication Failure | CGR1000 | Major |
| Dot1X Authentication Flood | C800, CGR1000, IR800 | Major |
| Down | AP800, ASR, C800, Cellular, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900, LORA | Major |
| Element Configuration Failed | C800,CGR1000, IR800 | Major |
| High CPU Usage | LORA | Major |
| High Flash Usage | LORA | Major |
| High Temperature | LORA | Major |
| HSM Down | FND | Major |
| Interface Down | ASR, ISR3900 | Major |
| Linecard Failure | C800, CGR1000, IR800 | Major |
| Line Power Failure | C800, CGR1000, IR800 | Major |
| Link Down | IR500 | Major |
| Low Flash Space | C800,CGR1000, IR800 | Major |
| Low Memory/Memory Low | C800,CGR1000, FND, IR800, LORA ( Memory Low) | Major |
| Low Temperature | LORA | Major |
| Mesh Connectivity Lost/ Node Connectivity Lost | CGMESH, IR500 | Major |

| Events | Devices | Severity |
| --- | --- | --- |
| Mesh Link Key Timeout/ Node Link Key Timeout | CGMESH, IR500 | Major |
| Metric Retrieval Failure | ASR, C800,CGR1000, IR800, ISR3900 | Major |
| Modem Temperature Cold Alarm | C800,CGR1000, IR800 | Major |
| Modem Temperature Warm Alarm | C800,CGR1000, IR800 | Major |
| Node Connectivity Lost | CGMESH, IR500 | Major |
| Node Link Key Timeout | CGMESH, IR500 | Major |
| Packet Forwarder Usage High | LORA | Major |
| Port Down | AP800, C800,CGR1000, IR800 | Major |
| Port Failure | AP800, C800,CGR1000, IR800 | Major |
| Refresh Router Mesh Key Failure | CGR1000, IR8100 | Major |
| RPL Tree Size Warning | CGR1000 | Major |
| Software Crash | C800,CGR1000, IR800 | Major |
| SSM Down | FND | Major |
| System Software Inconsistent | C800,CGR1000, IR800 | Major |
| Temperature Major Alarm | C800,CGR1000, IR800 | Major |
| Time Mismatch | CGMESH, IR500 | Major |
| Tunnel Down | C800,CGR1000, IR800 | Major |
| Tunnel Provisioning Failure | C800,CGR1000, IR800 | Major |
| Unknown WPAN Change | CGMESH, IR500 | Major |
| **MINOR EVENTS** | | |
| DB FRA Space Low | Database | Minor |
| Dot1X Re-authentication | CGMESH, IR500 | Minor |
| Temperature Minor Alarm | C800,CGR1000, IR800 | Minor |
| Temperature Low Minor Alarm | C800,CGR1000, IR800 | Minor |
| RPL Tree Reset | CGR1000 | Minor |
| **INFORMATION EVENTS** | | |
| Archive Log Mode Enabled | Database | Information |

| Events | Devices | Severity |
|---|---|---|
| Battery Normal | CGR1000 | Information |
| Battery Power | CGR1000 | Information |
| BBU Firmware Download Passed | CGR1000 | Information |
| Certificate Expiration Recovery | AP800, C800,CGR1000, FND, IR800 | Information |
| Cold Boot | AP800, C800,CGMESH, CGR1000, IR500, IR800 | Information |
| Configuration is Pushed | FND | Information |
| Configuration Rollback | AP800, C800,CGR1000, IR800 | Information |
| DB FRA Space Normal | Database | Information |
| DB Table Space Normal | Database | Information |
| Device Added | Cellular, C800,CGMESH, CGR1000, IR500, IR800 | Information |
| Device Location Changed | C800, CGR1000, IR800 | Information |
| Device Removed | Cellular, C800, CGMESH, CGR1000, IR500, IR800 | Information |
| Door Close | C800, CGR1000, IR800, LORA | Information |
| Dot11 Deauthenticate Send | C800, CGR1000, IR800 | Information |
| Dot11 Disassociate Send | C800, CGR1000, IR800 | Information |
| Dot11 Authentication Failed | C800, CGR1000, IR800 | Information |
| Hardware Insertion | C800, CGR1000, IR800 | Information |
| Hardware Removal | C800, CGR1000, IR800 | Information |
| High CPU Usage Recovery | LORA | Information |
| High Flash Usage Recovery | LORA | Information |
| High Temperature Recovery | LORA | Information |
| HSM Up | FND | Information |
| Interface Up | ASR, ISR3900 | Information |
| Line Power | C800, CGR1000, IR800 | Information |
| Line Power Restored | C800, CGR1000, IR800 | Information |
| Link Up | IR500 | Information |

| Events | Devices | Severity |
|---|---|---|
| Low Flash Space OK | C800, CGR1000, IR800 | Information |
| Low Memory OK/Low Memory Recovery | C800, CGR1000, IR800, LORA (Low Memory Recovery) | Information |
| Manual Close | ASR, Cellular, C800, CGMESH, CGR1000, IR500, IR800, ISR3900 | Information |
| Major RPL Tree Size Warning OK | CGR1000 | Information |
| Manual NMS Address Change | CGMESH, IR500 | Information |
| Manual Re-Registration | CGMESH, IR500 | Information |
| Mesh Certificate Change/ Node Certificate Change | CGMESH, IR500 | Information |
| Mesh Module Firmware Upgrade has been successful | CGR1000 | Information |
| Migrated To Better PAN | CGMESH, IR500 | Information |
| Modem Status Changed | LORA | Information |
| Modem Temperature Cold Alarm Recovery | C800, CGR1000, IR800 | Information |
| Modem Temperature Warm Alarm Recovery | C800, CGR1000, IR800 | Information |
| NMS Address Change | CGMESH, IR500 | Information |
| NMS Returned Error | CGMESH, IR500 | Information |
| Node Certificate Change | CGMESH, IR500 | Information |
| Packet Forwarded High Usage Recovery | LORA | Information |
| Packet Forwarder Status | LORA | Information |
| Packet Forwarded High Usage Recovery | LORA | Information |
| Port Up | AP800, C800, CGR1000, IR800 | Information |
| Power Source OK | C800, CGR1000, IR800 | Information |
| Power Source Warning | C800, CGR1000, IR800 | Information |
| Registered | ASR, ISR3900 | Information |
| Registration Failure | AP800, Cellular, C800, CGR1000, IR800, LORA | Information |

| Events | Devices | Severity |
|---|---|---|
| Registration Request | AP800, C800, CGR1000, IR800, LORA | Information |
| Registration Success | AP800, Cellular, C800, CGR1000, IR800, LORA | Information |
| Rejoined With New IP Address | CGMESH, IR500 | Information |
| Restoration | Cellular, CGMESH, IR500 | Information |
| Restoration Registration | CGMESH, IR500 | Information |
| RPL Tree Size Critical OK | CGR1000 | Information |
| Rule Event | ASR, C800, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900 | Information |
| SSM Up | FND | Information |
| Temperature Low Recovery | LORA | Information |
| Temperature Low Minor Alarm Recovery | C800, CGR1000, IR800 | Information |
| Temperature Major Recovery | C800, CGR1000, IR800 | Information |
| Temperature Low Major Alarm Recovery | C800, CGR1000, IR800 | Information |
| Temperature Minor Recovery | C800, CGR1000, IR800 | Information |
| Time Mismatch Resolved | CGMESH, IR500 | Information |
| Tunnel Provisioning Request | C800, CGR1000, IR800 | Information |
| Tunnel Provisioning Success | C800, CGR1000, IR800 | Information |
| Tunnel Up | C800, CGR1000, IR800 | Information |
| Unknown Event | AP800, ASR, C800, Cellular, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900, LORA | Information |
| Unknown Registration Reason | CGMESH, IR500 | Information |
| Unsupported | AP800, C800, CGR1000, IR800, LORA | Information |
| Up | AP800, ASR, C800, Cellular, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900, LORA, | Information |

| Events | Devices | Severity |
|---|---|---|
| Warm Start | IR500 | Information |
| WPAN Watchdog Reload | CGR1000 | Information |

# Monitoring Issues

This section provides an overview of issues and how to search for and close issues in IoT FND.

## Viewing Issues

IoT FND offers different ways to monitor issues:

The **OPERATIONS** > **ISSUES** page provides a snapshot of the health of the network by highlighting only major and critical issues that are active within the network.

You can also view the device information by clicking on one of the devices listed under router or endpoint on the left pane. The **Device Info** tab displays detailed information of the selected device along with the issues chart. You can view the issues chart of the device for default or custom-defined time intervals. For more information on viewing the chart for default or custom-defined time intervals, refer to Setting Time Filters To View Charts, on page 335.

The Figure 39: Issues Status Bar, on page 351 bar displays in the footer of the browser window and shows a count of all issues by severity for selected devices. You can set the device types for issues that display in the Issues status bar in User Preferences.

*Figure 38: OPERATIONS ISSUES*

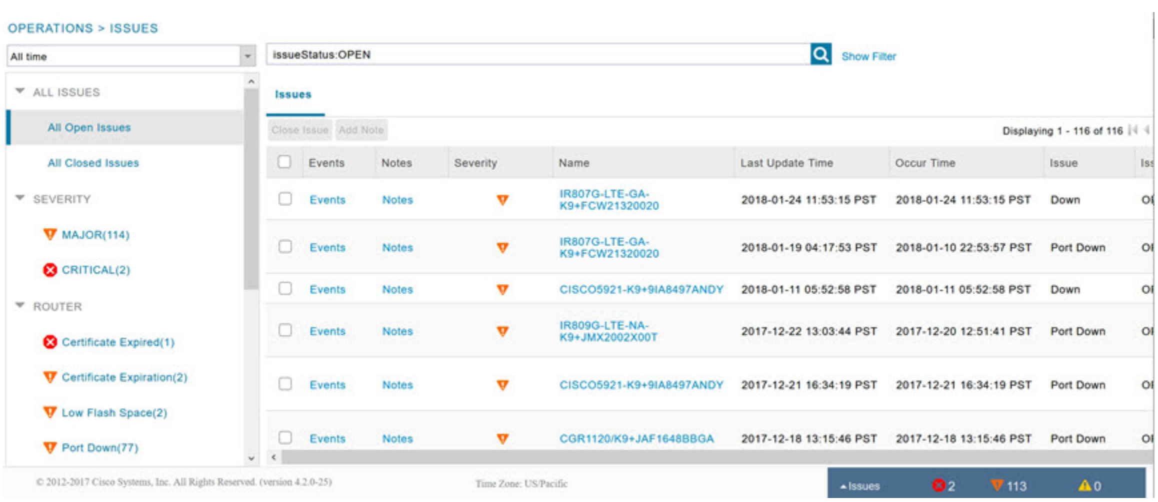


*Figure 39: Issues Status Bar*

The Issues page provides an abbreviated subset of unresolved network events for quick review and resolution by the administrator. Issues remain open until either the associated event is resolved (and IoT FND generates a resolution event) or the administrator manually closes the event.

Only one issue is recorded when multiple entries for the same event are reported. Each issue has a counter associated with it. As an associated event is closed, the counter decrements by one. Every open or closed issue has an associated event.

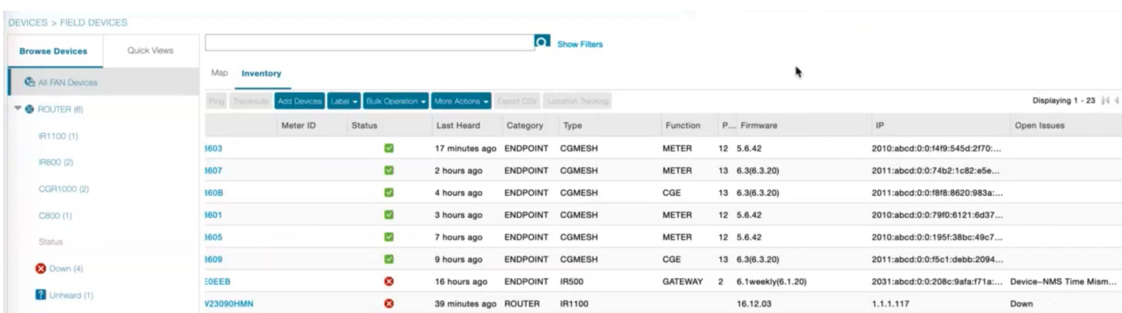
Click the Issues status bar to view the Issues Summary pane, which displays issues listed by the selected device category. Click count links in the Issues Summary pane to view complete issue criteria filtered by severity on the **OPERATIONS** > **Issues** page.

**Note** The closed issues data that displays on the Issues page is limited by the **Keep Closed Issues** for data retention setting (**ADMIN** > **System Management** > **Data Retention**), which is based on the time the issue was closed. When the issue was closed displays as the Last Update Time for the issue.

# Displaying Truncated Views of the OPERATIONS > Issues Page

At the **DEVICES** > **FIELD DEVICES** > **Browse Devices** > **Inventory** page, multiple entries of the same Open Issue (such as Device-NMS Time Mismatch, Down) for a given device will display as one entry only. This reduces multiple entries of the same Open Issue for a Field Device from filling up the display window.

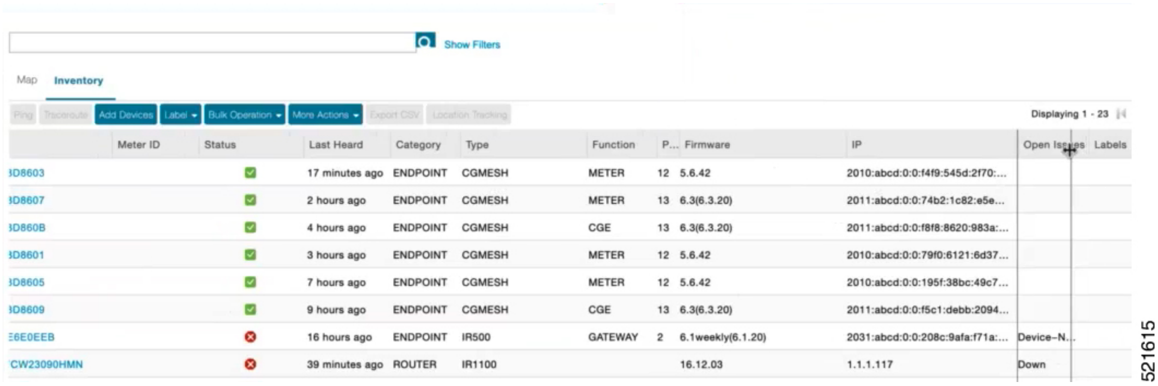
*Figure 40: DEVICES > FIELD DEVICES > Browse Devices > Inventory*




521614

At the **DEVICES** > **FIELD DEVICES** > **Browse Devices** > **Inventory** page, you can also minimize the width of the Open Issues column by clicking on the column and dragging the cursor to the left. For more information, refer to the Figure 41: DEVICES > FIELD DEVICES > Browse Devices > Inventory page with Open Issues Column Resized, on page 353 page with open issues column resized. To indicate that the column display has been reduced, the column displays three periods (...). You can later view the expanded view of that content by clicking on the column and expanding the column to the right. If you want to see more details for an Open Issue, you can go to the **OPERATIONS** > **Issues** page.

*Figure 41: DEVICES > FIELD DEVICES > Browse Devices > Inventory page with Open Issues Column Resized*




# Viewing Device Severity Status on the Issues Status Bar

A tally of issues listed by severity for the selected devices displays in the Issues status bar in the bottom-right of the browser window frame (Issue Status Bar). You can set the device types for issues that display in the Issues status bar in User Preferences.

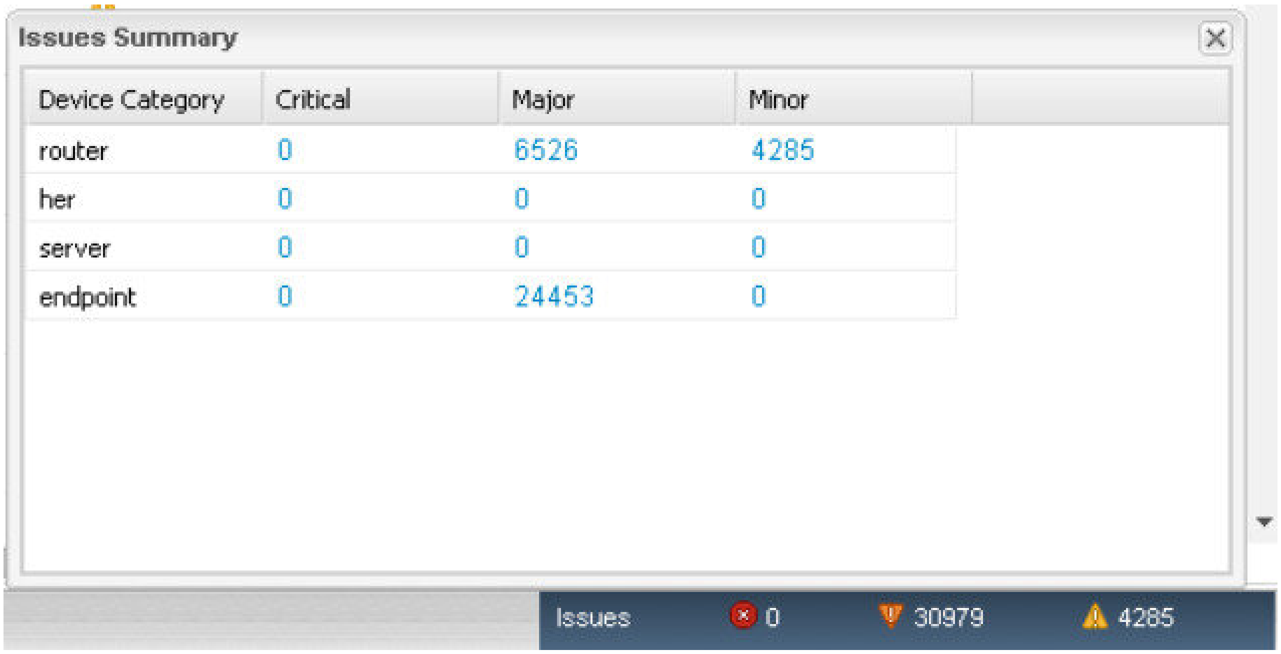
*Figure 42: Issues Status Bar*


To view the device severity status on the issue status bar:

**Step 1** Click the Issues status bar to view the Issues Summary pane, which displays issues listed by the selected device category.

**Step 2** Click the count links in the Issues Summary pane to view complete issue criteria filtered by severity on the **OPERATIONS** > **Issues** page.

*Figure 43: Issues Summary Pane*

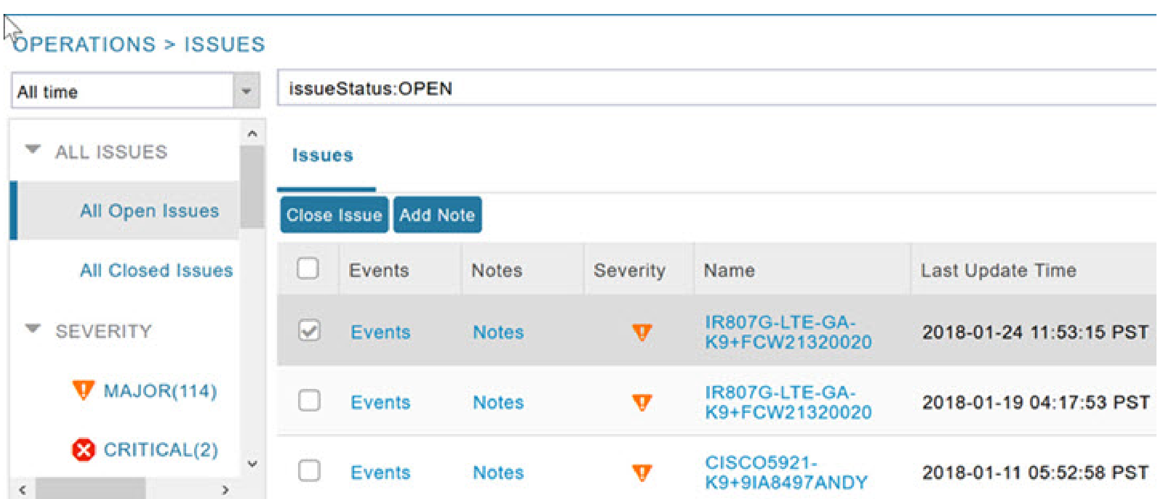



# Adding Notes to Issues

On the **OPERATIONS** > **Issues** page, you can add notes about Issues for a device.

Click the **Notes** link inline to access any notes entered for the Issue or add a note on the Notes for Issues Name page.

You can edit and delete notes from issues on this page. Issues can have multiple notes. Notes on the Issues Name page display the time the note was created, the name of the user who wrote the note, and the text of the note. You can also add a note when closing an Issue. Notes are purged from the database with the issue.



**Note** In some cases, existing notes may exist for the system and the Notes for Issues Name pane displays.

To add a note to an issue:

**Step 1** Click the **Notes** link inline or check the check box of the device and click **Add Note**.

The Notes for Issues Name pane displays.

**Step 2** Click **Add Note**.

The Add Note dialog displays.

**Step 3** Insert your cursor in the **Note** field and type your note.

**Step 4** Click **Add** when finished.

**To edit an existing note in an issue:**

a) Click the **Notes** link inline with the issue.

   The Notes for Issues Name pane displays.

b) Click the pencil icon at the right of the note that you want to edit.
c) Edit the note, and click **Done** when finished.

**To delete a note from an issue:**

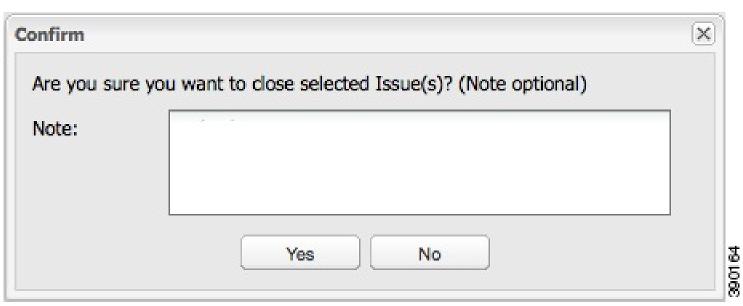
a) Click the **Notes** link inline with the issue.

   The Notes for Issues Name pane displays.

b) Click the red (X) icon at the right of the note.
c) Click **Yes** to confirm the deletion.

**To add a note when closing an issue:**

a) At the **Operations** > **Issues** page, check the box next to the issue you are closing.
b) Click the **Close Issue** button that appears above the event listings.
c) In the Confirm dialog box, insert your cursor in the Note field and type the note text.




d) To confirm that you want to close the issue and save the note, click **Yes**.

# Searching Issues Using Predefined Filters

To search for open issues for a specific system or severity level:

**Step 1** Choose **OPERATIONS** > **Issues**.

To list only open issues, click **All Open Issues** (left pane).

**Note** By default, IoT FND displays all issues that occurred within the specified data retention period (see Configuring Data Retention, on page 68):

- To see Closed Issues associated with an event type or severity level, change **issueStatus:OPEN** to **issueStatus:CLOSED** in the Search Issues field, and then click **Issues Search**.
- To list all closed issues, in the left pane, click **All Closed Issues**.

**Step 2** Click a device category, event type, or severity level to filter the list.

The filter syntax appears in the Search Issues field, and the search results display in the main pane.

# Search Issues Using Custom Filters

To search by creating custom filters:

**Step 1** Choose **OPERATIONS** > **Issues**.

**Step 2** Click **Show Filter**.

**Step 3** From the Filter drop-down menus, choose the appropriate options.

For example, to filter Severity levels by Name (EID):

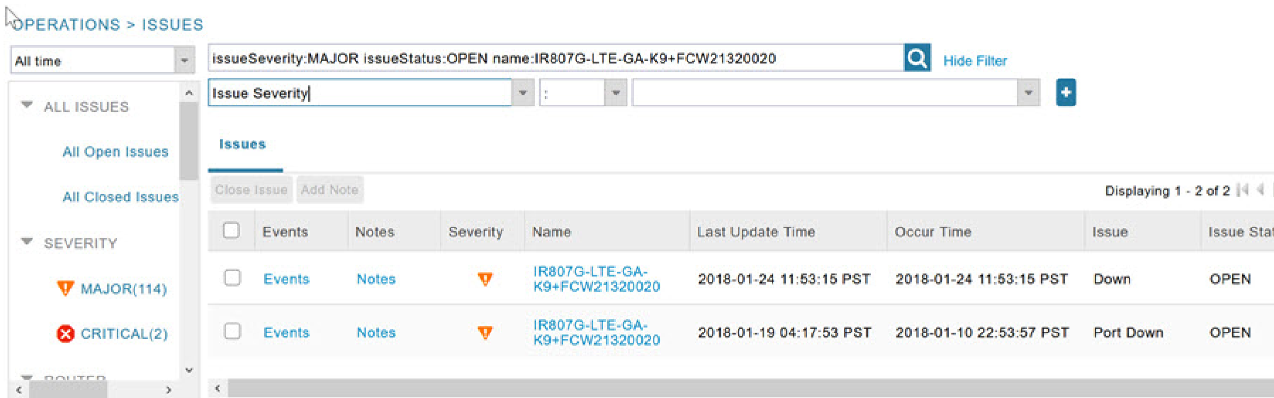
- In the left pane, select a Severity level (such as Major). The filter name populates the first field (top) of the Filter.
- From the second Filter drop-down menu on the left, choose **Name**.
- In the third Filter field, enter the EID of the device to discover issues about.
- Click the search icon (magnifying glass) to begin the search.

You can also enter the search string in the Search Issues field.

For example: issueSeverity:MAJOR issueStatus:OPEN name:IR807G-LTE-GA-K9+FCW21320020

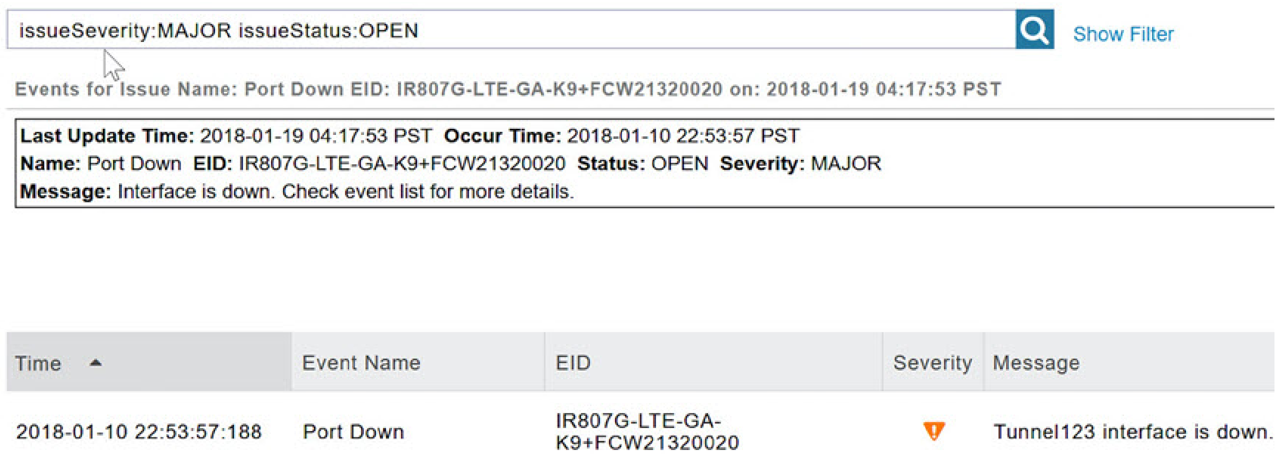
**Step 4** Click **Search Issues**.

The issues, if any, display in the Search Issues section (right pane).




**Step 5** Click the **Events** link to display events associated with an issue.

The Events for Issue Name pane displays all events for that device.




**Step 6** Click **Search Issues** or any link in the left pane to return to the Issues pane.

# Closing an Issue

In most cases, when an event is resolved, the issue is closed automatically by the software. However, when the administrator has actively worked on resolving the issue, it might make sense to close the issue directly. When the issue is closed, IoT FND generates an event.

To close a resolved issue:

**Step 1** Choose **OPERATIONS** > **Issues**.

**Step 2** Locate the issue by following the steps in either the Searching Issues Using Predefined Filtersor Search Issues Using Custom Filters, on page 356 section.

**Step 3** In the Search Issues section (right pane), check the check boxes of the issues to close.

**Step 4** Click **Close Issue**.

**Note** You can also add a note to the issue at this time.

**Step 5** Click **Yes**.

# Viewing Device Charts

This section explains about the router and mesh endpoint charts.

## Router Charts

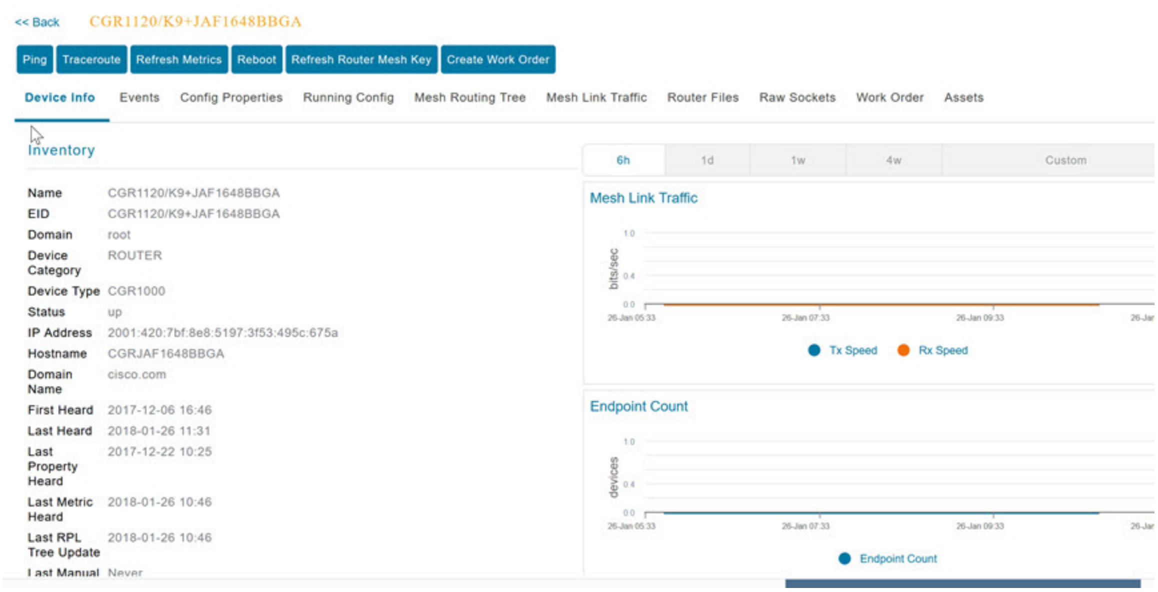
IoT FND provides these charts in the Device Info pane on the Device Details page for any router:

*Table 78: Device Detail Charts*

| Chart | Description |
|---|---|
| Link Traffic | Shows the aggregated WPAN rate for a router over time.<br>To view the chart for default or custom-defined time intervals, refer to Setting Time Filters To View Charts, on page 335. |
| Mesh Endpoint Count | Shows the number of MEs over time. |
| Cellular Link Metrics | Shows the metrics (transmit and receive speed), RSSI, Bandwidth Usage (current Billing Cycle) for all logical cellular GSM and CDMA interfaces. |
| Cellular Link Settings | Shows properties for cellular physical interfaces with dual and single modems. |
| Cellular Link Traffic | Shows the aggregated WPAN rate per protocol over time. |
| Cellular RSSI | Cellular RSSI. |
| WiMAX Link Traffic | Shows the receiving and sending rates of the WiMAX link traffic for the router over time. |
| WiMAX RSSI | Shows the receiving and sending rates of the WiMAX RSSI traffic for the router over time. |
| Ethernet Link Traffic | Shows the receiving and sending rates of the Ethernet traffic for the router over time. |
| Cellular Bandwidth Usage Over Time | Shows the bandwidth usage over time for the cellular interface. |
| Ethernet Bandwidth Usage Over Time | Shows the bandwidth usage over time for the Ethernet interface. |

The Router Device Page provides information on the router device.

*Figure 44: Router Device Page*




# Mesh Endpoint Charts

IoT FND provides the device detail charts in the Device Info pane on the Device Details page for any mesh endpoint.

*Table 79: Device Detail Charts*

| Chart | Description |
|---|---|
| Link Traffic | Shows the aggregated WPAN rate for an endpoint over time.<br>To view the chart for default or custom-defined time intervals, refer to Setting Time Filters To View Charts, on page 335 |
| Path Cost and Hops | Shows the RPL path cost value between the element and the root of the routing tree over time (see Configuring RPL Tree Polling). |
| Link Cost | Shows the RPL cost value for the link between the element and its uplink neighbor over time. |
| RSSI | Shows the measured RSSI value of the primary mesh RF uplink (dBm) over time. |

*Figure 45: Mesh Endpoint Device Info Page (partial view)*

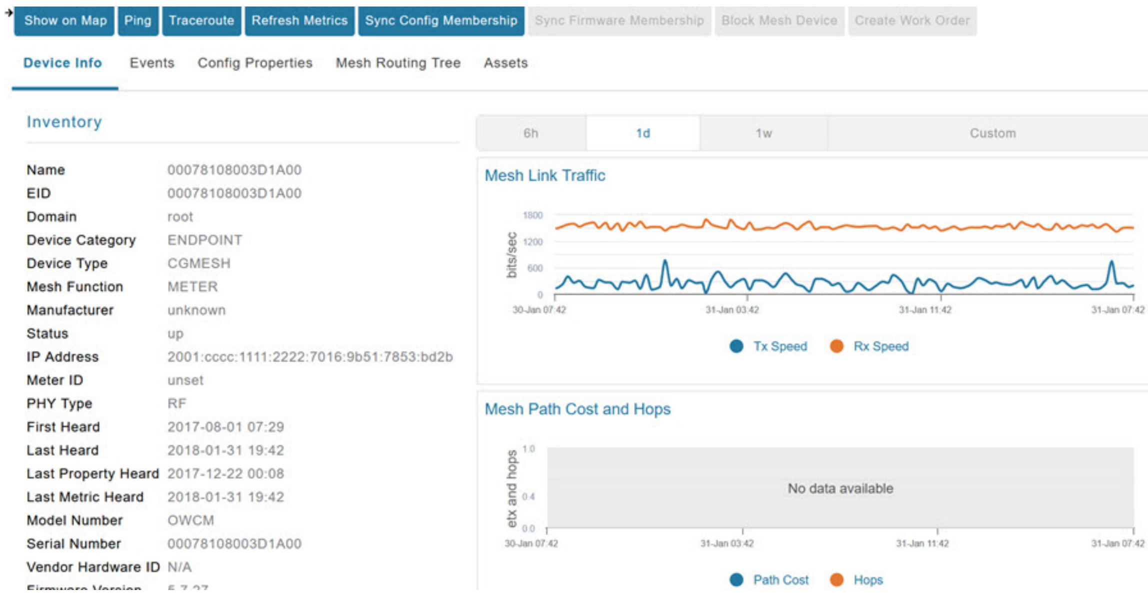
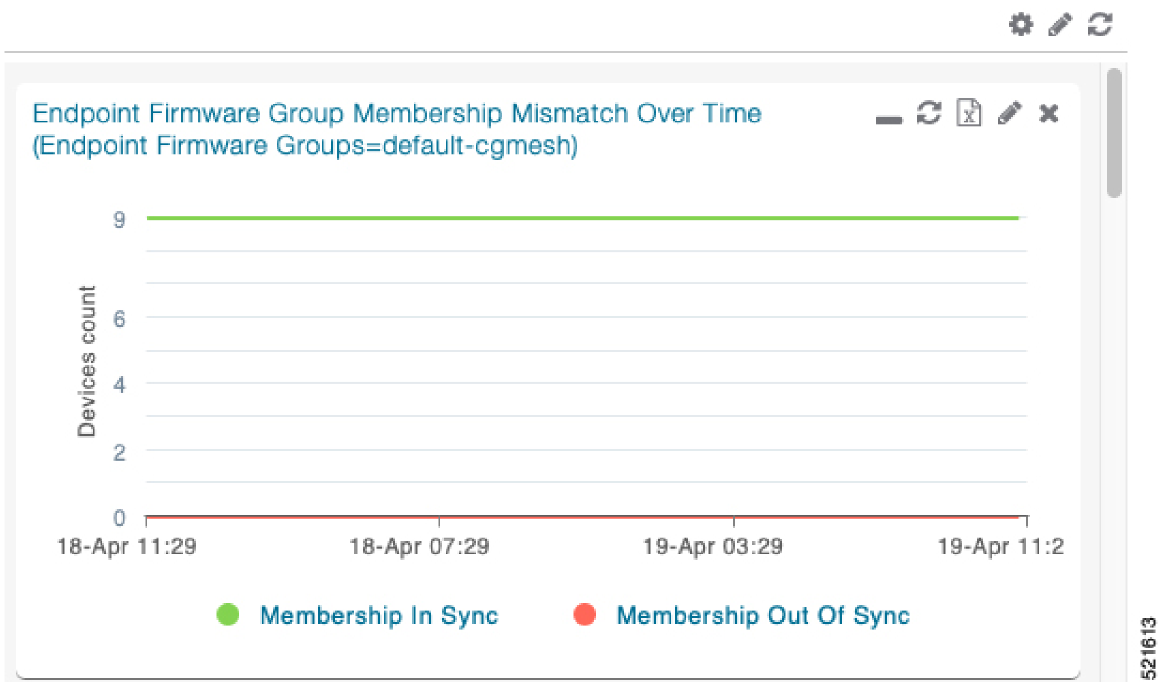



*Figure 46: Mesh Endpoint Firmware Group Mismatch Over Time Page*



CHAPTER 9

# Integrating Third-Party Endpoints in the Cisco IoT FND through CSMP

The CoAP Simple Management Protocol (CSMP) stack is open sourced as Open CSMP which allows the Cisco partners to register their endpoint devices in the Cisco IoT FND. The CSMP stack is a preferred lightweight communication protocol that encourages the community and vendors to use FND as their preferred NMS. While registering their devices, the partners can define their own set of metadata files for capturing metric, property, event, or issue types for the new device type.

In phase 1 of third-party generic endpoint integration, Cisco IoT FND 4.8.1 release supports only the registration process. Periodic notification handling, firmware upgrade, config push, mark down job, licensing, and other features will be developed in the upcoming releases.

***Table 80: Feature History***

| Feature Name | Release Information | Description |
| --- | --- | --- |
| Integrating Third-Party Endpoints in the Cisco IoT FND through CSMP | IoT FND 4.8.1 | The CSMP code is shared with the Cisco partners which helps the partners to register their endpoint devices in the Cisco IoT FND. When registering their devices, they can define their own set of metadata files for capturing metric, property, event, or issue types for the new device type. |



# Registering Third-Party Devices in IoT FND

For each device type to be added, multiple separate metadata files are available as templates under the endpoint-meta-templates directory. This directory is available when you install or upgrade to the latest Cisco IoT FND 4.8.1 version.

**Step 1** In the `opt/cgms/server/cgms/conf` directory, you can view the list of required templates to create an endpoint.

- defaultdeviceTypeTemplate.json.template
- defaultdeviceTypeTemplateNoIPRoute.json.template
- deviceTypeEventTypes.xml.template
- deviceTypeIssueTypes.xml.template
- deviceTypeMeta.json.xml.template
- deviceTypeMetricTypes.xml.template
- deviceTypePropertyTypes.xml.template
- deviceTypeSystemRules.xml.template

**Step 2** Run the `addGenericEndpoints.sh` script in `opt/cgms/bin` directory. The system prompts for the device type name.

**Step 3** Provide the device type name. The script creates the endpoint-meta directory under `opt/cgms/server/cgms/conf` directory, if not present already. If the name of the new device type is provided as endpointdevice1, then the sub directory is created under endpoint-meta directory:

opt/cgms/server/cgms/conf/endpoint-meta/endpointdevice1

The `addGenericEndpoints.sh` script copies all the template files from endpoint-meta-templates directory, renames them as per the device type name provided and moves it under new device type directory. The below example shows how the files will be renamed when the device type name is provided as endpointdevice1:

- defaultendpointdevice1Template.json
- defaultendpointdevice1TemplateNoIPRoute.json
- endpointdevice1EventTypes.xml
- endpointdevice1IssueTypes.xml
- endpointdevice1Meta.json.xml
- endpointdevice1MetricTypes.xml
- endpointdevice1PropertyTypes.xml
- endpointdevice1SystemRules.xml

**Note** Addition of new template files or removal of existing set of template files is not allowed.

**Step 4** Edit the `endpointdevice1Meta.json` file for registration of new device by providing values in the required fields.

```
{
 “device_info”: {
 “device_type”: “ ”,
 “device_function”: “ “,
 “device_description”: “ “,
 “display_string”: “ “,
 “pids”: [ ] ,
```

```
 "device_actions": [
 "reboot",
  "ping",
 "traceroute",
 "inventory",
     ]
   }
}
```

The description for each field is provided below.

| Field | Description |
|---|---|
| device_type | Enter alphanumeric characters for the name of the device type to be registered (for example, endpointdevice1). |
| device_function | Mention any of the existing mesh functions. The list of device functions currently supported in IoT FND are meter, extender, gateway, cge, root, controller, sensor, networknode, gasmeter. |
| device_description | Provide a brief information about the device type. |
| display_string | Enter only the display name for the endpoint device as it is displayed in the left side tree in Field Devices page under Endpoint category. The display string is in the format of <device function>-<display string> (for example, METER-ENDPOINTDEVICE1). The device function is obtained from the function entered by you. |
| pids | Enter the device pids as comma separated values (for example, "spid1", "spid2"). |
| device_actions | The actions that can be performed on the Device Details page are Show on Map, Ping, Traceroute, Refresh Metrics, Reboot, Sync Config Membership. |

**Step 5** Start Cisco IoT FND after adding or updating the metadata files. The Cisco IoT FND reads the endpoint-meta directory and creates the appropriate tables for each device type. If any issues occur during startup, it logs the errors in server.log and continues with the startup process.

**Step 6** After you restart the Cisco IoT FND, import the CSV file to add devices. For more information on adding endpoints, seenAdding Routers, Head-End Routers, IC3000 Gateway, Endpoint and Extenders and IR500 in Bulk. On addition, the device gets listed under Endpoints Category in the Field Devices page.

# Registering Devices in Cluster Environment

The devices are registered in IoT FND by executing the `addGenericEndpoints.sh` script and creating the endpoint-meta directory. You can edit the **devicetypeMeta.json** file in the endpoint-meta directory to add the device details and restart IoT FND. In a cluster,

- Run the script and add the device types in various IoT FND instances.
- Restart the service of all IoT FND instances that are part of the cluster.

On restart, IoT FND picks up the device types that are added in all the IoT FND instances.

# Adding Property Types, Metric Types, and Issue Types

To add mesh property types, mesh metric types, event types, and issue types for the newly registered device:

**Step 1** Create a new device type using the script, if not done already.

**Step 2** Edit the json or xml files present in the new device type directory for newer metric, property, event, or issue types.

For example, if you want to include other metric types apart from the available list, you can edit the existing template and include other metric types. The same applies for property types, event types, issue types, and system rules as well.

**Note** Restart IoT FND after editing the metadata files.

## Mesh Property Types

The following is a sample list of mesh property types for the end point device.


```
<?xml version="1.0" encoding="UTF-8" ?>
<cgms xmlns="http://www.w3schools.com"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://www.w3schools.com propertyTypes.xsd">
  <propertyTypes kind="cgmesh">
    <propertyType>
      <name>meshAddress</name>
      <displayName>Mesh Link IP Address</displayName>
     <description>The IP address of the mesh link. Assigned automatically by the NMS during
 registration</description>
    </propertyType>
    <propertyType>
      <name>meshLocalAddress</name>
      <displayName>Mesh Link Local Address</displayName>
      <description>The local WPAN address of the mesh link. Assigned automatically by the
NMS during registration</description>
    </propertyType>
    <propertyType>
      <name>meshPrefix</name>
      <displayName>Mesh Link Prefix</displayName>
      <description>The subnet prefix address</description>
    </propertyType>
    <propertyType>
      <name>meshPrefixLength</name>
      <displayName>Mesh Link Prefix Length</displayName>
      <description>The subnet prefix address length</description>
    </propertyType>
    <propertyType>
      <name>meshSsid</name>
      <displayName>SSID</displayName>
      <description>The mesh SSID</description>
    </propertyType>
    <propertyType>
      <name>meshPanid</name>
      <displayName>PANID</displayName>
      <description>The subnet PAN ID</description>
    </propertyType>
    <propertyType>
      <name>meshTxPower</name>
```

```
      <displayName>Transmit Power</displayName>
      <description>The mesh transmit power</description>
    </propertyType>
    <propertyType>
      <name>meshSecMode</name>
      <displayName>Security Mode</displayName>
      <description>Mesh Security mode: 0 indicates none, 1 indicates 802.1x with 802.11i
key management</description>
    </propertyType>
    <propertyType>
      <name>meterId</name>
      <displayName>Meter Id</displayName>
      <description>The Meter Id of comm module</description>
    </propertyType>
    <propertyType>
      <name>meterCert</name>
      <displayName>Meter Certificate</displayName>
      <description>The subject name of the meter certificate</description>
    </propertyType>
    <propertyType>
      <name>toneMapFwdModulation</name>
      <displayName>Mesh Tone Map Forward Modulation</displayName>
      <description>Mesh tone map forward modulation: 0 = 'Robo', 1 = 'DBPSK', 2 = 'DQPSK',
 3 = 'D8PSK'</description>
    </propertyType>
    <propertyType>
      <name>toneMapFwdMap</name>
      <displayName>Mesh Tone Map Forward Map</displayName>
      <description>Mesh tone map forward map bit vector, e.g.,
"0011000011100111"</description>
    </propertyType>
    <propertyType>
      <name>toneMapRevModulation</name>
      <displayName>Mesh Tone Map Reverse Modulation</displayName>
      <description>Mesh tone map reverse modulation: 0 = 'Robo', 1 = 'DBPSK', 2 = 'DQPSK',
 3 = 'D8PSK'</description>
    </propertyType>
    <propertyType>
      <name>toneMapRevMap</name>
      <displayName>Mesh Tone Map Reverse Map</displayName>
      <description>Mesh tone map reverse map bit vector, e.g.,
"0011000011100111"</description>
    </propertyType>
    <propertyType>
      <name>manufacturer</name>
      <displayName>Manufacturer of the Endpoints</displayName>
      <description>Manufacturer of the endpoint as reported through CSMP from the
mesh</description>
    </propertyType>
    <propertyType>
      <name>physicalDescr</name>
      <displayName>Physical Description</displayName>
      <description>Description of the hardware</description>
    </propertyType>
    <propertyType>
   <name>bbuPresent</name>
      <displayName>BBU Present</displayName>
      <description>Battery Backup is present.</description>
    </propertyType>
    <propertyType>
      <name>bbuReady</name>
      <displayName>BBU Ready</displayName>
      <description>Battery Backup Unit is ready.</description>
    </propertyType>
```

```
    <propertyType>
      <name>powerSource</name>
      <displayName>Power Source</displayName>
      <description>The current power source of the device.</description>
    </propertyType>
    <propertyType>
      <name>batteryState</name>
      <displayName>Battery State</displayName>
      <description>The current battery state of the device.</description>
    </propertyType>
    <propertyType>
      <name>lastRegReason</name>
      <displayName>Last Registration Reason</displayName>
      <description>Reason for the most recent device registration</description>
      <propertyValueMap text="unknown" value="0"/>
      <propertyValueMap text="Cold boot" value="1"/>
      <propertyValueMap text="Manual re-registration" value="2"/>
      <propertyValueMap text="Rejoined with new IP" value="3"/>
      <propertyValueMap text="NMS address changed" value="4"/>
      <propertyValueMap text="Redirected NMS address" value="5"/>
      <propertyValueMap text="NMS error" value="6"/>
      <propertyValueMap text="Certificate changed" value="7"/>
      <propertyValueMap text="Power restoration" value="8"/>
      <propertyValueMap text="Parent node changed" value="9"/>
      <propertyValueMap text="Firmware updated" value="10"/>
    </propertyType>
    <propertyType>
      <name>previousMeshPanid</name>
      <displayName>Previous PANID</displayName>
      <description>The previous subnet PAN ID</description>
    </propertyType>
    <propertyType>
      <name>useCoap6</name>
      <displayName>Use CoAP Version 6</displayName>
      <description>Device is using CoAP version 6 for management messages</description>
    </propertyType>
    <propertyType>
      <name>meshProtocol</name>
      <displayName>Mesh Protocol</displayName>
      <description>Display the Mesh Protocol</description>
          <propertyValueMap text="Pre Wi-SUN" value="0"/>
          <propertyValueMap text="Wi-SUN 1.0" value="1"/>
    </propertyType>
    <propertyType>
      <name>sdkVersion</name>
      <displayName>SDK Version</displayName>
      <description>SDK version of the device</description>
    </propertyType>
    <propertyType>
      <name>patchCapability</name>
      <displayName>Patch Capability</displayName>
      <description>Patch Capability including patch support, version, window size and
lookahead size</description>
    </propertyType>
    <propertyType>
      <name>patchChopSize</name>
      <displayName>Patch Chop Size</displayName>
      <description>Maximum Chop Size nodes can support</description>
    </propertyType>
    <propertyType>
      <name>patchVolumeSize</name>
      <displayName>Patch Volume Size</displayName>
      <description>Patch Volume size</description>
    </propertyType>
```

```
    <propertyType>
      <name>certAutoRenewSettings</name>
      <displayName>Certificate Auto Renew Settings</displayName>
      <description>Display the Certificate Renew Settings</description>
    </propertyType>
    <propertyType>
      <name>aclInterfaceNameLp</name>
      <displayName>Interface Name</displayName>
      <description>Interface Name for Low Pan Interface</description>
    </propertyType>
    <propertyType>
      <name>aclDroppedCounterLp</name>
      <displayName>Dropped Counter</displayName>
      <description>Dropped Counter for Low Pan Interface</description>
    </propertyType>
    <propertyType>
      <name>aclDroppedSrcIpLp</name>
      <displayName>Dropped Source IP</displayName>
      <description>Dropped Source IP for Low Pan Interface</description>
    </propertyType>
    <propertyType>
      <name>aclDroppedDstIpLp</name>
      <displayName>Dropped Destination IP</displayName>
      <description>Dropped Destination IP for Low Pan Interface</description>
    </propertyType>
    <propertyType>
      <name>aclProtocolLp</name>
      <displayName>Protocol</displayName>
      <description>Protocol for Low Pan Interface</description>
    </propertyType>
    <propertyType>
      <name>aclDirectionLp</name>
      <displayName>Direction</displayName>
      <description>Direction for Low Pan Interface</description>
    </propertyType>
    <propertyType>
      <name>aclSrcPortLp</name>
      <displayName>Source Port</displayName>
      <description>Source Port for Low Pan Interface</description>
    </propertyType>
    <propertyType>
      <name>aclDstPortLp</name>
      <displayName>Destination Port</displayName>
      <description>Destination Port for Low Pan Interface</description>
    </propertyType>
    <propertyType>
      <name>aclMaxRateLimit</name>
      <displayName>ACL Max Rate Limit (kb/s)</displayName>
      <description>ACL Max Rate Limit used for Rate Limit validation</description>
    </propertyType>
  </propertyTypes>
</cgms>
```

# Mesh Metric Types

The following is a sample list of mesh metric types for the end point device.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cgms xmlns="http://www.w3.org"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <metricTypes kind="cgmesh">
    <metricType>
      <name>uptime</name>
```

```
      <valueType>gauge</valueType>
      <displayName>Uptime</displayName>
      <unit>sec</unit>
      <description>The amount of time in seconds that the element has been running since
last boot</description>
      <lowerBound>0</lowerBound>
      <upperBound>31536000</upperBound>
      <displayFormat>secondsToTime</displayFormat>
    </metricType>
    <metricType>
      <name>meshTxSpeed</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Link Transmit Speed</displayName>
      <unit>bits/sec</unit>
     <description>The current speed of data transmission over the uplink network interface,
 measured in bits per second, averaged over a short element-specific time period (e.g. an
hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
      <displayFormat>###,###</displayFormat>
    </metricType>
    <metricType>
      <name>meshTxDrops</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Link Transmit Packet Drops</displayName>
      <unit>drops/sec</unit>
      <description>The rate of packets that were dropped while trying to transmit on the
uplink interface because the outbound queue was full</description>
      <lowerBound>0</lowerBound>
      <upperBound>1</upperBound>
      <displayFormat>###,###</displayFormat>
    </metricType>
    <metricType>
      <name>meshRxSpeed</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Link Receive Speed</displayName>
      <unit>bits/sec</unit>
     <description>The rate of data that has been received by the uplink network interface,
 measured in bits per second, averaged over a short element-specific time period (e.g. an
hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
      <displayFormat>###,###</displayFormat>
    </metricType>
    <metricType>
      <name>meshRxReassemblyDrops</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Link Receive Packet Reassembly Drops</displayName>
      <unit>drops/sec</unit>
      <description>The rate of incoming packet fragments that were dropped because there
was no space in the reassembly buffer</description>
      <lowerBound>0</lowerBound>
      <upperBound>1</upperBound>
    </metricType>
    <metricType>
      <name>meshHops</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Route RPL Hops</displayName>
      <unit>hops</unit>
      <description>The number of hops that the element is from the root of its RPL routing
 tree</description>
      <lowerBound>1</lowerBound>
      <upperBound>8</upperBound>
      <displayFormat>###</displayFormat>
```

```
    </metricType>
    <metricType>
      <name>meshLinkCost</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Route RPL Link Cost</displayName>
      <unit></unit>
      <description>The RPL cost value for the link between the element and its uplink
neighbor</description>
      <lowerBound>1</lowerBound>
      <upperBound>3</upperBound>
      <invalidValue>65535</invalidValue>
      <displayFormat>###.##</displayFormat>
    </metricType>
    <metricType>
      <name>meshAbsolutePhase</name>
      <valueType>gauge</valueType>
      <displayName>Mesh absolute phase of power</displayName>
      <unit></unit>
      <description>Relative position of current and voltage waveforms for a PLC
Node</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <name>meshPathCost</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Route RPL Path Cost</displayName>
      <unit></unit>
      <description>The RPL path cost value between the element and the root of the routing
 tree</description>
      <lowerBound>1</lowerBound>
      <upperBound>24</upperBound>
      <invalidValue>65535</invalidValue>
      <displayFormat>###.##</displayFormat>
    </metricType>
    <metricType>
      <name>meshRssi</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Route RSSI</displayName>
      <unit>dBm</unit>
      <description>The measured RSSI value of the primary mesh RF uplink</description>
      <lowerBound>-80</lowerBound>
      <upperBound>20</upperBound>
      <invalidValue>-128</invalidValue>
    </metricType>
    <metricType>
      <name>meshReverseRssi</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Route Reverse RSSI</displayName>
      <unit>dBm</unit>
     <description>The RSSI value measured by the element's mesh uplink neighbor</description>

      <lowerBound>-80</lowerBound>
      <upperBound>20</upperBound>
      <invalidValue>-128</invalidValue>
    </metricType>
    <metricType>
      <name>toneMapFwdTxResRaw</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Tone Map Forward Tx Res Raw</displayName>
      <unit></unit>
      <description>The txres field integer value in tone map forward message</description>
      <lowerBound>-1000</lowerBound>
      <upperBound>1000</upperBound>
```

```
</metricType>
<metricType>
  <name>toneMapFwdTxGainRaw</name>
  <valueType>gauge</valueType>
  <displayName>Mesh Tone Map Forward Tx Gain Raw</displayName>
  <unit></unit>
  <description>The txres gain integer value in tone map forward message</description>
  <lowerBound>-1000</lowerBound>
  <upperBound>1000</upperBound>
</metricType>
<metricType>
  <name>toneMapFwdTxGain</name>
  <valueType>gauge</valueType>
  <displayName>Mesh Tone Map Forward Tx Gain</displayName>
  <unit></unit>
  <description>Equals to txResRaw * txResGain</description>
  <lowerBound>-1000000</lowerBound>
  <upperBound>1000000</upperBound>
</metricType>
<metricType>
  <name>toneMapFwdToneQuality</name>
  <valueType>gauge</valueType>
  <displayName>Mesh Tone Map Forward Tone Quality</displayName>
  <unit></unit>
  <description>The number of bits set in the tone map forward vector</description>
  <lowerBound>0</lowerBound>
  <upperBound>24</upperBound>
</metricType>
<metricType>
  <name>toneMapRevTxResRaw</name>
  <valueType>gauge</valueType>
  <displayName>Mesh Tone Map Reverse Tx Res Raw</displayName>
  <unit></unit>
  <description>The txres field integer value in tone map reverse message</description>
  <lowerBound>-1000</lowerBound>
  <upperBound>1000</upperBound>
</metricType>
<metricType>
  <name>toneMapRevTxGainRaw</name>
  <valueType>gauge</valueType>
  <displayName>Mesh Tone Map Reverse Tx Gain Raw</displayName>
  <unit></unit>
  <description>The txres gain integer value in tone map reverse message</description>
  <lowerBound>-1000</lowerBound>
  <upperBound>1000</upperBound>
</metricType>
<metricType>
  <name>toneMapRevTxGain</name>
  <valueType>gauge</valueType>
  <displayName>Mesh Tone Map Reverse Tx Gain</displayName>
  <unit></unit>
  <description>Equals to txResRaw * txResGain</description>
  <lowerBound>-1000000</lowerBound>
  <upperBound>1000000</upperBound>
</metricType>
<metricType>
  <name>toneMapRevToneQuality</name>
  <valueType>gauge</valueType>
  <displayName>Mesh Tone Map Reverse Tone Quality</displayName>
  <unit></unit>
  <description>The number of bits set in the tone map reverse vector</description>
  <lowerBound>0</lowerBound>
  <upperBound>24</upperBound>
</metricType>
```

```
    <metricType>
      <name>meshRank</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Route RPL Rank</displayName>
      <unit></unit>
      <description>Rank is a representation of the location of the node within the RPL
tree</description>
      <lowerBound>0</lowerBound>
      <upperBound>100</upperBound>
    </metricType>
    <metricType>
      <name>meshActiveLinkType</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Active Link Type</displayName>
      <unit></unit>
      <description>Most recent device link type.
      Metric is populated only when RPL info is pulled from the associated router.
      </description>
      <lowerBound>0</lowerBound>
      <upperBound>4</upperBound>
      <displayFormat>valueToEnum</displayFormat>
    </metricType>
    <metricType>
      <name>meshRfPhyRxSpeed</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Receive Speed (RF)</displayName>
      <unit>bits/sec</unit>
      <description>The rate of data that has been received by the network interface over
RF, measured in bits per second, averaged over a short element-specific time period (e.g.
an hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
      <displayFormat>###,###</displayFormat>
    </metricType>
    <metricType>
      <name>meshRfPhyTxSpeed</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Transmit Speed (RF)</displayName>
      <unit>bits/sec</unit>
      <description>The rate of data that has been transmitted by the network interface over
 RF, measured in bits per second, averaged over a short element-specific time period (e.g.
 an hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
      <displayFormat>###,###</displayFormat>
</metricType>
    <metricType>
      <name>meshPlcPhyRxSpeed</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Receive Speed (PLC)</displayName>
      <unit>bits/sec</unit>
      <description>The rate of data that has been received by the network interface over
PLC, measured in bits per second, averaged over a short element-specific time period (e.g.
 an hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
      <displayFormat>###,###</displayFormat>
    </metricType>
    <metricType>
      <name>meshPlcPhyTxSpeed</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Transmit Speed (PLC)</displayName>
      <unit>bits/sec</unit>
      <description>The rate of data that has been transmitted by the network interface over
```

```
 PLC, measured in bits per second, averaged over a short element-specific time period (e.g.
 an hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
      <displayFormat>###,###</displayFormat>
    </metricType>
    <metricType>
      <name>meshPlcRoboLinkUsage</name>
      <valueType>gauge</valueType>
      <displayName>Modulation Robo link usage</displayName>
      <unit></unit>
      <description>Cumulative link usage of modulation Robo</description>
      <lowerBound>0</lowerBound>
    </metricType>
    <metricType>
      <name>meshPlcBpskLinkUsage</name>
      <valueType>gauge</valueType>
      <displayName>Modulation Bpsk link usage</displayName>
      <unit></unit>
      <description>Cumulative link usage of modulation Bpsk</description>
      <lowerBound>0</lowerBound>
    </metricType>
    <metricType>
      <name>meshPlcQpskLinkUsage</name>
      <valueType>gauge</valueType>
      <displayName>Modulation Qpsk link usage</displayName>
      <unit></unit>
      <description>Cumulative link usage of modulation Qpsk</description>
      <lowerBound>0</lowerBound>
    </metricType>
    <metricType>
      <name>meshPlcPsk8LinkUsage</name>
      <valueType>gauge</valueType>
      <displayName>Modulation 8PSK link usage</displayName>
      <unit></unit>
      <description>Cumulative link usage of modulation 8PSK</description>
      <lowerBound>0</lowerBound>
    </metricType>
    <metricType>
      <name>meshPlcOpskLinkUsage</name>
      <valueType>gauge</valueType>
      <displayName>Modulation Opsk link usage</displayName>
      <unit></unit>
      <description>Cumulative link usage of modulation Opsk</description>
      <lowerBound>0</lowerBound>
    </metricType>
    <metricType>
      <name>meshRfFsk2C150WFecLU</name>
      <valueType>gauge</valueType>
      <displayName>Modulation Classic 2FSK 150 with FEC link usage</displayName>
      <unit></unit>
     <description>Cumulative link usage of modulation Classic 2FSK 150 with FEC</description>

      <lowerBound>0</lowerBound>
    </metricType>
    <metricType>
      <name>meshRfFsk2C150WtFecLU</name>
      <valueType>gauge</valueType>
      <displayName>Modulation Classic 2FSK 150 without FEC link usage</displayName>
      <unit></unit>
      <description>Cumulative link usage of modulation Classic 2FSK 150 without
FEC</description>
      <lowerBound>0</lowerBound>
    </metricType>
```

```
    <metricType>
      <name>meshRfFsk2Dr50WtFecLU</name>
      <valueType>gauge</valueType>
      <displayName>Modulation 2FSK 50 without FEC link usage</displayName>
      <unit></unit>
      <description>Cumulative link usage of modulation 2FSK 50 without FEC</description>
      <lowerBound>0</lowerBound>
    </metricType>
    <metricType>
      <name>meshRfFsk2Dr150WtFecLU</name>
      <valueType>gauge</valueType>
      <displayName>Modulation 2FSK 150 without FEC link usage</displayName>
      <unit></unit>
      <description>Cumulative link usage of modulation 2FSK 150 without FEC</description>
      <lowerBound>0</lowerBound>
    </metricType>
    <metricType>
      <name>meshRfFsk2Dr150WFecLU</name>
      <valueType>gauge</valueType>
      <displayName>Modulation 2FSK 150 with FEC link usage</displayName>
      <unit></unit>
      <description>Cumulative link usage of modulation 2FSK 150 with FEC</description>
      <lowerBound>0</lowerBound>
    </metricType>
    <metricType>
      <name>meshLowpanTxSpeed</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Link Transmit Speed for Lowpan</displayName>
      <unit>bits/sec</unit>
     <description>The current speed of data transmission over the uplink network interface,
 measured in bits per second, averaged over a short element-specific time period (e.g. an
hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
      <displayFormat>###,###.##</displayFormat>
    </metricType>
    <metricType>
      <name>meshLowpanTxDrops</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Link Transmit Packet Drops for Lowpan</displayName>
      <unit>drops/sec</unit>
      <description>The rate of packets that were dropped while trying to transmit on the
uplink interface because the outbound queue was full</description>
      <lowerBound>0</lowerBound>
      <upperBound>1</upperBound>
      <displayFormat>###,###.##</displayFormat>
    </metricType>
    <metricType>
      <name>meshLowpanRxSpeed</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Link Receive Speed for Lowpan</displayName>
      <unit>bits/sec</unit>
     <description>The rate of data that has been received by the uplink network interface,
 measured in bits per second, averaged over a short element-specific time period (e.g. an
hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
      <displayFormat>###,###.##</displayFormat>
    </metricType>
    <metricType>
      <name>meshLowpanPhyTxSpeed</name>
      <valueType>gauge</valueType>
      <displayName>Physical Mesh Link Transmit Speed</displayName>
      <unit>bits/sec</unit>
```

```
      <description>The current speed of data transmission over the physical layer, measured
 in bits per second, averaged over a short element-specific time period (e.g. an
hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
      <displayFormat>###,###.##</displayFormat>
    </metricType>
    <metricType>
      <name>meshLowpanPhyRxSpeed</name>
      <valueType>gauge</valueType>
      <displayName>Physical Mesh Link Receive Speed</displayName>
      <unit>bits/sec</unit>
      <description>The rate of data that has been received by the phyical layer, measured
in bits per second, averaged over a short element-specific time period (e.g. an
hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
      <displayFormat>###,###.##</displayFormat>
    </metricType>
    <metricType>
      <deviceType>loopback</deviceType>
      <name>txSpeed</name>
      <valueType>counter</valueType>
      <displayName>Transmit Speed</displayName>
      <unit>bits/sec</unit>
      <description>The current speed of data transmission over the interface, measured in
bits per second, averaged over a short element-specific time period (e.g. an
hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>loopback</deviceType>
      <name>txDrops</name>
      <valueType>counter</valueType>
      <displayName>Transmit Packet Drops</displayName>
      <unit>drops/sec</unit>
      <description>The rate of packets that were dropped while trying to transmit on the
interface because the outbound queue was full</description>
      <lowerBound>0</lowerBound>
      <upperBound>1</upperBound>
    </metricType>
    <metricType>
      <deviceType>loopback</deviceType>
      <name>rxSpeed</name>
      <valueType>counter</valueType>
      <displayName>Receive Speed</displayName>
      <unit>bits/sec</unit>
     <description>The rate of data that has been received by the network interface, measured
 in bits per second, averaged over a short element-specific time period (e.g. an
hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>loopback</deviceType>
      <name>txUnicastPackets</name>
      <valueType>counter</valueType>
      <displayName>Transmit Unicast Packets</displayName>
      <unit>packets/sec</unit>
     <description>The current packet send rate over the interface, measured in packets per
 second, averaged over a short element-specific time period (e.g. an hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
```

```
    </metricType>
    <metricType>
      <deviceType>loopback</deviceType>
      <name>rxUnicastPackets</name>
      <valueType>counter</valueType>
      <displayName>Receive Unicast Packets</displayName>
      <unit>packets/sec</unit>
      <description>The current packet receive rate over the interface, measured in packets
 per second, averaged over a short element-specific time period (e.g. an hour)</description>

      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>txSpeed</name>
      <valueType>counter</valueType>
      <displayName>Transmit Speed</displayName>
      <unit>bits/sec</unit>
      <description>The current speed of data transmission over the interface, measured in
bits per second, averaged over a short element-specific time period (e.g. an
hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>wpan</deviceType>
        <name>queueJumpRate</name>
        <valueType>counter</valueType>
        <displayName>Rate of queue jump</displayName>
        <unit>packets/sec</unit>
       <description>The rate at which the packets were dropped from the queue due to higher
 priority network traffic</description>
        <lowerBound>0</lowerBound>
        <upperBound>1000000000</upperBound>
        <displayFormat>###,###</displayFormat>
    </metricType>
    <metricType>
        <deviceType>wpan</deviceType>
        <name>queueEvictionRate</name>
        <valueType>counter</valueType>
        <displayName>Rate of queue evictions</displayName>
        <unit>packets/sec</unit>
        <description>The rate at which the packets were enqueued due to lower priority
network traffic</description>
        <lowerBound>0</lowerBound>
        <upperBound>1000000000</upperBound>
        <displayFormat>###,###</displayFormat>
    </metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>txDrops</name>
      <valueType>counter</valueType>
      <displayName>Transmit Packet Drops</displayName>
      <unit>drops/sec</unit>
      <description>The rate of packets that were dropped while trying to transmit on the
interface because the outbound queue was full</description>
      <lowerBound>0</lowerBound>
      <upperBound>1</upperBound>
    </metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>rxSpeed</name>
      <valueType>counter</valueType>
```

```
      <displayName>Receive Speed</displayName>
      <unit>bits/sec</unit>
      <description>The rate of data that has been received by the network interface, measured
 in bits per second, averaged over a short element-specific time period (e.g. an
hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>txUnicastPackets</name>
      <valueType>counter</valueType>
      <displayName>Transmit Unicast Packets</displayName>
      <unit>packets/sec</unit>
      <description>The current packet send rate over the interface, measured in packets per
 second, averaged over a short element-specific time period (e.g. an hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>rxUnicastPackets</name>
      <valueType>counter</valueType>
      <displayName>Receive Unicast Packets</displayName>
      <unit>packets/sec</unit>
      <description>The current packet receive rate over the interface, measured in packets
 per second, averaged over a short element-specific time period (e.g. an hour)</description>

      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>rfPhyRxSpeed</name>
      <valueType>counter</valueType>
      <displayName>Receive Speed on RF link</displayName>
      <unit>bits/sec</unit>
      <description>The rate of data that has been received by the network interface over
RF, measured in bits per second, averaged over a short element-specific time period (e.g.
an hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>rfPhyTxSpeed</name>
      <valueType>counter</valueType>
      <displayName>Transmit Speed on RF link</displayName>
      <unit>bits/sec</unit>
      <description>The rate of data that has been transmitted by the network interface over
 RF, measured in bits per second, averaged over a short element-specific time period (e.g.
 an hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
</metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>plcPhyRxSpeed</name>
      <valueType>counter</valueType>
      <displayName>Receive Speed on PLC link</displayName>
      <unit>bits/sec</unit>
      <description>The rate of data that has been received by the network interface over
PLC, measured in bits per second, averaged over a short element-specific time period (e.g.
 an hour)</description>
```

```
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>plcPhyTxSpeed</name>
      <valueType>counter</valueType>
      <displayName>Transmit Speed on PLC link</displayName>
      <unit>bits/sec</unit>
      <description>The rate of data that has been transmitted by the network interface over
 PLC, measured in bits per second, averaged over a short element-specific time period (e.g.
 an hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
</metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>rfFsk150LinkUsage</name>
      <valueType>cumulative</valueType>
      <displayName>Modulation Fsk150 link usage</displayName>
      <unit></unit>
      <description>Cumulative link usage of modulation fsk150</description>
      <lowerBound>0</lowerBound>
    </metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>plcRoboLinkUsage</name>
      <valueType>cumulative</valueType>
      <displayName>Modulation Robo link usage</displayName>
      <unit></unit>
      <description>Cumulative link usage of modulation Robo</description>
      <lowerBound>0</lowerBound>
    </metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>plcBpskLinkUsage</name>
      <valueType>cumulative</valueType>
      <displayName>Modulation Bpsk link usage</displayName>
      <unit></unit>
      <description>Cumulative link usage of modulation Bpsk</description>
      <lowerBound>0</lowerBound>
    </metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>plcQpskLinkUsage</name>
      <valueType>cumulative</valueType>
      <displayName>Modulation Qpsk link usage</displayName>
      <unit></unit>
      <description>Cumulative link usage of modulation Qpsk</description>
      <lowerBound>0</lowerBound>
    </metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>plcOpskLinkUsage</name>
      <valueType>cumulative</valueType>
      <displayName>Modulation Opsk link usage</displayName>
      <unit></unit>
      <description>Cumulative link usage of modulation Opsk</description>
      <lowerBound>0</lowerBound>
    </metricType>
    <metricType>
      <deviceType>wpan</deviceType>
      <name>rfFsk2C150WFecLU</name>
      <valueType>cumulative</valueType>
```

```
        <displayName>Modulation Classic 2FSK 150 with FEC link usage</displayName>
        <unit></unit>
       <description>Cumulative link usage of modulation Classic 2FSK 150 with FEC</description>

        <lowerBound>0</lowerBound>
      </metricType>
      <metricType>
        <deviceType>wpan</deviceType>
        <name>rfFsk2C150WtFecLU</name>
        <valueType>cumulative</valueType>
        <displayName>Modulation Classic 2FSK 150 without FEC link usage</displayName>
        <unit></unit>
        <description>Cumulative link usage of modulation Classic 2FSK 150 without
FEC</description>
        <lowerBound>0</lowerBound>
      </metricType>
      <metricType>
        <deviceType>wpan</deviceType>
        <name>rfFsk2Dr50WtFecLU</name>
        <valueType>cumulative</valueType>
        <displayName>Modulation 2FSK 50 without FEC link usage</displayName>
        <unit></unit>
        <description>Cumulative link usage of modulation 2FSK 50 without FEC</description>
        <lowerBound>0</lowerBound>
      </metricType>
      <metricType>
        <deviceType>wpan</deviceType>
        <name>rfFsk2Dr150WtFecLU</name>
        <valueType>cumulative</valueType>
        <displayName>Modulation 2FSK 150 without FEC link usage</displayName>
        <unit></unit>
        <description>Cumulative link usage of modulation 2FSK 150 without FEC</description>
        <lowerBound>0</lowerBound>
      </metricType>
      <metricType>
        <deviceType>wpan</deviceType>
        <name>rfFsk2Dr150WFecLU</name>
        <valueType>cumulative</valueType>
        <displayName>Modulation 2FSK 150 with FEC link usage</displayName>
        <unit></unit>
        <description>Cumulative link usage of modulation 2FSK 150 with FEC</description>
        <lowerBound>0</lowerBound>
      </metricType>
      <metricType>
        <deviceType>wpan</deviceType>
        <name>phyTxSpeed</name>
        <valueType>counter</valueType>
        <displayName>Transmit Speed on PHY layer(PLC and RF combined)</displayName>
        <unit>bits/sec</unit>
       <description>The rate of data that has been transmitted by the network interface over
 physical layer, measured in bits per second, averaged over a short element-specific time
period (e.g. an hour)</description>
        <lowerBound>0</lowerBound>
        <upperBound>76800</upperBound>
      </metricType>
      <metricType>
        <deviceType>wpan</deviceType>
        <name>phyRxSpeed</name>
        <valueType>counter</valueType>
        <displayName>Receive Speed on PHY layer(PLC and RF combined)</displayName>
        <unit>bits/sec</unit>
        <description>The rate of data that has been received by the network interface over
physical layer, measured in bits per second, averaged over a short element-specific time
period (e.g. an hour)</description>
```

```
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>ppp</deviceType>
      <name>txSpeed</name>
      <valueType>counter</valueType>
      <displayName>Transmit Speed</displayName>
      <unit>bits/sec</unit>
      <description>The current speed of data transmission over the interface, measured in
bits per second, averaged over a short element-specific time period (e.g. an
hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>ppp</deviceType>
      <name>txDrops</name>
      <valueType>counter</valueType>
      <displayName>Transmit Packet Drops</displayName>
      <unit>drops/sec</unit>
      <description>The rate of packets that were dropped while trying to transmit on the
interface because the outbound queue was full</description>
      <lowerBound>0</lowerBound>
      <upperBound>1</upperBound>
    </metricType>
    <metricType>
      <deviceType>ppp</deviceType>
      <name>rxSpeed</name>
      <valueType>counter</valueType>
      <displayName>Receive Speed</displayName>
      <unit>bits/sec</unit>
     <description>The rate of data that has been received by the network interface, measured
 in bits per second, averaged over a short element-specific time period (e.g. an
hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>ppp</deviceType>
      <name>txUnicastPackets</name>
      <valueType>counter</valueType>
      <displayName>Transmit Unicast Packets</displayName>
      <unit>packets/sec</unit>
      <description>The current packet send rate over the interface, measured in packets per
 second, averaged over a short element-specific time period (e.g. an hour)</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>ppp</deviceType>
      <name>rxUnicastPackets</name>
      <valueType>counter</valueType>
      <displayName>Receive Unicast Packets</displayName>
      <unit>packets/sec</unit>
      <description>The current packet receive rate over the interface, measured in packets
 per second, averaged over a short element-specific time period (e.g. an hour)</description>

      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>RPL</deviceType>
      <name>hops</name>
```

```
      <valueType>gauge</valueType>
      <displayName>Hops</displayName>
      <unit>hops</unit>
      <description>The number of hops that the element is from the root of its RPL routing
 tree</description>
      <lowerBound>1</lowerBound>
      <upperBound>8</upperBound>
      <displayFormat>###</displayFormat>
    </metricType>
    <metricType>
      <deviceType>RPL</deviceType>
      <name>linkCost</name>
      <valueType>gauge</valueType>
      <displayName>Link Cost</displayName>
      <unit></unit>
      <description>The RPL cost value for the link between the element and its uplink
neighbor</description>
      <lowerBound>1</lowerBound>
      <upperBound>3</upperBound>
      <invalidValue>65535</invalidValue>
      <displayFormat>###</displayFormat>
    </metricType>
    <metricType>
      <deviceType>RPL</deviceType>
      <name>pathCost</name>
      <valueType>gauge</valueType>
      <displayName>Path Cost</displayName>
      <unit></unit>
      <description>The RPL path cost value between the element and the root of the routing
 tree</description>
      <lowerBound>1</lowerBound>
      <upperBound>24</upperBound>
      <invalidValue>65535</invalidValue>
    </metricType>
    <metricType>
      <deviceType>RPL</deviceType>
      <name>rssi</name>
      <valueType>gauge</valueType>
      <displayName>RSSI</displayName>
      <unit>dBm</unit>
      <description>The measured RSSI value of the primary mesh RF uplink</description>
      <lowerBound>-80</lowerBound>
      <upperBound>20</upperBound>
      <invalidValue>-128</invalidValue>
    </metricType>
    <metricType>
      <deviceType>RPL</deviceType>
      <name>reverseRssi</name>
      <valueType>gauge</valueType>
      <displayName>Reverse RSSI</displayName>
      <unit>dBm</unit>
     <description>The RSSI value measured by the element's mesh uplink neighbor</description>

      <lowerBound>-80</lowerBound>
      <upperBound>20</upperBound>
      <invalidValue>-128</invalidValue>
    </metricType>
    <metricType>
      <deviceType>RPL</deviceType>
      <name>tmFwdTxResRaw</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Tone Map Forward Tx Res Raw</displayName>
      <unit></unit>
      <description>The txres field integer value in tone map forward message</description>
```

```
    <lowerBound>-1000</lowerBound>
    <upperBound>1000</upperBound>
  </metricType>
  <metricType>
    <deviceType>RPL</deviceType>
    <name>tmFwdTxGainRaw</name>
    <valueType>gauge</valueType>
    <displayName>Mesh Tone Map Forward Tx Gain Raw</displayName>
    <unit></unit>
    <description>The txres gain integer value in tone map forward message</description>
    <lowerBound>-1000</lowerBound>
    <upperBound>1000</upperBound>
  </metricType>
  <metricType>
    <deviceType>RPL</deviceType>
    <name>tmFwdTxGain</name>
    <valueType>gauge</valueType>
    <displayName>Mesh Tone Map Forward Tx Gain</displayName>
    <unit></unit>
    <description>Equals to txResRaw * txResGain</description>
    <lowerBound>-1000000</lowerBound>
    <upperBound>1000000</upperBound>
  </metricType>
  <metricType>
    <deviceType>RPL</deviceType>
    <name>tmFwdToneQuality</name>
    <valueType>gauge</valueType>
    <displayName>Mesh Tone Map Forward Tone Quality</displayName>
    <unit></unit>
    <description>The number of bits set in the tone map vector</description>
    <lowerBound>0</lowerBound>
    <upperBound>24</upperBound>
  </metricType>
  <metricType>
    <deviceType>RPL</deviceType>
    <name>tmRevTxResRaw</name>
    <valueType>gauge</valueType>
    <displayName>Mesh Tone Map Reverse Tx Res Raw</displayName>
    <unit></unit>
    <description>The txres field integer value in tone map reverse message</description>
    <lowerBound>-1000</lowerBound>
    <upperBound>1000</upperBound>
  </metricType>
  <metricType>
    <deviceType>RPL</deviceType>
    <name>tmRevTxGainRaw</name>
    <valueType>gauge</valueType>
    <displayName>Mesh Tone Map Reverse Tx Gain Raw</displayName>
    <unit></unit>
    <description>The txres gain integer value in tone map reverse message</description>
    <lowerBound>-1000</lowerBound>
    <upperBound>1000</upperBound>
  </metricType>
  <metricType>
    <deviceType>RPL</deviceType>
    <name>tmRevTxGain</name>
    <valueType>gauge</valueType>
    <displayName>Mesh Tone Map Reverse Tx Gain</displayName>
    <unit></unit>
    <description>Equals to txResRaw * txResGain</description>
    <lowerBound>-1000000</lowerBound>
    <upperBound>1000000</upperBound>
  </metricType>
  <metricType>
```

```
      <deviceType>RPL</deviceType>
      <name>tmRevToneQuality</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Tone Map Reverse Tone Quality</displayName>
      <unit></unit>
      <description>The number of bits set in the tone map reverse vector</description>
      <lowerBound>0</lowerBound>
      <upperBound>24</upperBound>
    </metricType>
    <metricType>
      <deviceType>RPL</deviceType>
      <name>absolutePhase</name>
      <valueType>gauge</valueType>
      <displayName>Mesh absolute phase of power</displayName>
      <unit></unit>
      <description>Relative position of current and voltage waveforms for a PLC
Node</description>
      <lowerBound>0</lowerBound>
      <upperBound>76800</upperBound>
    </metricType>
    <metricType>
      <deviceType>RPL</deviceType>
      <name>rank</name>
      <valueType>gauge</valueType>
      <displayName>Mesh Route RPL Rank</displayName>
      <unit></unit>
      <description>Rank is a representation of the location of the node within the RPL
tree</description>
      <lowerBound>0</lowerBound>
      <upperBound>100</upperBound>
    </metricType>
    <metricType>
      <name>nodeLocalTime</name>
      <valueType>gauge</valueType>
      <displayName>NodeTime</displayName>
      <unit>sec</unit>
      <description>UTC time as reported by the device</description>
      <lowerBound>0</lowerBound>
      <upperBound>4294967296</upperBound>
    </metricType>
    <metricType>
      <name>batteryLevel</name>
      <valueType>gauge</valueType>
      <displayName>Battery Level</displayName>
      <unit>percent</unit>
      <description>The percentage of charge remaining in battery</description>
      <lowerBound>0</lowerBound>
      <upperBound>101</upperBound>
    </metricType>
    <metricType>
      <name>batteryRuntime</name>
      <valueType>gauge</valueType>
      <displayName>Battery Remaining Time</displayName>
      <unit>minutes</unit>
      <description>The runtime remaining on battery</description>
      <lowerBound>0</lowerBound>
      <upperBound>65535</upperBound>
    </metricType>
    <metricType>
      <name>batteryChargeTime</name>
      <valueType>gauge</valueType>
      <displayName>Battery Charging Time</displayName>
      <unit>minutes</unit>
      <description>The time required to charge battery</description>
```

```
        <lowerBound>0</lowerBound>
        <upperBound>65535</upperBound>
      </metricType>
      <metricType>
          <name>totalQueueJumpCnt</name>
          <valueType>gauge</valueType>
          <displayName>Mesh Link Queue Jump Count</displayName>
          <unit>packets</unit>
         <description>Total count of jump packets or number of dequeue packets</description>

          <lowerBound>0</lowerBound>
          <upperBound>1000000000</upperBound>
          <displayFormat>###,###</displayFormat>
      </metricType>
      <metricType>
          <name>totalQueueEvictionCnt</name>
          <valueType>gauge</valueType>
          <displayName>Mesh Link Queue Eviction Count</displayName>
          <unit>packets</unit>
          <description>Total count of eviction packets or number of enqueue
packets</description>
          <lowerBound>0</lowerBound>
          <upperBound>1000000000</upperBound>
          <displayFormat>###,###</displayFormat>
      </metricType>
      <metricType>
          <name>meshQueueJumpRate</name>
          <valueType>gauge</valueType>
          <displayName>Mesh Link Queue Jump Rate</displayName>
          <unit>packets/sec</unit>
          <description>Rate at which the packets were dropped from the queue due to higher
priority network traffic</description>
          <lowerBound>0</lowerBound>
          <upperBound>1000000000</upperBound>
          <displayFormat>###,###</displayFormat>
      </metricType>
      <metricType>
          <name>meshQueueEvictionRate</name>
          <valueType>gauge</valueType>
          <displayName>Mesh Link Queue Eviction Rate</displayName>
          <unit>packets/sec</unit>
          <description>Rate at which the packets were enqueued due to lower priority network
 traffic</description>
          <lowerBound>0</lowerBound>
          <upperBound>1000000000</upperBound>
          <displayFormat>###,###</displayFormat>
      </metricType>
      <metricType>
          <name>interPanMigration</name>
          <valueType>gauge</valueType>
          <displayName>Inter Pan Migrations</displayName>
          <unit>count</unit>
          <description>Count of inter pan migrations</description>
          <lowerBound>0</lowerBound>
          <upperBound>1000000000</upperBound>
          <displayFormat>###,###</displayFormat>
      </metricType>
      <metricType>
          <name>intraPanMigration</name>
          <valueType>gauge</valueType>
          <displayName>Intra Pan Migrations</displayName>
          <unit>count</unit>
          <description>Count of intra pan migrations</description>
          <lowerBound>0</lowerBound>
```

```
        <upperBound>1000000000</upperBound>
        <displayFormat>###,###</displayFormat>
    </metricType>
    <metricType>
        <name>missedPeriodicInventory</name>
        <valueType>gauge</valueType>
        <displayName>Missed Periodic Inventory Collections</displayName>
        <unit>count</unit>
        <description>Count of Missed Periodic Inventory Collections</description>
        <lowerBound>0</lowerBound>
        <upperBound>1000000000</upperBound>
        <displayFormat>###,###</displayFormat>
    </metricType>
  </metricTypes>
</cgms>
```

# Event Types

The following is a sample list of event types for the end point device.

```
<?xml version="1.0" encoding="UTF-8" ?>
<event xmlns="http://www.w3schools.com" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.w3schools.com cmEvent.xsd">
<eventTypes kind="cgmesh">
<eventType>
<eventTypeName>UNKNOWN</eventTypeName>
<eventCategory>unknown</eventCategory>
<eventSearchName>unknown</eventSearchName>
<eventTypeDisplayString>Unknown Event</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Unknown event.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>restoration</eventTypeName>
<eventCategory>restoration</eventCategory>
<eventSearchName>restoration</eventSearchName>
<eventTypeDisplayString>Restoration</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Device restored from outage.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>up</eventTypeName>
<eventCategory>up</eventCategory>
<eventSearchName>up</eventSearchName>
<eventTypeDisplayString>Up</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Device is up.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>down</eventTypeName>
<eventCategory>down</eventCategory>
<eventSearchName>down</eventSearchName>
<eventTypeDisplayString>Down</eventTypeDisplayString>
<eventSeverity>MAJOR</eventSeverity>
<eventTypeDefaultMessage>Device is down.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>outage</eventTypeName>
<eventCategory>outage</eventCategory>
<eventSearchName>outage</eventSearchName>
<eventTypeDisplayString>Outage</eventTypeDisplayString>
<eventSeverity>CRITICAL</eventSeverity>
<eventTypeDefaultMessage>Outage detected on device.</eventTypeDefaultMessage>
```

```
</eventType>
<eventType>
<eventTypeName>UserEventType</eventTypeName>
<eventCategory>rule</eventCategory>
<eventSearchName>ruleEvent</eventSearchName>
<eventTypeDisplayString>Rule Event</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Event generated by rule.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>timeMismatch</eventTypeName>
<eventCategory>timeMismatch</eventCategory>
<eventSearchName>timeMismatch</eventSearchName>
<eventTypeDisplayString>Time Mismatch</eventTypeDisplayString>
<eventSeverity>MAJOR</eventSeverity>
<eventTypeDefaultMessage>NMS server time mismatches with the device local
time.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>timeMismatchResolved</eventTypeName>
<eventCategory>timeMismatchResolved</eventCategory>
<eventSearchName>timeMismatchResolved</eventSearchName>
<eventTypeDisplayString>Time Mismatch Resolved</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>NMS server time matches with the device local
time.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>manualCloseEvent</eventTypeName>
<eventCategory>Operation</eventCategory>
<eventSearchName>manualCloseEvent</eventSearchName>
<eventTypeDisplayString>Manual Close(Issue)</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Admin changed issue state to closed.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>unknownRegReason</eventTypeName>
<eventCategory>Registration</eventCategory>
<eventSearchName>unknownRegReason</eventSearchName>
<eventTypeDisplayString>Unknown Registration Reason</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Mesh node registered for unknown reason.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>coldBoot</eventTypeName>
<eventCategory>Registration</eventCategory>
<eventSearchName>coldBoot</eventSearchName>
<eventTypeDisplayString>Cold Boot</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Mesh node registered due to cold boot.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>manualReRegistration</eventTypeName>
<eventCategory>Registration</eventCategory>
<eventSearchName>manualReRegistration</eventSearchName>
<eventTypeDisplayString>Manual Re-Registration</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Mesh node registered due to manual
registration.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>rejoinedWithNewIP</eventTypeName>
<eventCategory>Registration</eventCategory>
<eventSearchName>rejoinedWithNewIP</eventSearchName>
```

```
<eventTypeDisplayString>Rejoined with New IP Address</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Mesh node registered with new IP address.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>nmsAddrChange</eventTypeName>
<eventCategory>Registration</eventCategory>
<eventSearchName>nmsAddrChange</eventSearchName>
<eventTypeDisplayString>NMS Address Change</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Mesh node registered due to NMS address
change.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>manualNMSAddrChange</eventTypeName>
<eventCategory>Registration</eventCategory>
<eventSearchName>manualNMSAddrChange</eventSearchName>
<eventTypeDisplayString>Manual NMS Address Change</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Mesh node registered due to manual NMS address
change.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>nmsError</eventTypeName>
<eventCategory>Registration</eventCategory>
<eventSearchName>nmsError</eventSearchName>
<eventTypeDisplayString>NMS Returned Error</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Mesh node registered due to NMS error.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>meterCertChange</eventTypeName>
<eventCategory>Registration</eventCategory>
<eventSearchName>meterCertChange</eventSearchName>
<eventTypeDisplayString>Mesh Certificate Change</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Mesh node registered due to certificate
change.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>unknownWPANChange</eventTypeName>
<eventCategory>WPAN Change</eventCategory>
<eventSearchName>unknownWPANChange</eventSearchName>
<eventTypeDisplayString>Unknown WPAN Change</eventTypeDisplayString>
<eventSeverity>MAJOR</eventSeverity>
<eventTypeDefaultMessage>Mesh node changed PAN for unknown reason.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>meshConnectivityLost</eventTypeName>
<eventCategory>WPAN Change</eventCategory>
<eventSearchName>meshConnectivityLost</eventSearchName>
<eventTypeDisplayString>Mesh Connectivity Lost</eventTypeDisplayString>
<eventSeverity>MAJOR</eventSeverity>
<eventTypeDefaultMessage>Mesh node lost all connectivity.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>meshLinkKeyTimeout</eventTypeName>
<eventCategory>WPAN Change</eventCategory>
<eventSearchName>meshLinkKeyTimeout</eventSearchName>
<eventTypeDisplayString>Mesh Link Key Timeout</eventTypeDisplayString>
<eventSeverity>MAJOR</eventSeverity>
<eventTypeDefaultMessage>Mesh node link key timed out.</eventTypeDefaultMessage>
</eventType>
<eventType>
```

```
<eventTypeName>defaultRouteLost</eventTypeName>
<eventCategory>WPAN Change</eventCategory>
<eventSearchName>defaultRouteLost</eventSearchName>
<eventTypeDisplayString>Default Route Lost</eventTypeDisplayString>
<eventSeverity>MAJOR</eventSeverity>
<eventTypeDefaultMessage>Mesh node lost default route.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>migratedToBetterPAN</eventTypeName>
<eventCategory>WPAN Change</eventCategory>
<eventSearchName>migratedToBetterPAN</eventSearchName>
<eventTypeDisplayString>Migrated to Better PAN</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Mesh node migrated to better PAN.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>METER_REAUTHENTICATION</eventTypeName>
<eventCategory>Authentication</eventCategory>
<eventSearchName>dot1xReauth</eventSearchName>
<eventTypeDisplayString>Dot1x Reauthentication</eventTypeDisplayString>
<eventSeverity>MINOR</eventSeverity>
<eventTypeDefaultMessage>Multiple attempts to send the mesh-key to the meter failed.
Reauthenticating.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>AUTHENTICATION_FAILED</eventTypeName>
<eventCategory>Authentication</eventCategory>
<eventSearchName>dot1xAuthFailure</eventSearchName>
<eventTypeDisplayString>Dot1x Authentication Failure</eventTypeDisplayString>
<eventSeverity>MAJOR</eventSeverity>
<eventTypeDefaultMessage>Dot1x authentication failed for meter.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>restorationRegistration</eventTypeName>
<eventCategory>Registration</eventCategory>
<eventSearchName>restorationRegistration</eventSearchName>
<eventTypeDisplayString>Restoration Registration</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Mesh node registered after an outage.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>signatureFailure</eventTypeName>
<eventCategory>Security</eventCategory>
<eventSearchName>signatureFailure</eventSearchName>
<eventTypeDisplayString>Invalid CSMP Signature</eventTypeDisplayString>
<eventSeverity>CRITICAL</eventSeverity>
<eventTypeDefaultMessage>Invalid signature reported by mesh node</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>deviceAdded</eventTypeName>
<eventCategory>DeviceLifecycle</eventCategory>
<eventSearchName>deviceAdded</eventSearchName>
<eventTypeDisplayString>Device Added</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>New device is added</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>deviceRemoved</eventTypeName>
<eventCategory>DeviceLifecycle</eventCategory>
<eventSearchName>deviceRemoved</eventSearchName>
<eventTypeDisplayString>Device Removed</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Device is removed</eventTypeDefaultMessage>
</eventType>
```

```
<eventType>
<eventTypeName>registrationFailed</eventTypeName>
<eventCategory>Registration</eventCategory>
<eventSearchName>registrationFailed</eventSearchName>
<eventTypeDisplayString>Device Registration Failed</eventTypeDisplayString>
<eventSeverity>MAJOR</eventSeverity>
<eventTypeDefaultMessage>FND receive CGMSNotification with code = 3 during device
registration</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>registering</eventTypeName>
<eventCategory>registering</eventCategory>
<eventSearchName>registering</eventSearchName>
<eventTypeDisplayString>Registering</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Device is registering</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>blocked</eventTypeName>
<eventCategory>blocked</eventCategory>
<eventSearchName>blocked</eventSearchName>
<eventTypeDisplayString>Blocked</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Device is blocked</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>blockMeshDeviceFailed</eventTypeName>
<eventCategory>Security</eventCategory>
<eventSearchName>blockMeshDeviceFailed</eventSearchName>
<eventTypeDisplayString>Block Mesh Device Failure</eventTypeDisplayString>
<eventSeverity>MAJOR</eventSeverity>
<eventTypeDefaultMessage>Block mesh device operation failed.</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>estError</eventTypeName>
<eventCategory>EST</eventCategory>
<eventSearchName>estError</eventSearchName>
<eventTypeDisplayString>EST Error</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Error occurred processing EST request from the
device</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>sslError</eventTypeName>
<eventCategory>EST</eventCategory>
<eventSearchName>sslError</eventSearchName>
<eventTypeDisplayString>SSL Error</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>SSL Error occurred processing EST request from the
device</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>cacertRequest</eventTypeName>
<eventCategory>EST</eventCategory>
<eventSearchName>cacertRequest</eventSearchName>
<eventTypeDisplayString>CACert Request</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Received EST CACert request from the device</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>cacertResponse</eventTypeName>
<eventCategory>EST</eventCategory>
<eventSearchName>cacertResponse</eventSearchName>
<eventTypeDisplayString>CACert Response</eventTypeDisplayString>
```

```
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Sent EST CACert response to the device</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>enrollRequest</eventTypeName>
<eventCategory>EST</eventCategory>
<eventSearchName>enrollRequest</eventSearchName>
<eventTypeDisplayString>Enroll Request</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Received EST Enroll request from the device</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>reenrollRequest</eventTypeName>
<eventCategory>EST</eventCategory>
<eventSearchName>reenrollRequest</eventSearchName>
<eventTypeDisplayString>Re-Enroll Request</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Received EST Re-Enroll request from the
device</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>enrollSuccess</eventTypeName>
<eventCategory>EST</eventCategory>
<eventSearchName>enrollSuccess</eventSearchName>
<eventTypeDisplayString>Enroll Success</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Device EST Enrollment succeeded</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>reenrollSuccess</eventTypeName>
<eventCategory>EST</eventCategory>
<eventSearchName>reenrollSuccess</eventSearchName>
<eventTypeDisplayString>Re-Enroll Success</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Device EST Re-Enrollment succeeded</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>enrollFailure</eventTypeName>
<eventCategory>EST</eventCategory>
<eventSearchName>enrollFailure</eventSearchName>
<eventTypeDisplayString>Enroll Failure</eventTypeDisplayString>
<eventSeverity>CRITICAL</eventSeverity>
<eventTypeDefaultMessage>Device EST Enrollment failed</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>reenrollFailure</eventTypeName>
<eventCategory>EST</eventCategory>
<eventSearchName>reenrollFailure</eventSearchName>
<eventTypeDisplayString>Re-Enroll Failure</eventTypeDisplayString>
<eventSeverity>CRITICAL</eventSeverity>
<eventTypeDefaultMessage>Device EST Re-Enrollment failed</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>authenticationSuccess</eventTypeName>
<eventCategory>EST</eventCategory>
<eventSearchName>authenticationSuccess</eventSearchName>
<eventTypeDisplayString>Authentication Success</eventTypeDisplayString>
<eventSeverity>INFO</eventSeverity>
<eventTypeDefaultMessage>Device EST authentication succeeded</eventTypeDefaultMessage>
</eventType>
<eventType>
<eventTypeName>authenticationFailure</eventTypeName>
<eventCategory>EST</eventCategory>
<eventSearchName>authenticationFailure</eventSearchName>
```

```
<eventTypeDisplayString>Authentication Failure</eventTypeDisplayString>
<eventSeverity>MAJOR</eventSeverity>
<eventTypeDefaultMessage>Device EST authentication failed</eventTypeDefaultMessage>
</eventType>
</eventTypes>
</event>
```

# Issue Types

The following is a sample list of issue types for the end point device.

```
<?xml version="1.0" encoding="UTF-8" ?>
<issue xmlns="http://www.w3schools.com" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.w3schools.com cgrEvent.xsd">
<issueTypes kind="cgmesh">
<issueType>
<issueTypeName>UNKNOWN</issueTypeName>
<issueCategory>unknown</issueCategory>
<issueSearchName>unknown</issueSearchName>
<issueTypeDisplayString>Unknown Issue</issueTypeDisplayString>
<issueSeverity>INFO</issueSeverity>
<issueTypeDefaultMessage>The issue raised/closed does not have a defined issue
type.</issueTypeDefaultMessage>
</issueType>
<issueType>
<issueTypeName>deviceDown</issueTypeName>
<issueCategory>Device</issueCategory>
<issueSearchName>down</issueSearchName>
<issueTypeDisplayString>Down</issueTypeDisplayString>
<issueSeverity>MAJOR</issueSeverity>
<issueTypeDefaultMessage>Device is down.</issueTypeDefaultMessage>
</issueType>
<issueType>
<issueTypeName>registrationFailed</issueTypeName>
<issueCategory>Device</issueCategory>
<issueSearchName>registrationFailed</issueSearchName>
<issueTypeDisplayString>Device Registration Failed</issueTypeDisplayString>
<issueSeverity>MAJOR</issueSeverity>
<issueTypeDefaultMessage>Device Registration failed due to configuration
error</issueTypeDefaultMessage>
</issueType>
<issueType>
<issueTypeName>deviceOutage</issueTypeName>
<issueCategory>Device</issueCategory>
<issueSearchName>Outage</issueSearchName>
<issueTypeDisplayString>Outage</issueTypeDisplayString>
<issueSeverity>CRITICAL</issueSeverity>
<issueTypeDefaultMessage>Device is in outage.</issueTypeDefaultMessage>
</issueType>
<issueType>
<issueTypeName>deviceTimeMismatch</issueTypeName>
<issueCategory>Device</issueCategory>
<issueSearchName>deviceTimeMismatch</issueSearchName>
<issueTypeDisplayString>Device-NMS Time Mismatch</issueTypeDisplayString>
<issueSeverity>MAJOR</issueSeverity>
<issueTypeDefaultMessage>Device time and NMS time are not in sync.</issueTypeDefaultMessage>
</issueType>
<issueType>
<issueTypeName>signatureFailure</issueTypeName>
<issueCategory>Security</issueCategory>
<issueSearchName>signatureFailure</issueSearchName>
<issueTypeDisplayString>Invalid CSMP Signature</issueTypeDisplayString>
<issueSeverity>CRITICAL</issueSeverity>
```

```
<issueTypeDefaultMessage>Verify certificate setup. Also verify that mesh node and IoT-FND
are time synchronized.</issueTypeDefaultMessage>
</issueType>
<issueType>
<issueTypeName>enrollFailure</issueTypeName>
<issueCategory>EST</issueCategory>
<issueSearchName>enrollFailure</issueSearchName>
<issueTypeDisplayString>Enroll Failure</issueTypeDisplayString>
<issueSeverity>CRITICAL</issueSeverity>
<issueTypeDefaultMessage>Device EST Enrollment failed.</issueTypeDefaultMessage>
</issueType>
<issueType>
<issueTypeName>reenrollFailure</issueTypeName>
<issueCategory>EST</issueCategory>
<issueSearchName>reenrollFailure</issueSearchName>
<issueTypeDisplayString>Re-Enroll Failure</issueTypeDisplayString>
<issueSeverity>CRITICAL</issueSeverity>
<issueTypeDefaultMessage>Device EST Re-Enrollment failed.</issueTypeDefaultMessage>
</issueType>
<issueType>
<issueTypeName>authenticationFailure</issueTypeName>
<issueCategory>EST</issueCategory>
<issueSearchName>authenticationFailure</issueSearchName>
<issueTypeDisplayString>Authentication Failure</issueTypeDisplayString>
<issueSeverity>CRITICAL</issueSeverity>
<issueTypeDefaultMessage>Device EST authentication failed.</issueTypeDefaultMessage>
</issueType>
</issueTypes>
</issue>
```

# System Rules

The following is a sample list of system rules for the end point device.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cgms xmlns="http://www.w3schools.com" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <rules kind="">
    <rule>
      <name>Down Rule</name>
      <username>system</username>
      <query>deviceType:{0} eventName:down</query>
      <action type="manage_issue" parameter="issueTypeName:deviceDown issueStatus:OPEN" />
    </rule>
    <rule>
      <name>Up from Down Rule</name>
      <username>system</username>
      <query>deviceType:{0} eventName:up</query>
      <action type="manage_issue" parameter="issueTypeName:deviceDown issueStatus:CLOSED"
/>
    </rule>

    <rule>
      <name>Registration Failed Rule</name>
      <username>system</username>
      <query>deviceType:{0} eventName:registrationFailed</query>
      <action type="manage_issue" parameter="issueTypeName:registrationFailed
issueStatus:OPEN" />
    </rule>
    <rule>
      <name>Up from Registration Failed Rule</name>
      <username>system</username>
      <query>deviceType:{0} eventName:up</query>
```

```
      <action type="manage_issue" parameter="issueTypeName:registrationFailed
issueStatus:CLOSED" />
    </rule>

    <rule>
      <name>Outage Rule</name>
      <username>system</username>
      <query>deviceType:{0} eventName:outage</query>
      <action type="manage_issue" parameter="issueTypeName:deviceOutage issueStatus:OPEN"
/>
    </rule>
    <rule>
      <name>Up from Outage Rule</name>
      <username>system</username>
      <query>deviceType:{0} eventName:up</query>
     <action type="manage_issue" parameter="issueTypeName:deviceOutage issueStatus:CLOSED"
 />
    </rule>
    <rule>
      <name>Restored from Outage Rule</name>
      <username>system</username>
      <query>deviceType:{0} eventName:restoration</query>
     <action type="manage_issue" parameter="issueTypeName:deviceOutage issueStatus:CLOSED"
 />
    </rule>

    <rule>
      <name>Time Mismatch Rule</name>
      <username>system</username>
      <query>deviceType:{0} eventName:timeMismatch</query>
      <action type="manage_issue" parameter="issueTypeName:deviceTimeMismatch
issueStatus:OPEN" />
    </rule>
    <rule>
      <name>Time Mismatch Resolved Rule</name>
      <username>system</username>
      <query>deviceType:{0} eventName:timeMismatchResolved</query>
      <action type="manage_issue" parameter="issueTypeName:deviceTimeMismatch
issueStatus:CLOSED" />
    </rule>
    <rule>
      <name>Signature Validation Failure</name>
      <username>system</username>
      <query>deviceType:{0} eventName:signatureFailure</query>
     <action type="manage_issue" parameter="issueTypeName:signatureFailure issueStatus:OPEN"
 />
    </rule>
  </rules>
</cgms>
```

CHAPTER 10

# Troubleshooting IoT FND

This chapter is moved to the Troubleshooting Guide for Cisco IoT Field Network Director.