Cisco IoT Field Network Director User Guide, Release 5.0

First Published: 2024-12-20

Last Modified: 2024-12-26

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 5.0 release.

New Features

Feature Name	Description	Business Outcome
Achieve Scale Beyond 25,000 Routers	Starting from Cisco IoT FND Release 5.0, you can manage up to 50,000 routers using Cisco IoT FND on a VM using Postgres + Influx database.	Scale your network operations significantly, accommodating growth without the need for additional hardware investments.
Autosync of CGMS Properties Files	Cisco IoT FND ensures that any changes made to the CGMS properties file, whether inside or outside the container, are automatically mirrored in the corresponding file. This synchronization maintains consistency across configurations, reducing the risk of errors and ensuring seamless application performance.	Maintain consistent configurations across Cisco IoT FND deployments. This reduces the likelihood of configuration errors that could disrupt operations, leading to fewer application downtimes and improved performance reliability.

Feature Name	Description	Business Outcome
Bootflash Space Cleanup	Check the **Remove unused firmware images from bootflash** check box to remove unused firmware bin files from the bootflash when Cisco IoT FND uploads the image to the router. The check box is enabled for the following devices running Cisco IOS-XE: • Cisco Catalyst IR1100 • Cisco Catalyst IR8100 • Cisco Catalyst IR1800	Clears up space in the bootflash when there is no more space available for an efficient firmware upload.
Enhancement to Firmware Update Page for Down and Active Device Status	Cisco IoT FND includes two additional device statuses in the **Firmware Update** page: **Down Devices** and **All Devices**.	Filter your search based on the device statuses for routers running a firmware group. View the count of all devices that are part of a given firmware group of routers.
Improved Audit Trail	When you add or remove or edit files using .CSV files on Cisco IoT FND, a log is generated in the **Audit Trail** page. You can download the .CSV file that you used to change the devices.	Provides a clear and detailed record of all changes made to devices via .CSV files, enhancing accountability and traceability. You can download the .CSV file used for these changes, it facilitates easier audits and ensures that you can verify and review modifications.
Manage Router Firmware Upgrades	Manage Router Firmware upload, install and retry counts using Cisco IoT FND, instead of editing the CGMS properties file.	Automating the firmware upgrade process and tracking install counts with Cisco IoT FND reduces the time and effort required for manual updates.
Manage Firmware Upgrade Properties For A Router Group	Cisco IoT FND includes a **Router Firmware Upload Retry Count** in the **Firmware Update** page. Customize the retry count at the router group level, allowing for tailored firmware update strategies for specific groups of routers.	Customizing the retry count at the router group level in Cisco IoT FND's Firmware Update page enhances the efficiency of firmware update strategies, resulting in improved operational uptime and reduced network downtime for specific groups of routers.

Feature Name	Description	Business Outcome
Manage Router Push Configuration Count	Define the number of router configuration changes or updates that you want to apply to routers within a specific group. Manage and track the number of configuration changes applied to a group of routers during the configuration push using Cisco IoT FND.	Defining and managing the number of router configuration changes for specific groups using Cisco IoT FND ensures precise control over network configurations, enhancing network stability and streamlining operations.
Search in the **Device Configuration** page	The **Device Configuration** page has a new search bar for you to search through the various device configurations.	The search bar on the **Device Configuration** page allows you to search through various device configurations, helping you narrow down your scope to easily identify a device.
Search Firmware Updates	Search through the existing firmware updates using the filters introduced in this release	The filters introduced allow you to search through the existing firmware updates, making the firmware updates page searchable.
Username and Password Validation	Cisco IoT FND includes username and password validation check for CSV file input.	The username and password validation helps in enhancing the security standards for usernames and passwords.

Modified Features

Feature Name	Description	Business Outcome
Additonal HER Support	The Cisco IoT FND supports Cisco Catalyst 8500 and 8300 series HER platforms: Cisco Catalyst 8500-12X and Cisco Catalyst 8300-1N1S-4T2X.	The additional HER platforms enhance network scalability and reliability, enabling more efficient management and monitoring of Cisco IoT devices. The additional HER support improves operational efficiency and reduces downtime.

Feature Name	Description	Business Outcome
User Experience Enhancements	The Cisco IoT FND dashboard includes pre-defined dashlets, where an additional **Name** field is added along with the Element Identifier (**EID**). You can delete the default views of the devices you select in the **Devices** > **Field Devices** page. You can also add the user-defined properties in the customized tab in the **Field Devices** page.	Easy to use dashlets which are more accessible, enhance your experience. The intuitive tab navigation facilitates faster task completion, allowing you to seamlessly switch between different tasks and functionalities. Additionally, you can also customize the dashboard to suit your specific needs, providing a more personalized and efficient workflow.
Device-Level Configuration Push	You can push the configurations at the device level using the **Push Configuration** tab in the **Field Devices** page when you click the device using two options: Config push without-rollback or Config push with-rollback.	You can manage configuration at the device level, providing more flexibility for managing siloed devices and reducing the time it takes to push new configuration
Show Registration Config vs Running Config	In the **Running Config** tab of a device page, you can see both the Registration Config and the active running config of the device.	You can track configuration changes at the device level which helps in managing and reducing configuration drift and provides better visibility to your network devices.
Admin Password Rotation	The Cisco IoT FND tools package includes a new script `rotate_admin_password.sh` with CSV input file. This script enables the seamless rotation of administrator passwords across Cisco IoT FND devices, supporting both Cisco IOS and Cisco IOS XE device types.	This enhancement streamlines the process of updating administrator credentials periodically, ensuring consistent security practices, and simplifying password management across your network infrastructure.

Feature Name	Description	Business Outcome
Full Open CoAP Simple Management Protocol Support	A Vendor TLV 127 value support is added to the Full Open CoAP Simple Management Protocol (CSMP) for the Cisco IoT FND devices. A new tab **Vendor TLV Info** is introduced where you can add the TLV details for a selected device. You can modify and retrieve Vendor TLV details and push the modified configuration to new endpoints. You can also upgrade and manage the firmware with supported TLVs.	This feature allows customization and flexibility, improves control over device settings and behaviors, enhances operational efficiency, and provides better visibility and monitoring.
EID Field	EID field is added in most of the Cisco IoT FND pages for you to access the **Device Info** of the devices which are associated with the EID.	The EID hyperlinks enhance your experience by allowing easy access to device information from any page which has device details in Cisco IoT FND.
Update Target Firmware Versions For All Users	In Cisco IoT FND Release 4.12.x and earlier releases, when you change the target firmware versions in the **Router Bootstrap Configuration** tab, the target firmware changes don't reflect in Cisco IoT FND. Starting from Cisco IoT FND Release 5.0, when you make changes to the target firmware version, the changes reflects for all the other associated Cisco IoT FND users.	Starting from Cisco IoT FND Release 5.0, you experience seamless synchronization of target firmware version changes across all associated accounts.

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

Table 1: Feature History

Feature Name	Release Information	Description
Additonal HER Support	Cisco IoT FND Release 5.0	The Cisco IoT FND supports Cisco Catalyst 8500 and 8300 series HER platforms: Cisco Catalyst 8500-12X and Cisco Catalyst 8300-1N1S-4T2X.

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.
- 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, 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 . 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:
    - AP803 embedded in IR829

- Cisco Aggregation Services Routers (ASR) 1000 series, Cisco Integrated Services Routers (ISR) 3900 series, ISR 4300, ISR 4400, and Cisco 8000 Series Routers are referred to as *head-end routers* or HERs in this document.

Table 2: PIDs Supported for Cisco 8000 Series Routers

Device Type	PID	Category
C8000	C8500L-8S4X	Head-End Routers
C8000	C8000V	Head-End Routers
C8000	C8500-12x	Head-End Routers
C8000	C8300-1N1S-4T2X	Head-End Routers

- 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

- Cisco Catalyst IR1800 Rugged Series Routers are secure, 5G routers designed with a high level of modularity that supports private LTE, FirstNet, Wi-Fi6 and Gigabit Ethernet. These routers offer enterprise-grade security from the hardware to the network communications all the way to the industrial assets. The routers are powered by Cisco IOS® XE, Cisco's fully programmable next-generation operating system. Automotive certifications and features such as Controller Area Network (CAN) bus support, dead reckoning and Global Navigation Satellite System (GNSS), and ignition power management make it ideal for secure, reliable connectivity in transit and public safety applications.

  IoT FND supports the following IR1800 models:
    - IR1821-K9
    - IR1831-K9
    - IR1833-K9
    - IR1835-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 ISRs, Cisco IRs, Cisco ASRs, C8000, 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 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/C8000 and Cisco CGRs, 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, 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 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, IR1101, IR800, N2450, 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, , 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/C8000.
- **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.

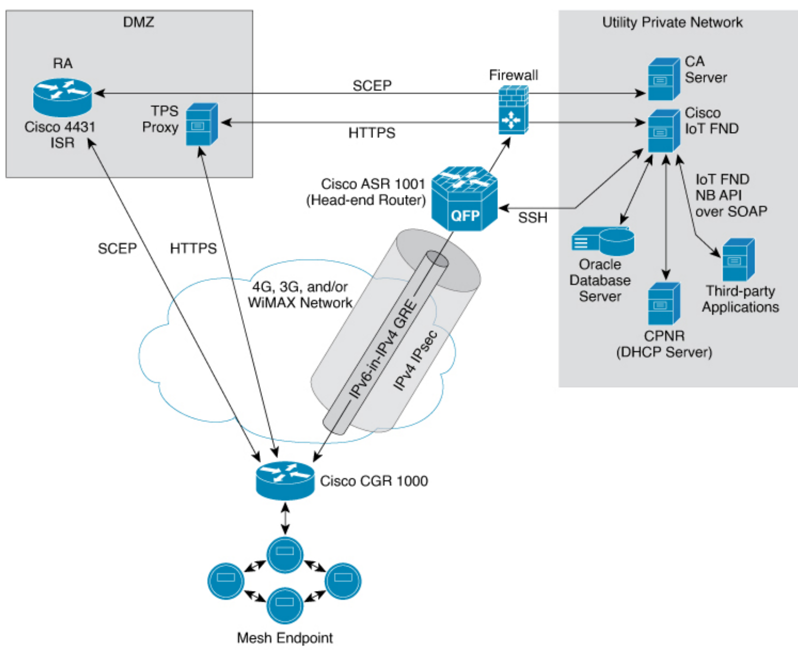
IoT FND Architecture

Figure 1: Zero Touch Deployment Architecture, on page 13 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 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 13), 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

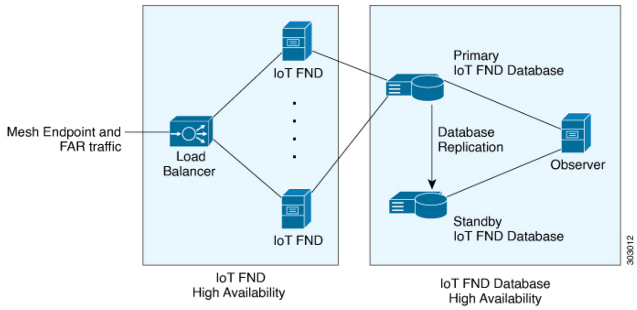
Component	Description
IoT FND Application Server	This is the heart of IoT FND deployments. It runs on an RHEL server and allows administrators to control different aspects of the IoT FND deployment using its browser-based graphical user interface. IoT FND HA deployments include two or more IoT FND servers 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/C8000), 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 13 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 15. 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.

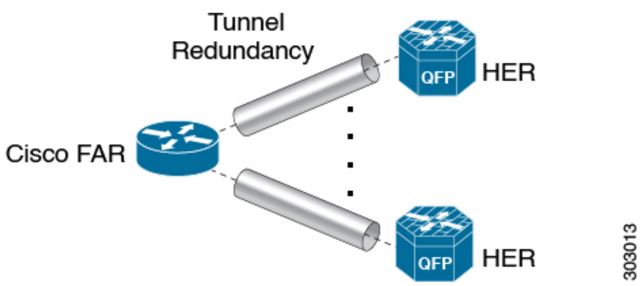
You could also deploy a standby Cisco IoT FND database to provide another layer of high availability in the system with minimal data loss.

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/C8000, as shown in Figure 3: IoT FND Tunnel Redundancy, on page 15.

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
Oracle DB Server	1522

Service	Port
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 3: 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. 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.

Scale Support

Cisco IoT FND provides the following deployments for the mesh management and router-only management.

- Bare Metal Deployment with Oracle (Mesh Management)
- VM Deployment with Oracle
- VM Deployment with Postgres

- Bare Metal Deployment with Oracle (Router Management)

Bare Metal Deployment with Oracle (Mesh Management)

This deployment is a large-scale AMI deployment for mesh management and supports up to 8,000 routers / 8,000,000 endpoints.

VM Deployment with Oracle

This deployment is a large-scale AMI deployment for mesh management and supports up to 2,000 routers / 2,000,000 endpoints.

VM Deployment with Postgres

This deployment is for router management with the following scale support:

Cisco IoT FND Release	Scale Support
5.0	50,000 routers
4.11.0 to 4.12.0	25,000 routers
4.9.1 to 4.10.0	15,000 routers
4.9.0	10,000 routers
4.7.x to 4.8.x	6,000 routers

Bare Metal Deployment with Oracle (Router Management)

This deployment is a small-scale deployment for router management with the following scale support:

Cisco IoT FND Release	Scale Support
4.11.0 and later releases	25,000 routers
4.3 to 4.10	10,000 routers

Achieve Scale Beyond 25,000 Routers

Achieve Scale Beyond 25,000 Routers

Table 4: Feature History

Feature Name	Release	Description
Achieve Scale Beyond 25,000 Routers	Cisco IoT FND Release 5.0	Starting from Cisco IoT FND Release 5.0, you can manage upto 50,000 routers using Cisco IoT FND on a VM using Postgres + Influx databases.

Information About Achieve Scale Beyond 25,000 Routers

Starting from Cisco IoT FND Release 5.0, you manage up to 50,000 routers efficiently on a virtual machine utilizing a PostgreSQL database. This upgrade allows for seamless management of large-scale network deployments.

Benefits of Achieve Scale Beyond 25,000 Routers

- Scale your network operations significantly, accommodating growth without the need for additional hardware investments.
- Managing a large number of routers from a single platform helps you streamline operations, simplify configuration, and reduce the complexity of managing dispersed devices.

Achieving Scale Beyond 25,000 Routers

Here's how you can achieve scale beyond 25,000 routers using Cisco IoT FND:

1. Adjust InfluxDB configuration to manage memory usage.
2. Increase the disk space of Cisco IoT FND VM.
3. Increase the heap size of Cisco IoT FND.
4. Edit the retention policy and reduce the retention period.
5. Implement the recommended property settings.
6. Configure the metrics interval.
7. Information about the mhistory_da kapacitor task.

Note We recommend you onboard upto 15 devices, concurrently. Ensure that the number of devices attempting to PnP Bootstrap doesn't exceed 15.

Configure Influx Memory

When you upgrade to Cisco IoT FND Release 5.0 and attempt to achieve scale of 25,000 routers and beyond, the Influx DB uses a lot of memory that might bring down the performance of Cisco IoT FND. You can address the high memory usage issue using this topic.

To adjust the Influx DB configuration:

1. Locate the `influxdb.conf` file, typically found in `/etc/influxdb/influxdb.conf`.
2. Open the file using a text editor with root privileges:

   ```
   sudo nano /etc/influxdb/influxdb.conf
   ```

3. Modify the cache settings:
   a. Set the `cache-max-memory-size` to **1g**:

      ```
      cache-max-memory-size = "1g"
      ```

   b. Set the `cache-snapshot-memory-size` to **10m**:

      ```
      cache-snapshot-memory-size = "10m"
      ```

Note The `cache-snapshot-memory-size` property is by default commented out. You should uncomment the property and then enter 10m.

4. Save your changes and exit the editor.
5. Restart the Influx DB.

   ```
   sudo systemctl restart influxdb.service
   ```

6. Verify the status of the service to ensure it’s running correctly:

   ```
   sudo systemctl status influxdb.service
   ```

Configure Memory, CPU, And Disk Space Of Cisco IoT FND VM

Before You Begin

Here are the respective minimum CPU, memory, and disk space requirements to achieve scaling beyond 25,000 routers:

Scale	CPU	Memory	Add-on Disk space
10,000 routers	10	32 GB	600 GB
10,000 - 25,000 routers	24 (Cores per socket: 4 and sockets: 6)	96 GB	800 GB

Scale	CPU	Memory	Add-on Disk space
25,000- 50,000 routers	24 (Cores per socket: 4 and sockets: 6)	96 GB	800 GB

Increase The Disk Space

Here are the instructions to increase the disk space of Cisco IoT FND VM:

1. Intiate a graceful shut down of the VM from within the Cisco IoT FND VM shell.
2. Navigate to VMware vSphere and edit the CPU and memory size. For more information see, Change the Memory Configuration and Configure CPU Resources.

> **Note** We recommend you enter **96 GB** memory and **24** CPU (Cores per socket: 4 and sockets: 6) for a scale of 25,000 routers and beyond.

3. Save the memory and CPU configurations.
4. Add a new standard hard disk. For more information see, Add a New Hard Disk to a Virtual Machine.

> **Note** Choose **Thin Provision** from the **Disk Provisioning** drop-down list.

5. Switch on the VM.
6. As a root user, using the SSH command log in to Cisco IoT FND and present the disk changes to the internal Guest OS to extend the logical volume.
7. Log in to Cisco IoT FND server as root using the SSH command and use the `fdisk -l` command to view the partition table of all the disks available on the system.

   Note down the device file for the newly added disk space of 800GB. In our case, it is `/dev/sdb`:

```
[root@iot-fnd ~]# fdisk -l

Disk /dev/sdb: 800 GiB, 858993459200 bytes, 1677721600 sectors

Units: sectors of 1 * 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/sda: 450 GiB, 483183820800 bytes, 943718400 sectors

Units: sectors of 1 * 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes

Disklabel type: dos
```

```
Disk identifier: 0xb2ce243b

Device Boot Start End Sectors Size Id Type

/dev/sda1 * 2048 2099199 2097152 1G 83 Linux

/dev/sda2 2099200 943718399 941619200 449G 8e Linux LVM



Disk /dev/mapper/rhel-root: 70 GiB, 75161927680 bytes, 146800640 sectors

Units: sectors of 1 * 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/rhel-swap: 11.8 GiB, 12700352512 bytes, 24805376 sectors

Units: sectors of 1 * 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/rhel-home: 367.2 GiB, 394243604480 bytes, 770007040 sectors

Units: sectors of 1 * 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes
```

8. Navigate to the device file for the newly added disk and execute the following commands, In our case device file is `/dev/sdb` as noted in step 7.

```
[root@iot-fnd ~]# fdisk /dev/sdb


Welcome to fdisk (util-linux 2.32.1).

Changes will remain in memory only, until you decide to write them.

Be careful before using the write command.


Device does not contain a recognized partition table.

Created a new DOS disklabel with disk identifier 0xbd4033c8.


Command (m for help): p

Disk /dev/sdb: 800 GiB, 858993459200 bytes, 1677721600 sectors
```

```
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xbd4033c8

Command (m for help): n
Partition type
p primary (0 primary, 0 extended, 4 free)
e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1):
First sector (2048-1677721599, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-1677721599, default 1677721599):

Created a new partition 1 of type 'Linux' and of size 800 GiB.

Command (m for help): p
Disk /dev/sdb: 800 GiB, 858993459200 bytes, 1677721600 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xbd4033c8

Device Boot Start End Sectors Size Id Type
/dev/sdb1 2048 1677721599 1677719552 800G 83 Linux

Command (m for help): t
Selected partition 1
Hex code (type L to list all codes): L

0 Empty 24 NEC DOS 81 Minix / old Lin bf Solaris
1 FAT12 27 Hidden NTFS Win 82 Linux swap / So c1 DRDOS/sec (FAT-
2 XENIX root 39 Plan 9 83 Linux c4 DRDOS/sec (FAT-
```

```
3 XENIX usr 3c PartitionMagic 84 OS/2 hidden or c6 DRDOS/sec (FAT-
4 FAT16 <32M 40 Venix 80286 85 Linux extended c7 Syrinx
5 Extended 41 PPC PreP Boot 86 NTFS volume set da Non-FS data
6 FAT16 42 SFS 87 NTFS volume set db CP/M / CTOS / .
7 HPFS/NTFS/exFAT 4d QNX4.x 88 Linux plaintext de Dell Utility
8 AIX 4e QNX4.x 2nd part 8e Linux LVM df BootIt
9 AIX bootable 4f QNX4.x 3rd part 93 Amoeba e1 DOS access
a OS/2 Boot Manag 50 OnTrack DM 94 Amoeba BBT e3 DOS R/O
b W95 FAT32 51 OnTrack DM6 Aux 9f BSD/OS e4 SpeedStor
c W95 FAT32 (LBA) 52 CP/M a0 IBM Thinkpad hi ea Rufus alignment
e W95 FAT16 (LBA) 53 OnTrack DM6 Aux a5 FreeBSD 2e BeOS fs
f W95 Ext'd (LBA) 54 OnTrackDM6 a6 OpenBSD ee GPT
10 OPUS 55 EZ-Drive a7 NeXTSTEP ef EFI (FAT-12/16/
11 Hidden FAT12 56 Golden Bow a8 Darwin UFS f0 Linux/PA-RISC b
12 Compaq diagnost 5c Priam Edisk a9 NetBSD f1 SpeedStor
14 Hidden FAT16 <3 61 SpeedStor ab Darwin boot f4 SpeedStor
16 Hidden FAT16 63 GNU HURD or Sys af HFS / HFS+ f2 DOS secondary
17 Hidden HPFS/NTF 64 Novell Netware b7 BSDI fs fb Vmware VMFS
18 AST SmartSleep 65 Novell Netware b8 BSDI swap fc Vmware VMKCORE
1b Hidden W95 FAT3 70 DiskSecure Mult bb Boot Wizard hid fd Linux raid auto
1c Hidden W95 FAT3 75 PC/IX bc Acronis FAT32 L fe LANstep
1e Hidden W95 FAT1 80 Old Minix be Solaris boot ff BBT
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'.

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

Note You have successfully created the new partition for the add-on disk. Ensure to note down the device file for the new partition created `/dev/sdb1` as shown in the logs.

9. Restart the VM. Here's an example:

```
[root@iot-fnd ~]# reboot
```

Create A Physical Volume

1. Login to Cisco IoT FND server as root using the SSH command and Use `fdisk -l` command to view the partition table of all the disks available on the system.

```
[root@iot-fnd ~]# fdisk -l

Disk /dev/sda: 450 GiB, 483183820800 bytes, 943718400 sectors

Units: sectors of 1 * 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes

Disklabel type: dos

Disk identifier: 0xb2ce243b


Device Boot Start End Sectors Size Id Type

/dev/sda1 * 2048 2099199 2097152 1G 83 Linux

/dev/sda2 2099200 943718399 941619200 449G 8e Linux LVM


Disk /dev/sdb: 800 GiB, 858993459200 bytes, 1677721600 sectors

Units: sectors of 1 * 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes

Disklabel type: dos

Disk identifier: 0xbd4033c8


Device Boot Start End Sectors Size Id Type

/dev/sdb1 2048 1677721599 1677719552 800G 8e Linux LVM



Disk /dev/mapper/rhel-root: 70 GiB, 75161927680 bytes, 146800640 sectors

Units: sectors of 1 * 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disk /dev/mapper/rhel-swap: 11.8 GiB, 12700352512 bytes, 24805376 sectors

Units: sectors of 1 * 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/rhel-home: 367.2 GiB, 394243604480 bytes, 770007040 sectors

Units: sectors of 1 * 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes
```

2. Create a physical volume using `pvcreate <partition-file-name>` command. Use the partition file noted in the previous section. Here's an example:

```
[root@iot-fnd ~]# pvcreate /dev/sdb1
Physical volume "/dev/sdb1" successfully created.
```

3. Determine the volume group to extend using the command `vgdisplay`. Here's an example:

```
[root@iot-fnd ~]# vgdisplay

--- Volume group ---

VG Name rhel

System ID

Format lvm2

Metadata Areas 1

Metadata Sequence No 4

VG Access read/write

VG Status resizable

MAX LV 0

Cur LV 3

Open LV 3

Max PV 0

Cur PV 1

Act PV 1

VG Size <449.00 GiB

PE Size 4.00 MiB

Total PE 114943

Alloc PE / Size 114943 / <449.00 GiB

Free PE / Size 0 / 0
```

```
VG UUID Y0XXtt-lpyz-fkyc-9D3J-lBdV-rJyK-PYCGsH

[root@iot-fnd ~]# lvdisplay
--- Logical volume ---
LV Path /dev/rhel/swap
LV Name swap
VG Name rhel
LV UUID 7tB68Y-z54E-x5eI-sOld-Oeru-WQ3v-qrjGy6
LV Write Access read/write
LV Creation host, time localhost, 2022-02-16 01:14:55 -0500
LV Status available
# open 2
LV Size <11.83 GiB
Current LE 3028
Segments 1
Allocation inherit
Read ahead sectors auto
- currently set to 8192
Block device 253:1

--- Logical volume ---
LV Path /dev/rhel/home
LV Name home
VG Name rhel
LV UUID 0B5Jp4-fD08-JGlk-kf5n-gwY5-oiCk-W5kZ0z
LV Write Access read/write
LV Creation host, time localhost, 2022-02-16 01:14:55 -0500
LV Status available
# open 1
LV Size <367.17 GiB
Current LE 93995
Segments 1
Allocation inherit
```

```
Read ahead sectors auto
- currently set to 8192
Block device 253:2

--- Logical volume ---
LV Path /dev/rhel/root
LV Name root
VG Name rhel
LV UUID s8Yhkw-gmYQ-B9TR-Zemj-M2gA-xPVx-eXWdnP
LV Write Access read/write
LV Creation host, time localhost, 2022-02-16 01:14:56 -0500
LV Status available
# open 1
LV Size 70.00 GiB
Current LE 17920
Segments 1
Allocation inherit
Read ahead sectors auto
- currently set to 8192
Block device 253:0
```

As highlighted above, you need to extend the **Volume Group** named **rhel**.

4. Extend the physical volume using the `vgextend rhel/dev/sdb1` command. Here's an example:

```
[root@iot-fnd ~]#
[root@iot-fnd ~]# vgextend rhel /dev/sdb1
Volume group “rhel” successfully extended
[root@iot-fnd ~]#
```

5. View the logical volumes:

```
[root@iot-fnd ~]# lvdisplay
--- Logical volume ---
LV Path /dev/rhel/swap
LV Name swap
VG Name rhel
LV UUID 7tB68Y-z54E-x5eI-sOld-Oeru-WQ3v-qrjGy6
```

```
LV Write Access read/write
LV Creation host, time localhost, 2022-02-16 01:14:55 -0500
LV Status available
# open 2
LV Size <11.83 GiB
Current LE 3028
Segments 1
Allocation inherit
Read ahead sectors auto
- currently set to 8192
Block device 253:1

--- Logical volume ---
LV Path /dev/rhel/home
LV Name home
VG Name rhel
LV UUID 0B5Jp4-fD08-JGlk-kf5n-gwY5-oiCk-W5kZ0z
LV Write Access read/write
LV Creation host, time localhost, 2022-02-16 01:14:55 -0500
LV Status available
# open 1
LV Size <367.17 GiB
Current LE 93995
Segments 1
Allocation inherit
Read ahead sectors auto
- currently set to 8192
Block device 253:2

--- Logical volume ---
LV Path /dev/rhel/root
LV Name root
VG Name rhel
```

```
LV UUID s8Yhkw-gmYQ-B9TR-Zemj-M2gA-xPVx-eXWdnP

LV Write Access read/write

LV Creation host, time localhost, 2022-02-16 01:14:56 -0500

LV Status available

# open 1

LV Size 70.00 GiB

Current LE 17920

Segments 1

Allocation inherit

Read ahead sectors auto

- currently set to 8192

Block device 253:0
```

6. Extend the Logical Volume: Increases the size of the logical volume `/dev/rhel/root` by 799 GB using space from `/dev/sdb1`.

```
[root@iot-fnd ~]# lvextend -L+799.00G /dev/rhel/root /dev/sdb1

Size of logical volume rhel/root changed from 70.00 GiB (17920 extents) to 869.00 GiB
(222464 extents).

Logical volume rhel/root successfully resized.
```

Note Note that an add-on 800 GB hard disk is added in the example. This results in extending the logical volume by 799 GB. The appropriate value should be used based on the disk space added.

7. Display the **Volume Group** information:

```
[root@iot-fnd ~]# vgdisplay

--- Volume group ---

VG Name rhel

System ID

Format lvm2

Metadata Areas 2

Metadata Sequence No 6

VG Access read/write

VG Status resizable

MAX LV 0

Cur LV 3
```

```
Open LV 3

Max PV 0

Cur PV 2

Act PV 2

VG Size <1.22 TiB

PE Size 4.00 MiB

Total PE 319742

Alloc PE / Size 319487 / <1.22 TiB

Free PE / Size 255 / 1020.00 MiB

VG UUID Y0XXtt-lpyz-fkyc-9D3J-lBdV-rJyK-PYCGsH
```

8. Grow the filesystem: Expand the filesystem on the logical volume `/dev/rhel/root` to use the newly added space.

```
[root@iot-fnd ~]# xfs_growfs /dev/rhel/root

meta-data=/dev/mapper/rhel-root isize=512 agcount=4, agsize=4587520 blks

= sectsz=512 attr=2, projid32bit=1

= crc=1 finobt=1, sparse=1, rmapbt=0

= reflink=1 bigtime=0 inobtcount=0

data = bsize=4096 blocks=18350080, imaxpct=25

= sunit=0 swidth=0 blks

naming =version 2 bsize=4096 ascii-ci=0, ftype=1

log =internal log bsize=4096 blocks=8960, version=2

= sectsz=512 sunit=0 blks, lazy-count=1

realtime =none extsz=4096 blocks=0, rtextents=0

data blocks changed from 18350080 to 227803136
```

9. Check filesystem using the `df -h` command, the root directory size is updated to 869GB.

   Also, use the `lvdisplay` command to confirm that the logical volume is extended, viewing the updated size information.

```
[root@iot-fnd ~]# df -h

Filesystem Size Used Avail Use% Mounted on

devtmpfs 47G 0 47G 0% /dev

tmpfs 47G 52K 47G 1% /dev/shm

tmpfs 47G 9.4M 47G 1% /run

tmpfs 47G 0 47G 0% /sys/fs/cgroup
```

```
/dev/mapper/rhel-root 869G

/dev/sda1 1014M 254M 761M 26% /boot

/dev/mapper/rhel-home 367G 2.6G 365G 1% /home

tmpfs 9.4G 12K 9.4G 1% /run/user/42

overlay 869G 15G 855G 2%
/var/lib/docker/overlay2/c6cace1e574c1fb9212758ee5ceea08fea6da7fb9a3f1f0e65321e524665da09/merged

overlay 869G 15G 855G 2%
/var/lib/docker/overlay2/f34d0ef4ef597f6077357370a4546ad8966a4d576cd5b92806c8f3904d20c1a3/merged

tmpfs 9.4G 0 9.4G 0% /run/user/0

[root@iot-fnd ~]#


[root@iot-fnd ~]# lvdisplay

--- Logical volume ---

LV Path /dev/rhel/swap

LV Name swap

VG Name rhel

LV UUID 7tB68Y-z54E-x5eI-sOld-Oeru-WQ3v-qrjGy6

LV Write Access read/write

LV Creation host, time localhost, 2022-02-16 01:14:55 -0500

LV Status available

# open 2

LV Size <11.83 GiB

Current LE 3028

Segments 1

Allocation inherit

Read ahead sectors auto

- currently set to 8192

Block device 253:1


--- Logical volume ---

LV Path /dev/rhel/home

LV Name home

VG Name rhel

LV UUID 0B5Jp4-fD08-JGlk-kf5n-gwY5-oiCk-W5kZ0z
```

```
LV Write Access read/write
LV Creation host, time localhost, 2022-02-16 01:14:55 -0500
LV Status available
# open 1
LV Size <367.17 GiB
Current LE 93995
Segments 1
Allocation inherit
Read ahead sectors auto
- currently set to 8192
Block device 253:2

--- Logical volume ---
LV Path /dev/rhel/root
LV Name root
VG Name rhel
LV UUID s8Yhkw-gmYQ-B9TR-Zemj-M2gA-xPVx-eXWdnP
LV Write Access read/write
LV Creation host, time localhost, 2022-02-16 01:14:56 -0500
LV Status available
# open 1
LV Size 869.00 GiB
Current LE 222464
Segments 2
Allocation inherit
Read ahead sectors auto
- currently set to 8192
Block device 253:0
```

For a deployment of upto 25,000 routers, if you add 600 GB of secondary hard disk, the `/dev/mapper/rhel-root` would increase to approximately 670 GB (70 GB default + 600 GB additional).

For a deployment of 50,000 routers, when you add 800 GB of secondary hard disk, this would result in the `/dev/mapper/rhel-root` expanding to approximately 870 GB (70 GB default + 800 GB additional).

Configure Java Heap Size

Here are the steps to increase the heap size for Cisco IoT FND:

1. Log in to Cisco IoT FND server using the SSH command as a root user.
2. Navigate to and edit the file `/opt/fnd/conf/fnd-env.list`.
3. Add the following lines to configure the heap size if the lines don't exist already:

```
MAX_JVM_HEAP_SIZE=18g
MIN_JVM_HEAP_SIZE=1g
MAX_JVM_PERM_SIZE=512m
```

Note If the lines already exist, modify the values to 18g, 1g, and 512m.

4. Reload the Cisco IoT FND container using the upgrade script in the `/opt/fnd/scripts/upgrade.sh` directory:

```
[root@iot-fnd scripts]# ./upgrade.sh

This script must be run with root privileges.
Usage: Load container images: No resource required
       For container reload: No resource required

1) Load container images
2) Container reload
3) Quit
Enter your choice: 2
```

5. Verify the status:

```
/opt/fnd/scripts/fnd-container.sh status
```

6. Once Cisco IoT FND is up, log in to Cisco IoT FND using the browser.
7. From the Cisco IoT FND menubar, choose **Devices** > **Servers** > **NMS Servers**.
8. Click **IoT-FND+fnd-server** and ensure that the CPU is 24 or more.
9. Ensure that the memory is 93 GB or more.

Note The discrepancy between the 96 GB added and the 93 GB shown is due to the difference in storage measurement units—manufacturers use decimal (1 GB = 1 billion bytes), while systems use binary (1 GiB = 1,073,741,824 bytes)—plus some space is reserved for system overhead.

10. In the **IoT-FND Application Information** area, confirm that the memory allocation is 18 GB.

Edit The Retention Policy

To edit the retention policy and reduce the retention period:

1. From the Cisco IoT FND menubar, choose **ADMIN** > **Data Retention**.
2. Enter **15** days in the following fields:

- **Keep Event data for**
- **Keep Historical Dashboard data for**
- **Keep Historical Metrics Statistics for**

3. Retain the default value **7** for the **Keep Dashboard data for** and **Keep Device Network Statistics for** fields.
4. Click the **Save** button.

Note You'll see only data for 15 days in the dashlet that is set to display data for 4 weeks.

Implement The Recommended Property Settings

Here are the recommended property settings to achieve scale beyond 25,000 routers:

1. From the Cisco IoT FND menubar, choose **ADMIN** > **Server Settings** > **Property Settings**.
2. Enter the following values in the respective fields:
   - **Maximum Router Firmware Upload Count**: **5**.
   - **Maximum Router Firmware Install Count:**: **5**.
   - **Router Firmware Upload Retry Count**: **5**.
   - **Router Push Configuration Count Per Group**: **16**.

Note We recommend that you enter **16** or lesser as the value for the **Router Push Configuration Count Per Group** field.

Configure The Metrics Interval

To configure the metrics interval:

1. From the Cisco IoT FND menubar, choose **CONFIG** > **Device Configuration**.
2. Choose a router group and navigate to the **Edit Configuration Template** tab.

Note Ensure that you don't exceed 5 groups and a maximum of 1000 devices per configuration group.

3. To adjust the periodic inventory notification interval, find the line `cgna profile cg-nms-periodic`, which is set to report metrics every hour. Change the interval from 60 to 480 or more. Here is an example:

```
cgna profile cg-nms-periodic
interval 480
exit
```

4. Save the Configuration template.
5. Perform a push configuration.

Information about the mhistory_da Kapacitor Task

Starting from Cisco IoT FND Release 5.0, we are disabling the `mhistory_da` task, which runs every 24 hours to aggregate historical metrics, to address the high memory usage by Influx DB. This change has no impact on existing functionalities of Cisco IoT FND.

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 5: Common Tasks

Task	Use
Device Viewing Tasks	
View Devices	Working with Router Views, on page 162 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 247
Diagnostics and Troubleshooting Tasks	
Ping	Pinging Devices, on page 239
Traceroute	Tracing Routes to Devices, on page 240
Download logs	Downloading Logs, on page 132
Monitoring Tasks	
View and search events	Monitoring Events, on page 466 in the Monitoring System chapter.

Task	Use
View and search issues	Monitoring Issues, on page 478 in the Monitoring System chapter.
View tunnel status	Monitoring Tunnel Status, on page 441 in the Managing Tunnel Provisioning chapter.
General Tasks	
Change password	Resetting Passwords, on page 112
Set time zone	“Configuring the Time Zone” in the Document Title, Release 4.x.
Set user preferences	Setting Preferences for the User Interface, on page 152 in the Managing Devices chapter.

CGR Tasks

The table lists CGR tasks. For information about user roles, see System-Defined User Roles, on page 119

Table 6: CGR Tasks

Task	Use
Router Configuration Group Tasks	
Add CGRs to configuration groups	Creating Device Groups, on page 261
Delete a configuration group	Deleting Device Groups, on page 268
List devices in a configuration group	Listing Devices in a Configuration Group, on page 270
Assign devices to groups	• Adding Routers to IoT FND, on page 252 • Adding HERs to IoT FND, on page 251 • Moving Devices to Another Configuration Group in Bulk, on page 269 • Moving Devices to Another Configuration Group Manually, on page 269
Rename configuration groups	Renaming a Device Configuration Group, on page 267
Router Configuration Tasks	
Change device configuration properties	Changing Device Configuration Properties, on page 264
Edit configuration templates	• Editing the ROUTER Configuration Template, on page 271 • Editing the AP Configuration Template, on page 273
Push configurations	Pushing Configurations to Endpoints, on page 307
Monitoring a Guest OS	Monitoring a Guest OS in the Managing Devices chapter.
Tunnel Provisioning Tasks	

Task	Use
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. • 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 385
Upload images to firmware groups	Uploading a Firmware Image to a Router Group, on page 391

Mesh Endpoint Tasks

The table lists Mesh Endpoint (ME) tasks. For information about user roles, see System-Defined User Roles, on page 119.

Table 7: Mesh Endpoint Tasks

Task	Use
ME Configuration Group Tasks	
Add mesh endpoint configuration groups	Creating Device Groups, on page 261
Delete mesh endpoint configuration groups	Deleting Device Groups, on page 268
Rename mesh endpoint configuration groups	Renaming a Device Configuration Group, on page 267
Assign mesh endpoint devices to a configuration group	Moving Devices to Another Group, on page 269
List devices in a configuration group	Listing Devices in a Configuration Group, on page 270
ME Configuration Tasks	
Change mesh endpoint configuration properties	Changing Device Configuration Properties, on page 264
Edit mesh endpoint configuration templates	Editing the ENDPOINT Configuration Template, on page 296
Push configuration to mesh endpoints	Pushing Configurations to Endpoints, on page 307
Add mesh endpoint firmware groups	Creating Device Groups, on page 261
Assign devices to firmware groups	Moving Devices to Another Configuration Group Manually, on page 269
Upload images to firmware groups	Uploading a Firmware Image to a Resilient Mesh Endpoint (RME) Group, on page 375

Administration Tasks

The table lists administration tasks.

Table 8: Administration Tasks

Task	Use
Access Management Tasks	
Set password policies	Managing Password Policy, on page 89
Define roles	Managing Roles and Permissions, on page 117
Manage user accounts	Managing Users, on page 110
Manage Authentication	Managing User Authentication, on page 90
Manage Domains	Managing Domains, on page 114
System Management Tasks	
Manage active sessions	Managing Active Sessions, on page 124
Display the audit trail	Displaying the Audit Trail, on page 125
Manage certificates	Managing Certificates, on page 127
Configure data retention	Configuring Data Retention, on page 130
Manage licenses	Managing Licenses, on page 131
Manage logs	Managing Logs, on page 131
Configure server settings	Configuring Server Settings, on page 138
Manage the syslog	Managing System Settings, on page 123
Configure tunnel settings	Configuring Provisioning Settings, on page 133
View logs	Managing Logs, on page 131

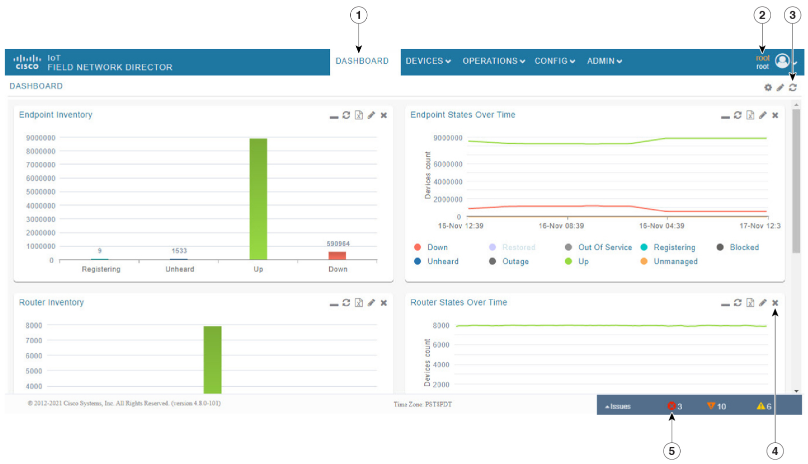
Interface Overview

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

- Icons, on page 44
- Main Menus, on page 46

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

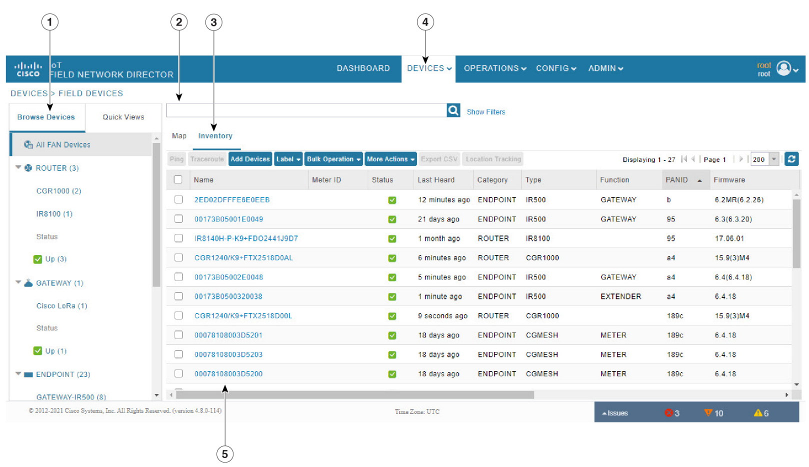
Figure 4: IoT FND Dashboard



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

2	*<user name>* menu • Preferences: Sets display settings of the user interface. • Switch Domain • Change Password • Time Zone • Guided Tour • Log Out	**5**	Issues Status bar Summary of issues by devices (routers, head-end routers, servers, endpoints) and their severity (critical, major, minor) Viewing Device Severity Status on the Issues Status Bar, on page 481
3	• Dashboard Settings-Allows you to set the refresh rate for the page and Add Dashlets to the Dashboard. • Filter-Allows you to define custom filters and by selectable time periods. • 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 247. 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 42).

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 236 and Viewing Mesh Endpoints in Map View, on page 178).

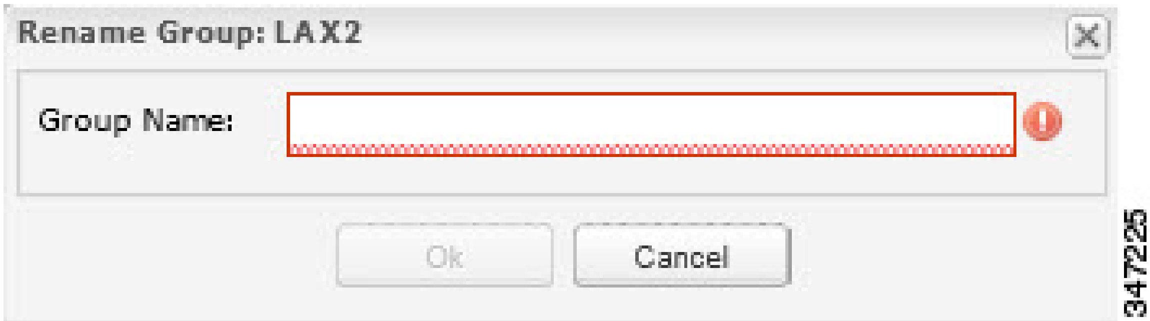
Working with Filters

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 42) 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 248).

Completing User-entry Fields

Figure 6: Errored Group Name User-entry Field, on page 44 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.

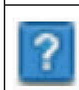
Figure 6: Errored Group Name User-entry Field

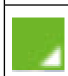
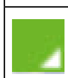


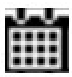
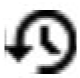
Icons

The table lists the icons that display in the UI.

Table 9: 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. The RPL tree connection displays as blue or orange lines. • Orange lines indicate that the link is up. • 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: • Critical • Major • Minor • Info 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.

EID Field

Table 10: Feature History

Feature Name	Release Information	Description
EID Field	Cisco IoT FND Release 5.0	EID field is added in most of the Cisco IoT FND pages for you to access the **Device Info** of the devices which are associated with the EID.

Information About EID Field

Endpoint Identifier (EID) is used to uniquely identify a device or entity within a system. Starting from Cisco IoT FND Release 5.0, a new column called EID is available in all the Cisco IoT FND interface pages. Each EID has a link which you can click, to access the details of each device. The EID column appears along with the device name column in all the tables and pages.

Benefits of EID Link

EID links allow easy navigation to the **Device Info** page with a single click. It is now easier to locate and view any device from any page using the EID link from any page in the Cisco IoT FND interface.

The EID links are present in:

Table 11: EID Links

EID Links	Navigation
Devices	Choose **Devices** > • **Field Devices**, • **Head-End Routers**, • **Servers**,
Operations	Choose **Operations** > • **Events**, • **Issues**, • **Tunnel Status**,

EID Links	Navigation
Config	Choose **Config** > • **Device Configuration**, • **Firmware Update**, • **Device File Management**, • **Tunnel Provisioning**. • **Groups**,

CHAPTER 3

Simplified IoT FND Architecture

Tunnel management with unique Pre-Shared Key (PSK) and assigning IP address with FND IP Address Management (IPAM) aim to simplify the configuration process and reduce the number of components in FND. In the proposed architecture, the PSK replaces the existing security components such as CA, AAA, RA and the IPAM replaces the existing external DHCP server. This simplified architecture is supported only in the greenfield deployments, namely, Bare Metal with Oracle DB and Virtual Machine with Oracle or Postgres DB.

However, using a unique PSK and the IPAM in the architecture is up to the discretion of the users. FND continues to support existing PKI-based certificate communication between FAR and FND, PKI-based certificate for tunnels between FAR and HER, and external DHCP servers for tunnel IP addressing.

Tunnel Management with Pre-Shared Key

A unique pre-shared key (PSK) solution is used for the tunnel management between FAR and HER, which significantly simplifies the authentication and authorization process in the headend infrastructure and allows the users to self-manage. The PSK is supported on all Cisco IOS and IOS-XE device types.

The table provides various scenarios where PSK can be used effectively in combination with either SUDI or a CA server in the greenfield deployment.

Deployment	Scenario	Recommendation
Greenfield deployment	Without CA server	• Use PSK for authentication and authorization of communication between FAR and HER. • Use SUDI for authentication and authorization of communication between FND and FAR.
	With CA server	Choose one of the following combinations: • Use PSK for authentication and authorization of communication between FAR and HER. • Use a custom CA certificate for authentication and authorization of communication between FND and FAR. (or) • Use a custom CA certificate for authentication and authorization of communication between both FAR and HER, FND and FAR.
Note In both scenarios, with or without CA server, it is mandatory to generate the IoT FND certificate from the CA server and install it on the IoT FND server (cgms_keystore).		

Note For the brownfield deployment, IoT FND continues to support CA, RA, and AAA for the FAR communication with FND and HER.

Configuring FND for Tunnel Management with PSK

Use the following steps to configure FND for managing tunnels with PSK.

Procedure

Step 1 Run the following script to configure FND with IPAM and PSK settings.

```
/opt/cgms/bin/setupCgms.sh
```

```
Do you want to change IPAM and PSK Settings (y/n)? y
```

Step 2 On entering **"y"**, you are provided with a new option to select PSK scheme for IPsec tunnel management.

```
Do you want to manage Tunnels using Unique Pre-Shared Keys (y/n)? y

08-20-2023 12:43:03 IST: INFO: User response: y
08-20-2023 12:43:03 IST: INFO: FND Configured to manage Tunnels using Unique Pre-Shared Keys
08-20-2023 12:43:03 IST: INFO: ========== IoT-FND Setup Completed Successfully ==========
```

Step 3 On entering **"y"**, FND is configured with PSK.

FND updates the Preferences table by setting the property `com.cisco.cgms.pnp.tunnelMgmtUsingPsk` as True. By default, this property is False.

Generating PSK

A unique pre-shared key is generated when you import a device through CSV or NB API. The pre-shared key is a 15-character alphanumeric string which is unique and generated randomly for each device. The generated key is encrypted and stored in the database for each router. For more information on tunnel management with PSK, see Workflow for Tunnel Management with PSK, on page 66.

Default Templates

The following default templates are available for the tunnel management.

Router Tunnel Addition Template

There are two default router addition templates available for authentication. Based on the configuration settings in `setupCgms.sh`, the default template is selected to manage tunnels using PSK or not.

A sample template for FlexVPN and DMVPN tunnel configuration is given below.

Note By default, the peer name is set to `her-tunnel` in `crypto ikev2 keyring FlexVPN_Keyring` and `Flexvpn_ikev2_profile`. Configure the peer name to match the name that is given in `identity local key-id` in the HER configuration.

```
<#-- This template only supports FARs running IOS. -->
<#if !far.isRunningIos()>
  ${provisioningFailed("FAR is not running IOS")}
</#if>

<#--
  For FARs running IOS configure a FlexVPN client in order to establish secure
  communications to the HER. This template expects that the HER has been
  appropriately pre-configured as a FlexVPN server.
-->
<#if far.isRunningIos()>
  <#assign sublist=far.eid?split("+")[0..1]>
  <#assign sn=sublist[1]>
  <#--
    Configure a Loopback0 interface for the FAR.
  -->
  interface Loopback0
```

```
    <#--
      If the loopback interface IPv4 address property has been set on the CGR
      then configure the interface with that address. Otherwise obtain an
      address for the interface now using DHCP.
    -->
    <#if far.loopbackV4Address??>
      <#assign loopbackIpv4Address=far.loopbackV4Address>
    <#elseif far.isIPAMForLoopbackSelected()??>
      <#assign loopbackIpv4Address=far.IPAMForLoopbackIpv4()>
    <#else>
      <#--
        Obtain an IPv4 address that can be used to for this FAR's Loopback
        interface. The template API provides methods for requesting a lease from
        a DHCP server. The IPv4 address method requires a DHCP client ID and a link
        address to send in the DHCP request. The 3rd parameter is optional and
        defaults to "IoT-FND". This value is sent in the DHCP user class option.
        The API also provides the method "dhcpClientId". This method takes a DHCPv6
        Identity association identifier (IAID) and a DHCP Unique IDentifier (DUID)
        and generates a DHCPv4 client identifier as specified in RFC 4361. This
        provides some consistency in how network elements are identified by the
        DHCP server.
      -->
      <#assign
loopbackIpv4Address=far.ipv4Address(dhcpClientId(far.enDuid,0),far.dhcpV4LoopbackLink).address>

    </#if>
    ip address ${loopbackIpv4Address} 255.255.255.255
    <#--
      If the loopback interface IPv6 address property has been set on the CGR
      then configure the interface with that address. Otherwise obtain an
      address for the interface now using DHCP.
    -->
    <#if far.loopbackV6Address??>
      <#assign loopbackIpv6Address=far.loopbackV6Address>
    <#elseif far.isIPAMForLoopbackSelected()??>
      <#assign loopbackIpv6Address=far.IPAMForLoopbackIpv6()>
    <#else>
      <#--
        Obtain an IPv6 address that can be used to for this FAR's loopback
        interface. The method is similar to the one used for IPv4, except clients
        in DHCPv6 are directly identified by their DUID and IAID. IAIDs used for
        IPv4 are separate from IAIDs used for IPv6, so we can use zero for both
        requests.
      -->
      <#assign
loopbackIpv6Address=far.ipv6Address(far.enDuid,0,far.dhcpV6LoopbackLink).address>
    </#if>
    ipv6 address ${loopbackIpv6Address}/128
  exit

  <#--
    Default to using FlexVPN for the tunnel configuration of FARs running IOS.
  -->
 <#if (far.useFlexVPN!"true") = "true">
    <#--
      IPv4 ACL which specifies the route(s) FlexVPN will push to the HER.
      We want the HER to know the route to the CGR's loopback interface.
    -->
    ip access-list standard FlexVPN_Client_IPv4_LAN
      permit ${loopbackIpv4Address}
    exit

    <#--
      IPv6 ACL which specifies the route(s) FlexVPN will push to the HER.
```

```
        We want the HER to know the route to the CGR's loopback interface.
        If a mesh has been configured on this CGR we want the HER to know the route to the
mesh.
      -->
      ipv6 access-list FlexVPN_Client_IPv6_LAN
        <#if far.meshPrefix??>
          permit ipv6 ${far.meshPrefix}/64 any
        </#if>
        sequence 20 permit ipv6 host ${loopbackIpv6Address} any
      exit

      <#--
        FlexVPN authorization policy that configures FlexVPN to push the CGR LAN's
        specified in the ACLs to the HER during the FlexVPN handshake.
      -->
      crypto ikev2 authorization policy FlexVPN_Author_Policy
        route set access-list FlexVPN_Client_IPv4_LAN
        route set access-list ipv6 FlexVPN_Client_IPv6_LAN
        route set interface
      exit

      crypto ikev2 proposal FlexVPN_IKEv2_Proposal
        encryption aes-cbc-256
        group 14
        integrity sha256
      exit
      crypto ikev2 policy FLexVPN_IKEv2_Policy
        proposal FlexVPN_IKEv2_Proposal
      exit

      <#-- FlexVPN authorization policy is defined locally. -->
      aaa authorization network FlexVPN_Author local

      crypto ikev2 keyring FlexVPN_Keyring
        peer her-tunnel
          address ${far.ipsecTunnelDestAddr1}
          identity key-id her-tunnel
          pre-shared-key ${far.mgmtVpnPsk}
        exit
      exit

      crypto ikev2 profile FlexVPN_IKEv2_Profile
        match identity remote key-id her-tunnel
        identity local fqdn ${sn}.cisco.com
        authentication remote pre-share
        authentication local pre-share
        keyring local FlexVPN_Keyring
        dpd 120 3 periodic
        aaa authorization group psk list FlexVPN_Author FlexVPN_Author_Policy
      exit

      <#--
        If the headend router is an ASR then use a different configuration for the
        transform set as some ASR models are unable to support the set we'd prefer
        to use.
      -->
      <#if her.pid?contains("ASR")>
        crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes esp-sha-hmac
          mode tunnel
        exit
      <#else>
        crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes esp-sha256-hmac
          mode tunnel
        exit
```

```
   </#if>

   crypto ipsec profile FlexVPN_IPsec_Profile
     set ikev2-profile FlexVPN_IKEv2_Profile
     set pfs group14
     set transform-set FlexVPN_IPsec_Transform_Set
   exit

   <#assign wanInterface=far.interfaces(far.tunnelSrcInterface1!"Cellular")>
   interface Tunnel0
     description IPsec tunnel to ${her.eid}
     ip unnumbered loopback0
     ipv6 unnumbered loopback0
     tunnel destination dynamic
     tunnel protection ipsec profile FlexVPN_IPsec_Profile
     tunnel source ${wanInterface[0].name}
   exit

   <#if !(far.ipsecTunnelDestAddr1??)>
    ${provisioningFailed("FAR property ipsecTunnelDestAddr1 must be set to the destination
address to connect this FAR's FlexVPN tunnel to")}
   </#if>
   crypto ikev2 client flexvpn FlexVPN_Client
     peer 1 ${far.ipsecTunnelDestAddr1}
     client connect Tunnel0
   exit
   ip http secure-client-auth
   no ip http tls-version TLSv1.2
 <#else>
   <#--
     Configure the tunnel using DMVPN.
   -->
   router eigrp 1
     network ${loopbackIpv4Address}
   exit
   ipv6 router eigrp 2
     no shutdown
   exit
   interface Loopback0
     ipv6 eigrp 2
   exit
   crypto ikev2 proposal DMVPN_IKEv2_Proposal
     encryption aes-cbc-256
     group 14
     integrity sha256
   exit
   crypto ikev2 policy DMVPN_IKEv2_Policy
     proposal DMVPN_IKEv2_Proposal
   exit
   crypto ikev2 keyring DMVPN_Keyring
     peer her-tunnel
       address ${far.ipsecTunnelDestAddr1}
       identity key-id her-tunnel
       pre-shared-key ${far.mgmtVpnPsk}
     exit
   exit
   crypto ikev2 profile DMVPN_IKEv2_Profile
     match identity remote key-id her-tunnel
     identity local fqdn ${sn}.cisco.com
     authentication remote pre-share
     authentication local pre-share
     keyring local DMVPN_Keyring
     dpd 120 3 periodic
   exit
```

```
    <#--
      If the headend router is an ASR then use a different configuration for the
      transform set as some ASR models are unable to support the set we'd prefer
      to use.
    -->
    <#if her.pid?contains("ASR")>
      crypto ipsec transform-set DMVPN_IPsec_Transform_Set esp-aes esp-sha-hmac
        mode tunnel
      exit
    <#else>
      crypto ipsec transform-set DMVPN_IPsec_Transform_Set esp-aes 256 esp-sha256-hmac
        mode tunnel
      exit
    </#if>
    crypto ipsec profile DMVPN_IPsec_Profile
      set ikev2-profile DMVPN_IKEv2_Profile
      set pfs group14
      set transform-set DMVPN_IPsec_Transform_Set
    exit
    <#if !(far.nbmaNhsV4Address??)>
      ${provisioningFailed("FAR property nbmaNhsV4Address has not been set")}
    </#if>
    <#if !(far.nbmaNhsV6Address??)>
      ${provisioningFailed("FAR property nbmaNhsV6Address has not been set")}
    </#if>
    <#assign wanInterface=far.interfaces(far.tunnelSrcInterface1!"Cellular")>
    interface Tunnel0
      <#assign lease=far.ipv4Address(dhcpClientId(far.enDuid,1),far.dhcpV4TunnelLink)>
      ip address ${lease.address} ${lease.subnetMask}
      ip nhrp map ${far.nbmaNhsV4Address} ${far.ipsecTunnelDestAddr1}
      ip nhrp map multicast ${far.ipsecTunnelDestAddr1}
      ip nhrp network-id 1
      ip nhrp nhs ${her.interfaces("Tunnel0")[0].v4.addresses[0].address}
      ipv6 address ${far.ipv6Address(far.enDuid,1,far.dhcpV6TunnelLink).address}/128
      ipv6 eigrp 2
      ipv6 nhrp map ${far.nbmaNhsV6Address}/128 ${far.ipsecTunnelDestAddr1}
      ipv6 nhrp map multicast ${far.ipsecTunnelDestAddr1}
      ipv6 nhrp network-id 1
      ipv6 nhrp nhs ${far.nbmaNhsV6Address}
      tunnel mode gre multipoint
      tunnel protection ipsec profile DMVPN_IPsec_Profile
      tunnel source ${wanInterface[0].name}
    exit
    router eigrp 1
      network ${lease.address}
    exit
  </#if>
</#if>
```

HER Tunnel Addition Template

Similar to Router Tunnel Addition templates, there are two default HER Tunnel Addition templates available. Based on the configuration settings in `setupCgms.sh`, the default template is selected to manage tunnels using PSK or not.

The following commands are pushed to HER for every router during device on-boarding (PnP). The configurations are added to a queue which are processed by a configurable number of threads and pushed to HER.

Note Ensure that the keyring name mentioned in "crypto ikev2 keyring FlexVPN_Keyring" and "FlexVPN_IKEv2_Profile" match the HER keyring name.

```
per-Router HER Config

<#-- This template only supports HERs running IOS or IOS XE. -->
<#if !her.isRunningIos() && !her.isRunningIosXe()>
  ${provisioningFailed("HER is not running IOS or IOS XE")}
</#if>

<#if far.isRunningIos()>
  <#assign sublist=far.eid?split("+")[0..1]>
  <#assign sn=sublist[1]>

  crypto ikev2 keyring FlexVPN_Keyring
    peer ${sn}
      identity fqdn ${sn}.cisco.com
      pre-shared-key ${far.mgmtVpnPsk}
   exit
  exit
</#if>
```

Router Bootstrap Configuration Template

Note For SUDI authentication, you must use `cgna initiator profile` as the tunnel profile.

Note Based on the device types, the following ports are used:

- For Cisco IOS-XE device types, use port 443.
- For Cisco IOS device types, use port 8443.

A sample router bootstrap configuration template:

```
<#assign sublist=far.eid?split("+")[0..1]>
<#assign pid=sublist[0]>
<#assign sn=sublist[1]>

hostname ${sn}
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
aaa session-id common
aaa password restriction
!
!
!
!
ip host fnd.iot.cisco.com <fnd ip address>
```

```
ip host tps.iot.cisco.com <tps ip address>
ip domain name cisco.com
!
password encryption aes
!
!
archive
  path bootflash:archive/
maximum 8
!
!
!
!
username admin privilege 15 password <router password>
!
!
no cdp run
!
!
!
!
interface Loopback999
 ip address <ip address for the interface> 255.255.255.255
!
!
ip forward-protocol nd
!
no ip http server
ip http tls-version TLSv1.2
ip http authentication aaa login-authentication default
ip http secure-server
ip http secure-port 443
ip http max-connections 5
ip http timeout-policy idle 600 life 86400 requests 3
ip http client connection timeout 5
ip http client connection retry 5
ip http client source-interface lo0
ip http client secure-trustpoint CISCO_IDEVID_SUDI

ip ssh time-out 60
ip ssh authentication-retries 2
crypto key generate rsa
ip ssh version 2
!
ipv6 unicast-routing
!
control-plane
!
!
line con 0
length 0
transport preferred none
escape-character 3
stopbits 1

!

line vty 6 15
session-timeout 10
exec-timeout 5 0
session-limit 2
transport input ssh
!
wsma agent exec
```

```
profile exec
!
wsma agent config
profile config
!
!wsma agent filesys
!
!wsma agent notify
!
!
wsma profile listener exec
transport https path /wsma/exec
!
wsma profile listener config
transport https path /wsma/config

event manager directory user policy "flash:/managed/scripts"
event manager policy no_config_replace.tcl type system authorization bypass
!
!
cgna gzip
!
!
cgna initiator-profile cg-nms-tunnel
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show version | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 callhome-url https://tps.iot.cisco.com:9120/cgna/ios/config
 execution-url https://<ip address of Loopback999 interface>:443/wsma/config
 interval 10
 gzip
 post-commands
 active
```

ACL Configuration (Optional)

You can include ACL configuration in this template for additional security.

A sample ACL configuration:

```
access-list 10 permit <IP address of TPS>
access-list 10 deny any

interface gigabitEthernet 0/0/0
ip access-group 10 in
exit
```

Note In the above sample configuration, the communication with FAR is only through IP address of TPS until the tunnel is established.

After the tunnel is established, you can remove the ACL configuration.

To remove the ACL configuration, add the following commands in the Router Tunnel Addition Template

```
no access-list 10
interface gigabitEthernet 0/0/0
no ip access-group 10 in
exit
```

HER Tunnel FlexVPN Configuration Template

A sample HER tunnel FlexVPN configuration template:

```
version 17.12
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
platform sslvpn use-pd
platform console virtual
!
hostname xxxxxxx
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login AUTH local
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
aaa authorization network NET local !
!
aaa session-id common
clock timezone IST 0 0
!
!

ip domain name cisco.com
!
!
!
login on-success log
!
!
subscriber templating
vtp version 1
!
!
!
!
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-141726200
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-141726200
 revocation-check none
 rsakeypair TP-self-signed-141726200
 hash sha256
!
crypto pki trustpoint SLA-TrustPoint
```

```
 enrollment pkcs12
 revocation-check crl
 hash sha256
!
!
crypto pki certificate chain TP-self-signed-141726200
 certificate self-signed 01
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxx
        quit
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  xxxxxxxxxxxxxx
        quit
!
!
!
!
!
!
!
!
!
license udi pid C8000V sn 9OA9SRYYZVZ
license boot level network-advantage addon dna-advantage
memory free low-watermark processor 203066
diagnostic bootup level minimal
```

```
!
!
spanning-tree extend system-id
!
!
!
username xxxxxx privilege 15 password 0 xxxxxxxxxx
!
redundancy
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
 route set access-list FlexVPN_Client_Default_IPv4_Route
!
crypto ikev2 redirect client
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
!
crypto ikev2 keyring FlexVPN_Keyring
 peer far1_sn
  identity fqdn far1_sn.cisco.com
  pre-shared-key GE39jy3Qe8Uo1Ro
!
 peer far2_sn
  identity fqdn far2_sn.cisco.com
  pre-shared-key LE73pj2Pk8Jh8Ui
!
 peer far3_sn
  identity fqdn far3_sn.cisco.com
  pre-shared-key FB86gn4Ns1Fm1Dj
!
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
 match identity remote fqdn domain cisco.com
 identity local key-id CLUSTER-2
 authentication remote pre-share
 authentication local pre-share
 keyring local FlexVPN_Keyring
 dpd 120 3 periodic
 aaa authorization group psk list FlexVPN_Author FlexVPN_Author_Policy
 virtual-template 1 !
!
!
!
!
!
!
!
!
!
!
crypto isakmp invalid-spi-recovery
!
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes esp-sha256-hmac
 mode transport
!
crypto ipsec profile FlexVPN_IPsec_Profile
```

```
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group14
 set ikev2-profile FlexVPN_IKEv2_Profile
 responder-only !
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address xx.xx.xx.xx 255.255.255.255
!
interface GigabitEthernet1
 ip address xx.xx.xx.xx 255.255.255.128
 negotiation auto
 no mop enabled
 no mop sysid
!
interface GigabitEthernet2
 ip address xx.xx.xx.xx 255.255.255.0
 negotiation auto
 no mop enabled
 no mop sysid
!
interface GigabitEthernet3
 no ip address
 shutdown
 negotiation auto
 no mop enabled
 no mop sysid
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip mtu 1200
 ip tcp adjust-mss 1240
 tunnel source GigabitEthernet2
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
ip default-gateway xx.xx.xx.xx
ip forward-protocol nd
!
ip http server
ip http authentication local
ip http secure-server
ip http secure-active-session-modules none
ip http active-session-modules none
ip dns server
ip ssh bulk-mode 131072 !
!
ip access-list standard FlexVPN_Client_Default_IPv4_Route
 10 permit any
!
!
!
!
!
!
!
control-plane
!
```

```
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable !
mgcp profile default
!
!
!
!
!
!
line con 0
 stopbits 1
line aux 0
line vty 0 4
 password cisco123
 transport input ssh
!
!
netconf legacy
netconf ssh
!
!
!
!
!
End
```

HER Tunnel Deletion Template

Note Ensure that the keyring name mentioned in "crypto ikev2 keyring FlexVPN_Keyring" and "FlexVPN_IKEv2_Profile" match the HER keyring name.

A sample HER tunnel deletion template for HERs on Cisco IOS and Cisco IOS-XE.

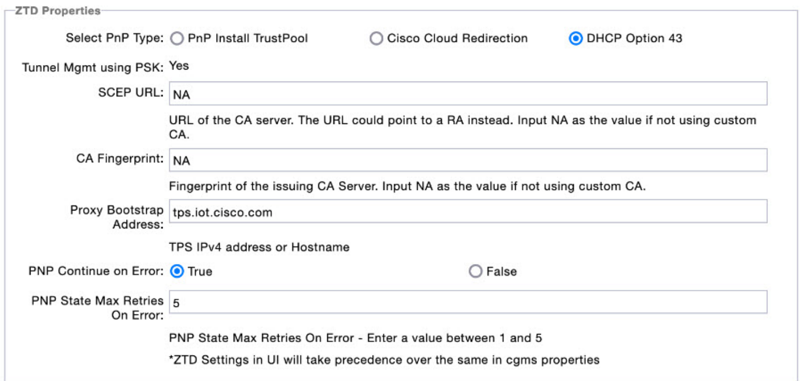
```
Remove Router PSK config from HER
<#-- This template only supports HERs running IOS or IOS XE. -->
<#if !her.isRunningIos() && !her.isRunningIosXe()>
  ${provisioningFailed("HER is not running IOS or IOS XE")}
</#if>

<#if far.isRunningIos()>
  <#assign sublist=far.eid?split("+")[0..1]>
  <#assign sn=sublist[1]>

  crypto ikev2 keyring FlexVPN_Keyring
    no peer ${sn}
  exit
</#if>
```

Configuring ZTD Properties

The ZTD Properties section allows you to manage the device certificates with either SUDI or a CA server. On configuring FND with PSK for tunnel management, by default, the devices use SUDI certificate for the communication with FND. However, if you want to manage using a CA server, provide details in the **SCEP URL** and **CA Fingerprint** fields (**ADMIN** > **SYSTEM MANAGEMENT** > **PROVISIONING SETTINGS**).



Workflow for Tunnel Management with PSK

This section provides the workflow for tunnel management with PSK.

Staging

To stage the router with FND TPS URL:

Procedure

Step 1 Configuring FND for PSK-based tunnels differ for each deployment as given below.

For **Bare Metal or Virtual Machine deployments with Oracle DB**, run the `setupCgms.sh` script before starting the cgms service for configuration with PSK based tunnel management. In these deployments, either the default Tunnel Provisioning group or a newly created Tunnel Provisioning group is used for PSK based tunnel management.

a) Before starting the cgms service, run the following script to configure FND with PSK tunnels.

```
/opt/cgms/bin/setupCgms.sh
```

For **Virtual Machine deployment with Postgres DB**, as the cgms service will already be running on OVA installation, the cgms service is restarted using the steps below while executing `setupCgms.sh` script. In this deployment, user creates a new Tunnel Provisioning group for PSK based tunnel management configuration.

a) Stop the cgms service.

```
./fnd-container.sh stop
```

b) Run the following script to configure FND to create IPsec tunnels for management with PSK.

```
/opt/cgms/bin/setupCgms.sh
```

c) Start the cgms service.

```
./fnd-container.sh start
```

d) Create new groups in the tunnel provisioning to on board devices that use PSK tunnels.

Step 2 Generate a public CA signed server certificate for TPS and FND using the existing CSR generation workflow.

Step 3 Configure FlexVPN on HER. For more information on the configuration, see HER Tunnel FlexVPN Configuration Template, on page 61.

Step 4 Import the device to FND through CSV or NB API.

a) During the device import, set the **tunnelHerEid** property on FAR to know the associated HERs. Ensure to set this property for the PnP to continue, else, the PnP cannot proceed.

FND generates a unique pre-shared key for each device and adds the generated key to the device property while storing in the database.

Step 5 Stage the router with FND TPS URL using DHCP option 43 or PnP Install Trustpool / Cloud Redirection for PnP.

What to do next

PnP Bootstrapping

PnP Bootstrapping

To bootstrap a device:

Before you begin

Staging.

Procedure

Step 1 Field area router (PnP agent) calls FND (through FND TPS).

Step 2 FND pushes the Trust Anchor (root certificate) to the device.

Step 3 To push the FAR PSK to the associated HER, a new state `CONFIGURING_HEADEND` is added in PnP.

Note
This state is executed only if IPsec tunnels are configured for management with PSK.

a) FND pushes the PSK to HER associated with the device in a separate batch process.

- On successful PSK configuration push on HER, an event is generated on FAR with the following message.

  ```
  PSK Tunnel configuration pushed successfully to HER
  ```

- On failure to push the PSK configuration on HER, an event is generated on FAR with the following message.

  ```
  PSK Tunnel configuration failed on HER
  ```

  Note
  FND keeps retrying (no limit) to push the configuration to HER until it succeeds as long as PnP requests come in.

Step 4 FND pushes the Bootstrap template to the device, which includes a tunnel creation profile and loopback IP configuration. For more information on the default templates, see Default Templates, on page 53.

a) Set the following commands in the bootstrap template for SUDI-based authentication.

```
no ip http secure-client-auth
ip http tls-version TLSv1.2
ip http client secure-trustpoint CISCO_IDEVID_SUDI
```

Use the `cgna initiator` profile as a tunnel creation profile. This is due to a platform limitation for Cisco IOS-XE device types, which does not support SUDI when the device is acting as a server in the TLS communication.

Step 5 On successful completion of PnP, the device status is marked as `Bootstrapped` in FND.

What to do next

Tunnel Provisioning, on page 68

Tunnel Provisioning

To push the PSK configuration to the router:

Before you begin

• Staging, on page 66
• PnP Bootstrapping, on page 67

Procedure

Step 1 Field area router calls FND (through FND TPS).

Authentication based on mTLS:

a) Validate the FND server based on the FND trust anchor.
b) Validate the field area router based on SUDI.

Step 2 FND pushes the PSK along with other tunnel configurations present in the Router Tunnel Addition template to the router and activates the registration profile.

a) Ensure that the following command is added in the Router Tunnel Addition template for the registration to work.

```
ip http secure-client-auth

no ip http tls-version TLSv1.2
```

What to do next

Device Configuration, on page 68

Device Configuration

To push device configuration to the router:

Before you begin

Complete the following workflows:

• Staging, on page 66

• PnP Bootstrapping, on page 67
• Tunnel Provisioning, on page 68

Procedure

Step 1 Field area router calls FND (through IPsec).

Authentication based on mTLS:

- Validate the FND server based on FND trust anchor.
- Validate the field area router based on SUDI.

Step 2 FND pushes the device configuration present in the Configuration Template to the router.

Step 3 On successful completion, the device is marked as `UP` in FND.

Pushing PSK Configuration to HER Cluster

This section explains the steps that are required to push the PSK configuration to HER in the cluster.

Pushing PSK Configuration to Existing HERs in the Cluster

Use the following steps to push the PSK configuration to the existing HERs in the cluster, which are added to the cluster before the tunnel establishment.

Procedure

Step 1 Import all HERs in the cluster to FND and have them managed with the device status as UP.

Step 2 For FND to be aware of the list of HERs in a cluster, add the list of HER eids separated by comma in the `tunnelhereid` property.

Step 3 On receiving a PnP request from a FAR, the `tunnelhereid` property is checked to get the list of HERs in the cluster.

Step 4 PSK configuration is pushed to each HER in the cluster.

- PnP continues if at least one of the HERs in the cluster receives the PSK configuration successfully.
- If the PSK configuration push fails on HERs, then correct the HER or replace it with a new HER by updating the `tunnelHerEid` property of the FAR.

The following events are generated for the PSK configuration push to HER in a cluster.

- If the PSK configuration push to HER is successful, then an event is generated for the router with the following message.

  ```
  "PSK Tunnel configuration pushed successfully to HER [**eid**]"
  ```

- If the PSK configuration push to HER fails, then an event is generated for the router with the following message.

```
"PSK Tunnel configuration failed on HER [**eid**]".
```

Pushing PSK Configuration to New HER in the Cluster

Use the following steps to push the PSK configuration to a new HER, which is added to the cluster after the tunnel is established.

Note The addition or removal of HERs from the `tunnelHerEid` list is added to a table named `pending_tunnel_her_in_cluster` in the DB. FND has a separate thread that runs every five minutes to pick up the entries from the table and based on the `add_peer` flag, it either pushes the PSK configuration or removes the PSK configuration to or from the HER.

Procedure

Step 1 Import the new HER to FND and have it managed with the device status as UP.

Step 2 Update the FAR using **Change Device Properties** to add the new HER to the `tunnelhereid` property list.

Note
HER must be managed by FND before updating FAR using **Change Device Properties**.

Step 3 The PSK configuration is pushed to the new HER added to the `tunnelHerEid` property list and an associated event (success or failure) is generated on the FAR.

If any HER is removed from the `tunnelHerEid` property, then the PSK configuration of that HER is removed and an event is generated for successful configuration removal on the HER.

Viewing Events

This section provides information on the events generated on FAR and HER when pushing and removing PSK tunnel configuration.

- Viewing FAR Events
- Viewing HER Events

Viewing FAR Events

Use the following steps to view the events generated when pushing PSK tunnel configuration on HER during FAR onboarding.

1. Choose **DEVICES** > **FIELD DEVICES**.
2. Select the device on the right pane. The Device Info page appears.
3. Click the **Events** tab to view the following events.

Event Name	Severity Level	Description
PSK Tunnel Configuration Pushed to HER	INFO	On successful completion of pushing PSK tunnel configuration on HER.
PSK Tunnel Configuration on HER Failed	Major	On failure to push the PSK tunnel configuration on HER.

Viewing HER Events

Use the following steps to view the events generated when removing the PSK tunnel configuration from HER and FAR during FAR decommissioning.

1. Choose **DEVICES** > **HEAD-END ROUTERS**.
2. Select the HER on the right pane. The Device Info page appears.
3. Click the **Events** tab to view the following events.

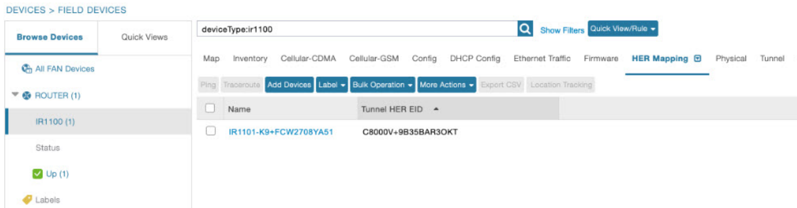
Event Name	Severity Level	Description
HER PSK Tunnel Configuration Removed for FAR	INFO	On successful removal of PSK configuration from HER.
HER PSK Tunnel Configuration Removal Failure for FAR	Major	On failure to remove the PSK configuration from HER. **Note** In this case, you should remove the PSK configuration from HER manually.

HER Mapping with FAR

Use the following steps to view the HERs associated with the FAR.

1. Choose **DEVICES** > **FIELD DEVICES**.
2. Select the device on the left pane.
3. Click the **HER Mapping** tab on the right pane.
4. The HER associated with the device appears under the **Tunnel HER EID** column.

   Use the filter option to search for HERs based on HER EID.



Decommissioning a Device

Whenever there is a device decommissioning, FND automatically removes the PSK configuration from HER using the HER deletion template which is available by default. If the HER is in a cluster, FND removes the PSK configuration from all HERs.

For information on HER deletion template, see HER Tunnel Deletion Template, on page 65.

For information on events generated during PSK configuration removal from HER, see Viewing HER Events, on page 71.

List of Ports used in Simplified IoT FND Architecture for Router only Deployments

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

Service	Port
GUI	443
Tunnel Provisioning	9120
TPS	9122
Oracle DB Server	1522
PostGreSql DB Server	5432
Influx	8086
Kapacitor	9092
WSMA (for IOS-XE)	443
WSMA (for Classic IOS)	8443
Registration + Periodic	9121
Bandwidth Op Mode	9124
PnP — HTTP	9125
Web Sockets — Device Communication	9121

Service	Port
DB Replication for HA	1622
SSH	22
NTP Server	123
SNMP (for polling)	161
SNMP (for notifications)	162
SSM Server	8445
FND Demo Mode	80
Syslog service	514

PSK Challenge String Support

The pre-shared key challenge string is supported to enhance the security between FND and FAR in the SUDI+PSK based tunnel management. In this process, FND generates the challenge string during its first communication with the device. The generated nonce is pushed to the device and signed using the SUDI certificate. The signed response is validated against the SUDI certificate and the hash of the nonce is verified against the nonce sent by FND. The nonce is verified only for the first time when a device communicates with FND.

Only Cisco IOS-XE devices support the challenge string using the SUDI certificate.

Note By default, the challenge string validation is enabled for PSK-based tunnels. However, you can skip the device validation using the challenge string by setting the cgms.properties to false. After disabling the property, you have to restart the cgms service.

```
enable-challenge-string-auth=false
```

Device Validation Using a Challenge String

FND validates the device during onboarding by sending a challenge string using the following command.

```
sh platform sudi certificate sign nonce <generated number>
```

- On successful verification, FND authenticates the device for further communications.
- If the verification fails, an error message is logged in the server.log file, and the device is not onboarded.

PSK Rotation

To protect against pre-shared key (PSK) vulnerabilities and hacks, PSK rotation is utilized in FND, which provides an additional layer of security for the device communication. This involves running the script either manually or schedule using a cron. The script is bundled with the cgms tools package of FND. The cgms tools package is installed on either FND Oracle Bare Metal or Postgres VM. However, you can also install the cgms tools package on a separate VM (It is not necessary to have FND installed in this VM). For information on installing cgms tools on a separate VM, see Installing CGMS Tools RPM on a Separate VM, on page 76.

When the script is run, it rotates the pre-shared key at both HER and FAR and flaps the tunnels for a secure network. The PSK rotation feature is available only to customers who use PSK for tunnel management with FlexVPN.

- Manual PSK Rotation
- Schedule PSK Rotation Using Cron

Prerequisites

Ensure that all prerequisites are met before running the PSK rotation script for every fresh install or upgrade.

- Run the script during the maintenance window.
- Ensure that the FND service is not active when executing the script.
- Ensure that there are no active operations (like configuration push, firmware upgrade) running in FND.
- Copy the following files from cgms rpm package (`/opt/cgms`) to cgms-tools package (`/opt/cgms-tools`).

Filename	Copy From (cgms package)	Copy To (cgms-tools package)
.fnd_psk_enc	/opt/cgms/server/cgms/conf/.fnd_psk_enc	/opt/cgms-tools/conf
fnd_psk.keystore	/opt/cgms/server/cgms/conf/fnd_keystore	/opt/cgms-tools/conf
jdbc.properties	/opt/cgms/tools/conf/jdbc.properties	/opt/cgms-tools/conf/jdbc.properties
cgms_keystore	/opt/cgms/server/cgms/conf/cgms_keystore	/opt/cgms-tools/conf
cgms.properties	/opt/cgms/server/cgms/conf/cgms.properties	/opt/cgms-tools/conf

Manual PSK Rotation

Run the following script (location: `/opt/cgms-tools/bin`) to rotate the PSK.

```
$ ./rotate-psk <csv-file>
```

The `<csv-file>` refers to the CSV file location, which contains the list of HER name or FAR name (with HER peer name).

- If the CSV file contains the name of the HER, then the HER PSK of all the FARs and the FAR PSK are rotated.
- If the CSV file contains the name of the FAR, then the PSK of the specified FAR and the HER associated with the FAR are rotated.

Sample CSV file with HER NAME:

```
HER_NAME,  HER_PEER_NAME, KEYRING_NAME
C8000V+9B35BAR3OKT, CLUSTER-2, FlexVPN_Keyring
C8000V+9OA9SRYYZVZ, CLUSTER-1, FlexVPN_Keyring1
```

> **Note** HER_PEER_NAME is the `identity local key-id name` configured on the HER.

Sample CSV file with FAR NAME:

```
FAR_NAME,     HER_PEER_NAME , KEYRING_NAME
IR1835-K9+FCW2730Y1UZ, CLUSTER-1, FlexVPN_Keyring
IR1101-K9+FCW2710ZA25, CLUSTER-2, FlexVPN_Keyring1
IR1101-K9+FCW2708YA53, CLUSTER-2, FlexVPN_Keyring2
```

The status of the device PSK rotation, for both success or a failure, is available in the CSV file (`rotate-psk-timestamp.csv`).

Log Location:

- The output status log of PSK rotation for each device is stored at: `/opt/cgms-tools/log/rotate-psk-<timestamp>.csv`.

  Sample CSV output:

  ```
  ROUTER,MESSAGE,STATUS
  IR1835-K9+FCW2730Y1UZ,PSK update for FAR IR1835-K9+FCW2730Y1UZ was failure as FAR is
  down ,FAILURE
  IR1835-K9+FCW2730Y2UZ,PSK update success for FAR IR1835-K9+FCW2730Y1UZ connected to HER
   C8000V+9B35BAR3OKT,SUCCESS
  ```

- Debug logs are stored at: `/opt/cgms-tools/log/rotate-psk.log`.

Schedule PSK Rotation Using Cron

Alternatively, cron is used to run the script automatically at a specific time and day of a month. You can schedule PSK rotation for the following deployments:

- Oracle Bare Metal
- Postgres OVA

The following prerequisites are must for both deployments:

- Ensure that the script is scheduled to run during the monthly maintenance window to avoid conflict with other active operations in FND.
- For a successful PSK rotation, it is recommended to allow a 24-hour gap between each script execution.

> **Note** After each successful PSK rotation, the tunnel is toggled. As a result, the tunnel between HER and FAR comes up with a new PSK value.

Oracle Bare Metal Deployment

Run the following script to schedule PSK rotation.

In the example below, the script is scheduled to run at 12.00 AM on the first day of every month.

```
$ cd /etc
$crontab -e
#Add below line in crontab. Save the file
0 0 1 * * /opt/cgms-tools/bin/rotate-psk <location to csv>
```

Postgres OVA Deployment

Follow the steps to schedule PSK rotation for Postgres OVA.

Procedure

Step 1 Install the tools `rpm` in VM.

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

```
host all all <IP of the VM to be entered here>/32 md5
```

Step 3 Restart `postgresql`.

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

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

a) `docker cp fnd-container:/opt/cgms/server/cgms/conf/.fnd_psk_enc /opt/cgms-tools/conf`

b) `docker cp fnd-container:/opt/cgms/server/cgms/conf/fnd_psk.keystore /opt/cgms-tools/conf`

c) `docker cp fnd-container:/opt/cgms/tools/conf/jdbc.properties /opt/cgms-tools/conf/jdbc.properties`

d) `docker cp fnd-container:/opt/cgms/server/cgms/conf/cgms_keystore /opt/cgms-tools/conf`

e) `docker cp fnd-container:/opt/cgms/server/cgms/conf/cgms.properties /opt/cgms-tools/conf`

Installing CGMS Tools RPM on a Separate VM

Follow the steps to install CGMS tools rpm on a separate VM.

Procedure

Step 1 Install the `cgms-tools` rpm.

- For the Oracle deployment, the `cgms-tools` package is part of <.iso> image.
- For the Postgres deployment, extract the cgms tools file (CISCO-IOTFND-VPI-K9-CGMS-TOOLS-<release>-<build>.zip) from the upgrade script (CISCO-IOTFND-VPI-K9-UPGRADE-SCRIPTS-<release>-<build number>.zip) and install the cgms tools in the server. For more information, see Postgres Installation Guide.

Step 2 Copy the prerequisite files from the FND server to the path where the `cgms-tools` package is installed.

- `copy .fnd_psk_enc from /opt/cgms/server/cgms/conf/.fnd_psk_enc to /opt/cgms-tools/conf`

- `copy fnd_psk.keystore from /opt/cgms/server/cgms/conf/fnd_psk.keystore to /opt/cgms-tools/conf`
- `copy jdbc.properties from /opt/cgms/tools/conf/jdbc.properties to /opt/cgms-tools/conf/jdbc.properties`
- `copy cgms_keystore from /opt/cgms/server/cgms/conf/cgms_keystore to /opt/cgms-tools/conf`
- `copy cgms.properties from /opt/cgms/server/cgms/conf/cgms.properties to /opt/cgms-tools/conf`

Step 3 Provide Postgres IP in the `jdbc.properties` as below.

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

Step 4 Add the route in the server for the device reachability.

On successful cgms tools installation, the PSK rotation script is executed.

IPAM for Loopback

Loopback IP addresses for FAR devices forming tunnels was assigned by an external DHCP Server with FND acting as the DHCP client. IoT FND now generates the IPv4 and IPv6 addresses for the provided subnet while forming the tunnels without relying on the third-party DHCP Server. The consumption of internal IP addresses applies only for first-time IoT FND installation and the users with administrative privileges only can access. This is supported only in root domain.

Procedure

Step 1 While setting up IoT FND, run the setupCgms.sh script on the IoT FND server and choose your preferred IP allocation method for loopback IPs in the user prompt. For more information about running the setupCgms.sh script, see Setting Up IoT FND.

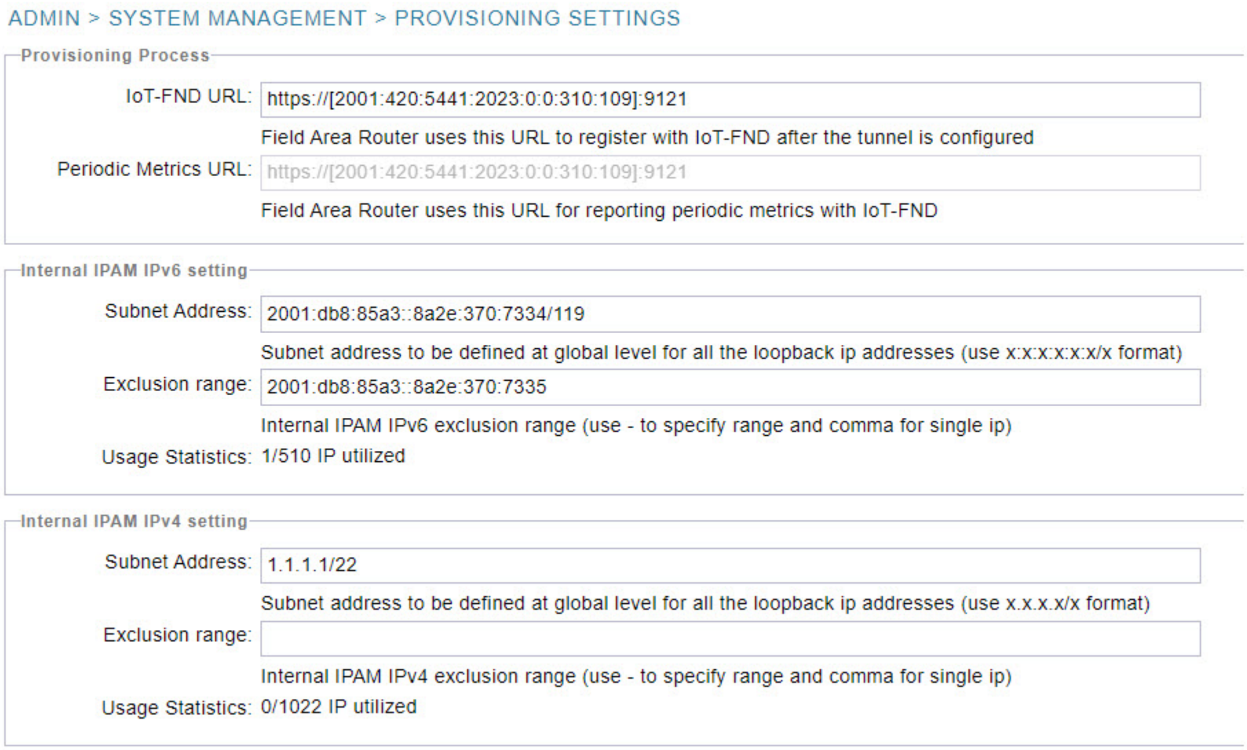
Step 2 If you choose IPAM, configure the subnet in the **Admin** > **System Management** > **Provisioning Settings** page.

Note
To configure the subnet range, set the limit in **ipam-ipv6-subnet-limit** or **ipam-ipv4-subnet-limit** property in cgms.properties file. The default values for the properties are 108 (generates around 1,048,576 IPv6) and 12 (generates around 1,048,576 IPv4) respectively.

Caution
Do not decrease the subnet size. If you intend to utilize more than 1 million IP addresses, we recommend consulting with Cisco for expert guidance and support.

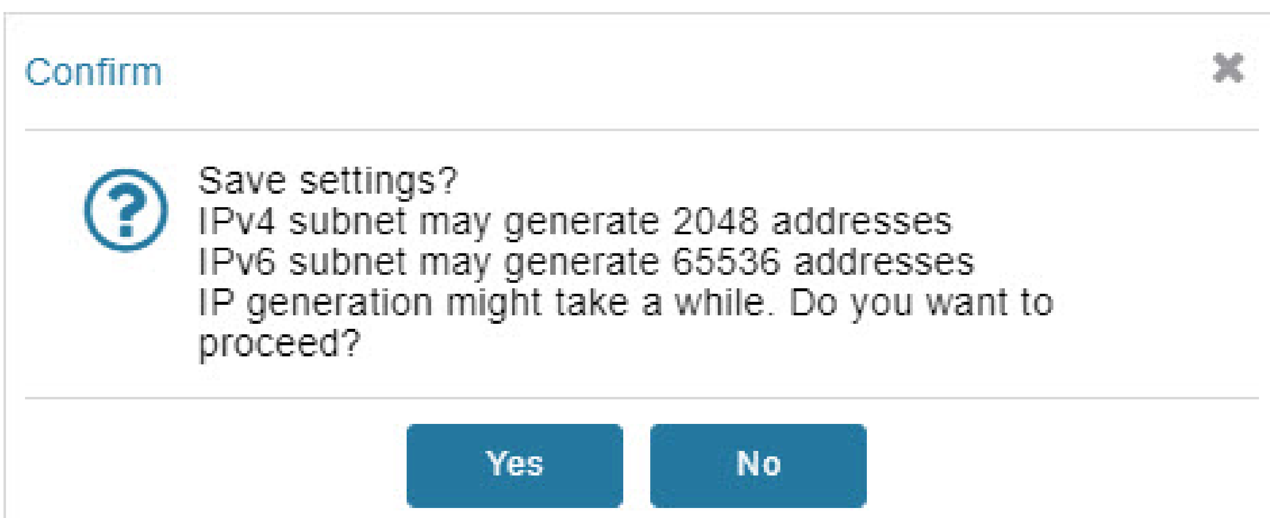
Step 3 Provide the exclusion range as a single IP address, a range, or a list of multiple IP addresses separated by commas. The Usage Statistics is a label that shows the IP addresses utilized for the provided subnet.

Note
Provide values in either or both of the IPAM IPv6 and IPAM IPv4 setting.



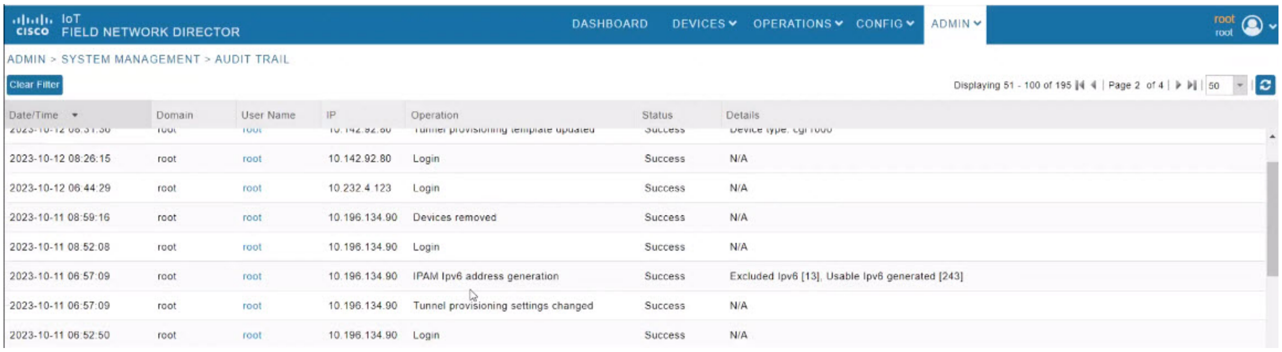
Step 4 Click the Disk icon to save changes. The following window pops up to show the probable IP addresses that will be generated.

Note
If you choose to modify the subnet after the warning, then IoT FND deletes all the existing ip addresses created under previous subnet except the one being used and generates fresh ip addreses for new subnet.



Step 5 Click **Yes**.

Step 6 Navigate to **ADMIN** > **SYSTEM MANAGEMENT** > **AUDIT TRAIL** page to check for the number of excluded IPs and the generated usable IPs.

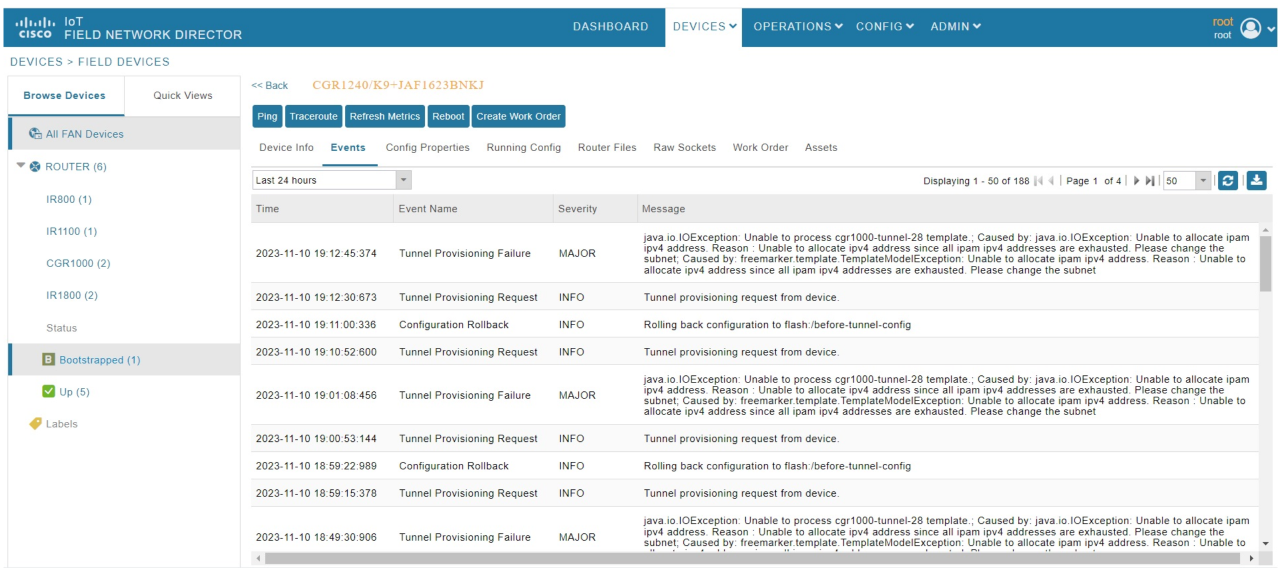


After configuring subnet settings and generating IP addresses, initiate the tunnel provisioning process.

Note

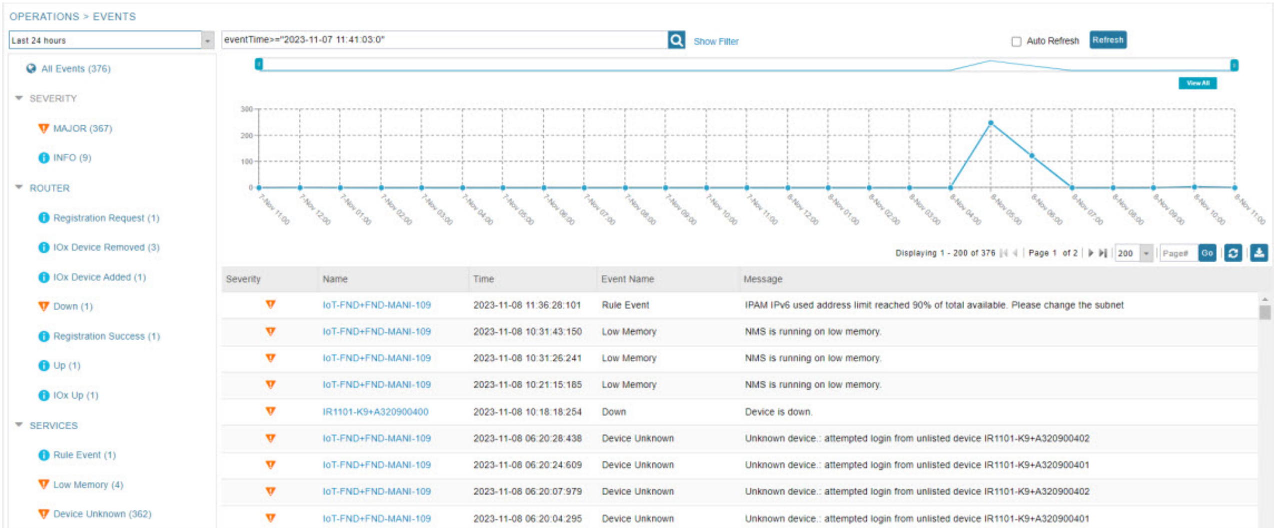
During tunnel provisioning, if the IP address is provided in the CSV in the `loopbackv4address` and `loopbackv6address` property when adding routers, it is utilized as the loopback IP address. In case the IP address is not provided in the CSV, then internal IP address is fetched.

If the tunnel provisioning fails as IP address lease exceeds, then the error message is seen in the **DEVICES** > **FIELD DEVICES** page under Events tab.



Note

In the **Operations** > **Events** page, check the event generated. A minor event is generated if the percentage of utilization crosses 80% of total generated IP. Similarly, a major event is generated if the percentage of utilization crosses 90% of total generated IP. You can configure the limit for major threshold in **ipam-ipAddress-pool-thresold-limit** property in cgms.properties file. The default value is set to 90, if not configured.



Once tunnels are assigned an IP address, the DB is also updated.

For tunnel reprovisioning, the router uses the same IP address.

IPAM for All Interfaces

The IP addresses for FAR devices forming tunnels was assigned by an external DHCP server with IoT FND acting as the DHCP client. IoT FND now generates the IPv4 and IPv6 addresses for the provided subnet while forming the tunnels without relying on the third-party DHCP server. The consumption of internal IP addresses applies only for first-time IoT FND installation and the users with administrative privileges only can access. This is supported only in root domain.

Starting from IoT FND release 4:12 onwards, IoT FND supports IPAM for all interfaces. You can define multiple subnets and IoT FND manages those subnets.

Note When you upgrade to IoT FND release 4:12, one subnet is migrated, subnet id is created and listed under the respective tabs in the Provisioning settings page.

Procedure

Step 1 To enable IPAM, run the setupCgms.sh script on the IoT FND server while setting up IoT FND. Choose IPAM in the user prompt. IPAM takes precedence over DHCP server for IP address management. For more information about running the setupCgms.sh script, see Setting Up IoT FND.

Step 2 If you choose IPAM, configure the subnet in the **Admin** > **System Management** > **Provisioning Settings** page.

Step 3 Click the IPAM-IPv4 and IPAM-IPv6 tabs to define the IPv4 and IPv6 subnets.

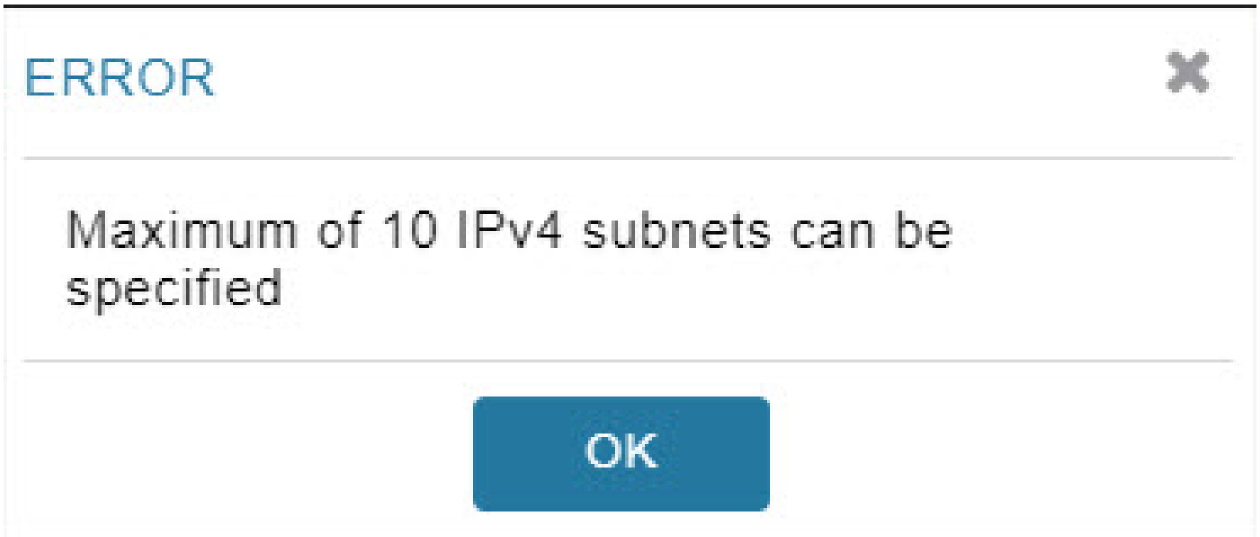
Note

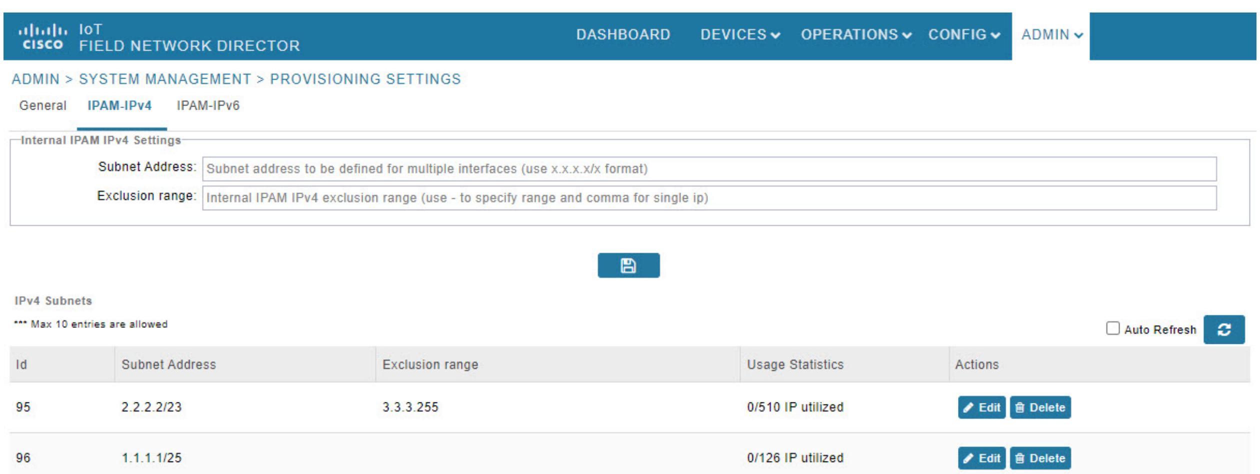
To configure the subnet range, set the limit in **ipam-ipv6-subnet-limit** or **ipam-ipv4-subnet-limit** property in cgms.properties file. The default values for IPv6 and IPv4 properties are 108 (generates around 1,048,576 IPv6) and 12 (generates around 1,048,576 IPv4) respectively.

Caution
Do not decrease the subnet size. If you intend to utilize more than 1 million IP addresses, we recommend consulting with Cisco for expert guidance and support.

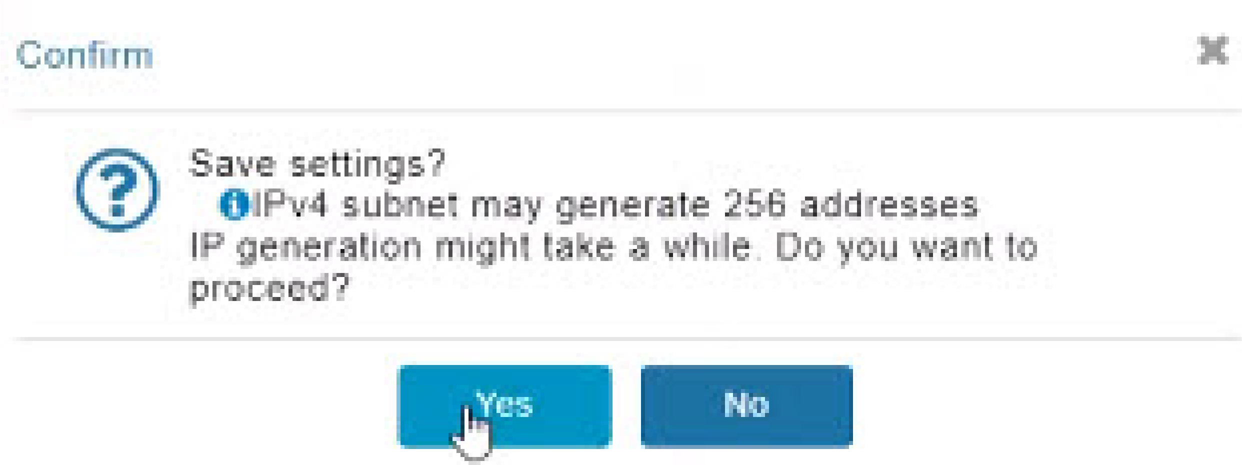
Step 4 Enter the Subnet Address and Exclusion range. The Exclusion range can be provided as a single IP address, range, or list of multiple IP addresses separated by commas.

Note
You cannot define more than 10 subnets. The following error message appears when you try to define additional subnets. This is applicable for IPv6 subnets as well.

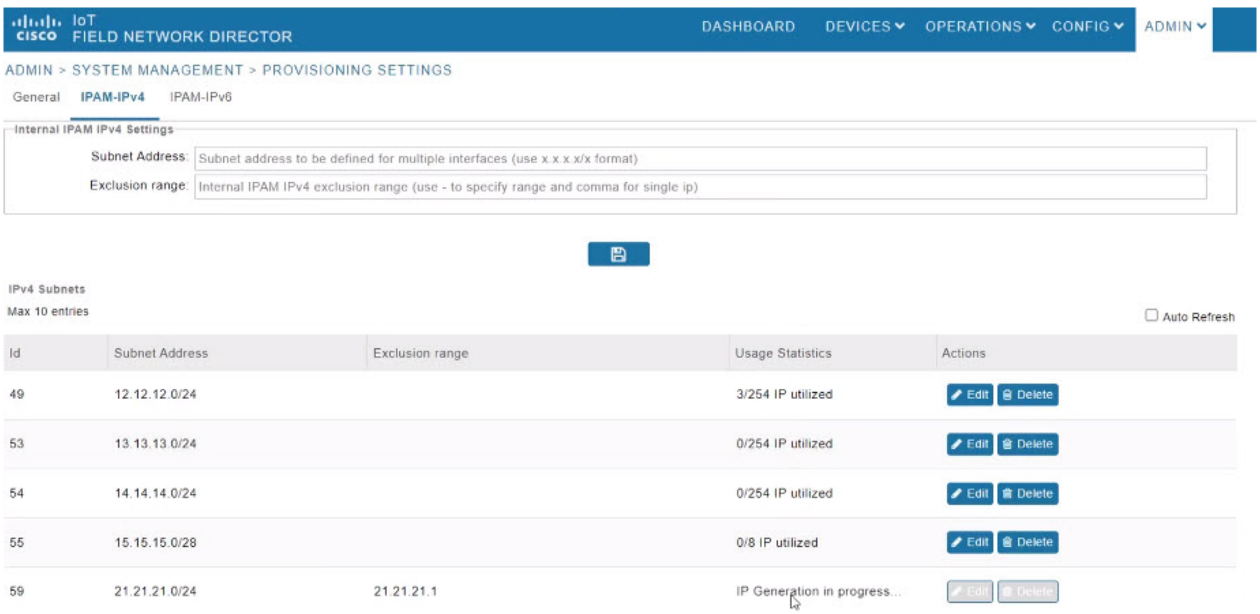




Step 5 Click the Disk icon to save changes. The following window pops up to show the probable IP addresses that will be generated.



Step 6 Click **Yes**. The IP address generation is in progress.



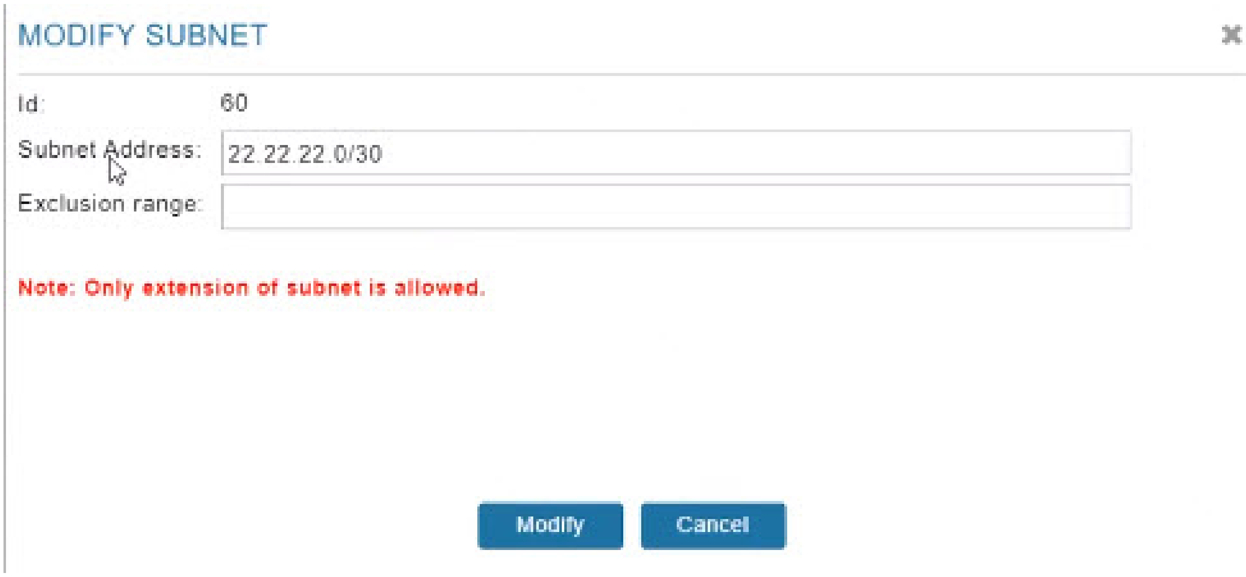
The following table describes the fields in the IPv4 Subnets tab.

Field	Description
Id	Indicates the subnet id allocated for the defined subnet.
Subnet Address	Indicates the defined subnet address.
Exclusion range	Indicates the range of IP addresses within a subnet that are excluded from being assigned to devices.
Usage Statistics	Indicates the IP addresses utilized for the provided subnet.
Actions	You can either modify or delete the subnets.

Step 7 To edit the subnet details:

- Click Edit to modify the subnet.
- Edit the Subnet Address and Exclusion range and click **Modify**.

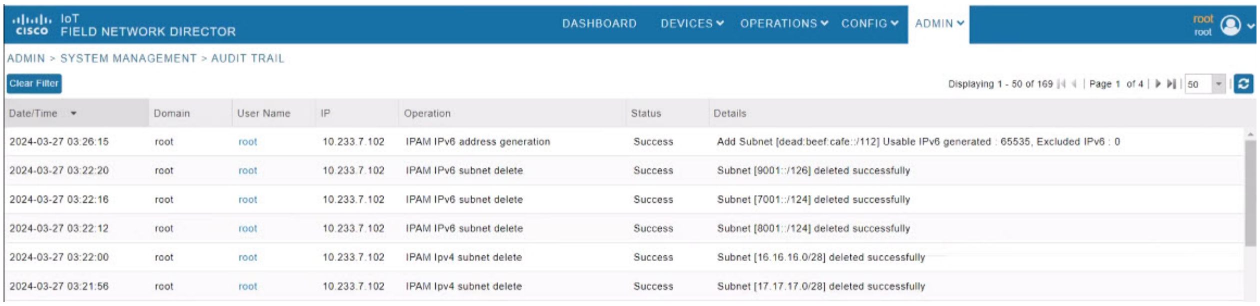
Important
You can only extend the subnet while editing and shrinking the subnet is not allowed.



You can also delete the subnet by clicking the delete icon. In case you delete the subnet where some of the IPs are utilized, the following warning pops up. Click **Yes** to proceed.

Note
It is recommended to recheck before proceeding as there are no restrictions in deletion.

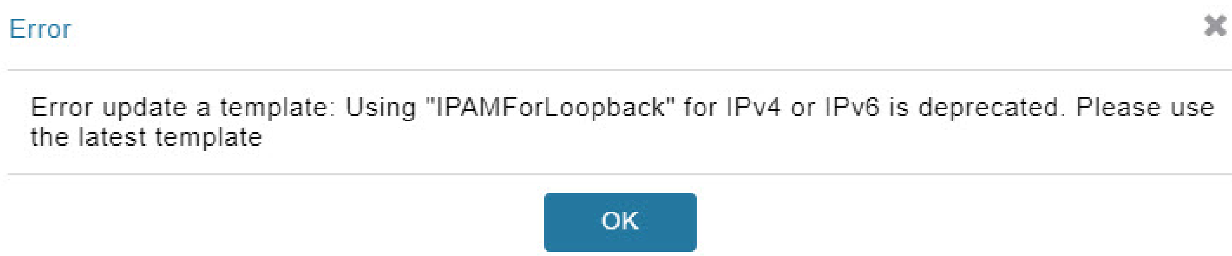
Step 8 Navigate to **ADMIN** > **SYSTEM MANAGEMENT** > **AUDIT TRAIL** page to see the addition, modification, and deletion of the subnets.



Step 9 Go to **CONFIG** > **TUNNEL PROVISIONING** and click Router Tunnel Addition. Enter the Subnet ID in the Router Tunnel Addition template and click Save.

```
interface Loopback0
    <#--
      If the loopback interface IPv4 address property has been set on the CGR
      then configure the interface with that address. Otherwise obtain an
      address for the interface now using DHCP.
    -->
    <#if far.loopbackV4Address??>
      <#assign loopbackIpv4Address=far.loopbackV4Address>
    <#elseif far.isIPAMSelected()??>
      <#assign loopbackIpv4Address=far.IPAMIpv4address(1)>
    <#else>
      <#--
        Obtain an IPv4 address that can be used to for this FAR's Loopback
        interface. The template API provides methods for requesting a lease from
        a DHCP server. The IPv4 address method requires a DHCP client ID and a link
        address to send in the DHCP request. The 3rd parameter is optional and
        defaults to "IoT-FND". This value is sent in the DHCP user class option.
        The API also provides the method "dhcpClientId". This method takes a DHCPv6
        Identity association identifier (IAID) and a DHCP Unique IDentifier (DUID)
        and generates a DHCPv4 client identifier as specified in RFC 4361. This
        provides some consistency in how network elements are identified by the
        DHCP server.
      -->
      <#assign
loopbackIpv4Address=far.ipv4Address(dhcpClientId(far.enDuid,0),far.dhcpV4LoopbackLink).address>
    </#if>
    ip address ${loopbackIpv4Address} 255.255.255.255
    <#--
      If the loopback interface IPv6 address property has been set on the CGR
      then configure the interface with that address. Otherwise obtain an
      address for the interface now using DHCP.
    -->
    <#if far.loopbackV6Address??>
      <#assign loopbackIpv6Address=far.loopbackV6Address>
    <#elseif far.isIPAMSelected()??>
      <#assign loopbackIpv6Address=far.IPAMIpv6address(21)>
    <#else>
```

Note
IoT FND throws the following error while processing the template during tunnel provisioning if the template contains obsolete methods.

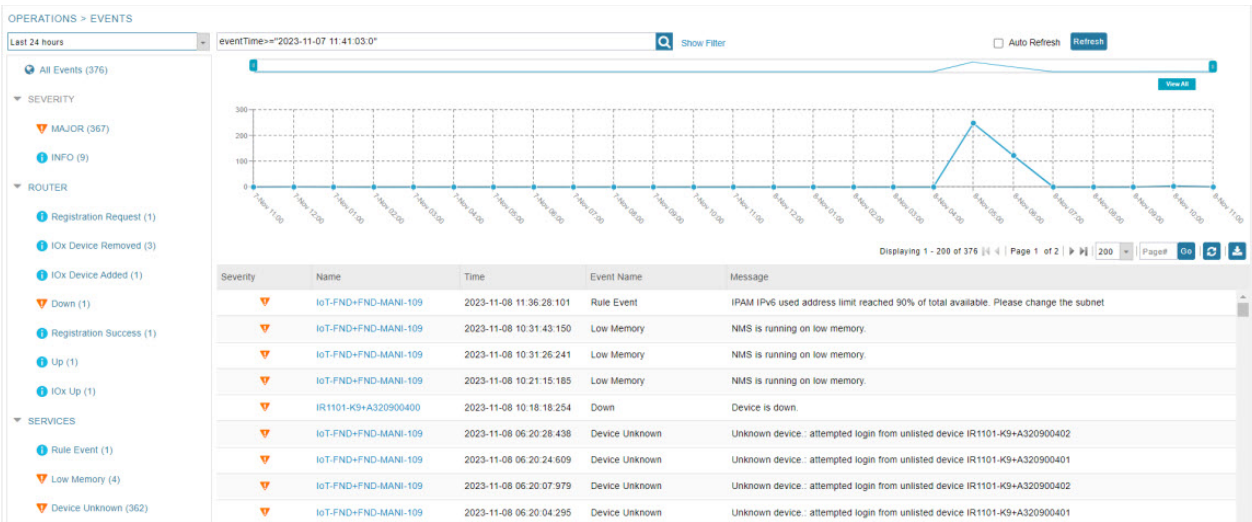


Step 10 After configuring subnet settings and generating IP addresses, initiate the tunnel provisioning process. Once the PNP is complete, the IP addresses are allocated to the respective interfaces which can be seen under the IPv4 and IPv6 tabs in the **Admin** > **System Management** > **Provisioning Settings** page.

Note

During tunnel provisioning, if the IP address is defined in the CSV in `loopbackv4address` and `loopbackv6address` property while adding routers, it is utilized as the loopback IP address. In case the IP address is not provided in the CSV, then internal IP address is fetched. This is applicable for loopback interface only.

Step 11 In the **Operations** > **Events** page, an event is generated if the percentage of utilization crosses 90% of total generated IP.You can configure the limit for major threshold in **ipam-ipAddress-pool-thresold-limit** property in cgms.properties file. The default value is set to 90, if not configured.



Once tunnels are assigned an IP address, the DB is also updated.

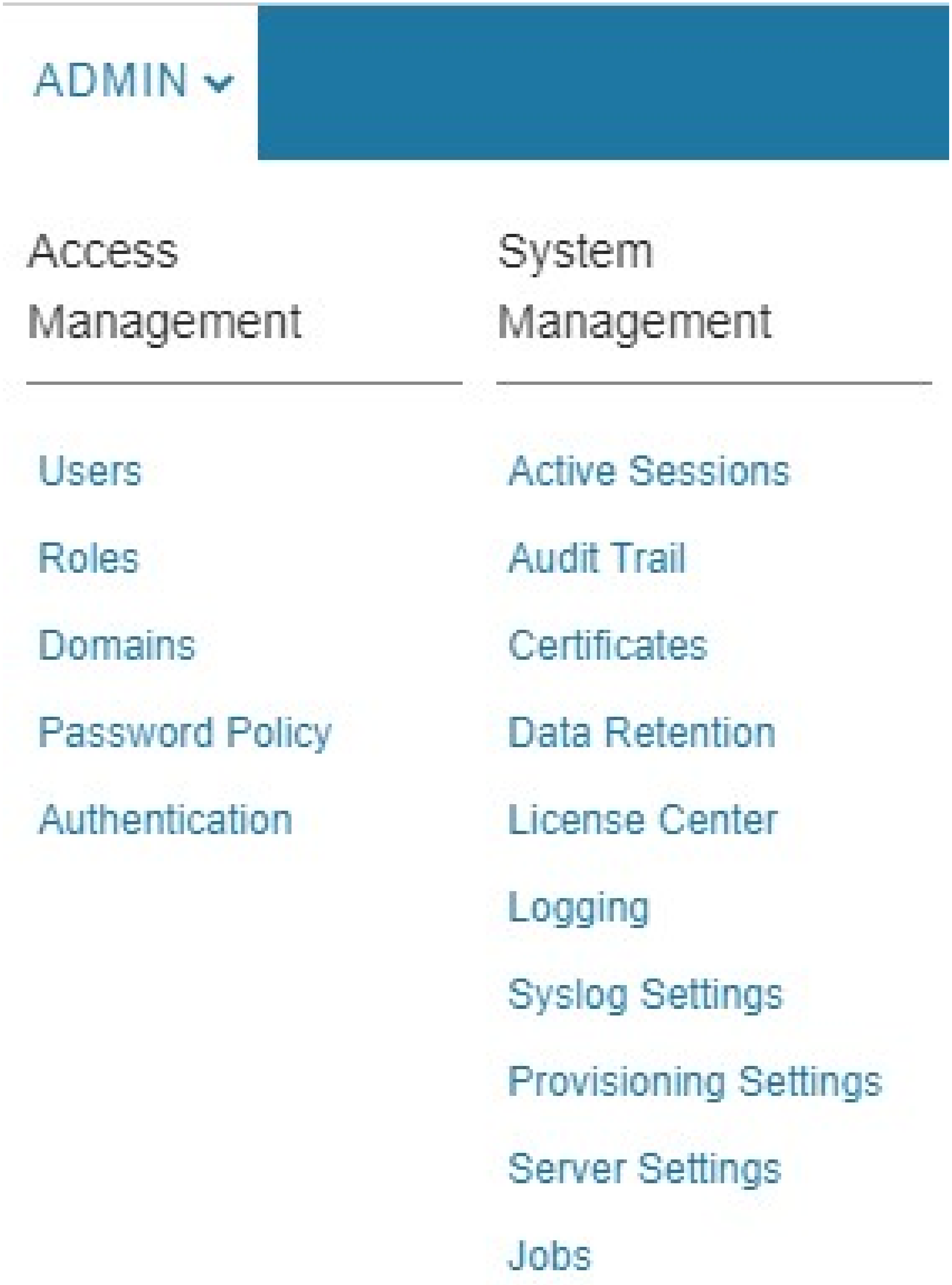
During decommissioning of the device or subnet, IPAM IP address is marked unused. Click Refresh and the IP addresses is released.

CHAPTER 4

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.


ADMIN
Access Management
System Management
Users
Roles
Domains
Password Policy
Authentication
Active Sessions
Audit Trail
Certificates
Data Retention
License Center
Logging
Syslog Settings
Provisioning Settings
Server Settings
Jobs

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.

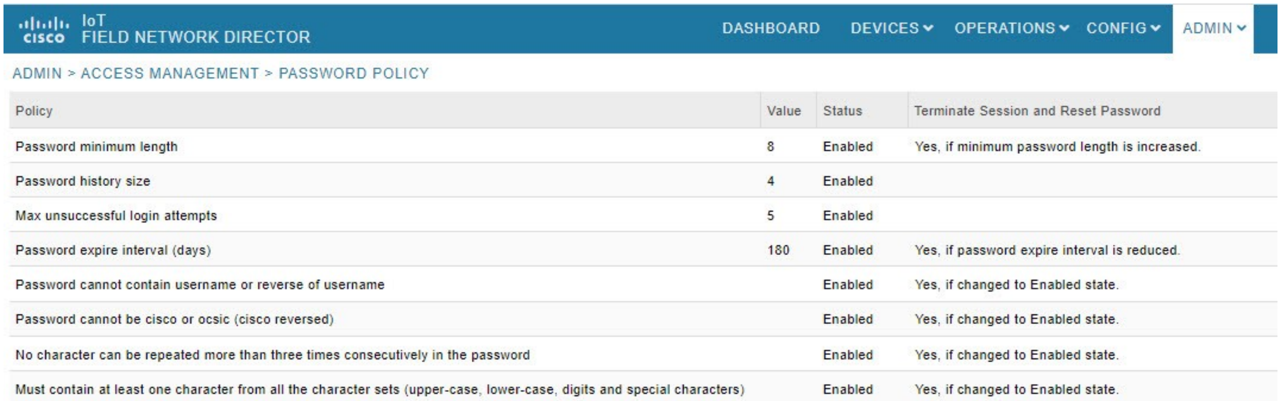
These changes ***invalidate*** all user sessions and expire their passwords (including the root user):

- 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:

Procedure

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.

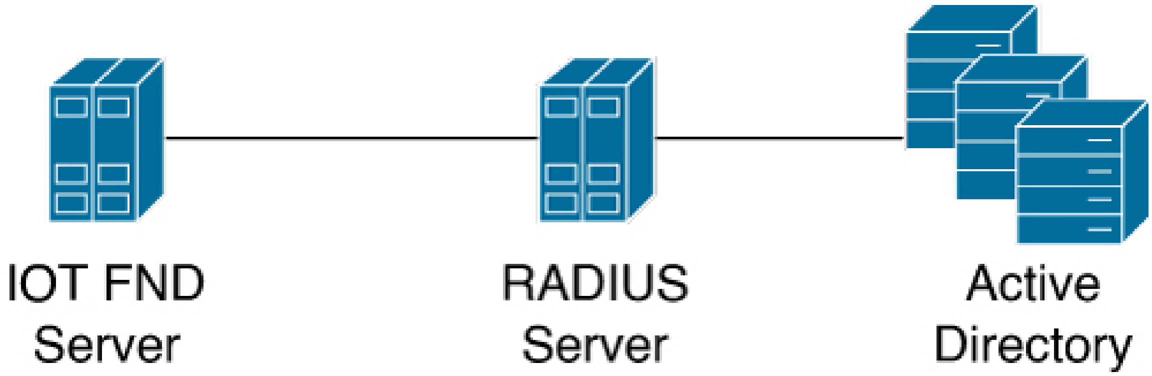
Configuring Remote Authentication

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:

Procedure

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.

Field	Description
Shared Secret	The shared secret you configured on the RADIUS server.
Confirm Shared Secret	
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.

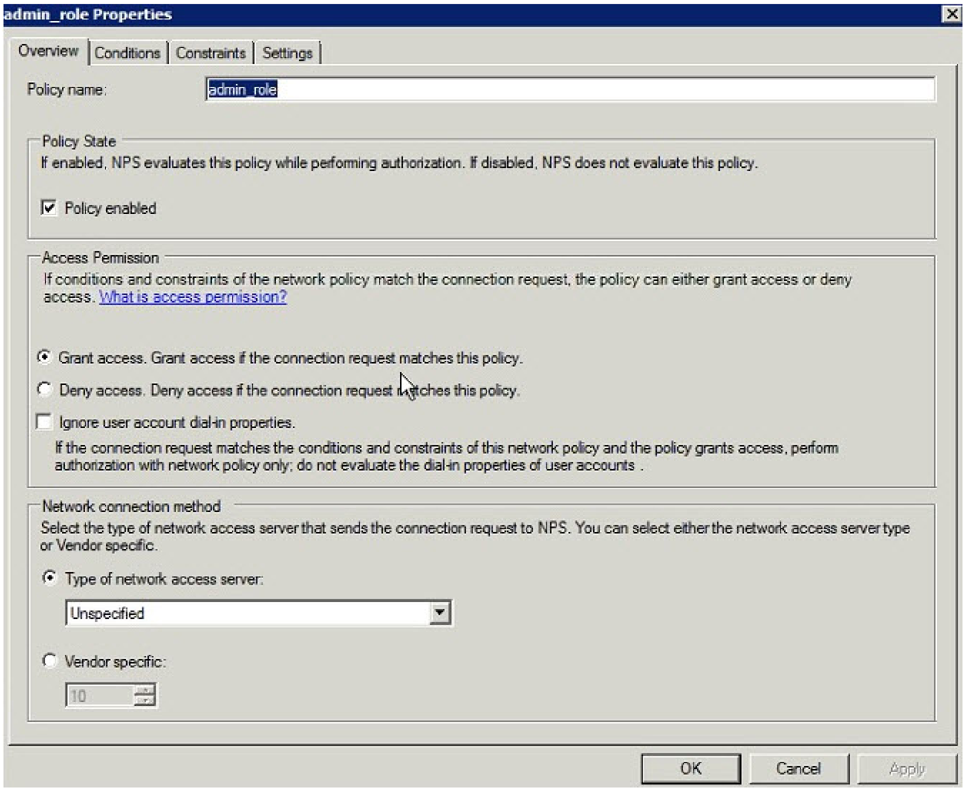
To configure security policies on the RADIUS server, follow these steps:

Procedure

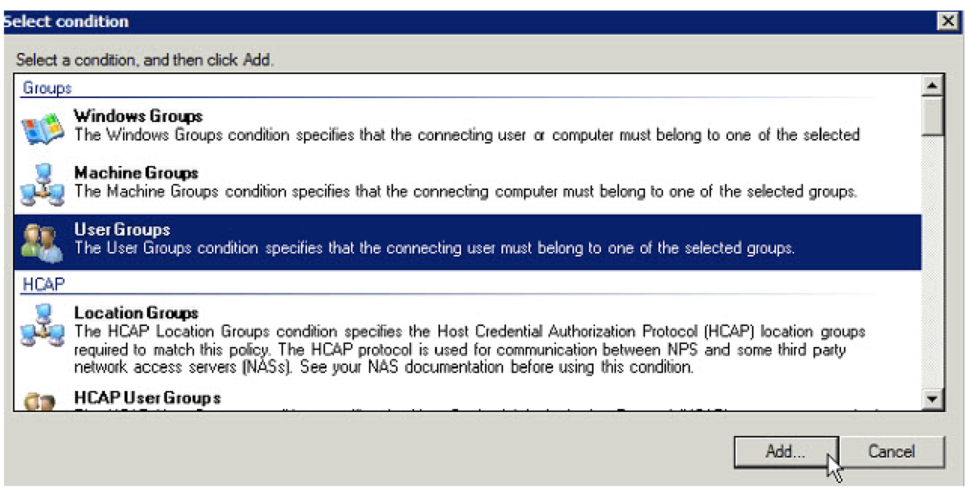
Step 1 Create a network policy for each security group you created in AD.

Step 2 Configure the policy as follows:

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

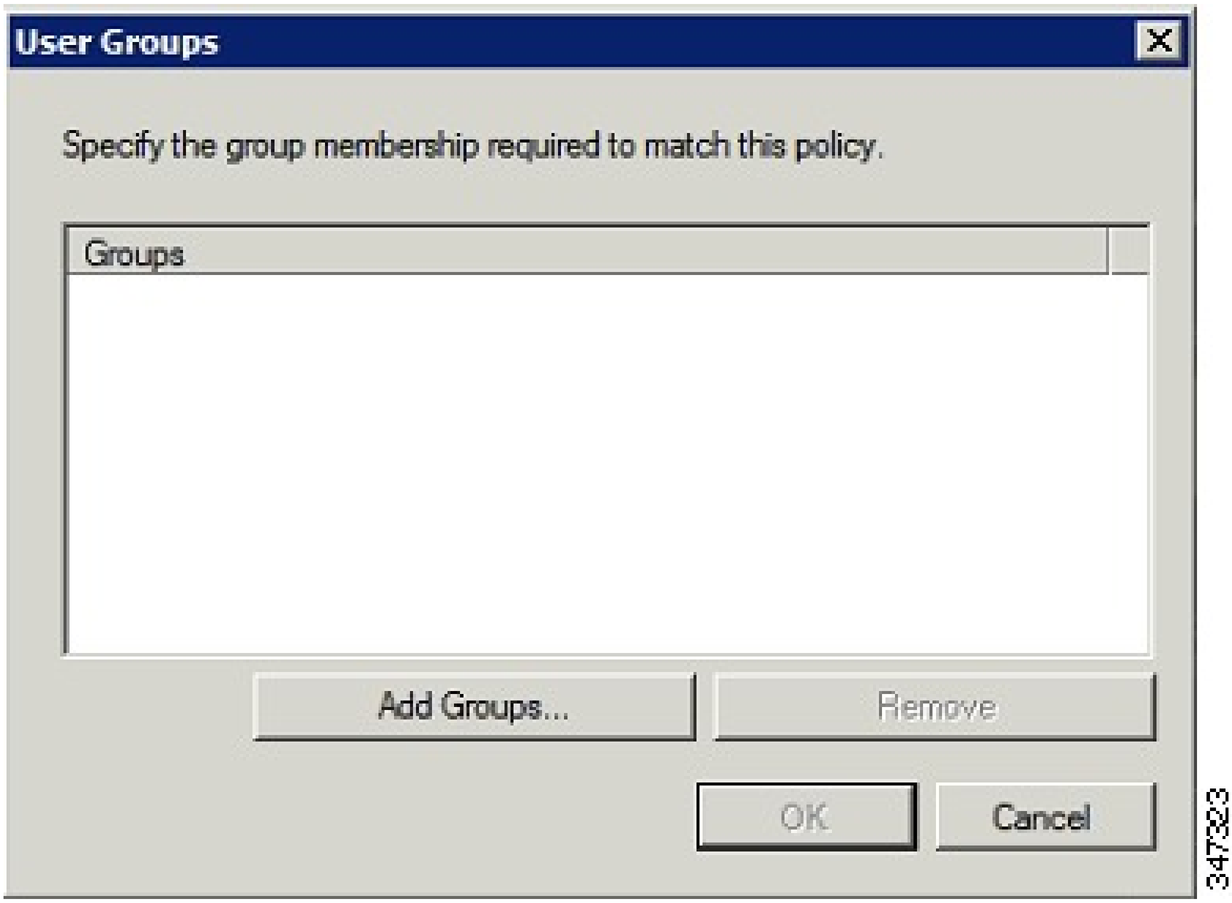


b) Click the **Conditions** tab, select the User Groups condition, and click **Add** .



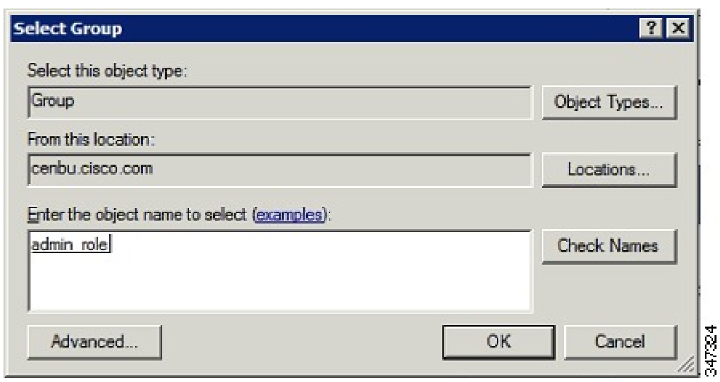
The User Groups condition specifies that the connecting user must belong to the selected group. For this policy to pass, the user being authorized must belong to the user group configured in this policy.

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

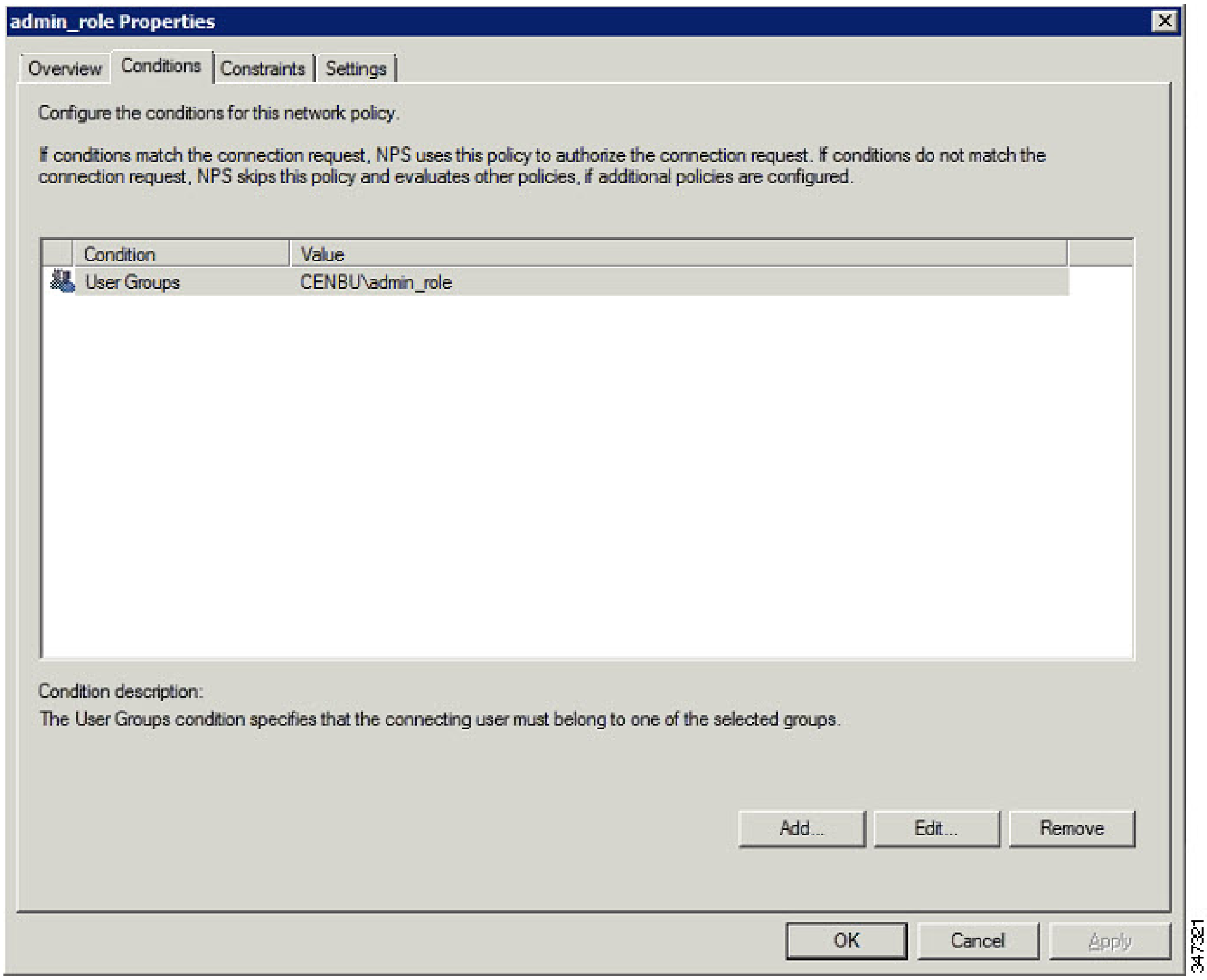


d) In the **Select Group** window, enter the name of the group

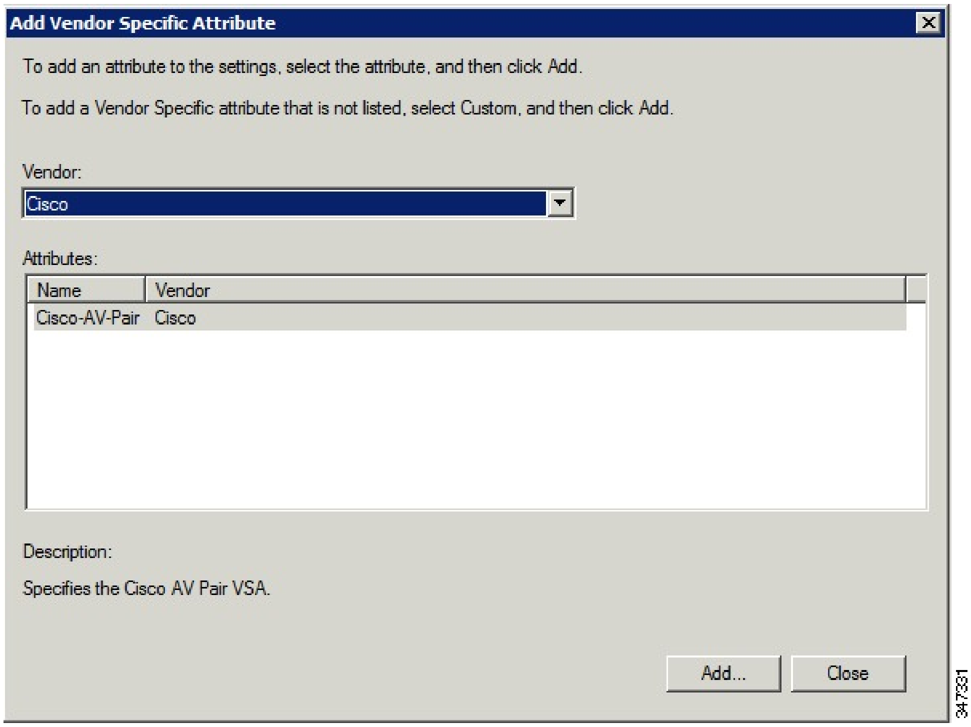
e) Click **OK** to close the **Select Group** dialog box, and then click **OK** to close the User dialog box.



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



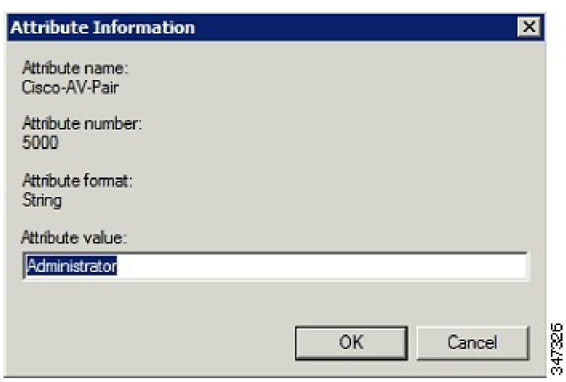
g) Click the Settings tab, and then click **Add** to display the Attribute Information window.



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.

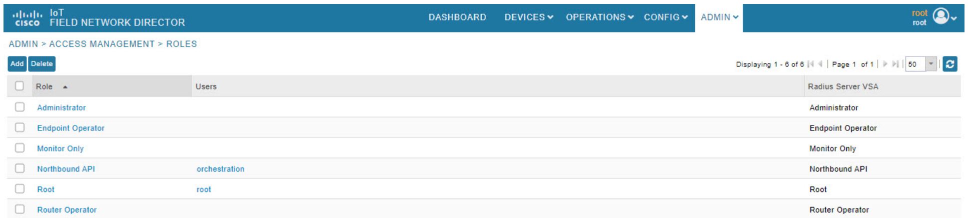
The VSA to configure is:

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

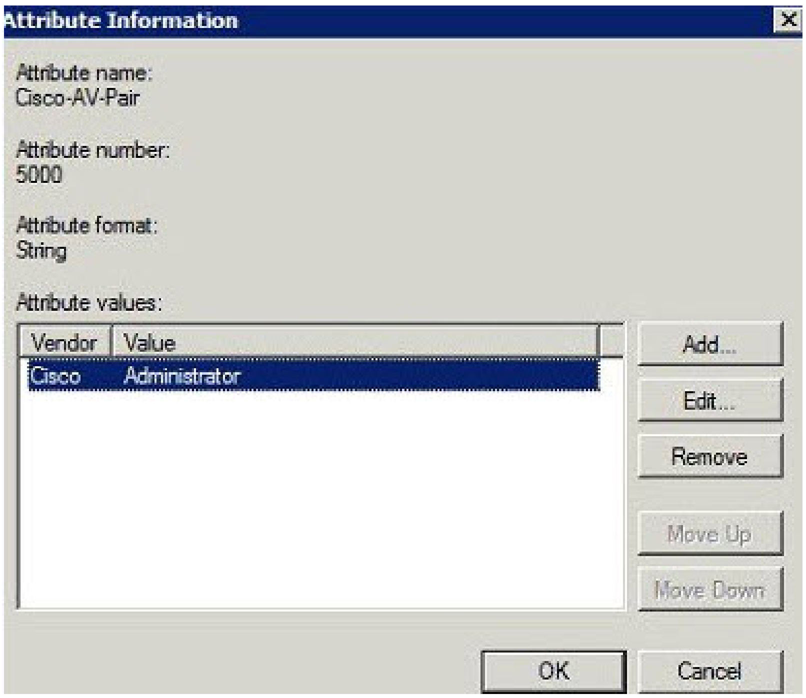


Note

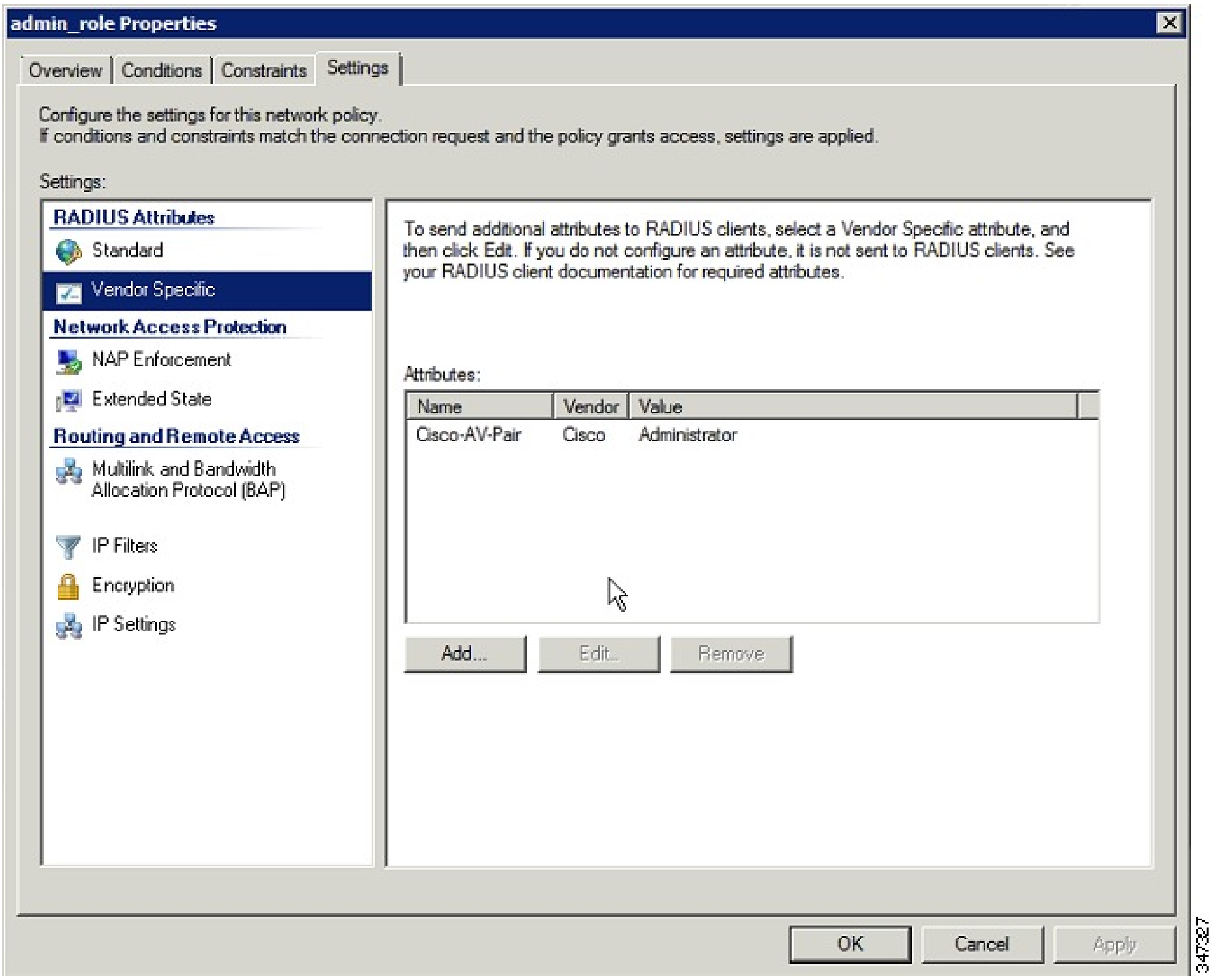
The string entered in the Attribute value field must be the exact string listed in the Radius Server VSA column on the Roles page in IoT FND (**ADMIN** > **Access Management** > **Roles**).



i) Click **OK**.



The VSA attribute appears in the Settings pane.



j) Click **OK**.

Configuring Remote Authentication in AD

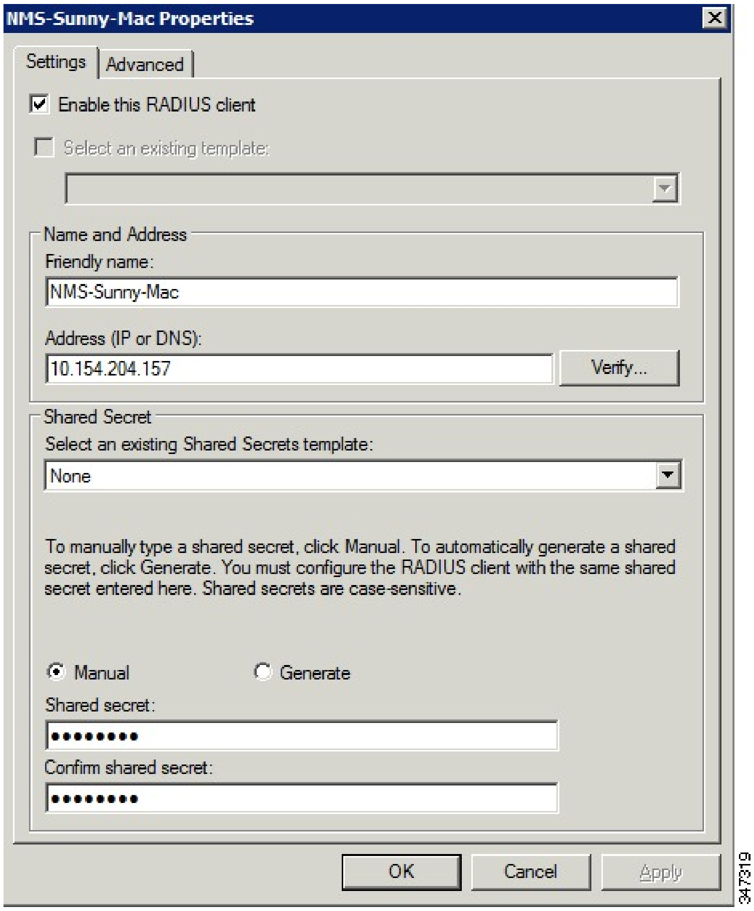
To allow IoT FND to remotely authenticate users, configure the following within Active Directory

Procedure

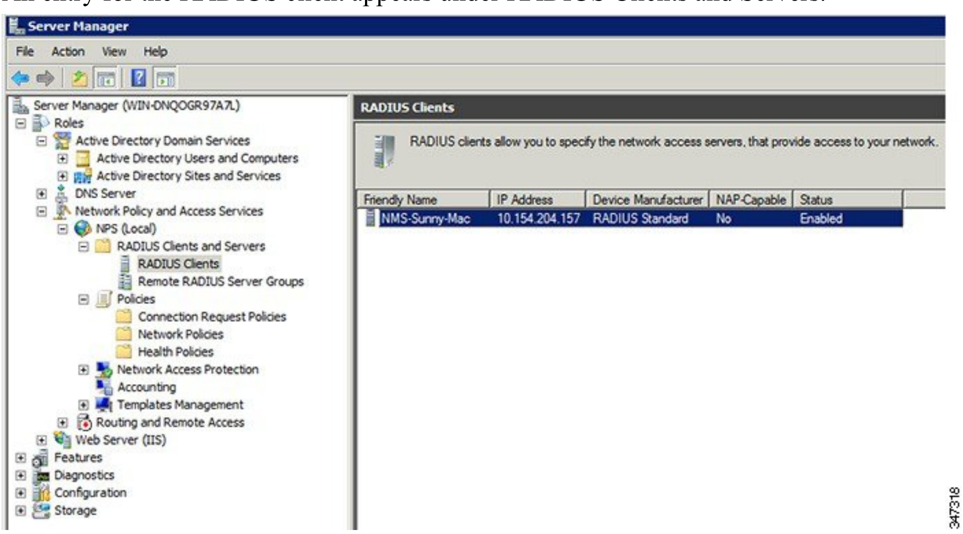
Step 1 Log in to NPS.

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.

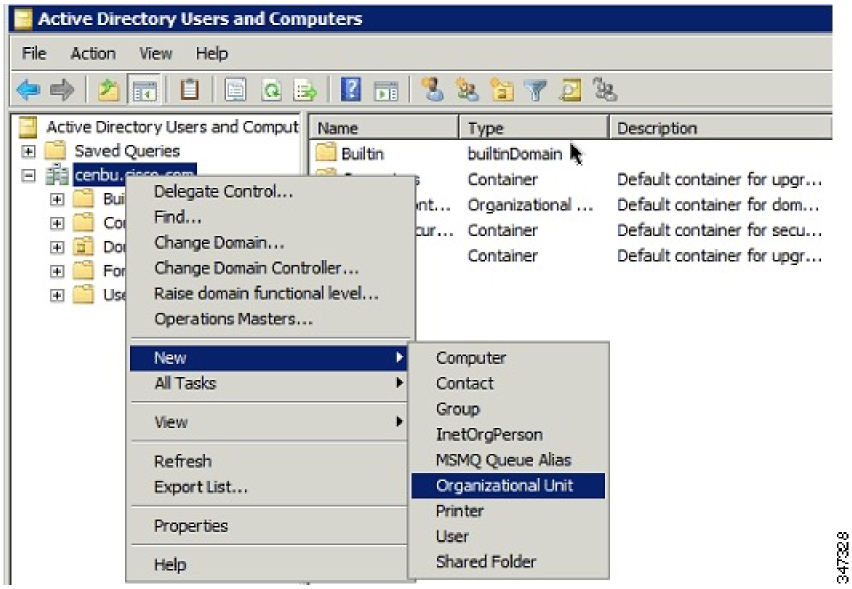


An entry for the RADIUS client appears under RADIUS Clients and Servers.



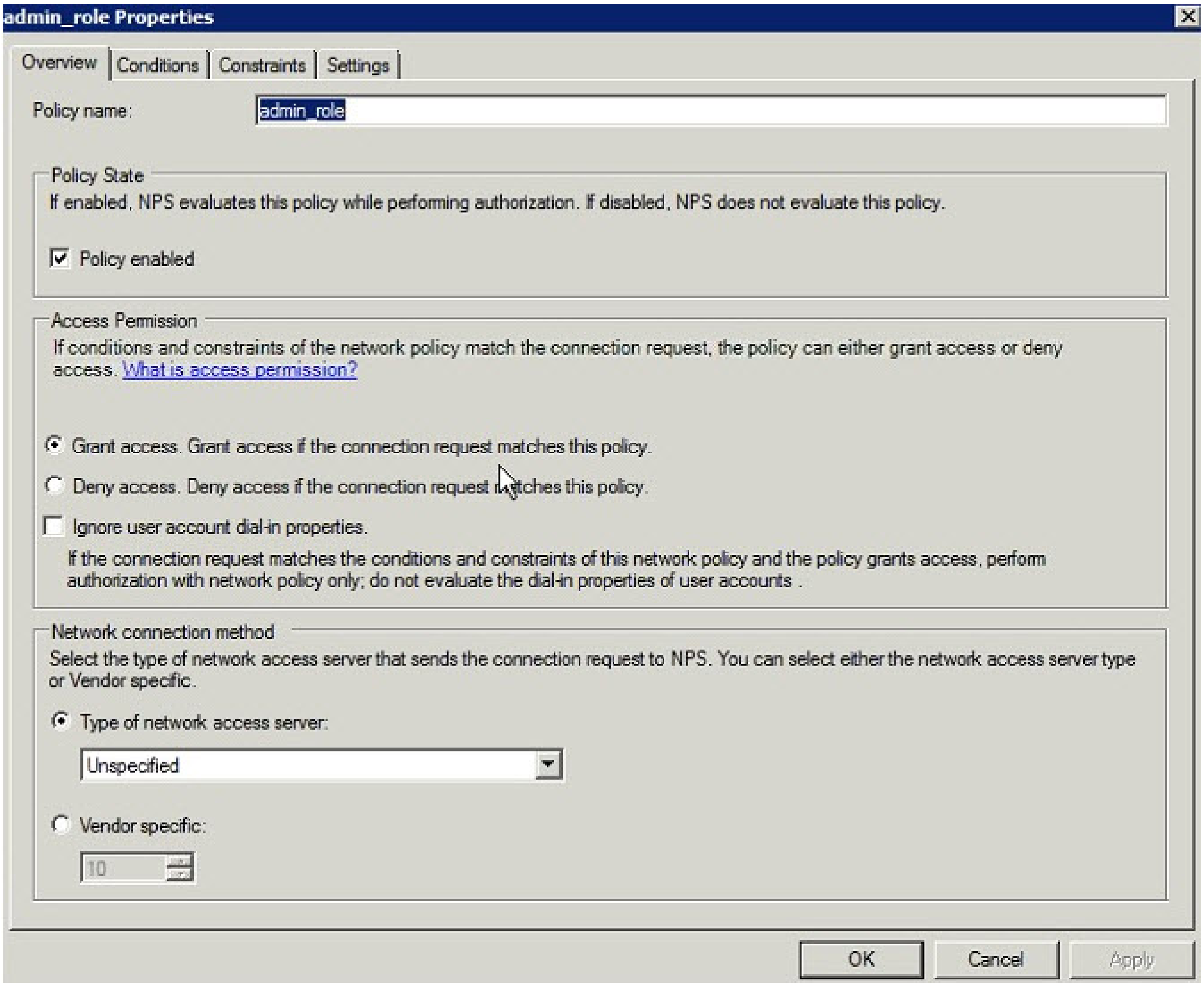
Step 3 Log in to AD and create an Organizational Unit.

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.

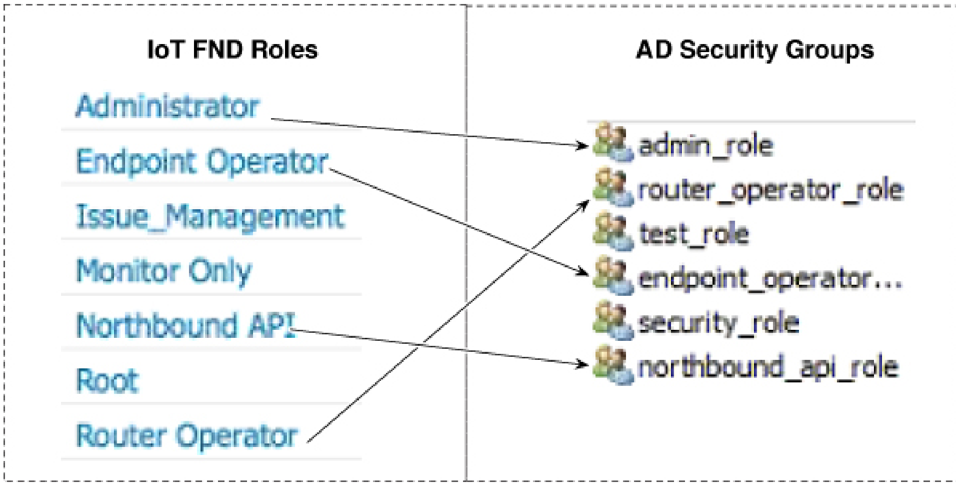
The following example shows the security groups defined in the NMS_ROLES Organizational Unit.



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

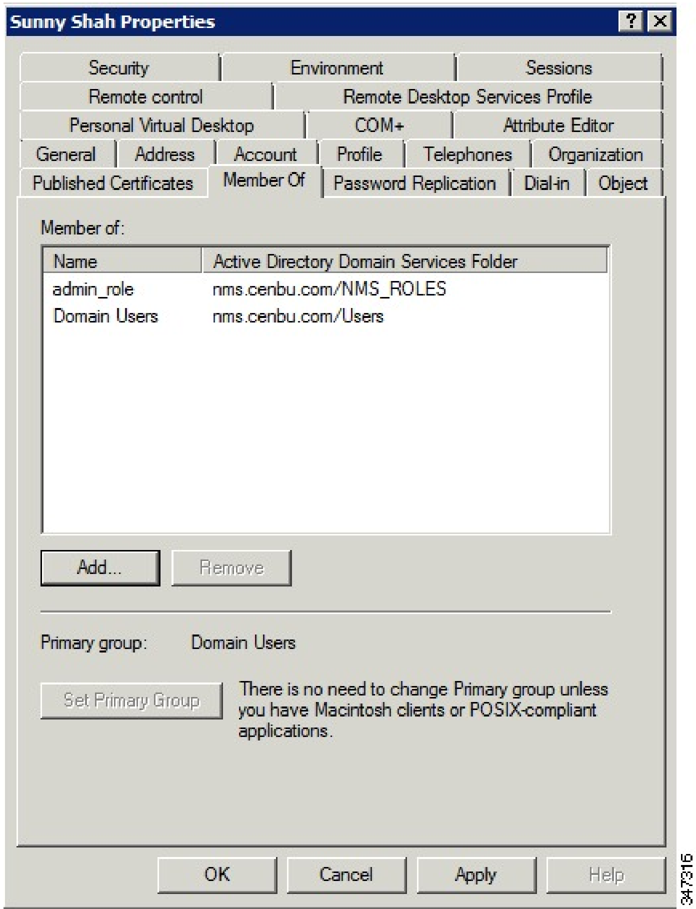
You cannot create or assign the IoT FND root role in AD.



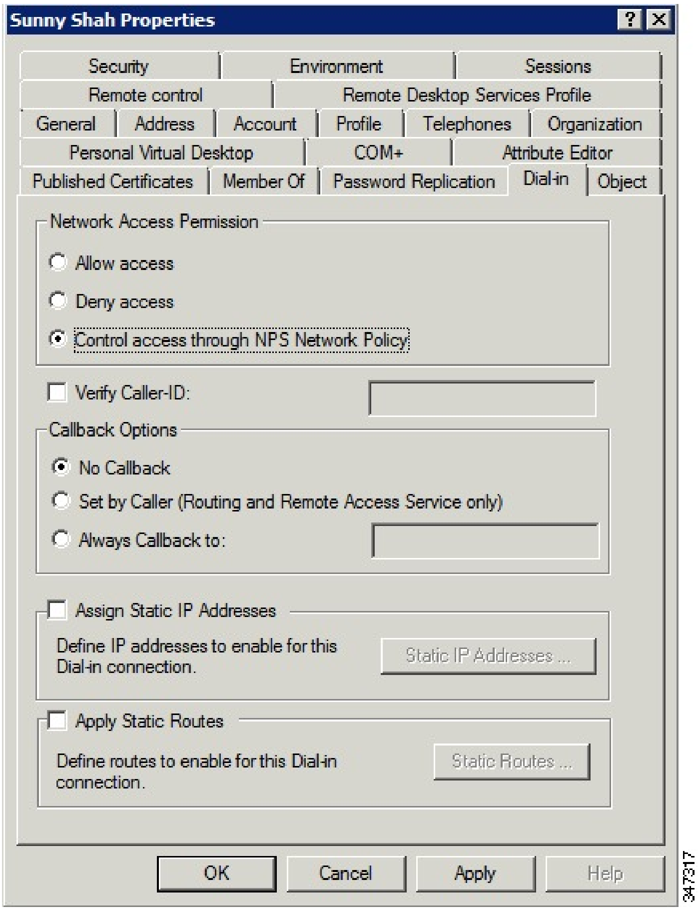
Step 5 Assign AD users a role by adding them to the security group mapping to that role.

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 12: 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 106
- How SAML Works, on page 107
- Limitations for SSO Authentication, on page 110
- Configuring IDP Manually for SSO Authentication, on page 107
- Importing IDP Metadata for SSO Authentication, on page 109

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 106

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. **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. • The service provider metadata file contains information such as entity ID, redirect URLs, certificate key. • 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 107
    - Importing IDP Metadata for SSO Authentication, on page 109
- 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:

Procedure

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

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

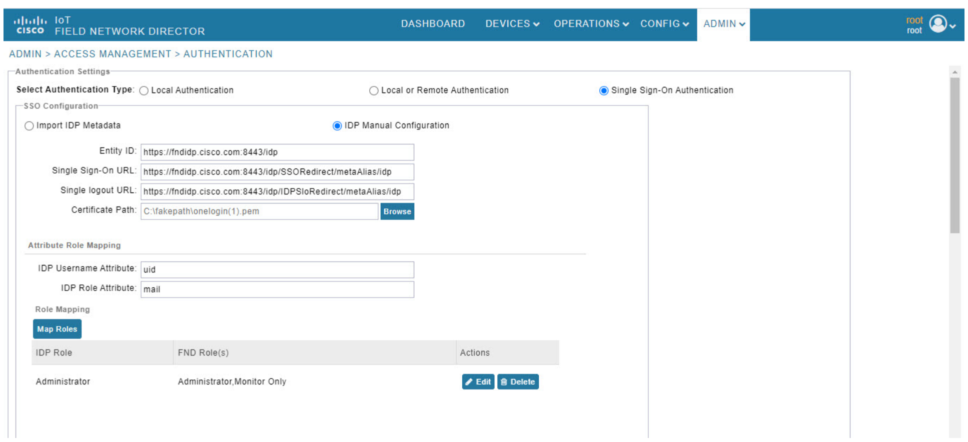
Step 3 Select the **IDP Manual Configuration** radio button.

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:

Procedure

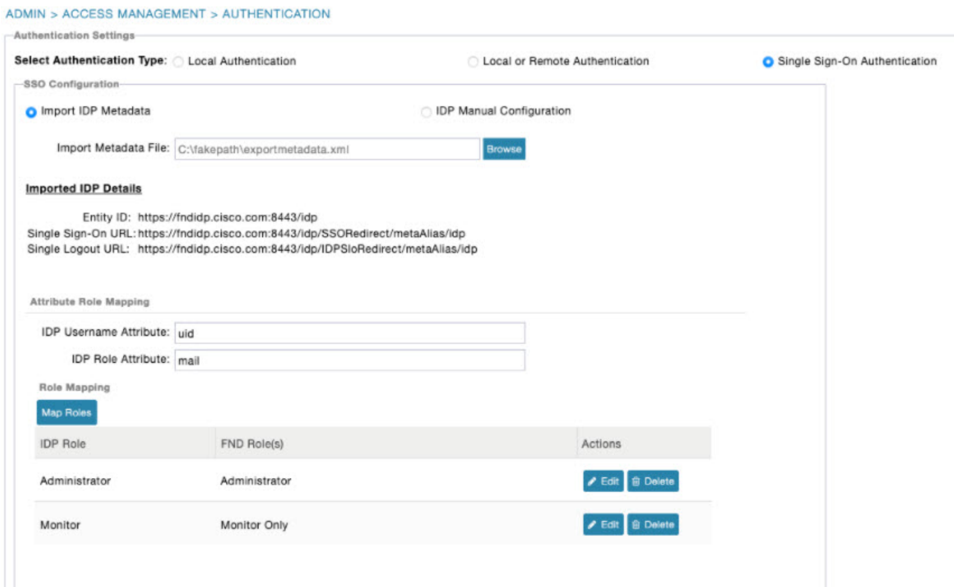
Step 1 Choose **ADMIN** > **Access Management** > **Authentication**.

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>/consolelogin.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:

Procedure

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:

Procedure

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:

Procedure

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:

Procedure

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:

Procedure

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.
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:

Procedure

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:

Procedure

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. • Root - The Admin user who defines root access for other users while creating a domain. • 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.

Field	Description
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:

Procedure

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: • Local - The domain administrator can add new user or choose an existing user. • Remote - The domain administrator can only add new users.
User Name	Enter the name of the new user.

Field	Description
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:

Procedure

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:

Procedure

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 13: 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.

Permission	Description
Battery Endpoint Operations	IoT FND supports the following special battery-powered endpoints: • ACT, BACT, CAM • L+G LFN 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.
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/C8000 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.

Permission	Description
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.
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/C8000 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 14: System-defined User Roles

Role	Description
Administrator	This role combines these basic permissions: • Administrative Operations • Label Management • Rules Management

Role	Description
Endpoint Operator	This role combines these basic permissions: • Label Management • Endpoint Configuration • Endpoint Firmware Update • Endpoint Group Management • Endpoint Reboot
Monitor Only	Optional role. This role is not defined for every user.
North Bound API	This role combines these basic permissions: • NB API Audit Trail • NB API Device Management • NB API Endpoint Operations • NB API Event Subscribe • NB API Orchestration Service • NB API Rules • 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: • Label Management • Router Configuration • Router Firmware Update • Router Group Management • 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 117). These permissions specify the type of actions users with this role can perform.

Adding Roles

To add IoT FND user roles:

Procedure

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:

Procedure

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:

Procedure

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:

Procedure

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.

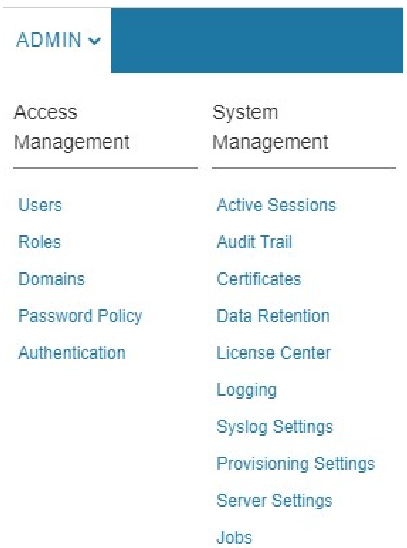
CHAPTER 5

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.



• Viewing Jobs, on page 145

Managing Active Sessions

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

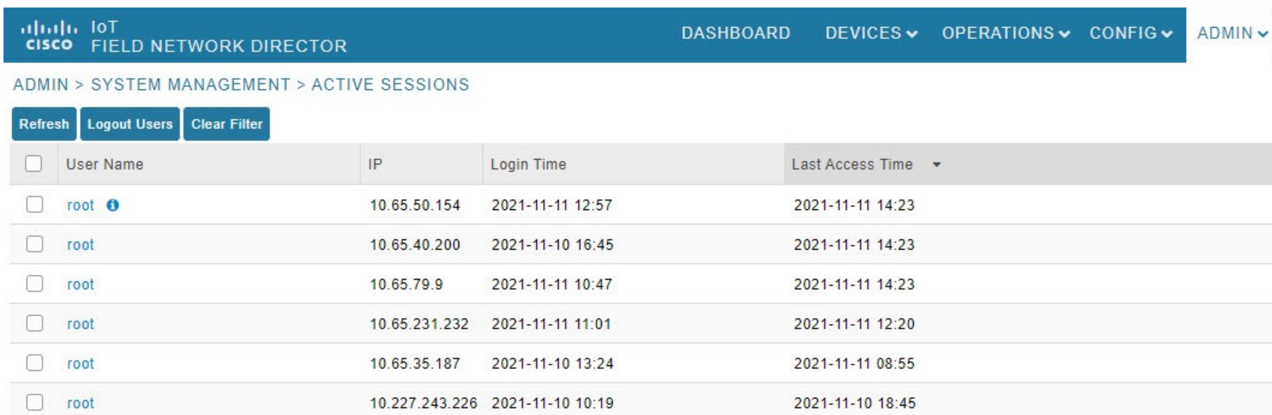
Viewing Active Sessions

To view active user sessions:

Procedure

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:

Procedure

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.

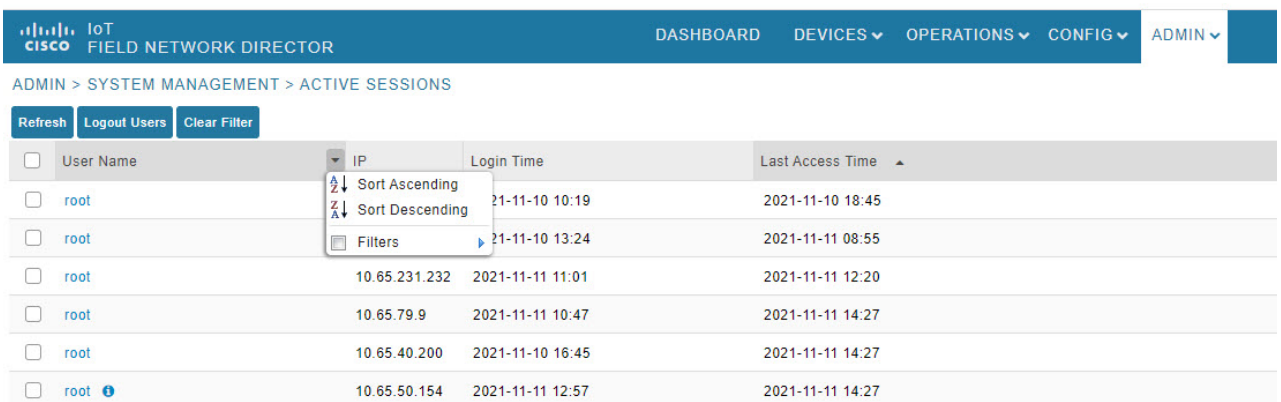
Filtering the Active Sessions List

To filter the Active Sessions list using column filtering:

Procedure

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**.

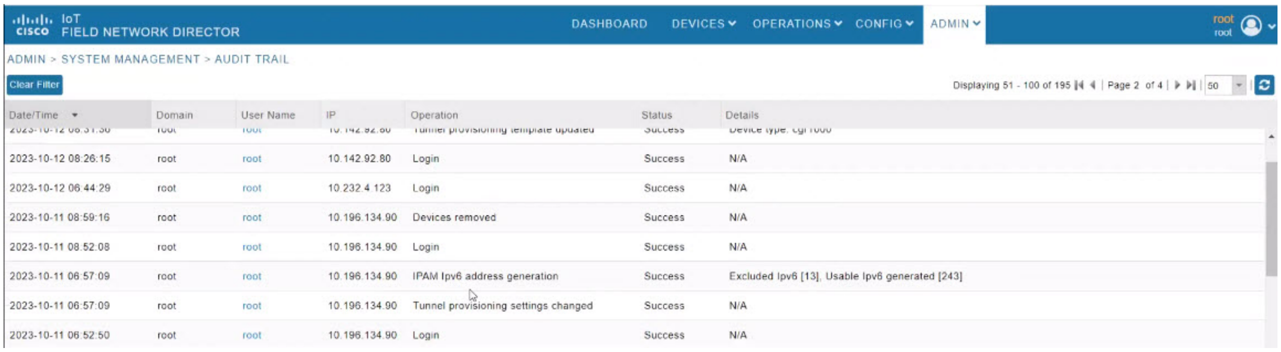
Displaying the Audit Trail

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

To display the Audit Trail:

Procedure

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. • Root - The Admin user who defines root access for other users while creating a domain. • 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:

Procedure

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

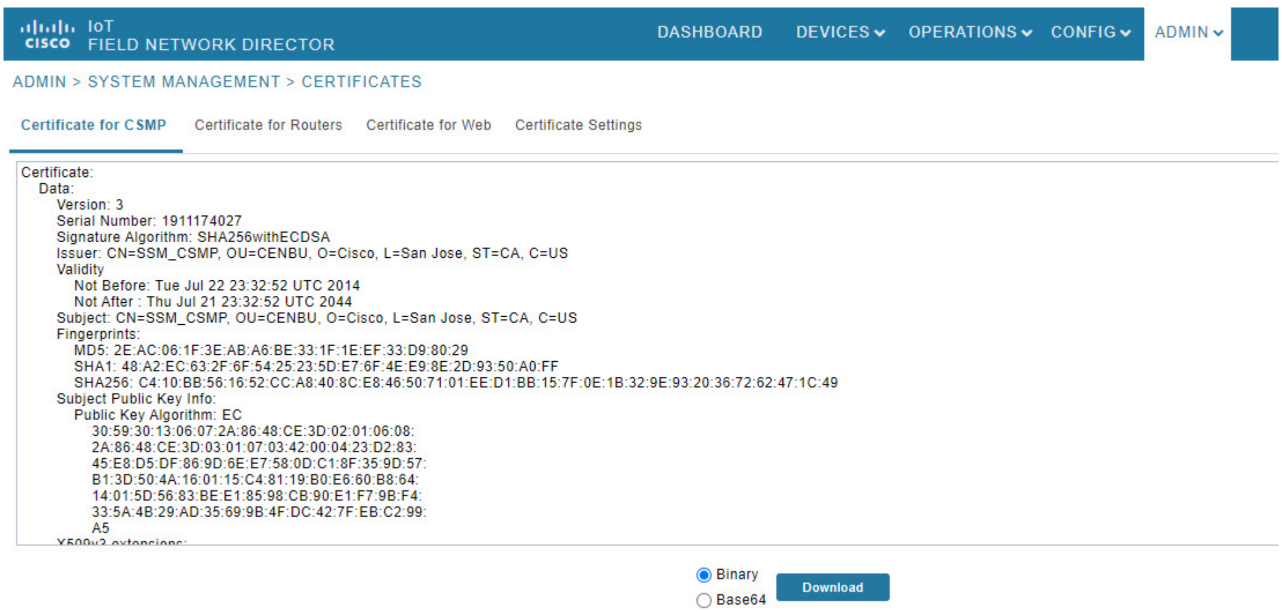
The Certificates page displays the certificates for CSMP (CoAP Simple Management Protocol), and Web certificates used by IoT FND and lets you download these certificates.

To display the CSMP, and Web certificates:

Procedure

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:

Procedure

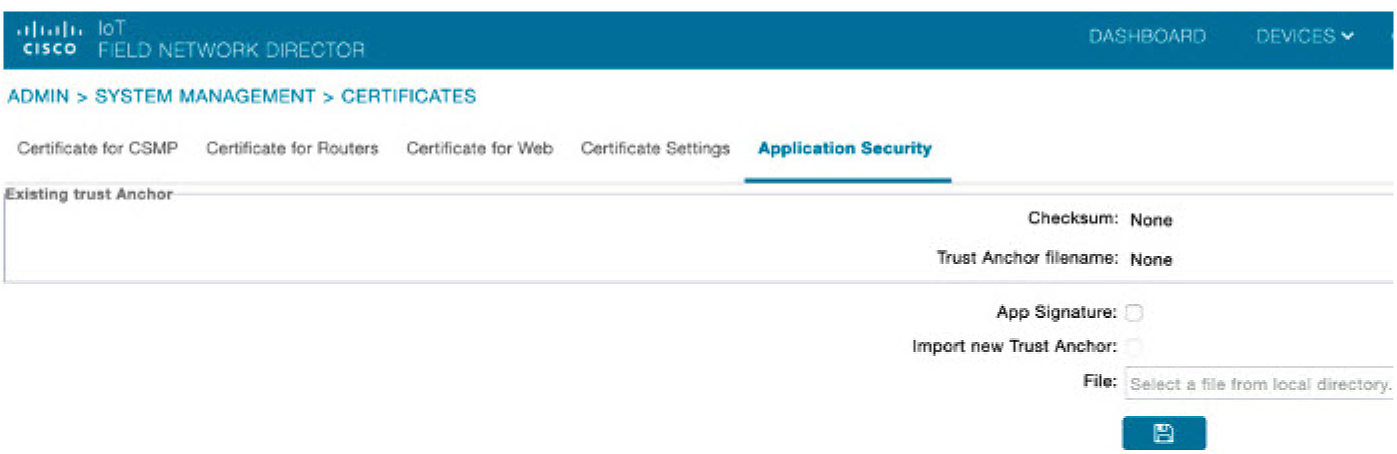
Step 1 Choose **ADMIN** > **System Management** > **Certificates**.

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.



CGMS Certificate Renewal for Routers

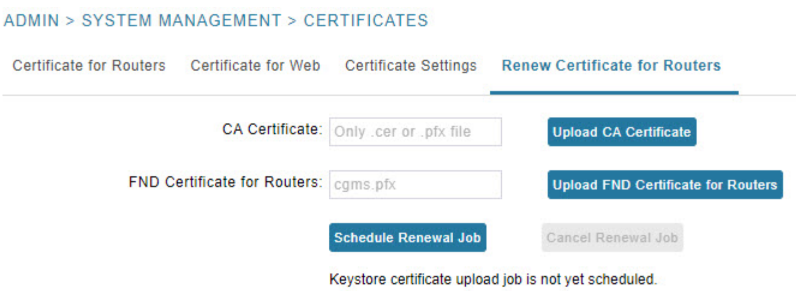
The **Renew Certificate for Routers** option in the UI automates the CGMS and/or CA certificate renewal process by updating the certificates in the keystore and encrypting the router password with new certificate. The supported certificate file extension is either (`.cer`) or (`.pfx`). We recommend you to schedule the automation job during the maintenance window to avoid conflict with other active operations (such as configuration push, firmware upgrade) running in FND.

To automate cgms or CA certificate renewal for routers:

Procedure

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

Step 2 Select the **Renew Certificate for Routers** tab.

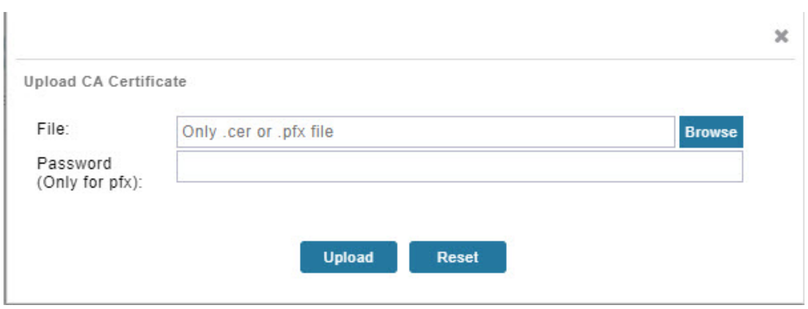


Step 3 Click either **Upload CA Certificate** or **Upload FND Certificate for Routers** to upload a CA or CGMS certificate.

Note
You can also upload both CA certificate and CGMS certificate simultaneously.

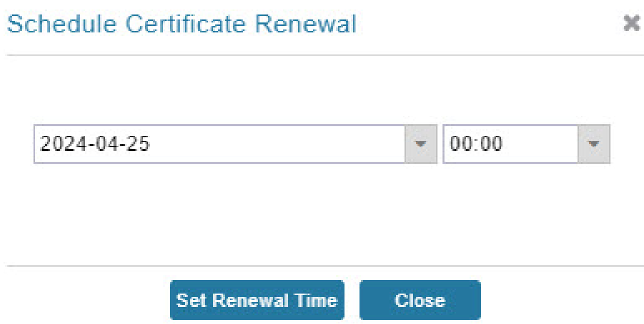
Step 4 Browse and select a valid CGMS or CA certificate in either (`.cer`) or (`.pfx`) format.

Step 5 Enter the password (applicable only for (`.pfx` file) and then click **Upload**.



Step 6 After uploading the certificate, click **Schedule Renewal Job**.

Step 7 Specify the date and time and then click **Set Renewal Time** to schedule the renewal job. The scheduled job appears in the page.



Use **Cancel Renewal Job** to cancel the scheduled job.

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:

Procedure

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 15: 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

Field	Minimum Values in Days	Maximum Values in Days	Default Values in Days
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

This section is moved to a new location with improved user experience. For more information on managing licenses on Cisco IoT FND see, Classic Licensing In Cisco IoT FND.

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.

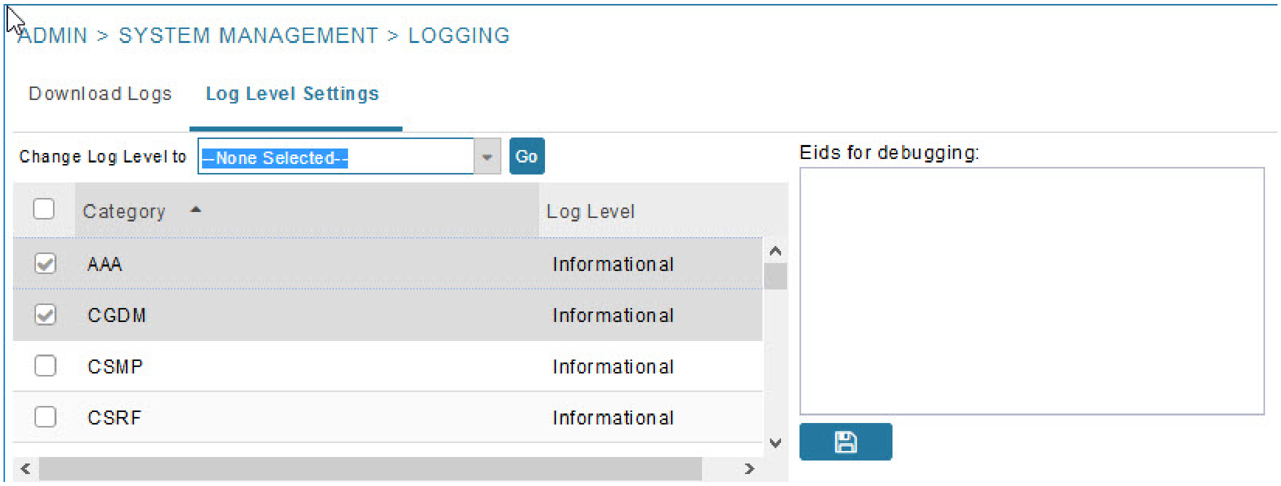
To configure the logging level:

Procedure

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:

Procedure

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/C8000 (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.

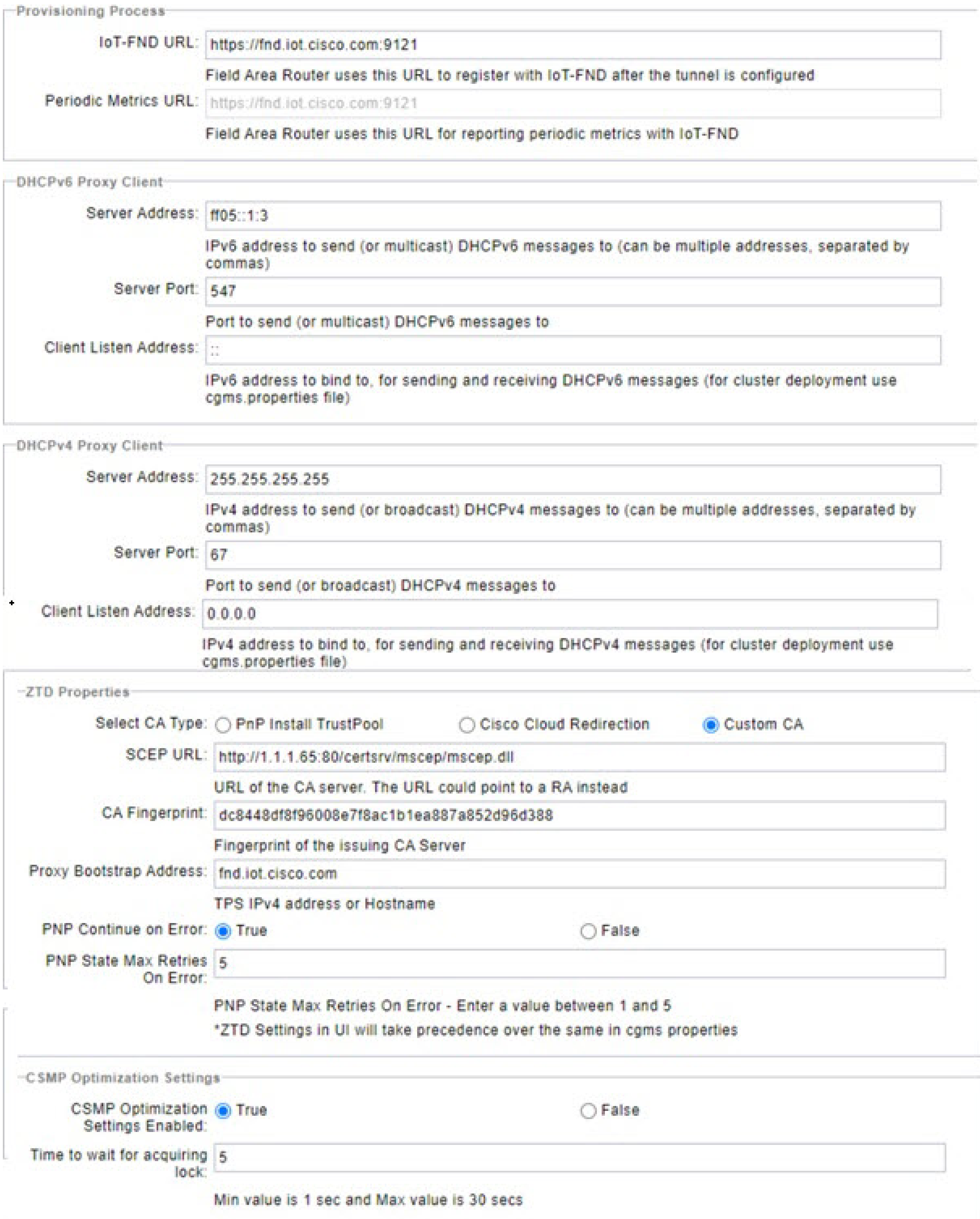
If the timeout happens, then during registration, the following message is displayed in the server.log file.

```
"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:

Procedure

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:

Procedure

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:

Procedure

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:

Procedure

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

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

Step 3 Configure these settings:

Table 16: 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:

Procedure

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, C8000) and other devices that are managed by IoT FND such as routers (CGR1000, IR800, IR8100,), 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 266

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:

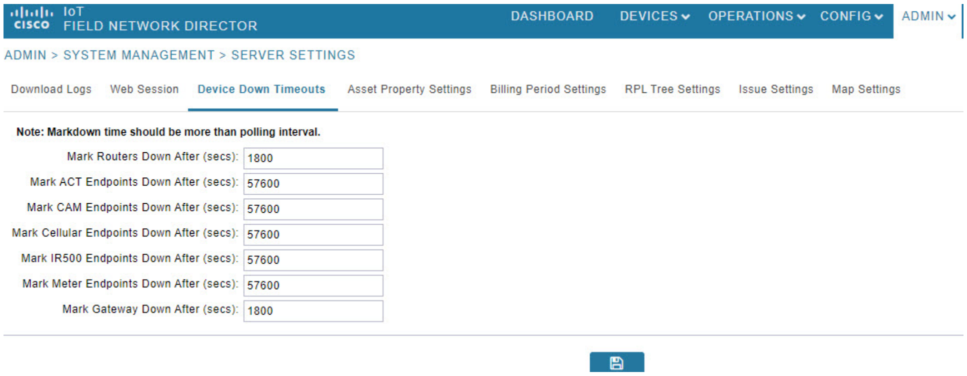
- Periodic inventory notifications
- Events
- Manual metric refreshes
- Device registrations

To configure device down timeout settings:

Procedure

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:

Procedure

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

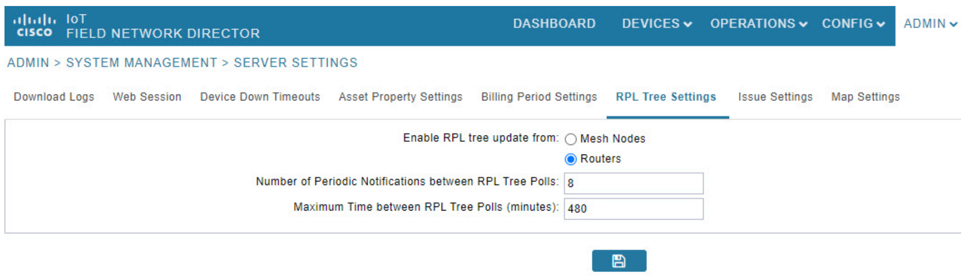


Table 17: Global RPL Tree Settings for Entire FND

Field	Description
Enable RPL tree update from	Select Routers. **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.
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

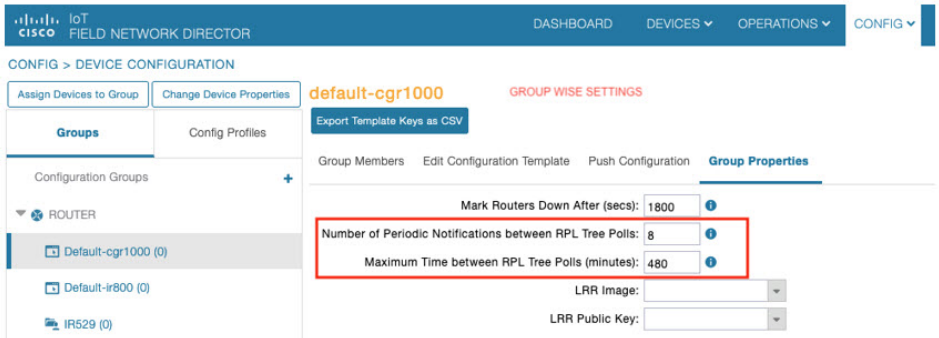


Table 18: Device Configuration Group Properties

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

When processing a periodic notification event, if either of these Table 18: 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.

Procedure

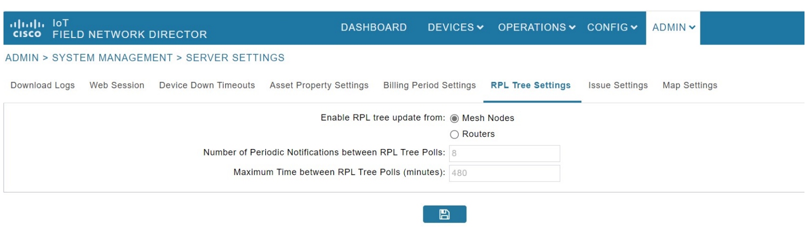
Step 1 Choose **ADMIN** > **System Management** > **Server Settings**.

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:

Procedure

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:

Procedure

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.

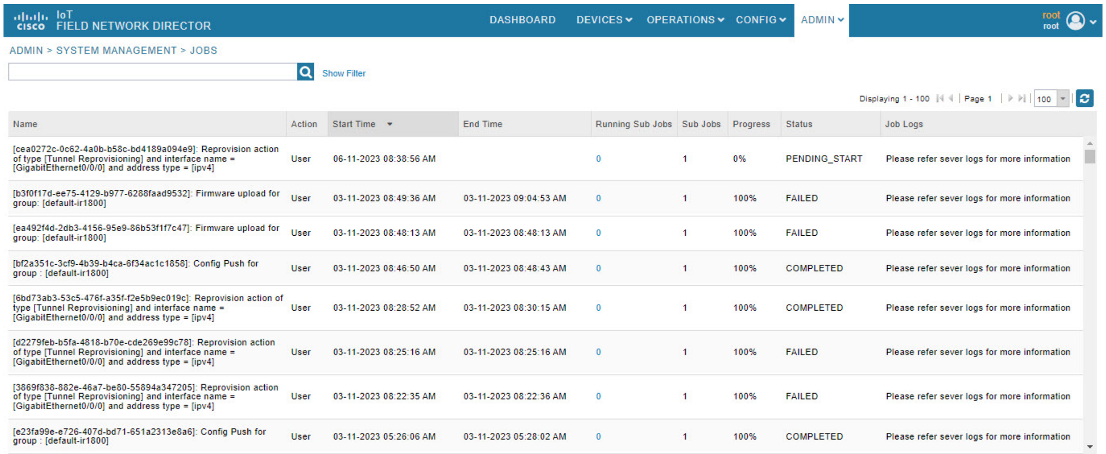
Viewing Jobs

The user triggered jobs in IoT FND are displayed in the Jobs page. The information about the jobs and their sub jobs are stored in the database in order to ensure that jobs are not lost in case of system restart or failure. IoT FND allows you to monitor and respond to job scheduling events, such as job completion or failure. The status of the jobs of IoT FND such as config push, firware upload and install, and reprovisioning can be seen in the Jobs page. This Jobs page provides a detailed summary of the jobs along with their respective sub jobs.

The supported job types are add/remove/export device, update statuses, change properties, add/remove labels (bulk operation), add/update/remove assets, upload firmware image to devices, install firmware image on devices, tunnel/factory re-provisioning, config push, and export events/dashboard dashlet data.

To view the jobs:

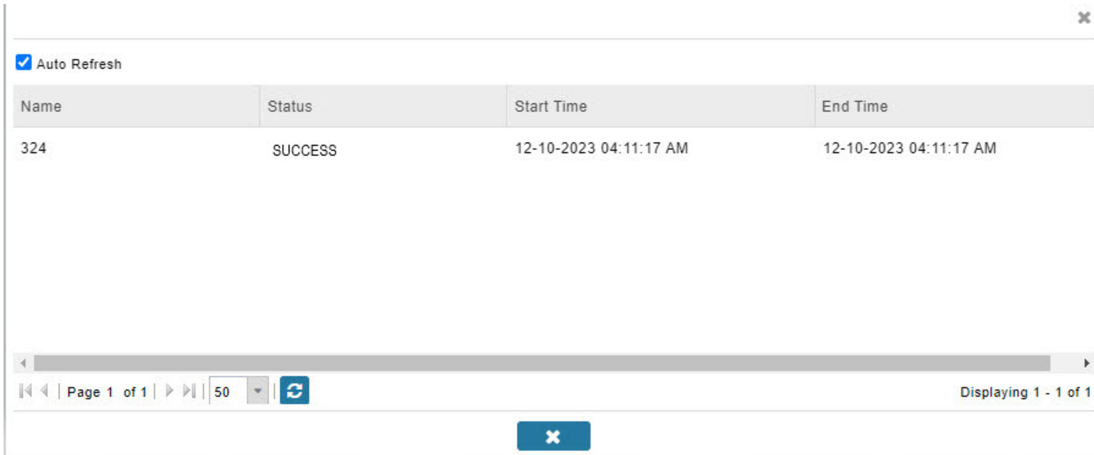
- Choose **ADMIN** > **SYSTEM MANAGEMENT** > **JOBS**. IoT FND displays the Jobs page.



Note

- The logs are not displayed for tunnel provisioning, config push, and firware upgrade. You can view the server logs for more information.
- The completed or failed jobs show 0 under running sub jobs.
- The jobs are displayed in the Jobs page as per their retention time.

- Clicking on Running Sub Jobs opens up the pop-up window to show the status of the running jobs.



- The filter allows you to filter jobs based on name, action, sub jobs, and status. To filter the job list using column filtering, click show filter to insert the search string. For example, click Name from the drop down and provide the search string. Click + icon to add the job selected and click search icon to display the search results.

CHAPTER 6

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.

Procedure

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

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

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

Note

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

Pluggable Module Info

PID P-LTEA-LA

Details :

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

Expansion Module Info

PID IRM-1100-SPMI

Details :

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

Cellular Link Settings

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

- To work with Head-End Routers (ASR1000, ISR3900, ISR4000, C8000) use the **DEVICES** > **Head-End Routers** page.

- To work with IoT FND NMS and database servers, use the **DEVICES** > **Servers** page.
- To view assets associated with the Cisco Wireless Gateway for LoRaWAN (IXM-LPWA-900), use the **DEVICES** > **Assets** page.

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

Guided Tours

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

Procedure

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

Step 2 Click GUIDED TOUR.

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

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

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

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

Note

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

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.

Setting Preferences for the User Interface

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

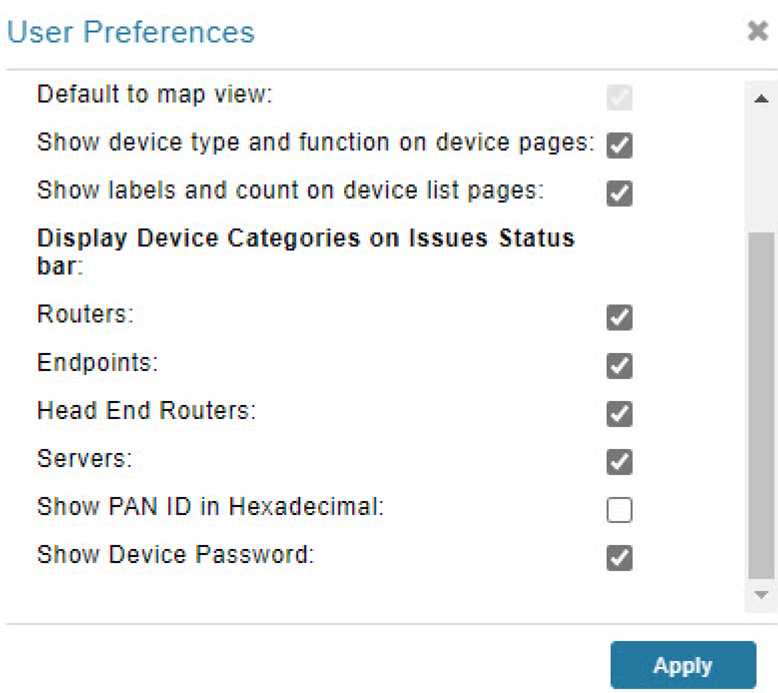


Table 19: User Preference Settings

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

Options	Description
Show PAN ID in hexadecimal	Displays the PAN ID in hexadecimal in the Device Listing page.

Cisco IoT FND Username and Password Validation

Table 20: Feature History

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

Information about Cisco IoT FND Username and Password Validation

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

Benefits of Cisco IoT FND Validation for Usernames and Passwords

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

Validation Criteria for Admin Passwords

Admin passwords:

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

Validation Criteria for Usernames or Passwords

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

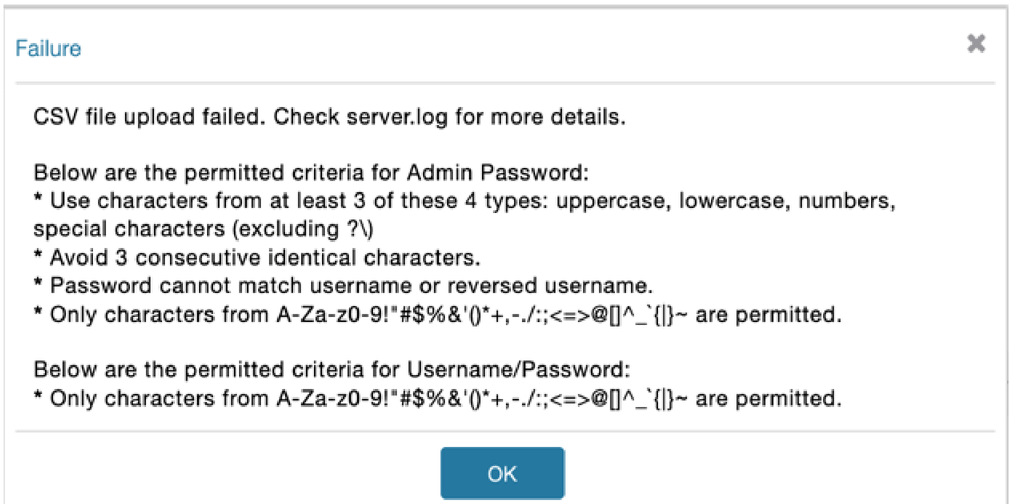
Cisco IoT FND UI CSV File Operations

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

- adminUsername=Admin1

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

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



Server log example:

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

Cisco IoT FND NBAPI CSV File Operations

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

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

SOAP UI, fault string example:

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

Server log example:

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

Password Rotation for Router Admin

Table 21: Feature History

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

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

You can run the `rotate_admin_password.sh` script as given in the example.

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

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

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

- For the router-specific rotation, specify the router EID and the password in the CSV file. The password can be plaintext, secret, or system generated.
- For the HER level rotation, specify the HER in the CSV file and the password is system-generated. The password is rotated for all the devices that tunnel with the HER specified in the CSV file.

The cgms tools package is installed on either FND Oracle Bare Metal or Postgres Virtual Machine. However, you can also install the cgms tools package on a separate VM (It is not necessary to have FND installed in this VM). For information on installing cgms tools on a separate VM, Installing CGMS Tools RPM on a Separate VM, on page 76.

Supported Platforms

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

Prerequisites

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

- Setting Password Preferences, on page 158 in the `command.txt` file and the device configuration.
- Define parameters in the CSV File.
- Ensure that routers are in `Up` state.
- No active operation such as config push, firmware upgrade should be running in FND.
- Based on the deployment type (Oracle or Postgres), copy the following files to the `cgms-tools` package.
  - **Oracle Bare Metal Deployment**

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

  - **Postgres Virtual Machine Deployment**

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

Setting Password Preferences

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

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

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

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

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

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

Device Configuration	Command.txt
Plaintext	Secret
Secret	Plaintext

What to do next

Define the parameters in the CSV File, on page 158.

CSV File

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

- **EID**: It can be either router specific or HER EID.
  - If you provide the EID of the HER, then the admin password is rotated for all the routers that are associated with the HER.
  - If you provide the EID of the router, which is device-specific, then the admin password is rotated for that specific router.
- **Password**: FND provides three options for the password field in the CSV file, which includes:

- Plaintext Password, on page 159
- Encrypted Password, on page 159
- Blank, on page 159

Note

- Regardless of the password preference (plaintext, encrypted, or blank) specified in the CSV file:
  - The admin password appears encrypted in the FND logs, which is decrypted using the signature tool.
  - The admin password appears either in plaintext or secret format depending on the password preference set in the `command.txt` file and the device configuration. For more information, see Setting Password Preferences, on page 158.
- To see the password in the FND UI, go to **DEVICES** > **FIELD DEVICES** > **Config Properties Tab** > **Router Credentials**.

Plaintext Password

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

Sample CSV file:

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

Encrypted Password

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

Sample CSV file: In the following example, the plaintext password is encrypted using the signature tool.

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

Blank

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

Sample CSV file:

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

Manual Router Admin Password Rotation

To rotate the admin password manually:

Before you begin

Completing the Prerequisites, on page 157 is a must.

Procedure

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

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

The CSV file contains the list of EIDs and admin passwords. For more information, see CSV File, on page 158.

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

a) If the password update is successful, the database is updated with the new password and the Tcl script updates the password in the `before-tunnel-config`, `before-registration-config`, and `express-setup-config`.

b) If the password update fails, refer to the log for more information.

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

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

   For example, rotate_admin_password_status_123.csv

What to do next

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

Schedule Admin Password Rotation with CronJob

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

The script automation is supported for the following deployments:

- Schedule for Oracle Bare Metal Deployment, on page 161
- Schedule for Postgres VM Deployment, on page 161

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

Schedule for Oracle Bare Metal Deployment

To schedule admin password rotation for Oracle BM deployment:

Before you begin

Prerequisites, on page 157

Procedure

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

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

Note
Ensure the CSV file is properly formatted and accessible. For more information, see CSV File, on page 158.

What to do next

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

Schedule for Postgres VM Deployment

To schedule admin password rotation for Postgres VM deployment:

Before you begin

Prerequisites, on page 157

Procedure

Step 1 Install the tools rpm in VM.

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

Step 3 Restart postgresql.

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

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

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

- docker cp fnd-container:/opt/cgms/server/cgms/conf/cgms.properties /opt/cgms-tools/conf

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

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

Step 6 Add the route in the server for the device reachability.

What to do next

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

Managing Routers

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

Working with Router Views

The router or routers you select determine which tabs display.

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

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

For information on how to customize router views, see Customizing Device Views, on page 232.

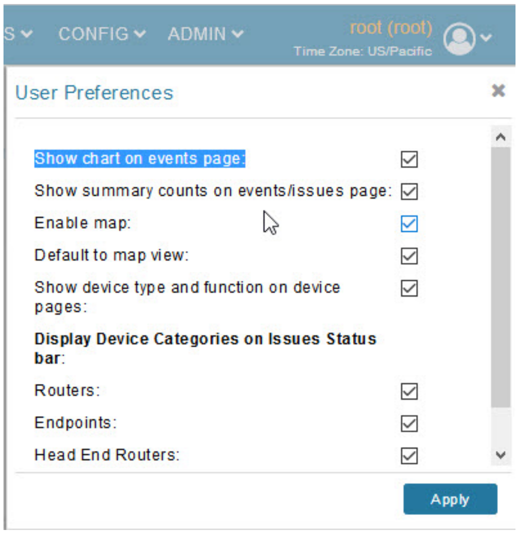
For information about the device properties that display in each view, see Device Properties, on page 343.

For information about common actions performed in these views (for example, adding labels and changing device properties), see Common Device Operations, on page 231.

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.

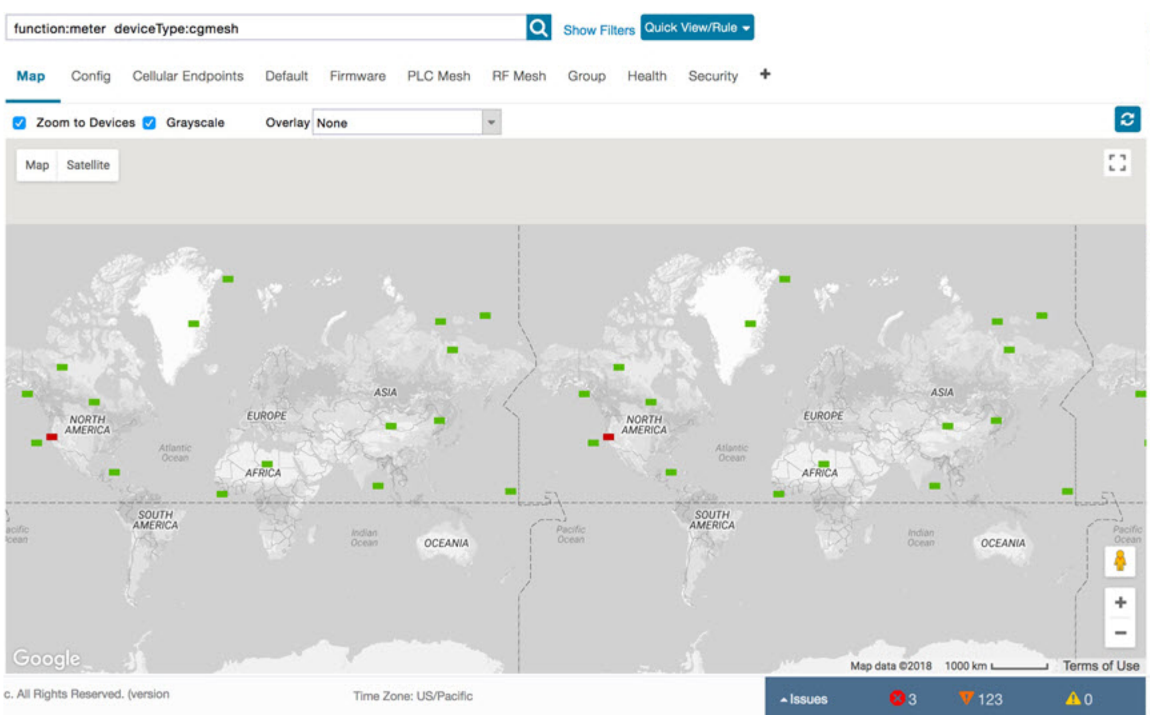
Figure 7: Setting User Preferences for User Interface Display



Note The additional options (not seen in the Figure 7: Setting User Preferences for User Interface Display, on page 163) 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 Router Mesh FFN Key

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

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

To refresh the router mesh FFN key:

Procedure

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

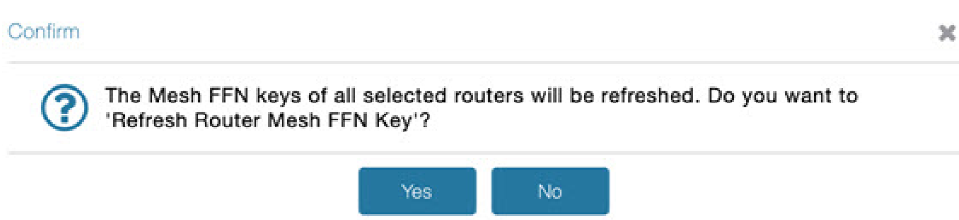
Step 2 Select CGR1000 or IR8100 routers from the left pane.

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

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

Step 5 Click **Yes** to continue.

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



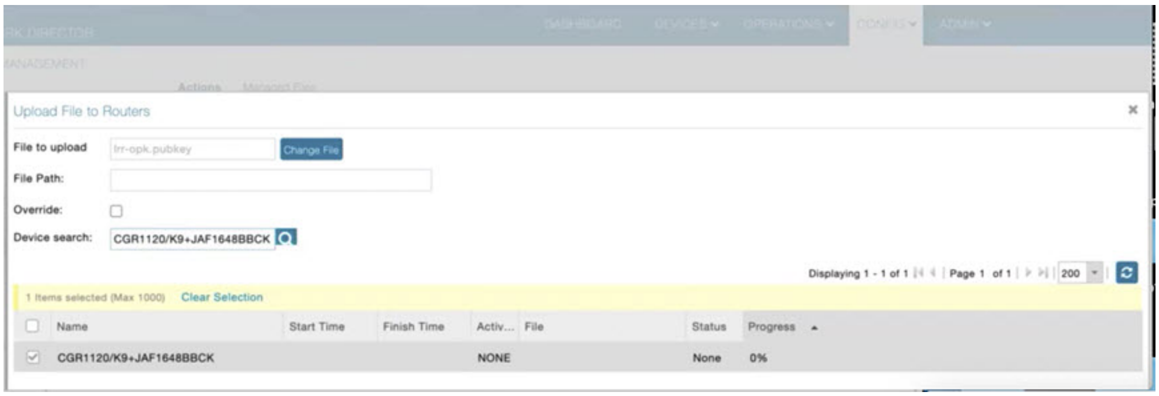
Device File Management for Routers

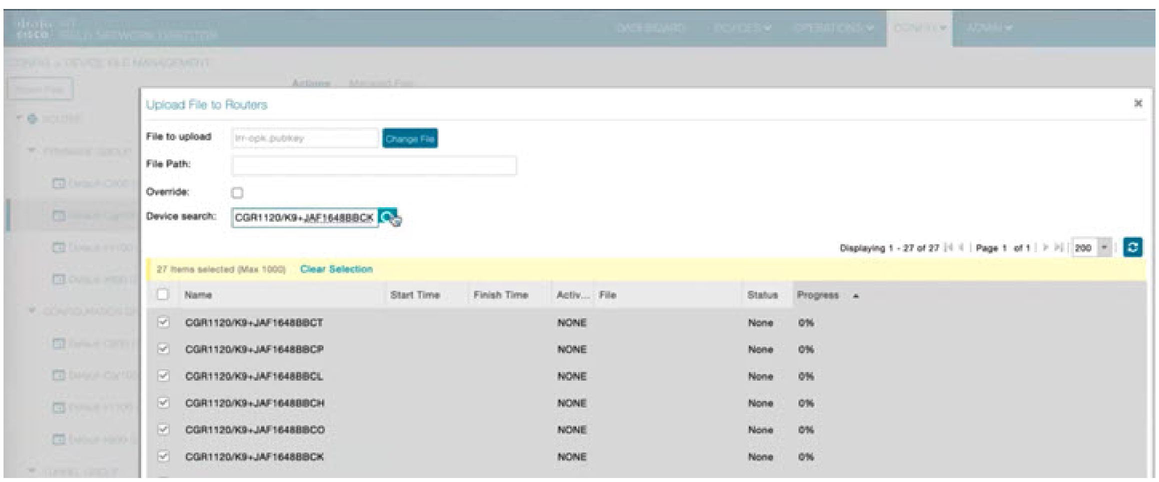
When you want to upload router device files to be managed by IoT FND, go to **CONFIG** > **DEVICE FILE MANAGEMENT** within the application. At that page, select **Actions** > **Upload** to get to the Upload File to Routers page. This page provides you the ability to:

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

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

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





Managing Embedded Access Points on Cisco IR829 ISRs

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

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

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

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

Note Not all IR800 routers have embedded APs. . The IR829 ISR features matrix is here.

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

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

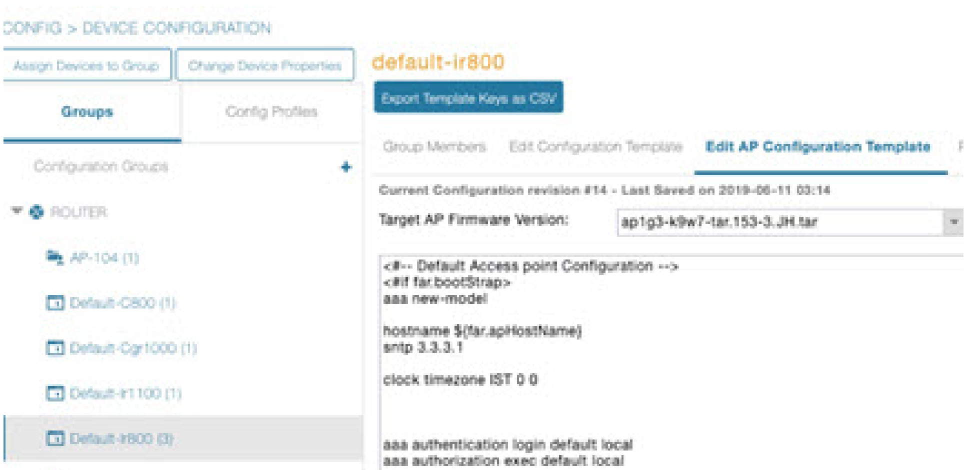
You can only define a unified image (k9w8 - factory shipped) for update via ZTD

Defining the Unified Mode Option

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

Procedure

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



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

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

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

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

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.

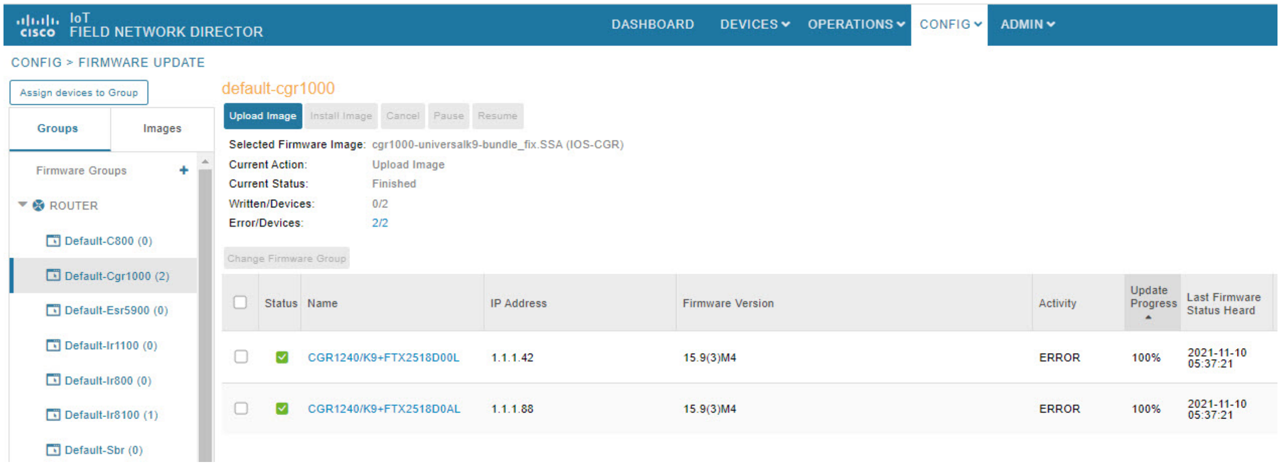
Displaying Router Configuration Groups

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

Procedure

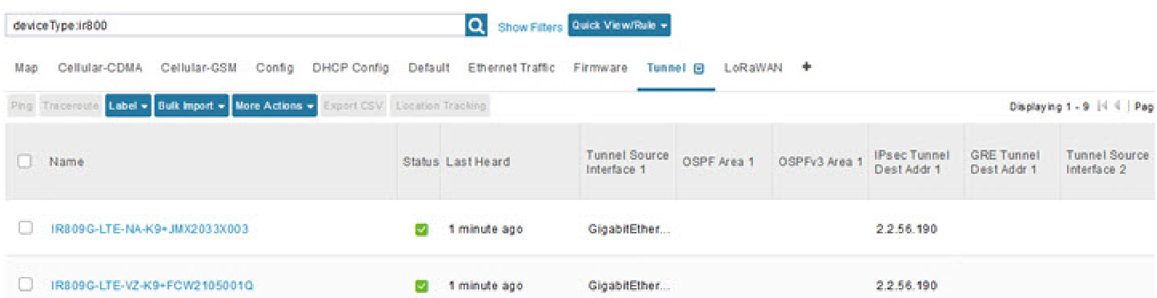
Step 1 At the **CONFIG** > **Firmware Update** page, select the Groups tab (left pane) and then choose one of the ROUTER Groups (such as Default-cgr1000, Default-ir1100, Default-ir800 or).



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



Exporting Mesh Routing Tree Data

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

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

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

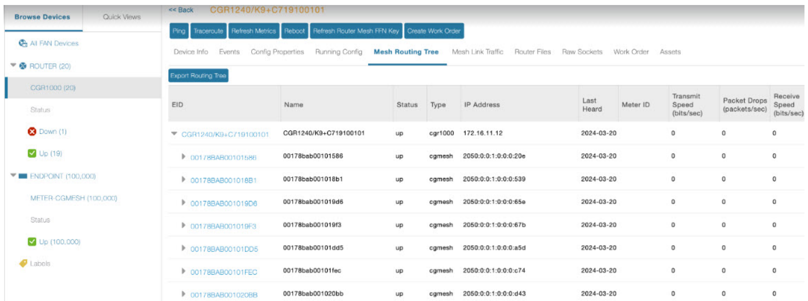
To export mesh routing tree data:

Procedure

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

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

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



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

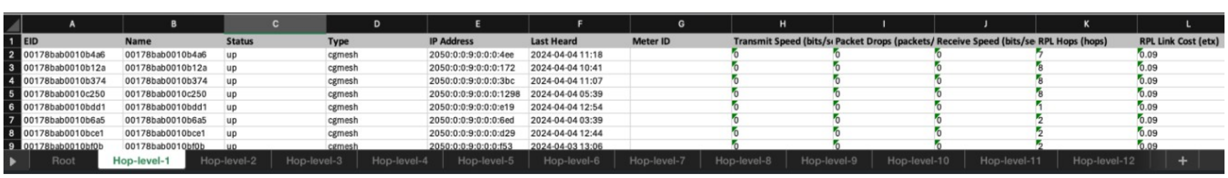
The Excel file is stored in the file system with the following name.

`export-routingtree-<timestamp>.xlsx`

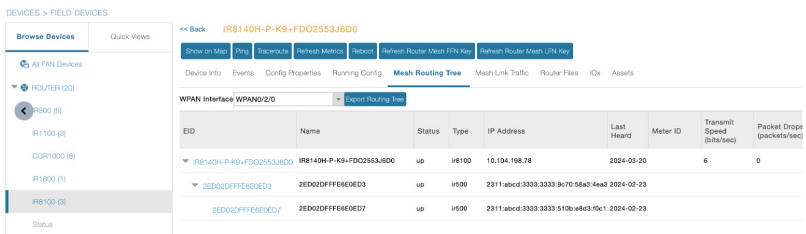
The exported data captures the relationships between the root node and its associated child nodes in various sheets of the Excel file. The first sheet of the file is named as Root and the subsequent sheets are named as Hop-level-<hop number> (example: Hop-level-1, Hop-level-2, and so on).

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

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



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



Manage Router Push Configuration Count

Manage Router Push Configuration Count

Table 22: Feature History

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

Information About Manage Router Push Configuration Count

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

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

Benefits of Manage Router Push Configuration Count

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

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

Configure Manage Router Push Configuration Count

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

   The router push configuration count is set.

Viewing Router Usage Statistics

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

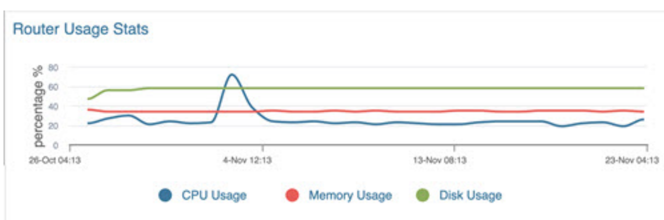
For more information, see Setting Time Filters To View Charts, on page 461.

Procedure

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

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

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



Search in the Device Configuration Page

Search In The Device Configuration Page

Table 23: Feature History

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

Information About Search in the Device Configuration Page

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

Benefits of Search in the Device Config Page

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

Use the Search in the Device Configuration Page

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

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

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

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

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

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

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

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

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

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

Managing Endpoints

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

Viewing Endpoints in Default View

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

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

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

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

For information on how to customize endpoint views, see Customizing Device Views, on page 232.

For information about the device properties displayed in each view, see Device Properties, on page 343.

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 231.

Viewing Mesh Endpoints in Map View

To view mesh endpoints in Map view:

Procedure

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

Step 2 Click the **Map** tab.

Blocking Mesh Devices to Prevent Unauthorized Access

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

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

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

Procedure

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

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

Note

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

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

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

Displaying Mesh Endpoint Configuration Groups

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

Displaying Mesh Endpoint Firmware Groups

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

Troubleshooting On-Demand Statistics for Endpoints

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

Report	Description
All TLVs	Generates a report from the list of available TLV identifiers in the device.
Connectivity	Generates a device connectivity report with the following parameters: • WPAN Status • PPP Link Stats • Neighbor 802.15.4g

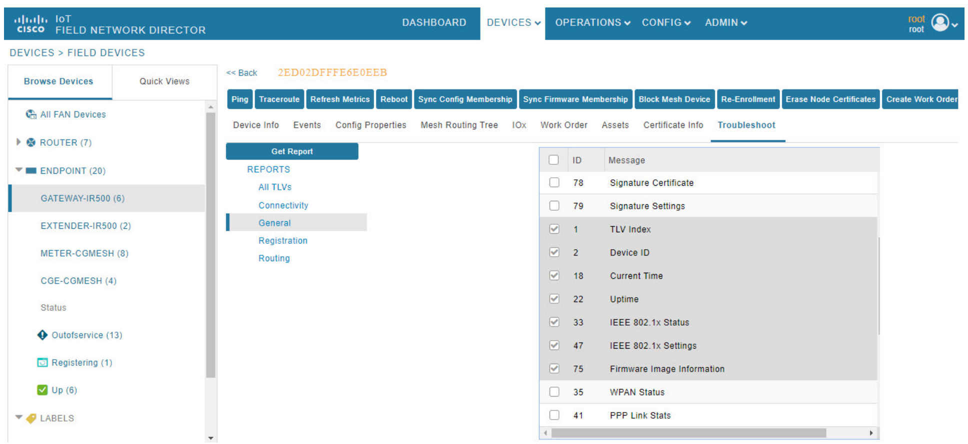
Report	Description
General	Generates a report with the following general parameters associated to the device: • TLV Index • Device ID • Current Time • Uptime • IEEE 802.1x Status • IEEE 802.1x Settings • Firmware Image Information
Registration	Generates a report with the following registration parameters: • Network Management System Redirect Request • Report Subscribe • Connected Grid Management System Settings • Connected Grid Management System Status • Connected Grid Management System Notification • Connected Grid Management System Stats • Signature Certificate • Signature Settings
Routing	Generates a report with the following routing parameters: • IP Address • RPL Settings • IEEE 802.11i Status • DHCPv6 Client Status • IEEE 802.15.4 Beacon Stats • Stored Information • Fast Synchronization Status • RPL Stats

To generate a troubleshooting report for endpoints:

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

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

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



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

Table 24: Feature History

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

Managing MMB GEN 2 Devices

Starting from release 4.11, IoT FND manages the MMB devices. These devices function as endpoints and are supported on the CGR1000 and IR8140 platforms. Additionally, the IR8140 offers dual WPAN support. FND allows you to install and register the devices, push the configuration template to the default configuration group, and update the firmware image. For more information, see Working with MMB Devices, on page 183.

Table 25: MMB Device Information Mapping in IoT FND

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

License

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

RBAC

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

Prerequisites

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

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

Devices	Firmware Version
MMB	2.4.8 and later
WPAN	6.6.5

Working with MMB Devices

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

Installing and Registering

To install and register the MMB devices:

Before you begin

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

Procedure

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

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

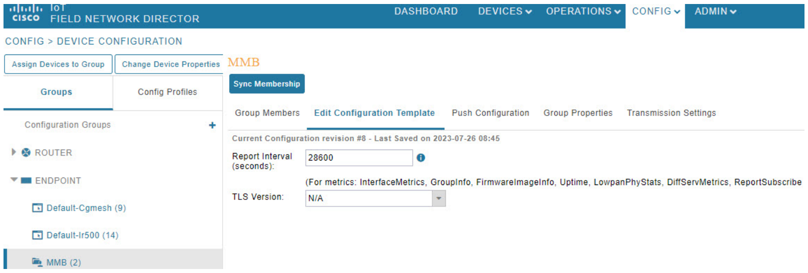
Step 3 Browse and select the CSV file, then click **Add**. The CSV file should have the minimum required fields such as EID, device type, and device function.

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

For more information, see Integrating Third-Party Endpoints in the Cisco IoT FND through CSMP, on page 489.

Configuration Group

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



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

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

Related Topics

Unsupported Features, on page 188

Firmware Group

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

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

Viewing on Dashboard

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

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

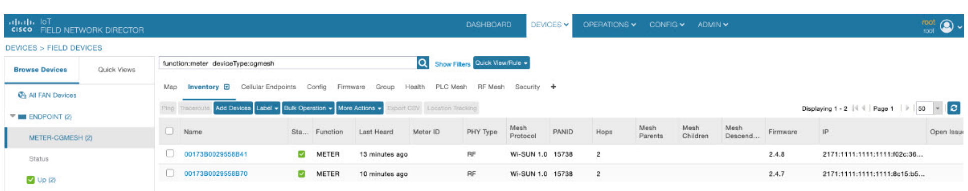
Viewing Device Details

To list and view the device details:

Procedure

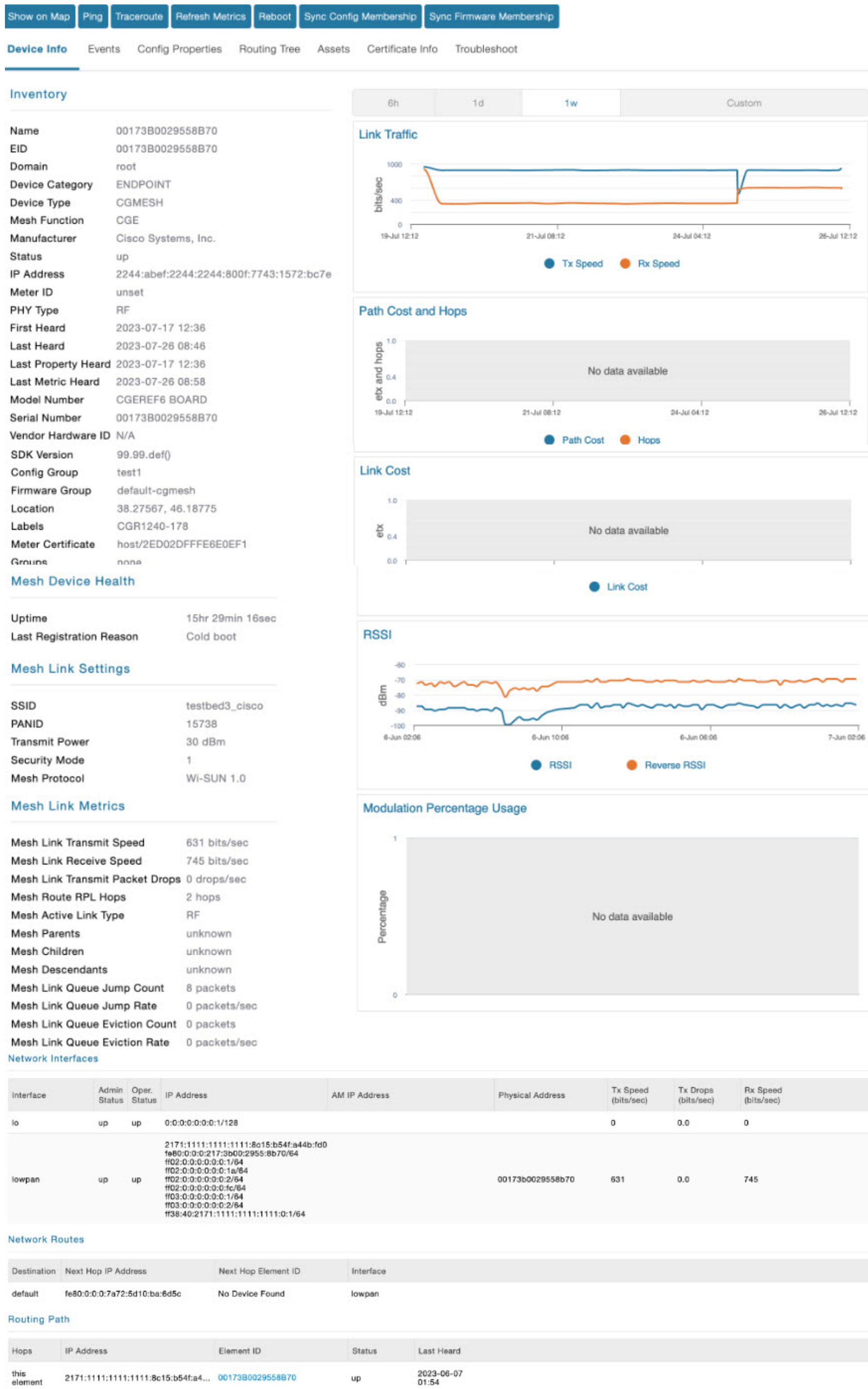
Step 1 Choose **DEVICES** > **FIELD DEVICES** > **Browse Devices** > **ENDPOINTS**.

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



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

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


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

Viewing Events and Issues

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

For information on viewing and filtering the events and issues, see Viewing Events, on page 467 and Viewing Issues, on page 479.

Limitations

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

Unsupported Features

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

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

Managing Out-of-Service Devices

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

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

Table 26: Feature History

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

Managing OOS Devices Using CSV — IoT FND UI

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

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

Adding OOS Devices Using CSV — IoT FND UI

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

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

To add OOS devices:

Procedure

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

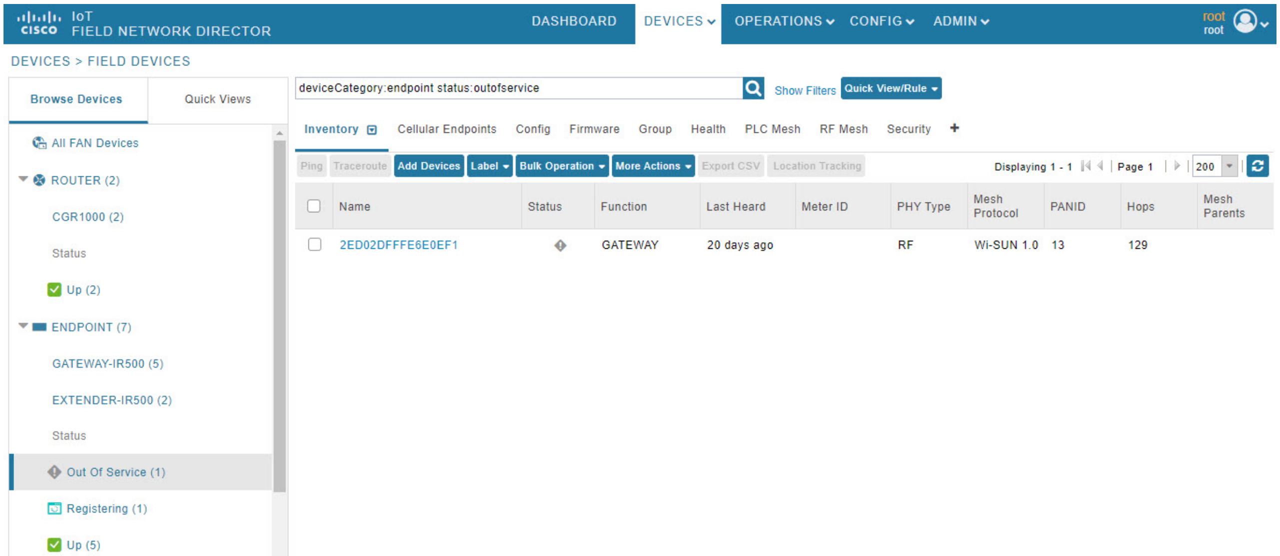
Step 2 Click **Add Devices** button on the right pane to add devices of router, endpoint, or gateway.

Step 3 Click Browse to locate the csv file that has the OOS devices.

Step 4 Click **Open**.

Step 5 Click **Add**.

Step 6 Click **Close** when done.



Updating Device Status Using CSV — IoT FND UI

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

Note You cannot move Unmanaged devices to OOS state.

To update OOS devices:

Procedure

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

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

Step 3 Click Browse to locate the CSV file.

Step 4 Click **Open**.

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

Step 6 Click **Close** when done.

Deleting OOS Devices Using CSV — IoT FND UI

Deleting OOS devices does not change the license count.

To delete OOS devices:

Procedure

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

Step 2 On the right pane, click **Bulk Operation** > **Remove Devices**.

Step 3 Click Browse to locate the CSV file containing the list of devices (in OOS status) to delete.

Step 4 Click **Open**.

Step 5 Click **Remove**.

Step 6 Click **Close** when done.

Managing OOS Devices Using CSV — IoT FND NB API

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

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

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

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

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

To add, update, or delete OOS devices:

Procedure

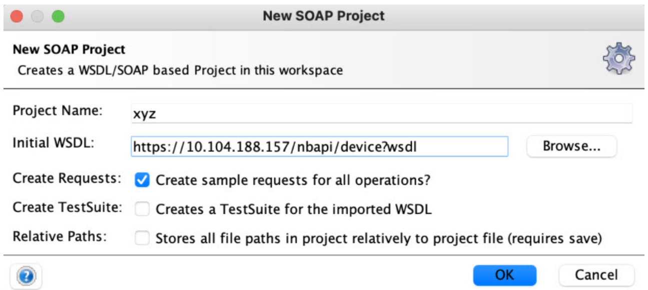
Step 1 Open the IoT FND NB API (SOAP UI:https://www.soapui.org/).

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

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

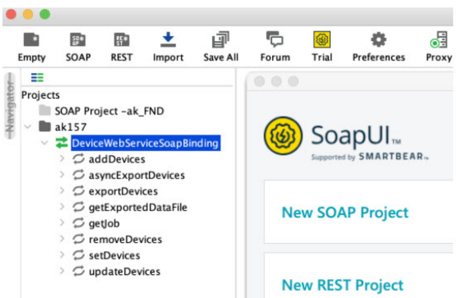
- Project Name.
- Click **Browse** to locate the Initial WSDL (Web Services Description Language).

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



Step 4 Click **OK** when done.

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

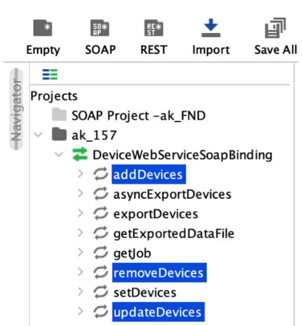


Step 5 Right-click one of the following API options and select NewRequest:

a. addDevices — To add OOS devices.

b. updateDevices — To update device status to OOS.

c. removeDevices — To delete OOS devices.



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

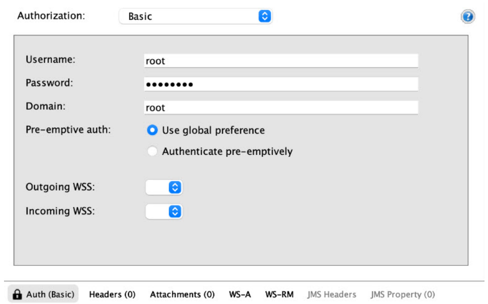
An XML window appears on the right pane.

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

Add Authorization window appears.

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

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



Step 10 Click **Attachments** tab.

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

You can perform one of the following actions:

a) **Add** — Select the CSV file to add OOS devices to FND.

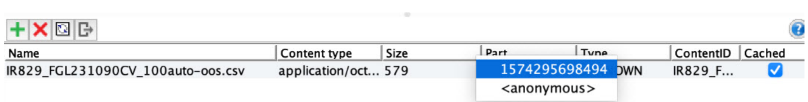
b) **Update** — Select the CSV file to update the device state as OOS in FND.

c) **Delete** — Select the CSV file to delete OOS devices from FND.

Step 12 Click **Open**.

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

Step 14 Select the Part Number.

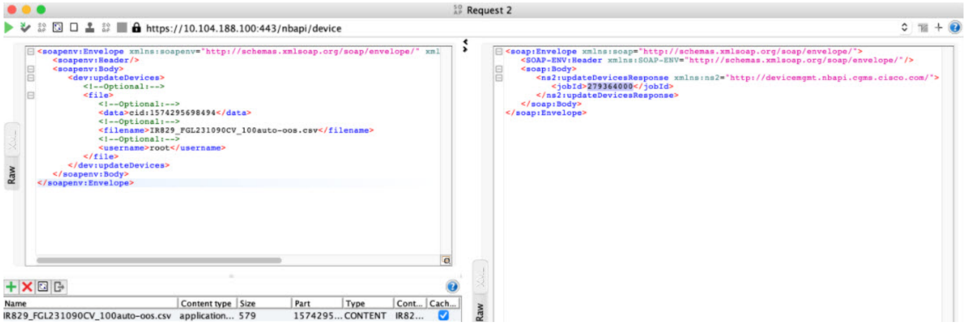


Step 15 In the XML file, provide the following information:

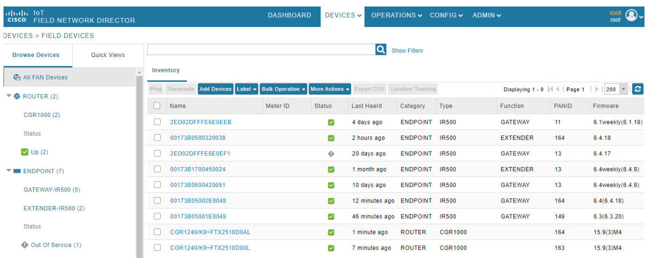
- Update the filename (copy the .csv filename from the Name field).
- Enter root as username.
- Update the HTTPS URL with FND IP details.

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

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



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



Managing License for OOS Devices

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

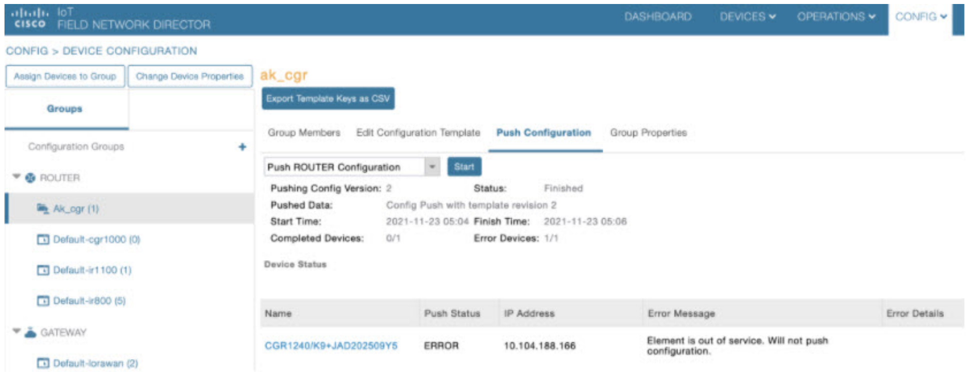
Supported Actions for OOS Devices

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

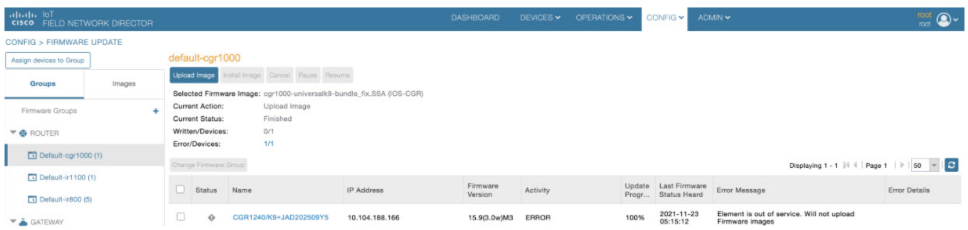
Restrictions for OOS Device Actions

The following actions are not supported for OOS device state:

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

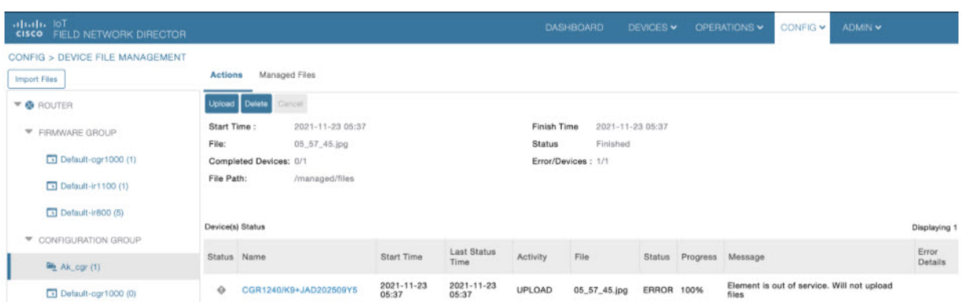


- In the **CONFIG** > **Firmware Update** page, when you use the upload or install image option on OOS devices, an error message appears.



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

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



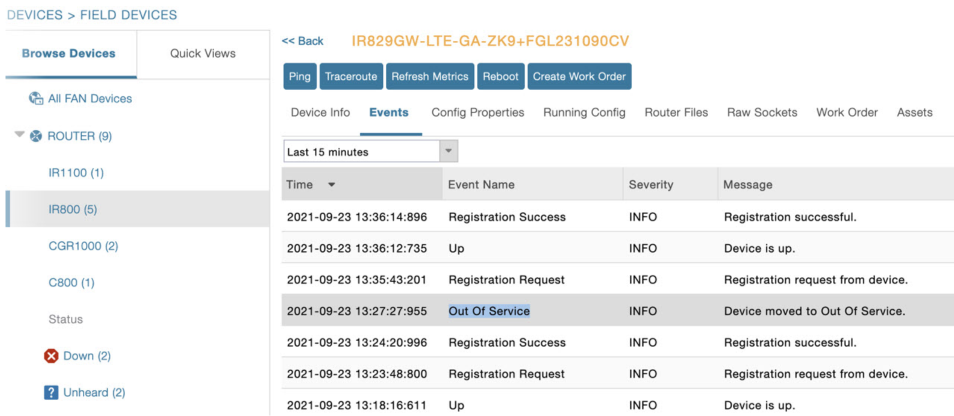
Viewing Events and Audit Trails for OOS Devices

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

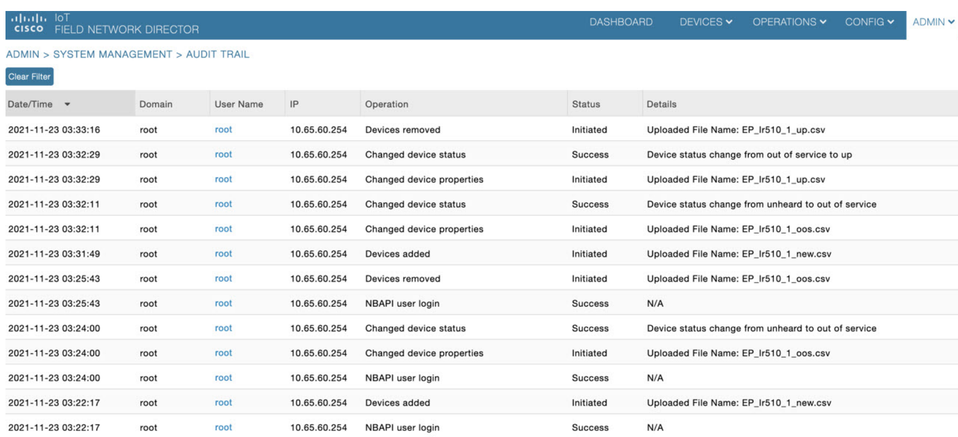
Note You cannot generate events for the devices that are currently in OOS state.

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

To filter existing OOS device events, refer to Viewing OOS Devices Using Filters, on page 196.



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



Viewing OOS Devices Using Filters

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

Procedure

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

Step 2 Click **Show Filter** option.

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

b) Select **Out of Service** option from the third drop-down list.

c) Click + icon to add the event name selected.

Step 3 Click the search icon.

The OOS device events are displayed.

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

Managing Itron Bridge Meters

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

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

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

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

There are two new properties associated with this feature:

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

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

There are two new properties for this feature:

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

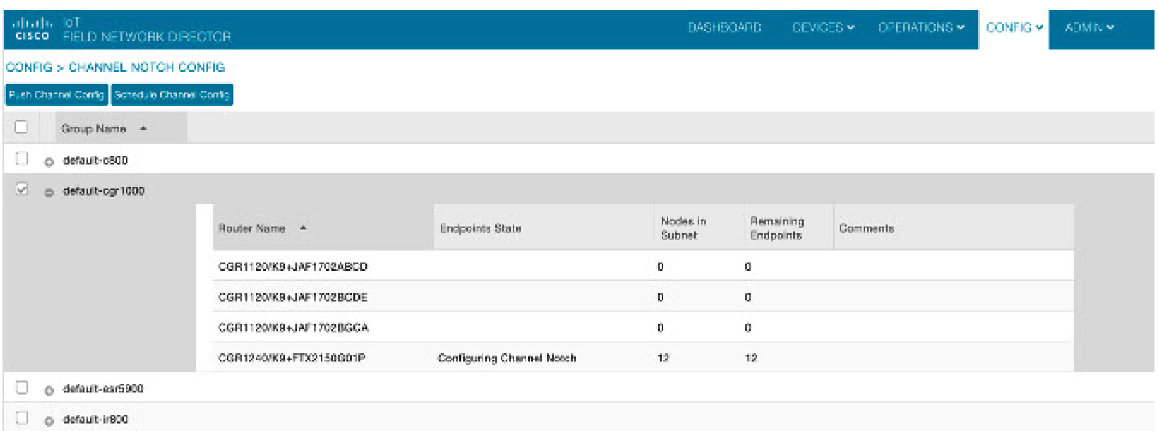
You can define up to four pairs of Notch Range Start and End Channels on the Channel Notch Settings page. These channel ranges must have increasing channel numbers for each range and cannot have any overlapping ranges. The ranges are blacklist ranges which are used to prohibit nodes from using the ranges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

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

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

Two additional properties are available:

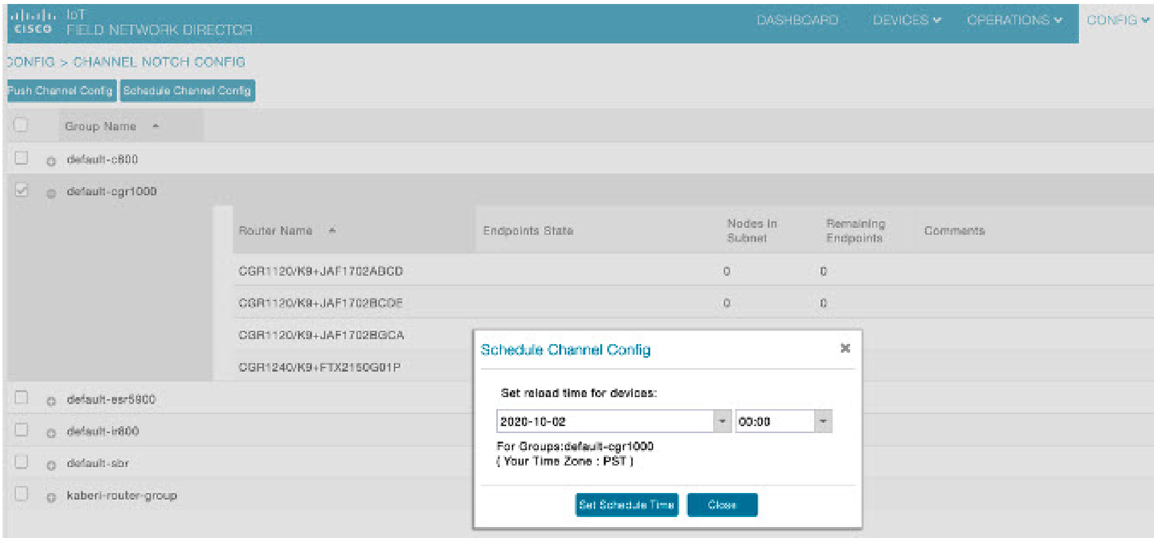
- channelNotchMaxAttempts = 20: This setting defines the maximum attempts that the software will attempt to send the config and schedule information to all of the endpoints.
- allowNewNotchSettings=true: This setting allows notch settings to be changed at will and defines those setting that will be used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

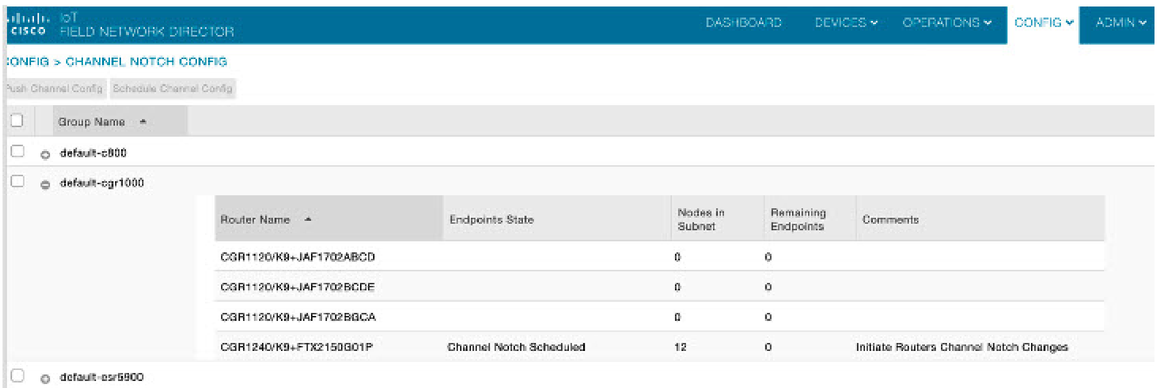


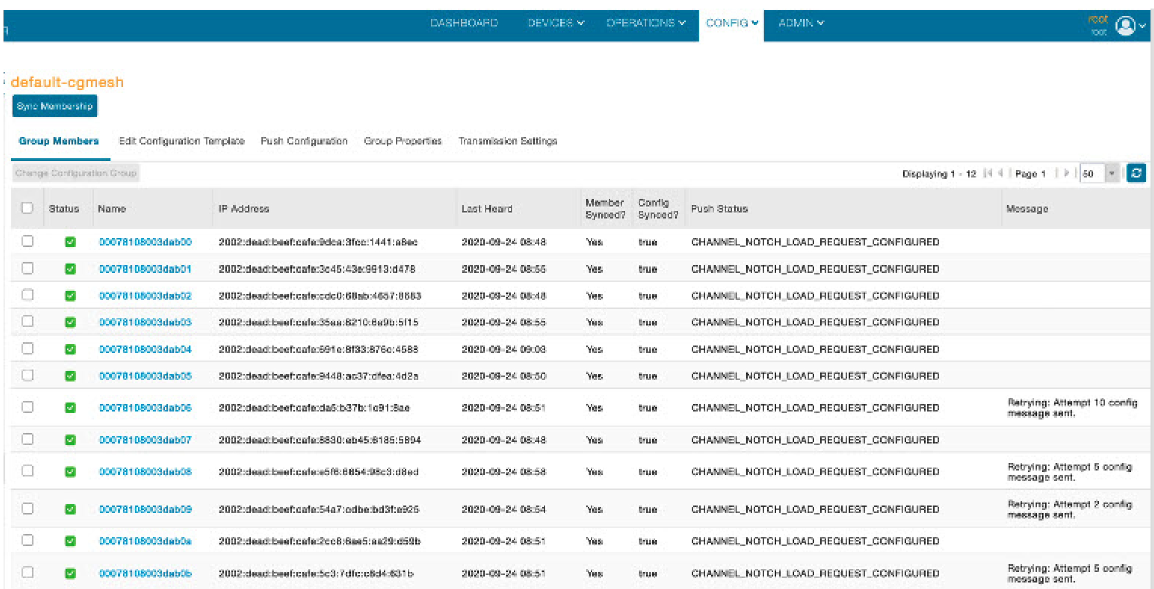
Note Before you can schedule activation of a Channel Notch Config, the router config groups must have successfully received their channel notch configuration. Note: Before you can schedule activation of a Channel Notch Config, the router config groups must have successfully received their channel notch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

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

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


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


IoT FIELD NETWORK DIRECTOR
DASHBOARD
DEVICES
OPERATIONS
CONFIG
ADMIN
CONFIG > CHANNEL NOTCH CONFIG
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 0 0
CGR1120/K9+JAF1702BCDE 0 0
CGR1120/K9+JAF1702BGCA 0 0
CGR1240/K9+FTX2150G01P Channel Notch Scheduled 12 0 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 2002:dead:beef:cafe:9dea:3fec:1441:a8ec 2020-09-24 08:48 Yes true CHANNEL_NOTCH_LOAD_REQUEST_CONFIGURED
00078108003dab01 2002:dead:beef:cafe:3c45:43e:9913:d478 2020-09-24 08:55 Yes true CHANNEL_NOTCH_LOAD_REQUEST_CONFIGURED
00078108003dab02 2002:dead:beef:cafe:cdc0:68ab:4657:8683 2020-09-24 08:48 Yes true CHANNEL_NOTCH_LOAD_REQUEST_CONFIGURED
00078108003dab03 2002:dead:beef:cafe:35aa:8210:6a9b:5f15 2020-09-24 08:55 Yes true CHANNEL_NOTCH_LOAD_REQUEST_CONFIGURED
00078108003dab04 2002:dead:beef:cafe:591e:8f33:876c:4588 2020-09-24 09:03 Yes true CHANNEL_NOTCH_LOAD_REQUEST_CONFIGURED
00078108003dab05 2002:dead:beef:cafe:9448:ac37:cfea:4d2a 2020-09-24 08:50 Yes true CHANNEL_NOTCH_LOAD_REQUEST_CONFIGURED
00078108003dab06 2002:dead:beef:cafe:da6:b37b:1c91:8ae 2020-09-24 08:51 Yes true CHANNEL_NOTCH_LOAD_REQUEST_CONFIGURED Retrying: Attempt 10 config message sent.
00078108003dab07 2002:dead:beef:cafe:8830:eb45:6185:5894 2020-09-24 08:48 Yes true CHANNEL_NOTCH_LOAD_REQUEST_CONFIGURED
00078108003dab08 2002:dead:beef:cafe:e5f6:8854:98c3:d8ed 2020-09-24 08:58 Yes true CHANNEL_NOTCH_LOAD_REQUEST_CONFIGURED Retrying: Attempt 5 config message sent.
00078108003dab09 2002:dead:beef:cafe:54a7:cdbe:bd3f:e926 2020-09-24 08:54 Yes true CHANNEL_NOTCH_LOAD_REQUEST_CONFIGURED Retrying: Attempt 2 config message sent.
00078108003dab0a 2002:dead:beef:cafe:2cc8:8ae5:aa29:d59b 2020-09-24 08:51 Yes true CHANNEL_NOTCH_LOAD_REQUEST_CONFIGURED
00078108003dab0b 2002:dead:beef:cafe:5c3:7dfc:c8d4:631b 2020-09-24 08:51 Yes true CHANNEL_NOTCH_LOAD_REQUEST_CONFIGURED Retrying: Attempt 5 config message sent.

```
[root@iot-fnd-oracle bin]# ./csmp-request  -r [2002:dead:beef:cafe:9dca:3fcc:1441:a8ec] 365 366 367 20
2020-09-24 09:09:52,148:INFO:main:CoapClient: CoAP Client's traffic class set to 72
[365/NotchUpdReq]: {"notchrangenum": 1,"notchlist": [{"startChnl": 38,"stopChnl": 39}]}
[366/NotchUpdResp]: {"errcode": 7}
[367/NotchUpdLoadReq]: {"loadtime": 4293908595}
[20/WPANSettings]: {"ifIndex": 2,"panid": 5577,"bcastSlotsize": 125000,"bcastPeriod": 500000,"neighborProbeRate": 300,"SSID": "\x46\x4e\x44\x31","notchList": [{"startChnl": 20,"stopChnl": 25}],"dwell": {"window": 20000,"maxdwell": 400}}
[root@iot-fnd-oracle bin]#
```

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

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

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

Managing Landis+Gyr Devices in IoT FND

Cisco IoT FND supports the following Landis+Gyr (L+G) routers and endpoints.

Support for L+G Routers in IoT FND

1. **Series 6 N2450** — The Landis+Gyr Series 6 N2450 (RF Mesh IP) Network Gateway provides the basis for a powerful RF wireless mesh network for remote data collection and end-device monitoring and control. The Network Gateway offers advanced functionality, such as individual message prioritization, additional memory for localized intelligence and the Linux operating system.
2. **Series 6 R651** — The Landis+Gyr Gridstream RF Series 6 Network Router is designed for outdoor mounting. The router supports RS-232/485 serial interface for Transparent Packet Protocol (TPP) and RS-232 serial interface for LAN Packet Protocol (LPP). The LAN Packet Protocol line is used to communicate to devices which use LPP, such as a PC with configuration or diagnostic software, or an end device which has implemented LPP. The TPP provides a general data port and is used to transport byte-oriented data, such as that generated by industry standard protocols.

Support for L+G Endpoints in IoT FND

1. **M125 Gas Module** — The M125 RF Residential Gas Communications Module provides two-way AMI communications retrofit solution for small diaphragm gas meters over Landis+Gyr's scalable, secure, and interoperable Gridstream® Connect RF Mesh network. The module is designed to record and communicate consumption and one channel of interval data. This data equips utilities to develop flexible rate offerings and assists with capacity planning.

2. **M225 Gas Module** — The M225 C&I Gas Communications Module provides two-way AMI communications retrofit solution for large diaphragm gas meters over Landis+Gyr's scalable, secure, and interoperable Gridstream® Connect network. The M225 gas module automatically self-registers on the Gridstream Connect network upon installation, simplifying deployment by eliminating the need for field installation, configuration, and specialized tools. The module is designed to record and communicate both total consumption and two channels of interval data (configurable to intervals of 5, 15, 30 and 60 minutes), and can be configured to record and transmit data at different frequencies. This data equips utilities to develop flexible rate offerings and assists with capacity planning.
3. **E360/E660 (Revelo)** — Landis+Gyr proudly introduces the Revelo™ metering family, the industry-first IoT grid sensing electric meters benefiting both utilities and their customers. Demands on the grid edge are changing — today's energy consumers want more insight and control to manage energy better. Enhanced reliability, safety, and the growing adoption of Distributed Energy Resources (DER) require more than traditional meter-to-cash capabilities. Revelo is a true grid sensor, providing unprecedented insight and control through industry-leading waveform data technology, offering superior edge computing capabilities and a greater ability to sample, process, store, and deliver data to the right places in real-time.

Support Mesh Parent for L+G Endpoints

IoT FND displays the mesh parent value as 1 for L+G endpoints. In case of Cisco routers, such as CGR1000, IR8100, the mesh parent value is shared with FND considering the total number of primary and alternative mesh nodes. Likewise, FND does not receive the mesh parent value from the L+G N2450 router. As a result, FND always considers the mesh parent value as 1 for L+G endpoints.

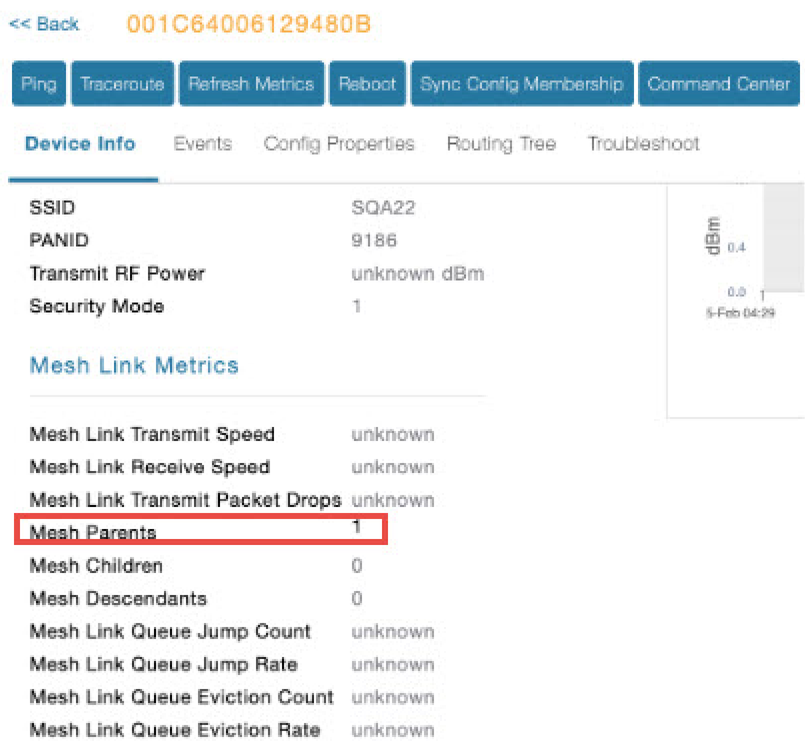
To view the mesh parent value for L+G endpoints:

Procedure

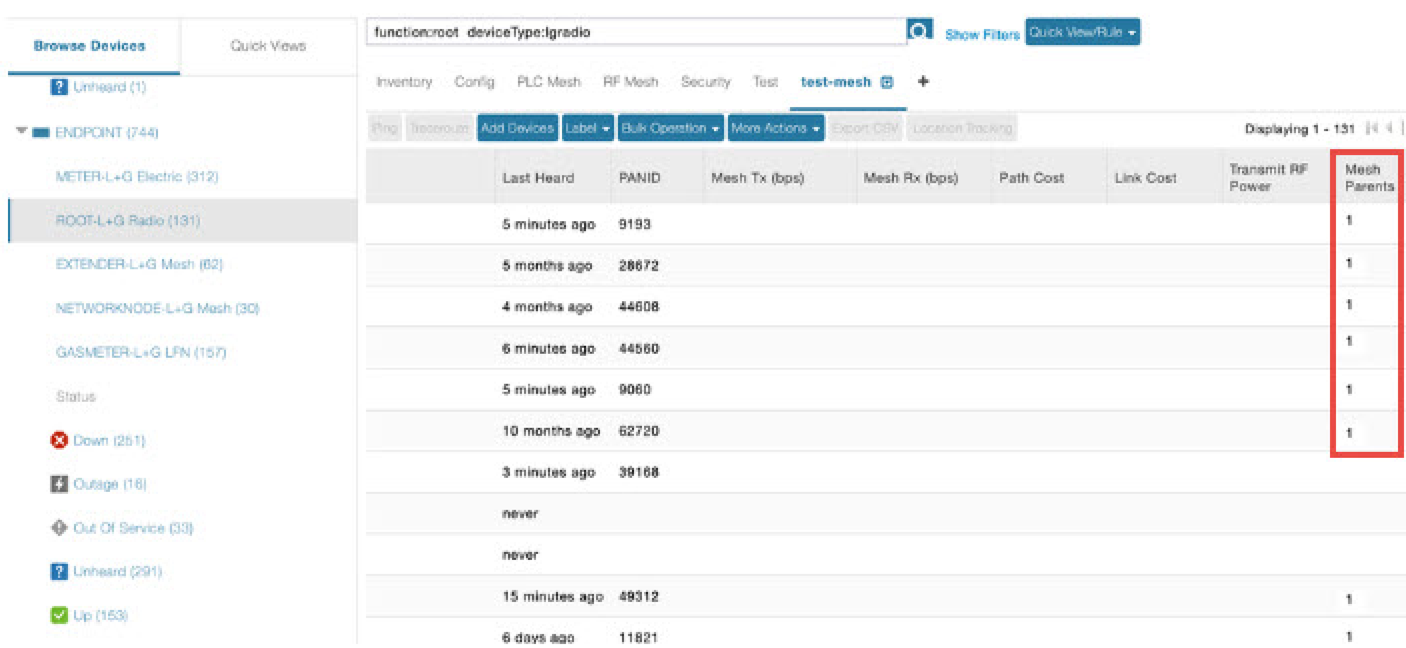
Step 1 Choose **DEVICES** > **FIELD DEVICES** > **Browse Devices** > **ENDPOINTS**.

Step 2 Click the device type in the left pane.

Step 3 Click the device in the right pane for which you want to view the mesh parent information. The Device Details page appears with the mesh parent information under **Mesh Link Metrics**.



Alternatively, you can view the mesh parent value in the Inventory table of the Field Devices page under the ENDPOINT device category.



LDevID: Auto-Renewal of Certs and Saving Configuration

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

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

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

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

Support Expired SUDI Certificate

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

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

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

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

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

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

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

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

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

Example Display

```
SUDI Certificate:

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

Issuer:
cn=ACT2 SUDI CA
o=Cisco

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

CA Certificate
Status: Available
Certificate Serial Number (hex): 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

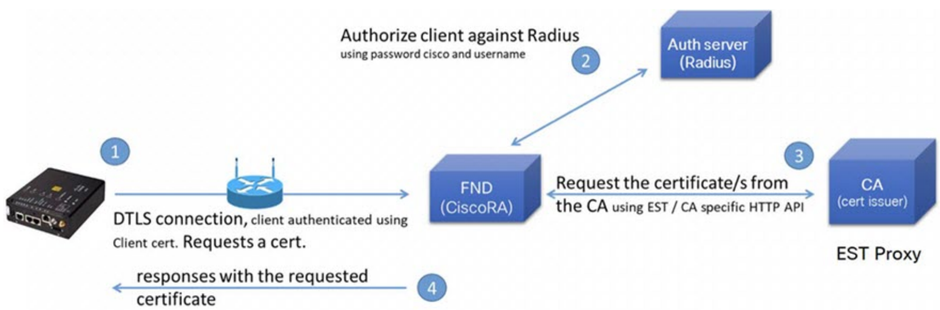
This section provides an overview of the components and configurations involved in integrating Enrollment over Secure Transport (EST) certificate enrollment for clients over the secure transport layer within the network. EST is based on public-private key exchange. This feature is supported on Itron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

Table 27: EST Support

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

EST Overview

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



EST also operates with the following protocols and authentication methods:

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

Configuring FND Registration Authority (RA)

Follow these steps to configure the FND Registration Authority:

Procedure

Step 1 Install FND-RA rpm.

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

```
[root@iot-fnd-ra fnd-ra]# cd /opt/fnd-ra/bin
python3.9 ra_setup.pyc
```

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

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

Authentication Server: 2

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

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

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

CA Server: 2

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

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

Enter CA/Auth credentials

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

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

Host Name or IP Address for the RA to listen on[]: 10.29.36.243
Path to the identity certificate of RA []: /home/certs/server-cert.pem
Path and file name to the trusted certificate store for the RA[]:
[/home/certs/est_trust_certificate.pem
Path and file name to the CACerts response file[]:
/home/certs/multicacerts.crt
RA log level (debug/info/warn/error) [debug]: debug
Transport protocol (http/coap) [coap]: coap
What is the DTLS handshake timeout (MIN=2, MAX=60) [5]:5
What is the DTLS MTU size (MIN=256, MAX=1152) [1152]:1152

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

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

Please find your selections below:

Host Name or IP address of the RADIUS server : 10.29.36.224
Port Number of the RADIUS server (MIN=1, MAX=65535) : 1812
Number of retries allowed for authentication requests (MIN=1, MAX=30) : 5
RADIUS timeout in seconds (MIN = 1, MAX = 30) : 5
```

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

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

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

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

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

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

DTLS Relay Configuration and Watchdog Cisco-RA Monitoring in FND

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

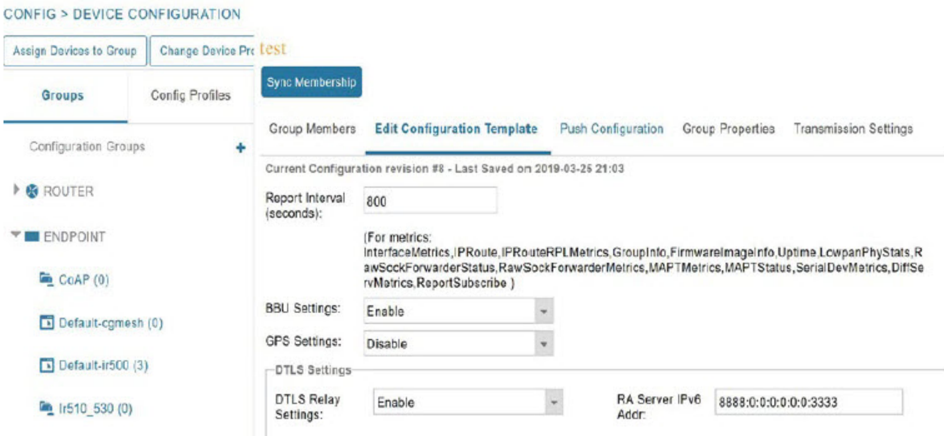
Note Supported from version 4.5.0.122 onwards.

Procedure

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

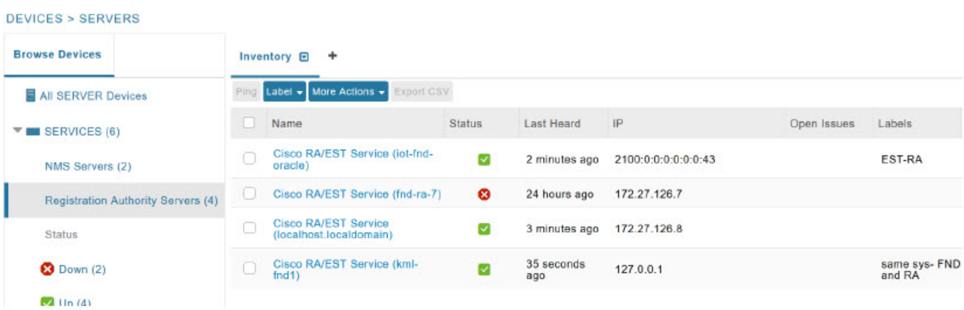
Step 2 Select **Enable** from the **DTLS Relay Settings** drop-down list.

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



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

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



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

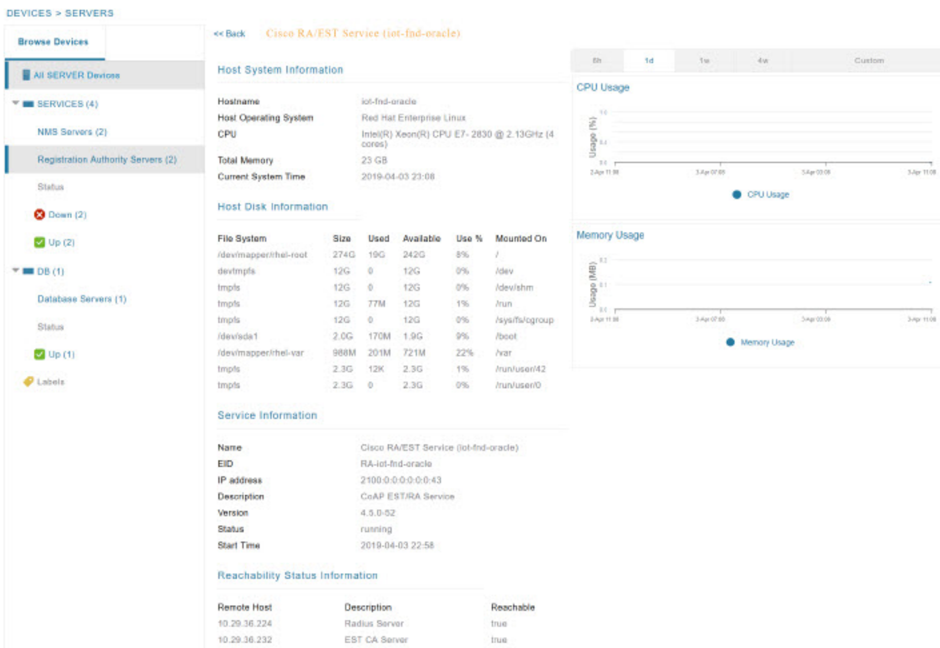


Figure 9: Events for FND-RA Service

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

Figure 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

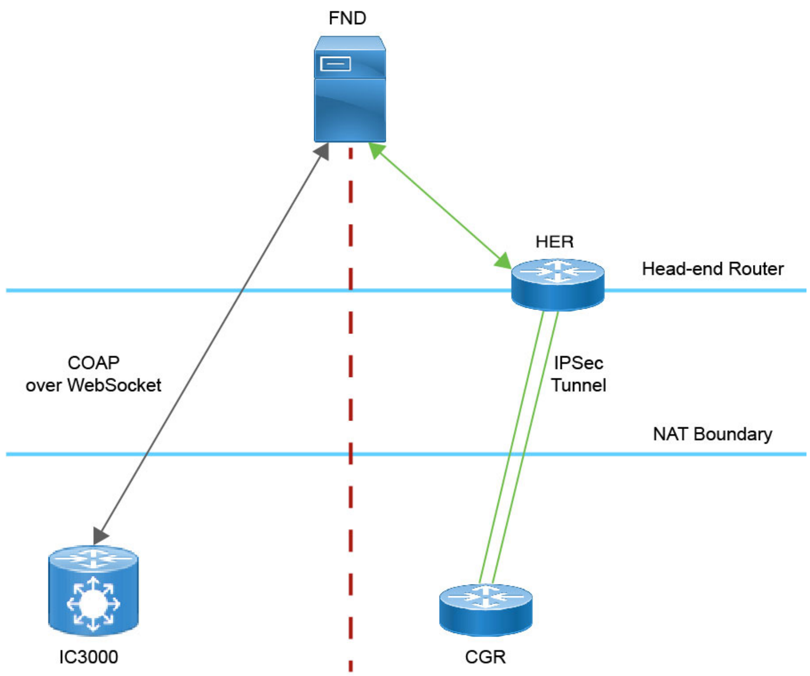
IC3000 supports edge computing and communicates with IoT FND through the IOx application, Cisco Fog Director which is accessible via IOT FND.

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.

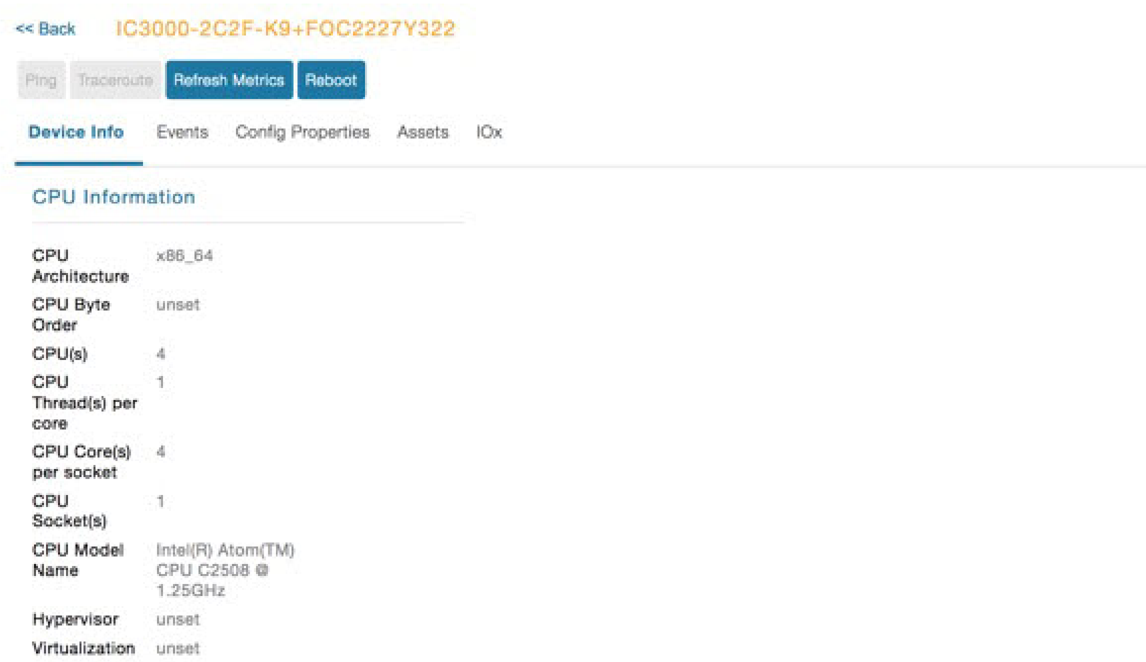


You can perform the following actions for an IC3000 device type on demand:

- 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:

Procedure

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

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

Step 3 Click **Edit Configuration Template**.

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

Step 5 Click **Save Changes**.

NTP Configuration

To push the NTP configuration via FND,

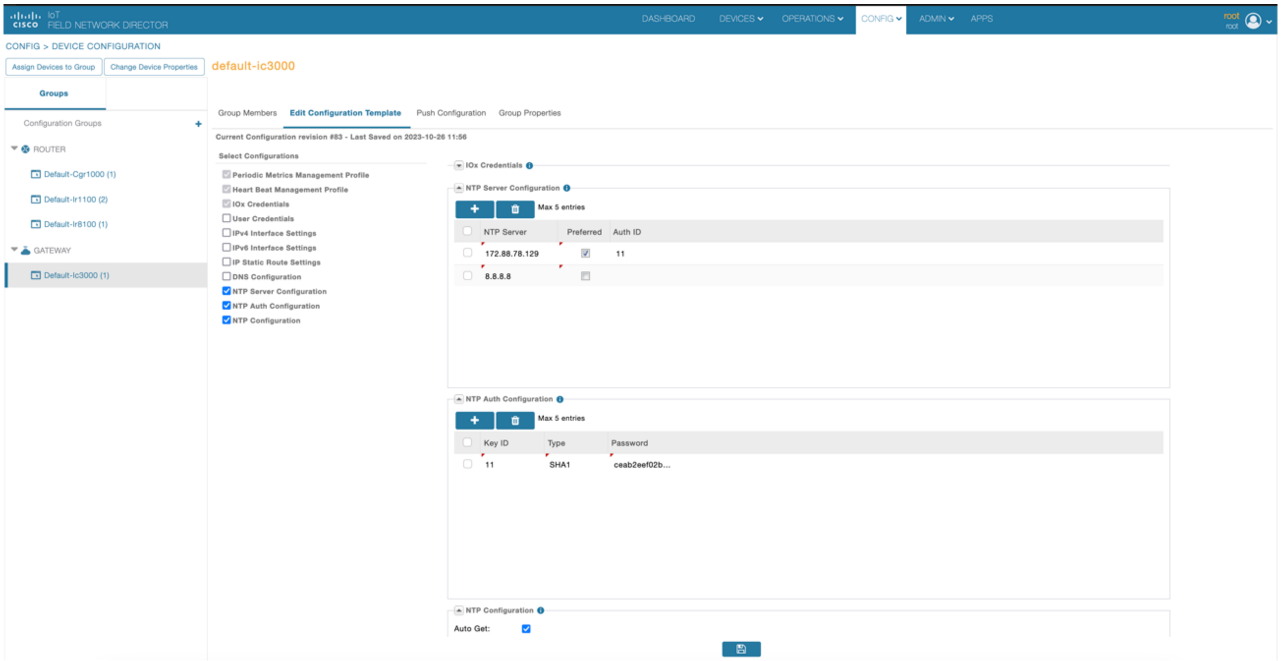
Procedure

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

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

Step 3 Click **Edit Configuration Template**.

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



Note

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

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

Step 6 Click **Save Changes**.

Managing the Cisco Wireless Gateway for LoRaWAN

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

The two Cisco Wireless Gateway for LoRaWAN products are:

- A virtual interface (IXM-LPWA-800-16-K9) of the Cisco 809 and 829 Industrial Integrated Service Routers (IR809, IR829) to provide LoRa radio access with the IR809 and IR829 providing an IP backhaul (Gigabit Ethernet, Fiber, 4G/LTE, and Wi-Fi). In this case, LoRaWAN has an Operating Mode of IOS Interface and displays the Hosting Device ID for the IR800 system to which it connects (See Managing External Modules, on page 226).

- 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.

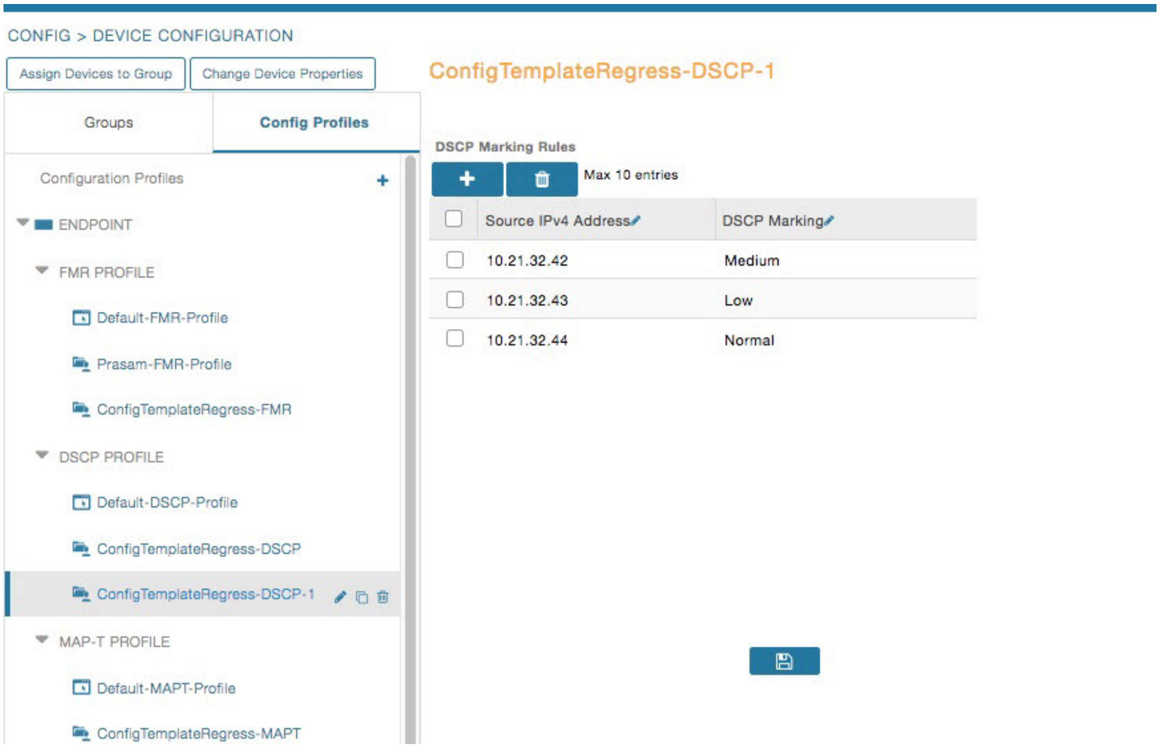
Table 28: Pre-defined Profiles for IR510

Profile Name	Description	Properties Configurable in CSV File
Forward Mapping Rule (FMR) Profile **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **FMR PROFILE** Interface configuration **CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template** Select the FMR profile from the drop-down menu	Processes IPv4 traffic between MAP nodes that are in two different MAP domains. Each FMR rule has IPv4 Prefix, IPv4 Prefix Length and EA Bits Length. You can define up to 10 FMR Profiles. FMR settings are pushed to the device as a part of MAP-T Settings during configuration push.	Forward Mapping Rule IPv6 Prefix: fmrIPv6Prefix0 to fmrIPv6Prefix9 Forward Mapping Rule IPv6 Prefix Length: fmrIPv6PrefixLen0 to fmrIPv6PrefixLen9
DSCP profile **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **DSCP PROFILE** Interface configuration **CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template** Select the DSCP profile from the drop-down menu	Sets the DSCP marking for the Ethernet QoS configuration. DSCP marking has eight (8) marking options to choose. - User Controlled - Default Queue (Best Effort) - Normal Queue: Low drop probability (AF11) - Normal Queue: Medium drop probability (AF12) - Normal Queue: High drop probability (AF13) - Medium Queue: Low drop probability (AF21) - Medium Queue: Medium drop probability (AF22) - Medium Queue: High drop probability (AF23) You can specify a maximum of 10 IPv4 addresses and associated DSCP markings.	NA

Profile Name	Description	Properties Configurable in CSV File
MAP-T Profile **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **MAP-T PROFILE** Interface configuration **CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template** Configures Basic Mapping Rule (BMR) and Default Mapping Rule (DMR) settings for IR509/IR510	Configures endUser properties.	endUserIPv6PrefixbmrIPv6PrefixLen
Serial Port Profile (DCE and DTE) **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **SERIAL PROFILE** Interface configuration **CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template** Select the Serial Port profile (DTE) and/or Serial Port profile (DCE) from the drop-down menu	You can use different serial port profiles for DCE and DTE serial port settings). You can configure the following settings on the serial interface: • Port affinity • Media Type • Data Bits • Parity • Flow Control • DSCP Marking • Baud rate • Stop Bit **Note** You can also configure Raw Socket Sessions settings at the this page.	NA

Profile Name	Description	Properties Configurable in CSV File
DHCP Client Profile **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **DHCP CLIENT PROFILE** Interface configuration **CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template** Select the DSCP Client profile from the drop-down menu	The DHCPv4 server allocates an address to each client according to a static binding between a client-id and an IPv4 address. FND configures this static binding supports up to 10 client mappings. The DHCP Client ID binding profile configuration associates a client ID to an IPv4 Host address. The Client-id of each Client is expected to be unique within a single IR510. Any string can be used as client-id (for example, client-id=”iox”) can be mapped to a binding address in the pool.	NA
DHCP Server Profile **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles tab** > **DHCP SERVER PROFILE** Interface configuration **CONFIG** > **DEVICE CONFIGURATION** > **GROUPS tab** > **Default-ir500** > **Edit Configuration Template** Select the DSCP Server profile from the drop-down menu	Information that the DHCPV4 Server returns as part of DHCP Options in the response, can be configured in the DHCP server profile configuration includes: **1.** Lease Time **2.** DNS server list	NA

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

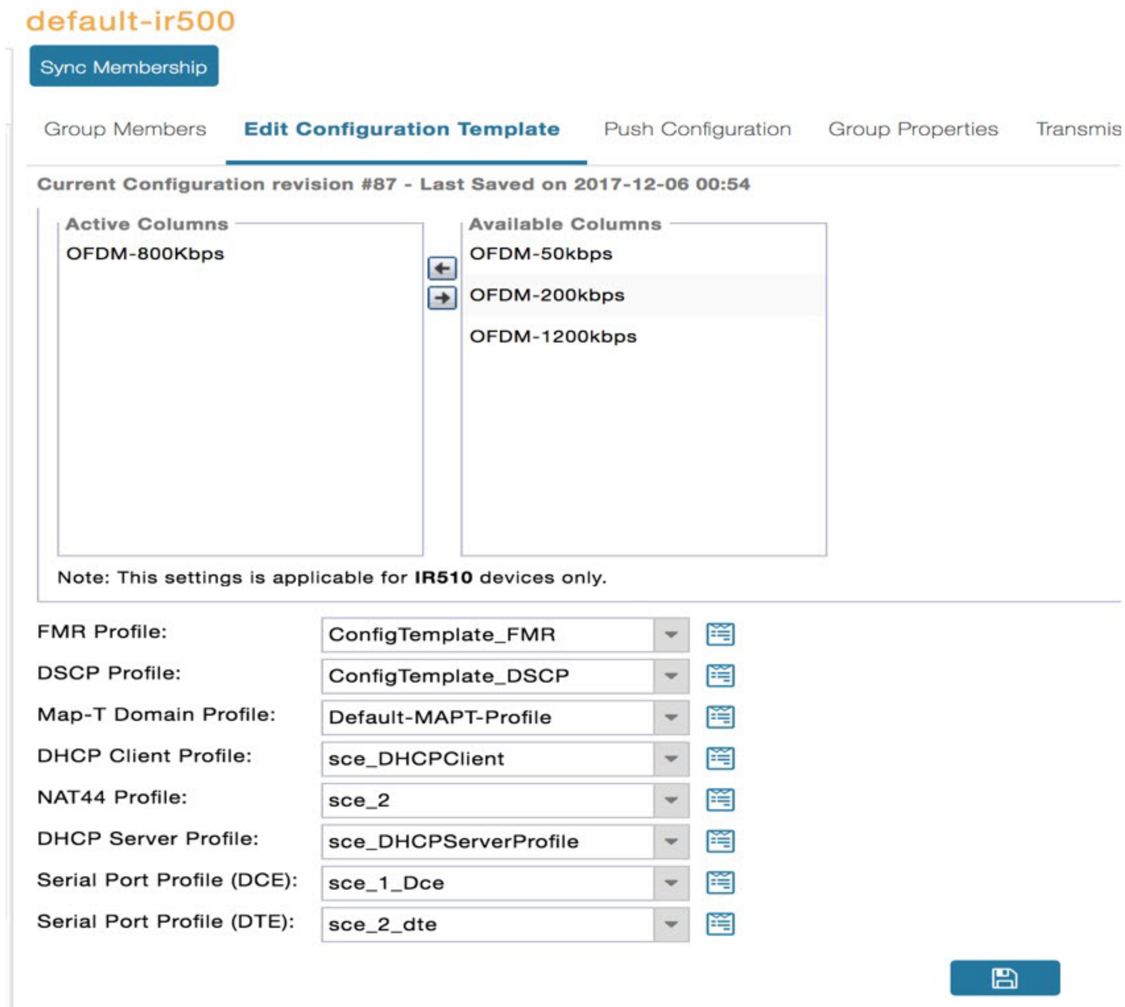


Configuration Notes:

- 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.

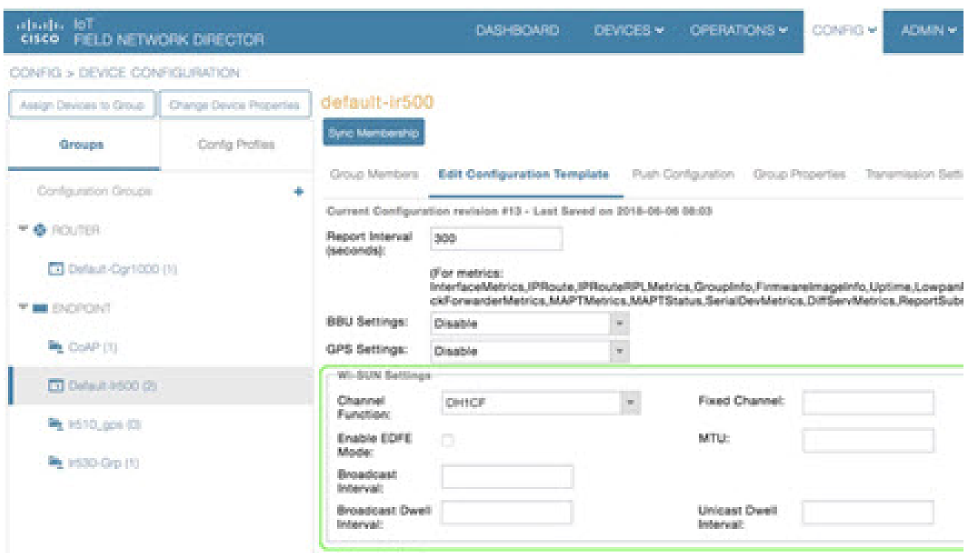
Note In Mesh Software 6.3, only the Wi-SUN 1.0 protocol is supported for all mesh endpoints. It displays Wi-SUN 1.0 from the mesh 6.3 firmware onward under the Mesh Protocol heading on the **DEVICES** > **FIELD DEVICES** > **ENDPOINT** > **Inventory** page.

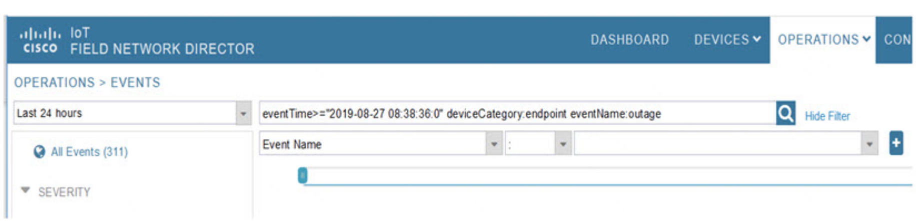
The Wi-SUN settings have been removed from the IR500 Config Group template: **CONFIG** > **DEVICE CONFIGURATION** > **Default-ir500** > **Edit Configuration Template** in IoT FND 4.7.

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.



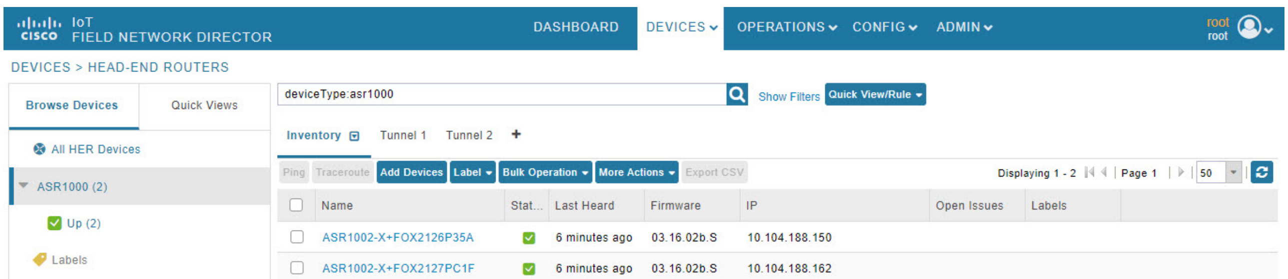


Managing Head-End Routers

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 232

For information about the device properties displayed in each view, see Device Properties, on page 343.

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 231

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.

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

Procedure

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

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

```
manage-actd=true
```

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

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

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

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

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

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

Lorawan Gateway Module

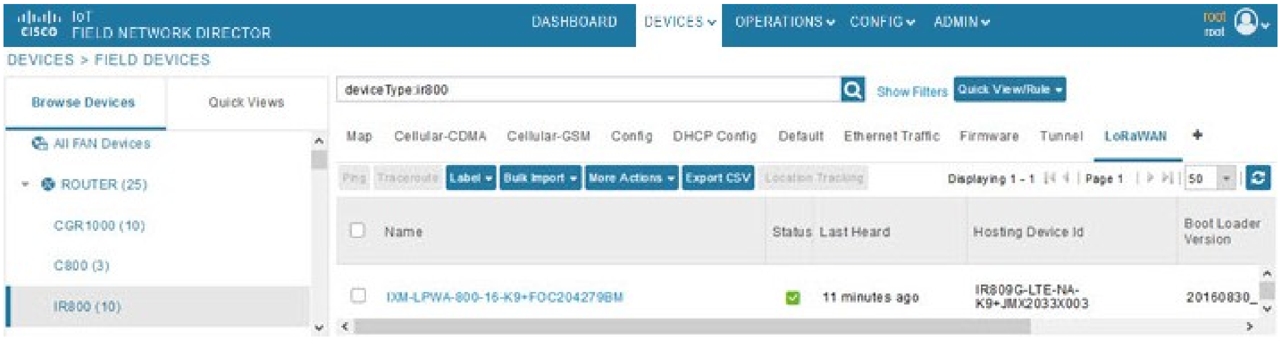
Procedure

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

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

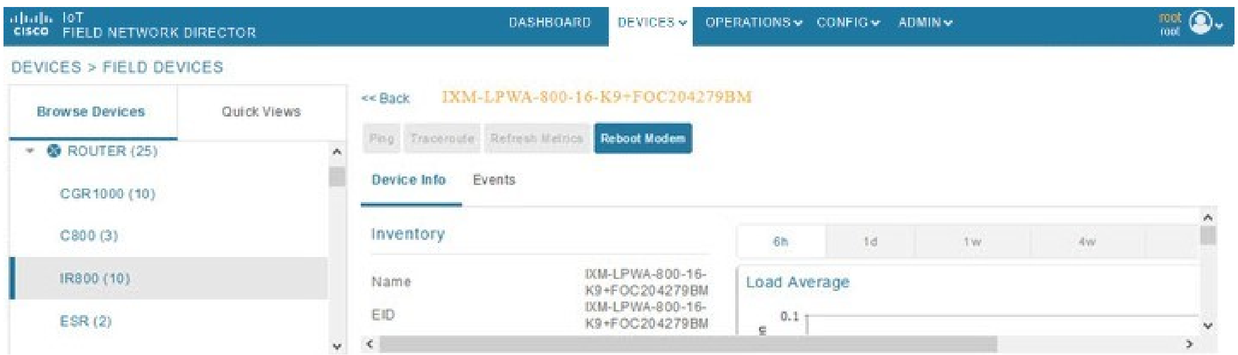
Note
IoT FND does not support discovery for the LoRaWAN module. Rather, IoT FND recognizes it as an IR800 module and will communicate with it via Cisco IOS.

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



Step 3 To reboot the modem on the LoRaWAN module:

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



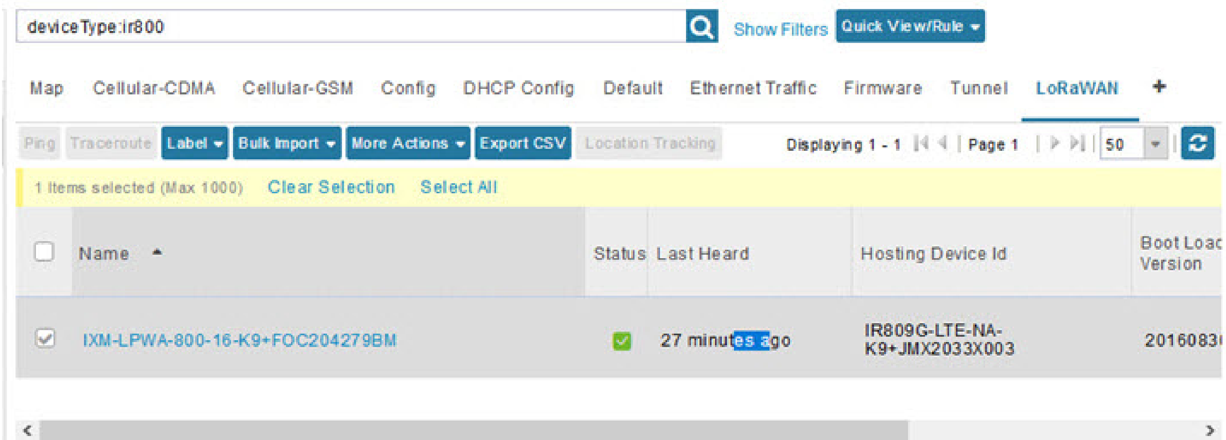
b) Click **Reboot Modem**. When the reboot completes, the date and time display in the Last Reboot Time field in the Device Info pane for the LoRaWAN module. You can only process one modem reboot at a time.

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

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

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

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



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

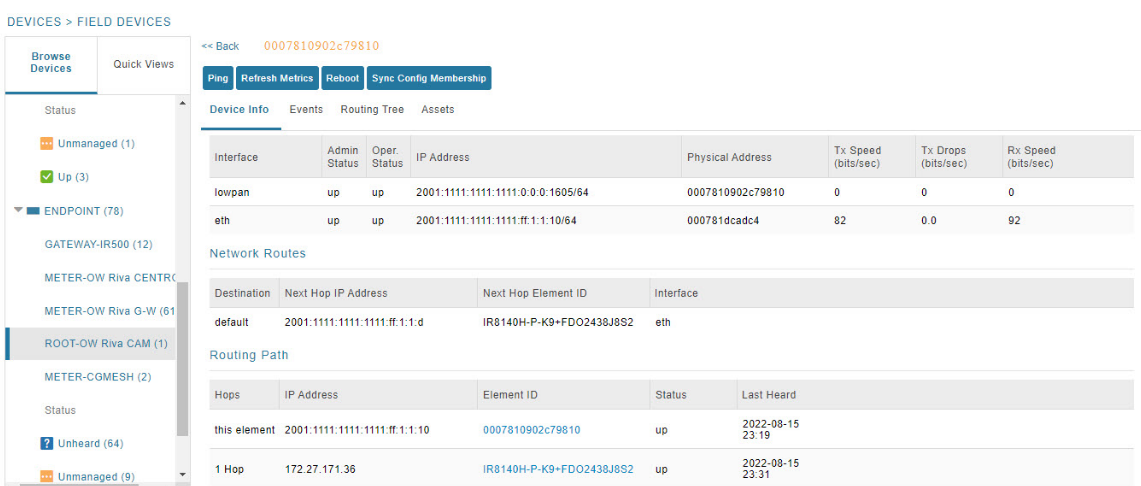
Step 5 To create a user-defined LoRaWAN (IXM) Tunnel, choose **CONFIG** > **Tunnel Provisioning**.

a) In the left-pane, under GATEWAY, select the LoRaWAN system for which you want to configure a tunnel.
b) Select the **Gateway Tunnel Addition** tab.
c) In the **Add Group** window that appears, enter a Name for the LoRaWAN (IXM) Tunnel and select Gateway as the Device Category.
d) Click **Add**.

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

Routing Path

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



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

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

Managing Servers

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

To add additional views, see Customizing Device Views, on page 232.

For more information about the device properties displayed in each view, see Device Properties, on page 343.

For information about the common actions in this view, see Common Device Operations, on page 231 .

Managing NMS and Database Servers

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

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

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

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

Managing Application Management Servers

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

Common Device Operations

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

Tracking Assets

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

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

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

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

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

  Example of Asset content in CSV file:

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

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

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

Guidelines for Adding or Associating an Asset with a Device:

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

Selecting Devices

- To select all devices listed on a page, check the check box next to **Name**.
- To select devices across all pages, click **Select All**.

- To select a group of devices, check the check boxes of individual devices listed on a page and across pages. The count increments with every device selected, and selections on all pages are retained.

Customizing Device Views

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

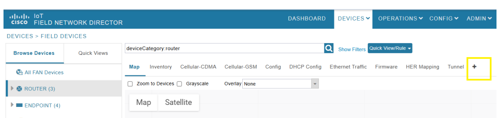
- Add and delete tabs
- Specify the properties to display in the columns for each view (see Device Properties by Category, on page 344 for available properties)
- Change the order of columns

Adding Device Views

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

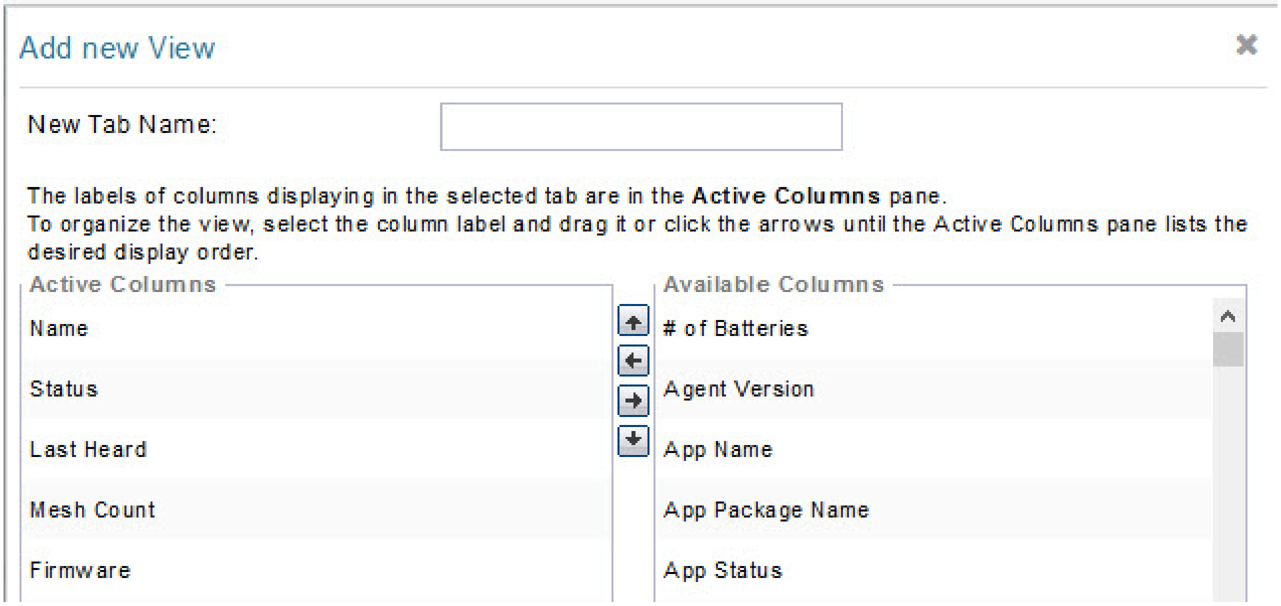
Procedure

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



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

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



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

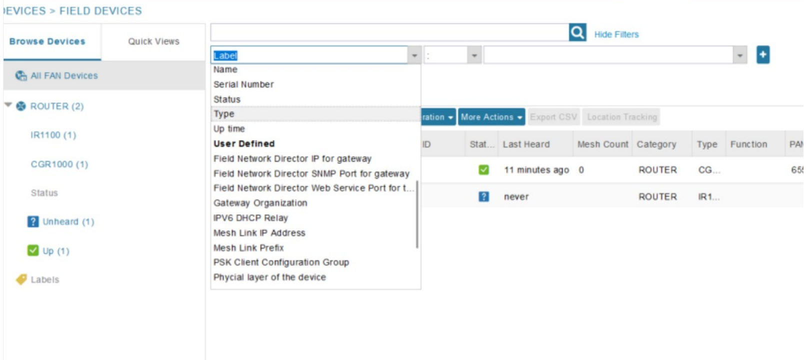
Table 29: Active and Available Columns

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

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

Note

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



Step 4 Click **Save View**.

Editing Device Views

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

Procedure

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

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

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

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

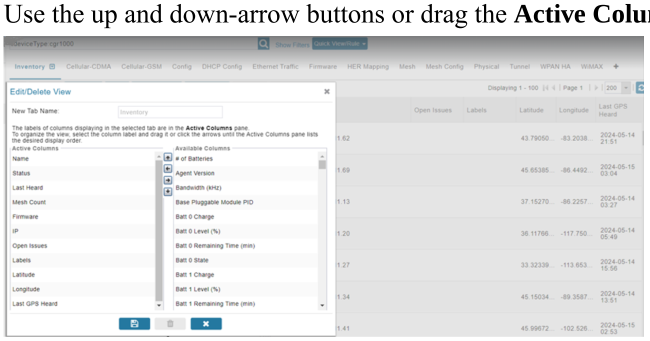
Step 4 In the **Edit/Delete View** dialog box:

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

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

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

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



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

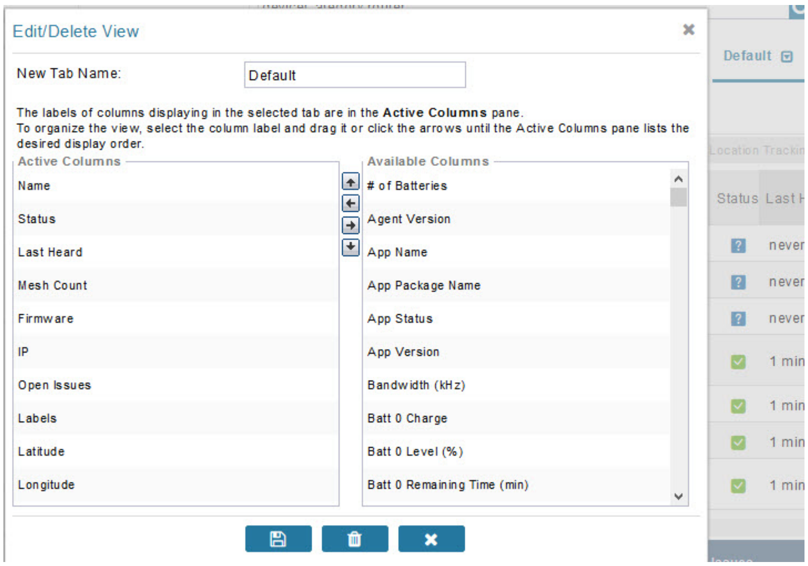
Step 5 Click the disk icon to save the view.

Deleting a Device View

Procedure

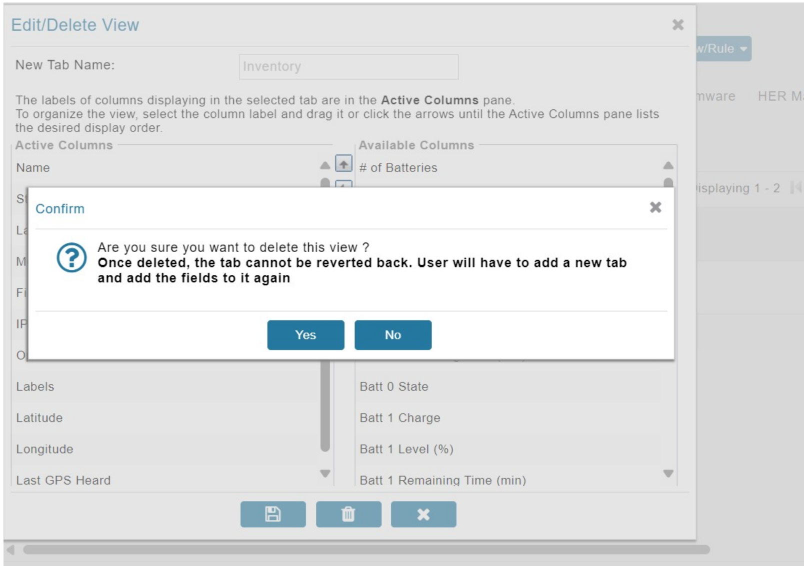
Step 1 Select a device type under the **Browse Devices** pane, and click the Default drop-down arrow to open the **Edit/Delete View** dialog box.

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



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

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



Viewing Devices in Map View

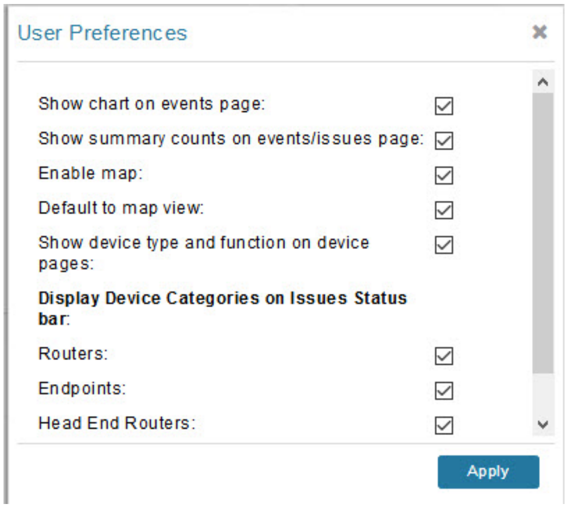
IoT FND provides a map view for visualizing device information based on geographic location. In Map view, IoT FND displays a Geographic Information System (GIS) map and uses GIS Map services to show device icons on the map based on the latitude and longitude information of the device. When this information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

To view devices in Map view:

Procedure

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

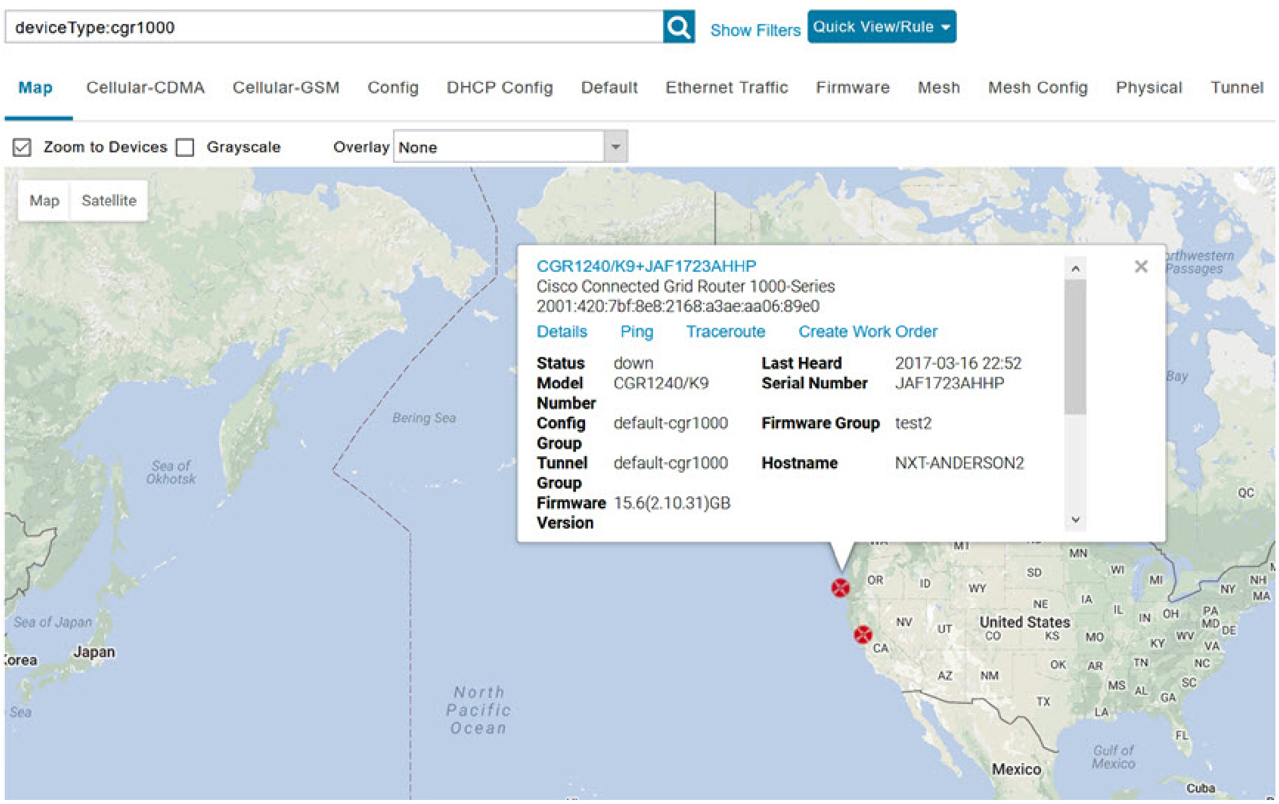
Step 2 Select the **Enable map** check box, and click **Apply**.



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

Step 4 Click the **Map** tab.

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



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

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

To display a subset of all devices, click one of the filters listed in the Browse Devices pane.
IoT FND changes the map region based on your selection and displays the devices found by the filter. For example, you can use the **Routers** > **Up** filter to display all routers that are up and running. You can also use saved custom filters in the Quick View pane (left pane) to filter the device view. For information about creating custom filters, see Creating a Quick View Filter, on page 248.
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 143 in the Managing System Settings chapter.

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

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

Configuring Map Settings

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

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

To configure map settings:

Procedure

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

Step 2 Click the **Map** tab.

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

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

Step 3 Click **OK** .

Changing the Sorting Order of Devices

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

Exporting Device Information

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

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

Procedure

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

Step 2 Click **Export CSV**.

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

What to do next

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

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

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

Pinging Devices

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

To ping selected devices, in List view:

Procedure

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

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

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

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

Step 3 To close ping display, click X icon.

Tracing Routes to Devices

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

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

To trace routes to selected devices, in List view:

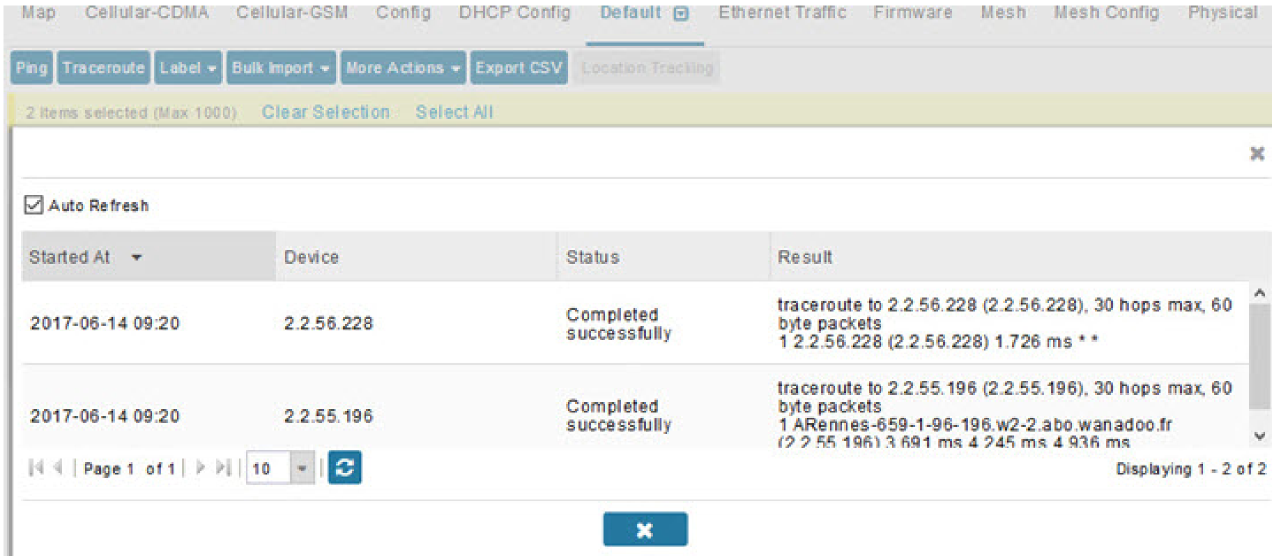
Procedure

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

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

Step 2 Click **Traceroute**.

A window displays with the route-tracing results.



Expand the Result column to view complete route information.

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

Step 3 Click X to close the window.

Managing Device Labels

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

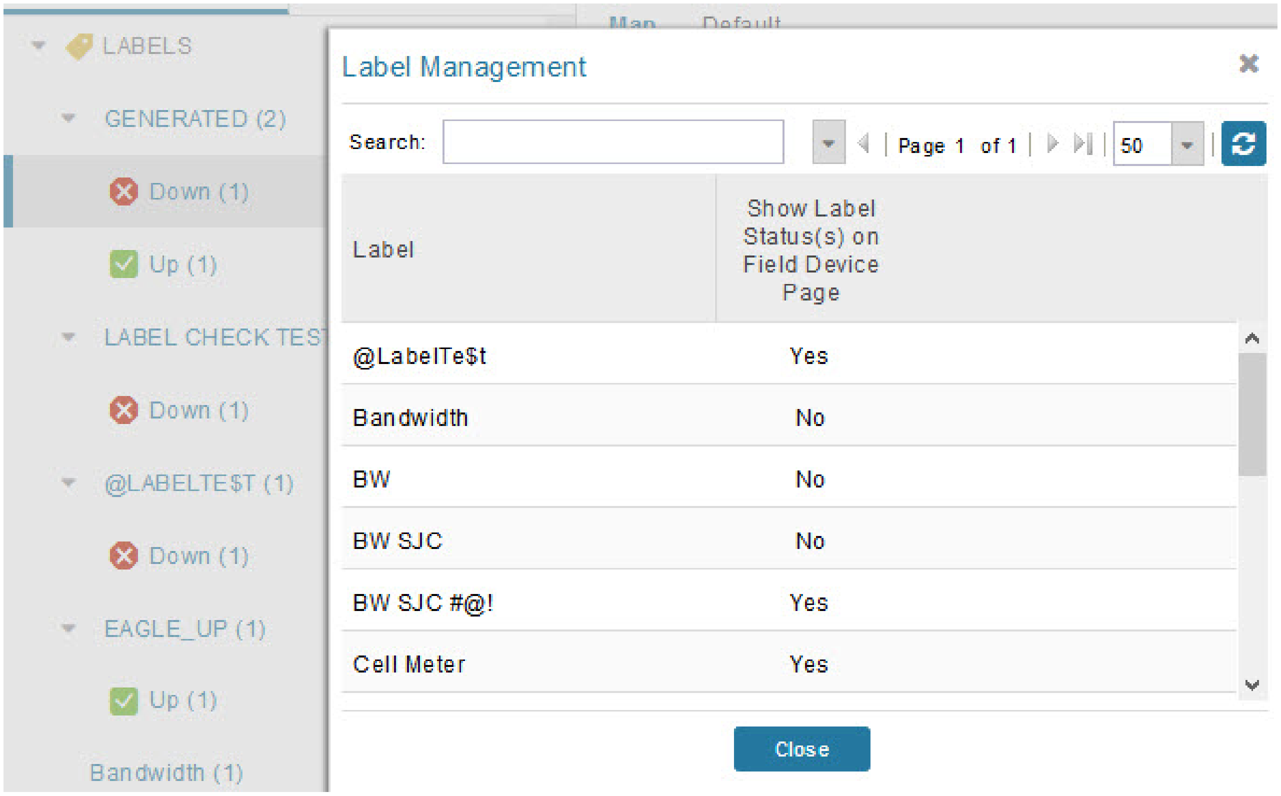
Managing Labels

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

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

Procedure

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



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

Tip
Click the arrowhead icon next to the Search field to reverse label name sort order.

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

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

Step 3 Click **Close**.

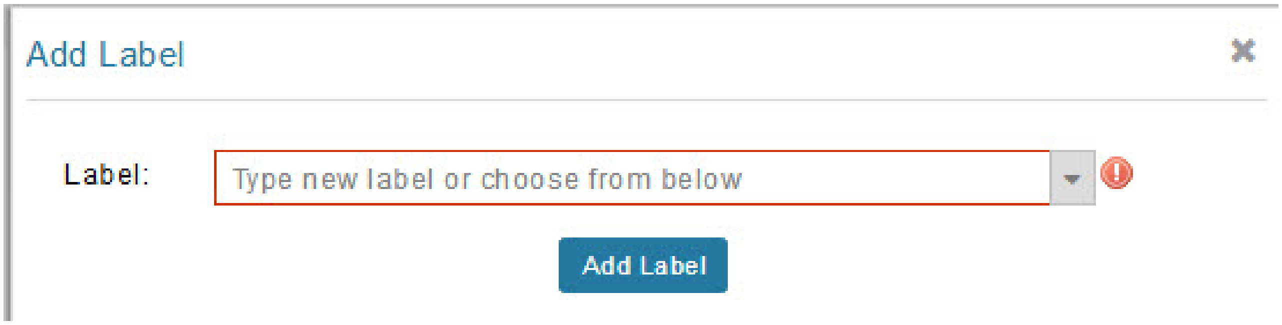
Adding Labels

To add labels to selected devices, in List view:

Procedure

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

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



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

Step 3 Click **Add Label**.

Tip
You can add multiple labels to one device.

Step 4 Click **OK**.

What to do next

To add labels in bulk, see Adding Labels in Bulk, on page 255.

Removing Labels

To remove labels from selected devices, in List view:

Procedure

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

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

Step 3 Click **OK**.

To remove labels in bulk, see Removing Labels in Bulk, on page 256.

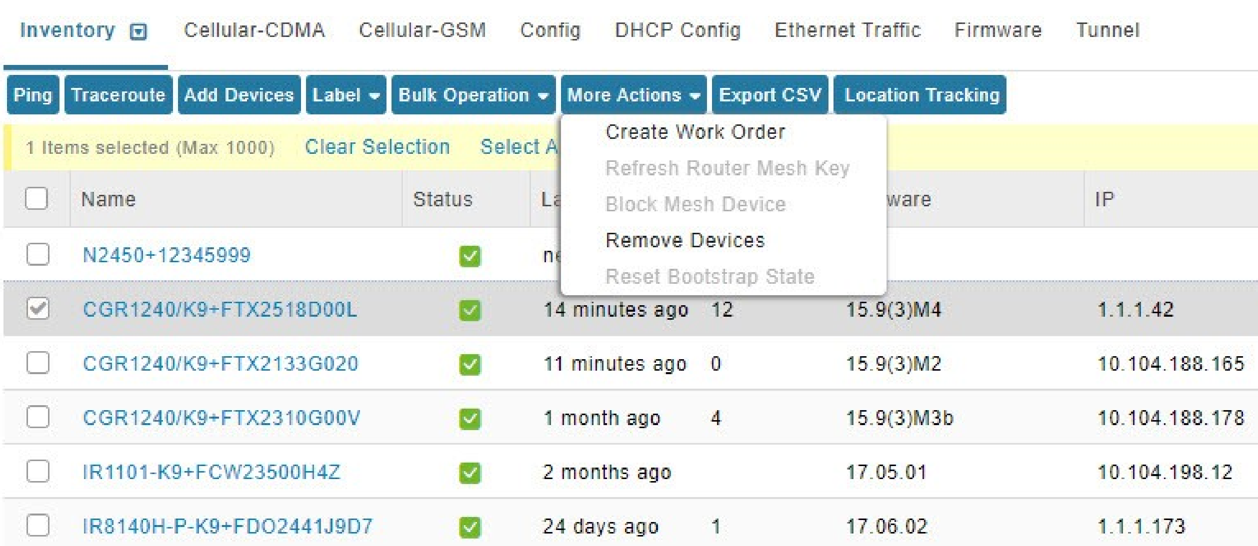
Removing Devices

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

To remove devices, in List view:

Procedure

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



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

Step 3 Click **Yes**.

Displaying Detailed Device Information

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

Detailed Device Information Displayed

- Server Information, on page 244
- Head-end Router, Router, and Endpoint Information, on page 245

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.

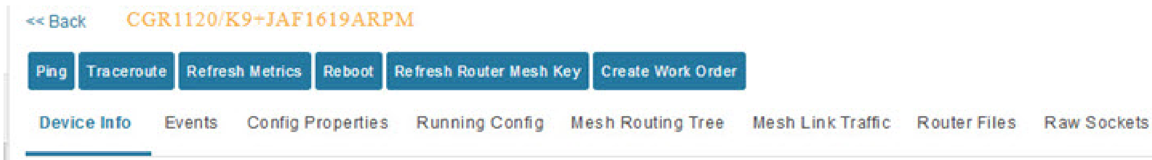
Table 30: NMS Server Pane Areas

Area and Field Name	Description
Host System Information	
Hostname	Hostname of the IoT FND server.
Host Operating System	Operating system.
CPU	CPU specifications and CPU Usage graph.
Total Memory	Total amount of RAM memory (GB) available on the system and Memory Usage graph.
Current System Time	Current system time.
Host Disk Information	
File System	File system.
Size	Size of file system disk space (GB).
Used	Amount of file system disk space used (GB).
Available	Available file system disk space (GB).
Use %	Percentage of file system disk space used.
Mounted On	The directory in which the file system is mounted.
IoT FND Application Information	
EID	EID of the server.
Start Time	Time when the IoT FND server started.
Number of Restarts	The number of times the IoT FND application has restarted.
Memory Allocation	Memory space allocation in GB for the IoT FND application.
Graphs	
CPU usage	Displays usage information during set and custom-defined intervals. For more information on viewing the chart for default or custom-defined time intervals, refer to Setting Time Filters To View Charts, on page 461
Memory Usage	Memory usage plotted in MB.
CSMP	CoAP Simple Management Protocol (CSMP) message statistics.

Head-end Router, Router, and Endpoint Information

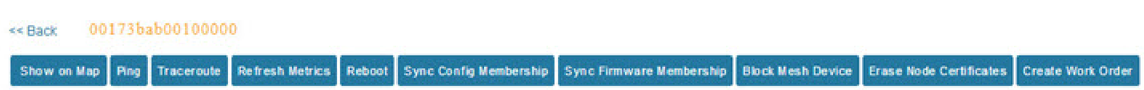
Select **DEVICES** > **Field Devices** and then select a device type (router, head-end router or endpoint) from the Browse Devices pane. Then, click on the Name of a specific system from the device list to see the available information (such as Device Info, Events, Config Properties, etc.) for that system 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 343). For routers and endpoints, IoT FND also displays charts (see Viewing Device Charts, on page 485 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 343). 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 264.
Running Config (routers)	Displays the running configuration on the device.
Routing Tree (CGR1000, endpoints: gateway-IR500, meter-cgmesh, meter-OW Riva)	Displays the routing tree. For routers, the pane displays all the possible routers from the endpoints to the router. For endpoints, the Routing Tree pane displays the mesh route to the router.
Link Traffic (routers)	Displays the type of link traffic over time in bits per second.
Router Files (routers)	Lists files uploaded to the .../managed/files/ directory.
Raw Sockets (routers)	Lists metrics and session data for the TCP Raw Sockets (see table in the Raw Sockets Metrics and Sessions).
Embedded AP (IR829 only)	Lists inventory (configuration) details and metrics for the attached access point.
AP Running Config (IR8829 only)	Lists the running configuration file for the attached access point.

Actions You Can Perform from the Detailed Device Information Page



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

Action	Description
Show on Map (endpoints)	Displays a popup window with a map location of the device. This is the equivalent of entering **eid:***Device_EID* in the search field in Map View.
Ping	Sends a ping to the device to determine its network connectivity. See Pinging Devices, on page 239.
Traceroute	Traces the route to the device. See Tracing Routes to Devices, on page 240.
Refresh Metrics (Head-end routers and routers only)	Instructs the device to send metrics to IoT FND. **Note** IoT FND assigns historical values for metrics for each device. To access historical metric values, use the GetMetricHistory North Bound API call.
Reboot	Enables a reboot of the modem on LoRaWAN.
Sync Config Membership (Mesh endpoints only)	Synchronizes the configuration membership for this device. See Synchronizing Endpoint Membership, on page 270.
Sync Firmware Membership (Mesh endpoints only)	Click **Firmware Membership**to synchronize the firmware membership for this device, and then click **Yes** to complete the process.
Block Mesh Device (Mesh endpoints only)	Blocks the mesh endpoint device. **Caution** This is a disruptive operation. **Note** You cannot use Block Mesh Device with the Itron OpenWay RIVA CAM module or the Itron OpenWay RIVA Electric devices and Itron OpenWay RIVA G-W (Gas-Water) devices.
Erase Node Certificates	Removes Node certificates.
Create Work Order (Routers and DA Gateway only)	Creates a work order. See Demo and Bandwidth Operation Modes, on page 339.

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:

Procedure

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 248.

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:

Procedure

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:

Procedure

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 162.

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

For more information about operators, see Filter Operators, on page 249. 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 31: 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 32: Filter Examples

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

Performing Bulk Import Actions

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

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

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

To add devices in bulk:

Procedure

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

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

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

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

For more information about adding gateways, see Adding an IC3000 Gateway, on page 251

For more information about adding HERs, see Adding HERs to IoT FND, on page 251

For more information about adding routers, see Adding Routers to IoT FND, on page 252

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

Step 3 Click **Add**.

Step 4 Click **Close**.

Adding an IC3000 Gateway

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

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

Adding HERs to IoT FND

Configuring HERs Before Adding them to IoT FND

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

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

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

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

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

Adding HERs

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

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

Note For device configuration field descriptions, see Device Properties, on page 343

Table 33: HER Import Fields

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

When you add an HER, IoT FND displays its status as Unheard. IoT FND changes the status to Up after it polls the HER. IoT FND polls HERs in the background every 15 minutes to collect device metrics, so it should take no more than 15 minutes for the status of HERs to change to Up after you add them to IoT FND. However, you can trigger the polling of HERs by clicking 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 343.

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

Table 34: Router Import Fields

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

Mapping Routers to HERs

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

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

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

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

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

For example:

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

Adding Router-to-HER Mappings to a CSV File

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

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

Removing Devices in Bulk

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

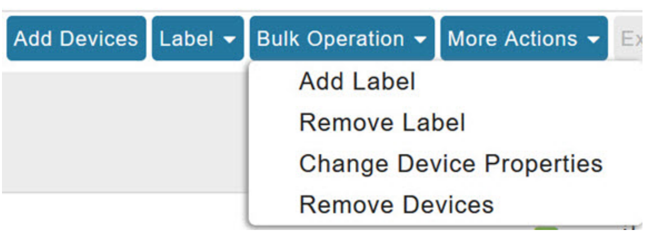
Caution When you remove routers, IoT FND returns all the leased IP addresses associated with these devices to CNR and removes the corresponding tunnels from the HERs.

To remove devices in bulk:

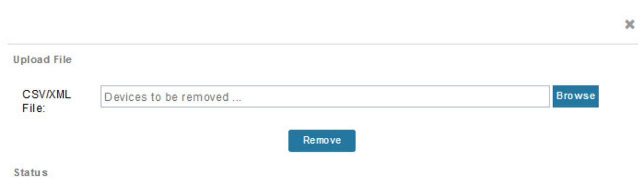
Procedure

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

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



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



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

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

Step 4 Click **Remove**.

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

Step 5 Click **Close** when done.

Changing Device Properties in Bulk

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

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

To configure device properties in bulk:

Procedure

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

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

Step 3 Click **Change**.

Step 4 Click **Close** when done.

Adding Labels in Bulk

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

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

To add device labels:

Procedure

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

Step 2 Click **Browse** to locate the CSV file that contains the list of devices to label, and then click *Open*.

This is an example of the expected CSV format:

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

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

Step 4 Click **Add Label**.

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

Step 5 Click **Close** when done.

Removing Labels in Bulk

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

To delete device labels:

Procedure

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

Step 2 Click **Browse** to locate the CSV containing the list of devices to remove the label from, and then click **Open**.

Step 3 From the drop-down menu, choose the label to remove.

Step 4 Click **Remove Label**.

Step 5 Click **Close**.

What to do next

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

Configuring Rules

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

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

When working with rules, you can do the following:

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

Viewing and Editing Rules

To view rules:

Procedure

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

IoT FND displays the list of rules stored in its database. 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.
Rule definition	The syntax of the rule. Some examples are listed below. • IoT FND executes this rule when a device battery 0 level drops below 50%: `battery0Level<50` • `deviceType:cgmesh eventName:up` • `deviceType:ir500 eventName:outage`
Rule Actions	The actions performed by the rule. For example: `Log Event With: CA-Registered, Add Label: CA-Registered` In this example, the actions: • Set the eventMessage property of the Rule Event generated by this rule to CA-Registered. • Add the label CA-Registered to the matching device.
Updated By	The username of user who last updated the rule.
Updated At	The date and time when the rule was last updated.

Step 2 To edit a rule, click its name.

For information on how to edit rules, see Creating a Rule, on page 257

Creating a Rule

To add a rule:

Procedure

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

Step 2 Click **Add**.

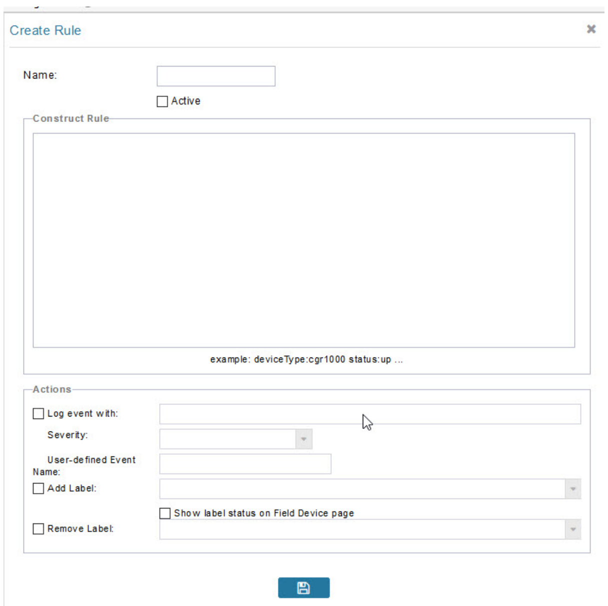
Step 3 Enter a name for the rule.

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

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

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

Use the same syntax used for creating filters. See Search Syntax, on page 249.



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

• **Log event with** — Specify the message to add to the log entry of the event in the server log, the severity, and event name.
  • **Severity** — Select the severity level to assign to the event.
  • **User-defined Event** — Assign a name to the event Searching By Event Name, on page 471.
 	
For example, if you enter Red Alert in this field, set the Severity to CRITICAL and enter CHECK ROUTER in the Event Name field, the eventMessage field in the logged entry for the event that matches the rule is set to Red Alert, as shown in this sample entry from the server log (server.log):
 	
`16494287: NMS-200-5: May 02 2017 22:32:41.964 +0000: %CGMS-7`
`-UNSPECIFIED: %`
`[ch=EventProducer][sev=DEBUG][tid=com.espertech.esper.Outbound-`
`CgmsEventProvider-1]: Event Object`
` which is send = EventObject`
`[netElementId=50071, eventTime=1335997961962, eventSeverity=0,`
` eventSource=cgr1000, eventType=UserEventType,`
` **eventMessage=Red Alert**`
`, **eventName=CHECK ROUTER**`
`, lat=36.319324, lng=-129.920815,`
`geoHash=9n7weedx3sdydv1b6ycjw, eventTypeId=1045,`
` eid=CGR1240/K9+JAF1603BBFF]`

In IoT FND, the message you define in the **Log event with** field appears in the Message field of the matching event entries listed on the Events page (**Operations** > **Events**), and the new Event Name is a new search filter.
Add Label — Enter the name of a new label or choose one from the **Add Label** drop-down menu.
Show label status on Field Devices page — Shows the status of the device that triggered this rule in the LABELS section of the Browse Devices pane.
Remove Label — Choose the label to remove from the **Remove Label** drop-down menu.

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

Activating Rules

IoT FND only applies rules that you activate.

To activate a rule:

Procedure

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

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

Step 3 Click **Activate**.

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

Step 5 Click **OK**.

Deactivating Rules

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

To deactivate rules:

Procedure

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

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

Step 3 Click **Yes** to deactivate the rule.

Step 4 Click **OK**.

Deleting Rules

To delete rules:

Procedure

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

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

Step 3 Click **Delete**.

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

Step 5 Click **OK**.

Configuring Devices

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

- Configuring Device Group Settings, on page 261
- Editing the ROUTER Configuration Template, on page 271
- Editing the ENDPOINT Configuration Template, on page 296
- Pushing Configurations to Routers, on page 304
- Pushing Configurations to Endpoints, on page 307

Configuring Device Group Settings

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

Creating Device Groups

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

Group Name	Description
Default-act	By default, all Itron OpenWay RIVA Electric devices (ENDPOINT) are members of this group. • Individual RIVA electric devices listed under the Group heading display as OW Riva CENTRON.
Default-bact	By default, all Itron OpenWay RIVA G-W (Gas-Water) devices (ENDPOINT) are members of this group. • Individual RIVA water meters listed under the Group heading display as OW Riva G-W. • Individual RIVA gas meters listed under the Group heading display as OW Riva G-W.
Default-cam	By default, all Itron OpenWay RIVA CAM modules (ENDPOINT) are members of this group. • Individual RIVA CAM modules listed under the CAM heading display as OW Riva CAM.
Default-lglfn	By default, all L+G LFN (limited function node) battery endpoints are members of this group.
Default-lgelectric	By default, all L+G electric endpoints are members of this group.
Default-lgnn	By default, all L+G grid management endpoints are members of this group.
Default-lgrouter	By default, all L+G routers are members of this group.
Default-ir800	By default, all IR807s, IR809s, and IR829s (ROUTER) are members of this group.
Default-cgmesh	By default, all crmesh endpoints (ENDPOINT) are members of this group.
Default-cgr1000	By default, all CGRs (ROUTER) are members of this group.
Default-ir500	By default, all IR500s (ENDPOINT) are members of this group.
Default-lorawan	By default all LoRaWAN Gateways (IOT GATEWAY) are members of this group.
Default-ir1100	By default, all IR1100 (ROUTER) are members of this group.

Group Name	Description
Default-ir8100	By default, all IR8100 (ROUTER) are members of this group.
Default-ir1800	By default, all IR1800 (ROUTER) are members of this group.

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

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

- Creating ROUTER Groups, on page 262
- Creating Endpoint Groups, on page 263

Creating ROUTER Groups

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

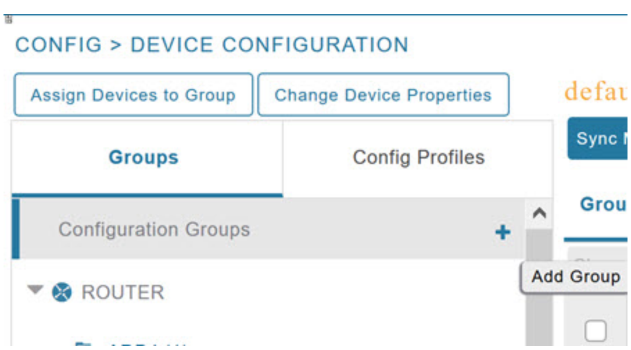
To create a router configuration group:

Procedure

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

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

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



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

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

Step 5 Click **Add**.

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

What to do next

- To change the name of a group, see Renaming a Device Configuration Group, on page 267
- To remove a group, see Deleting Device Groups, on page 268

Creating Endpoint Groups

To create an endpoint configuration group:

Procedure

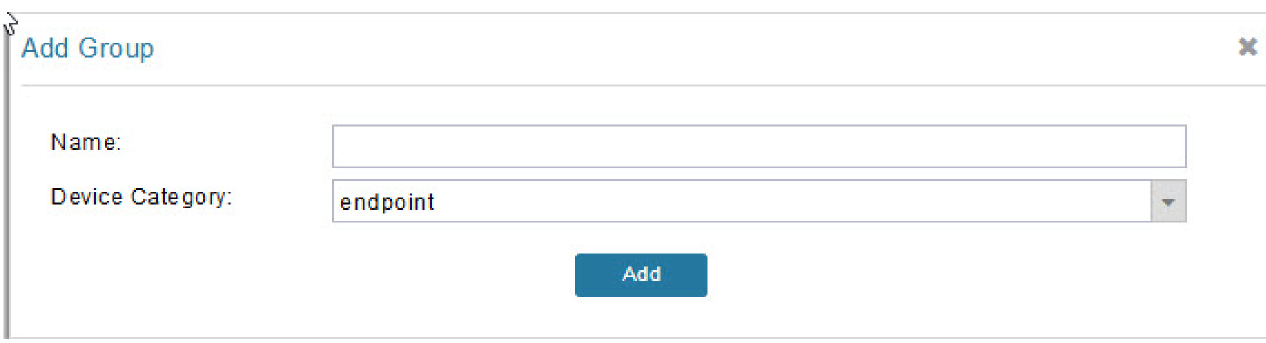
Step 1 Choose **CONFIG** > **Device Configuration**.

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

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

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

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



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

Step 5 Click **Add**.

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

What to do next

- To change the name of a group, see Renaming a Device Configuration Group, on page 267
- To remove a group, see Deleting Device Groups, on page 268

Changing Device Configuration Properties

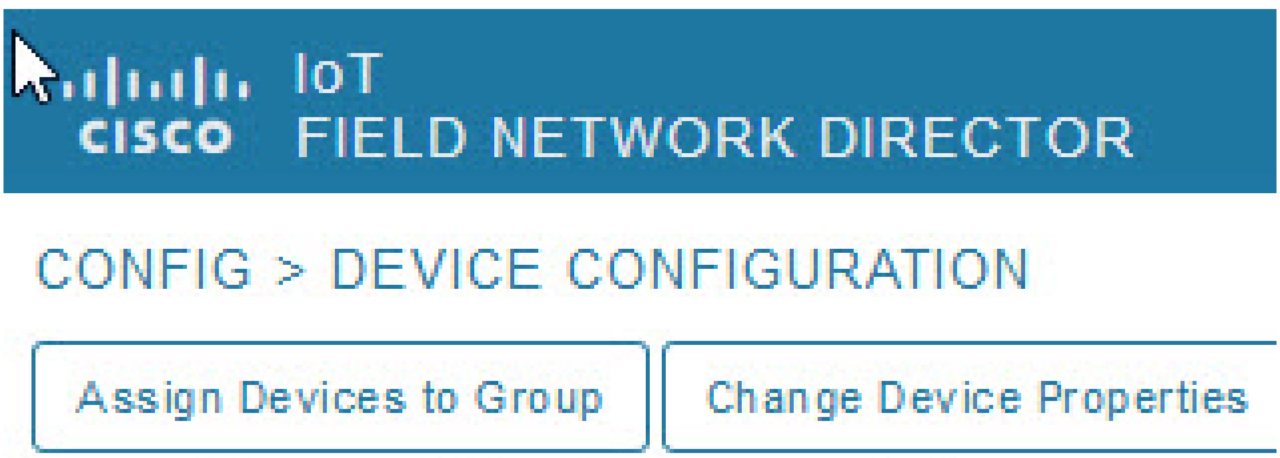
You can change the configurable properties of devices by uploading a Device Properties CSV file with modified values for the devices.

To change device configuration properties:

Procedure

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

Step 2 Click **Change Device Properties**.



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

Step 4 Click **Change**.

Step 5 Click **Close** when done.

For a list of configurable device properties in IoT FND, see Device Properties, on page 343.

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

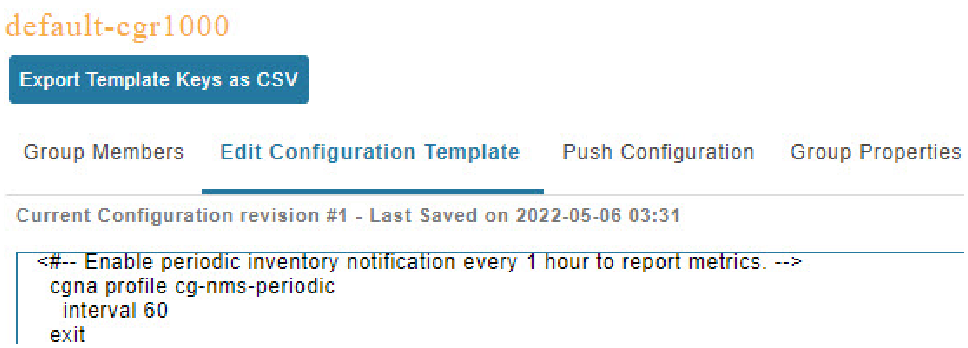
To configure the periodic inventory timer for a ROUTER configuration group:

Procedure

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

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

Step 3 Click **Edit Configuration Template** to configure the periodic inventory notification interval in the template. The default periodic inventory notification interval is 60 minutes for routers and 8 hours for endpoints.



Note

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

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

Step 4 Click the disk icon to save the changes.

Configuring Heartbeat Notification

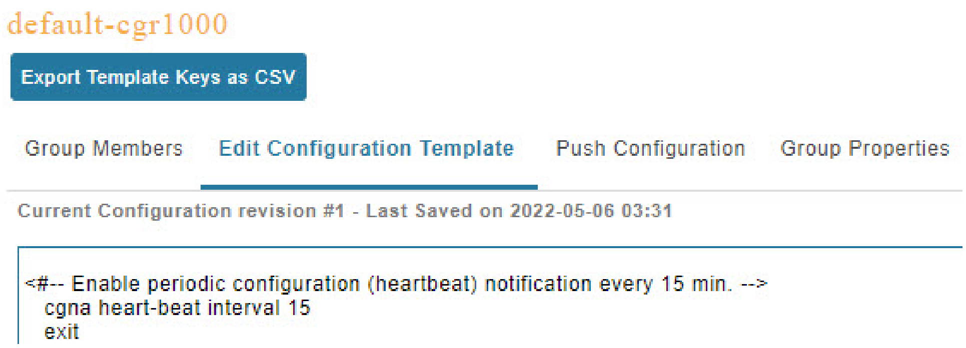
To configure the heartbeat notification for a ROUTER configuration group:

Procedure

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

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

Step 3 Click **Edit Configuration Template** to configure the heartbeat notification interval in the template. The default heartbeat notification interval is 15 minutes.



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

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

Note
Ensure that the heartbeat interval is less than the mark-down timer value set by you. For more information on the device mark-down timer, refer to Configuring Mark-Down Timer, on page 266.

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.

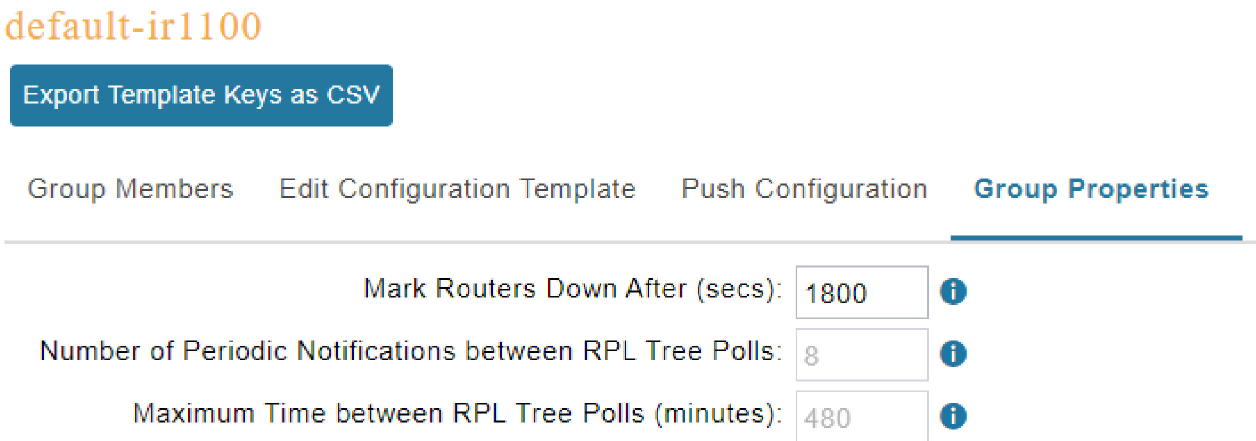
To configure the mark-down timer for a ROUTER configuration group:

Procedure

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

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

Step 3 Click **Group Properties**.



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

Note
Ensure that the periodic configuration notification frequency in the configuration template is less than the value you entered in the **Mark Routers Down After** field. We recommend 1:3 ratio of heartbeat interval to mark-down timer. For more information on configuring the heartbeat interval, refer to Configuring Heartbeat Notification , on page 265.

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

Renaming a Device Configuration Group

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

To rename a device configuration group:

Procedure

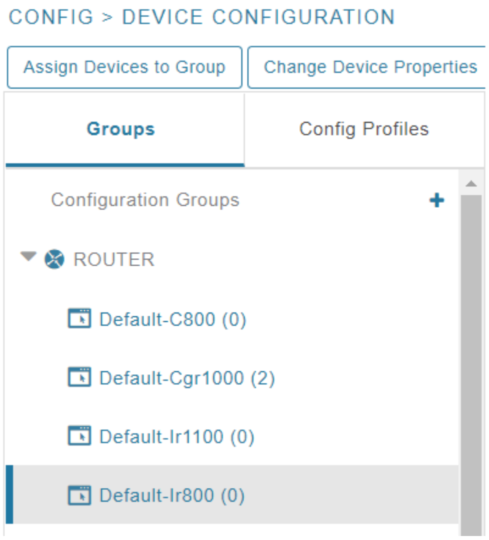
Step 1 Choose **CONFIG** > **Device Configuration**.

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

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

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

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



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

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

Deleting Device Groups

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

To delete a configuration group:

Procedure

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

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

Step 3 Ensure that the group is empty.

Step 4 Click **Delete Group** (-).

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

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

Moving Devices to Another Group

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

Moving Devices to Another Configuration Group Manually

To move devices to another configuration group:

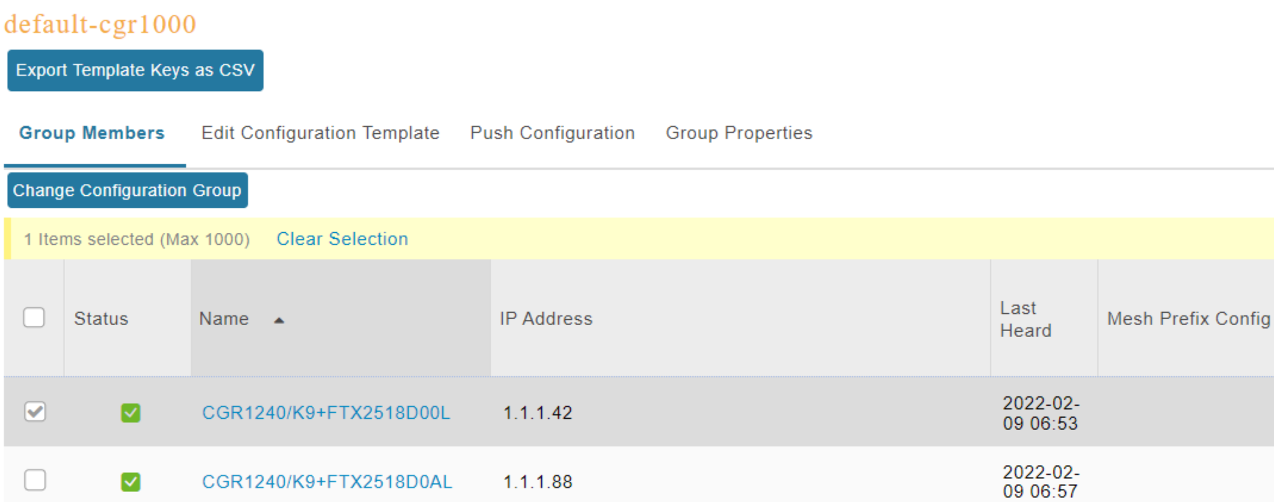
Procedure

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

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

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

Step 4 Click **Change Configuration Group**.



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

Step 6 Click **Change Config Group**.

Step 7 Click **OK**.

Moving Devices to Another Configuration Group in Bulk

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

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

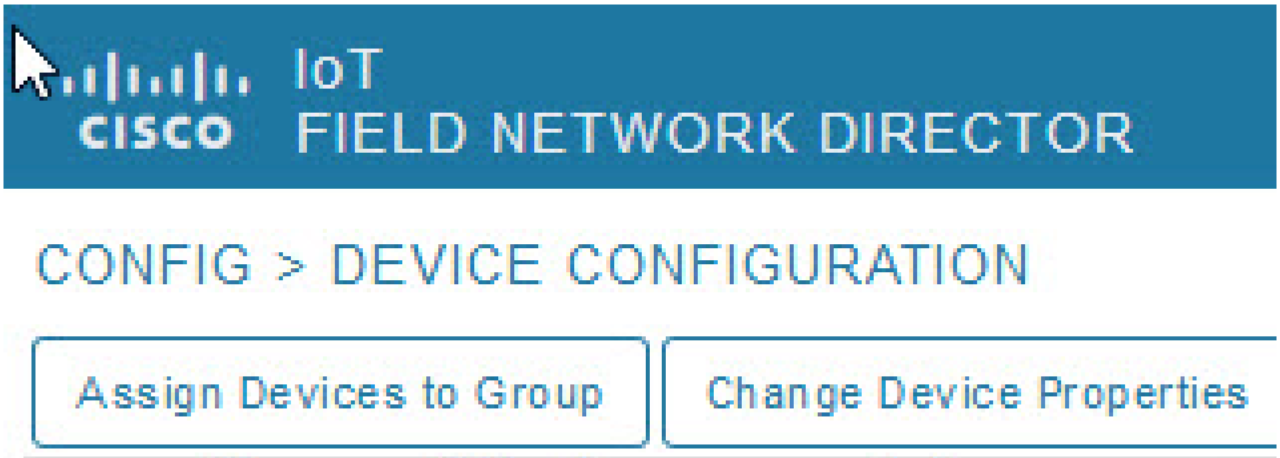
```
eid
CGR1120/k9+JS1
CGR1120/k9+JS2
CGR1120/k9+JS3
```

To move devices to another configuration group in bulk:

Procedure

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

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



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

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

Step 5 Click **Assign to Group**.

Step 6 Click **OK**.

Listing Devices in a Configuration Group

To list the devices in a configuration group:

Procedure

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

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

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

Synchronizing Endpoint Membership

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

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

To send group information to endpoints:

Procedure

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

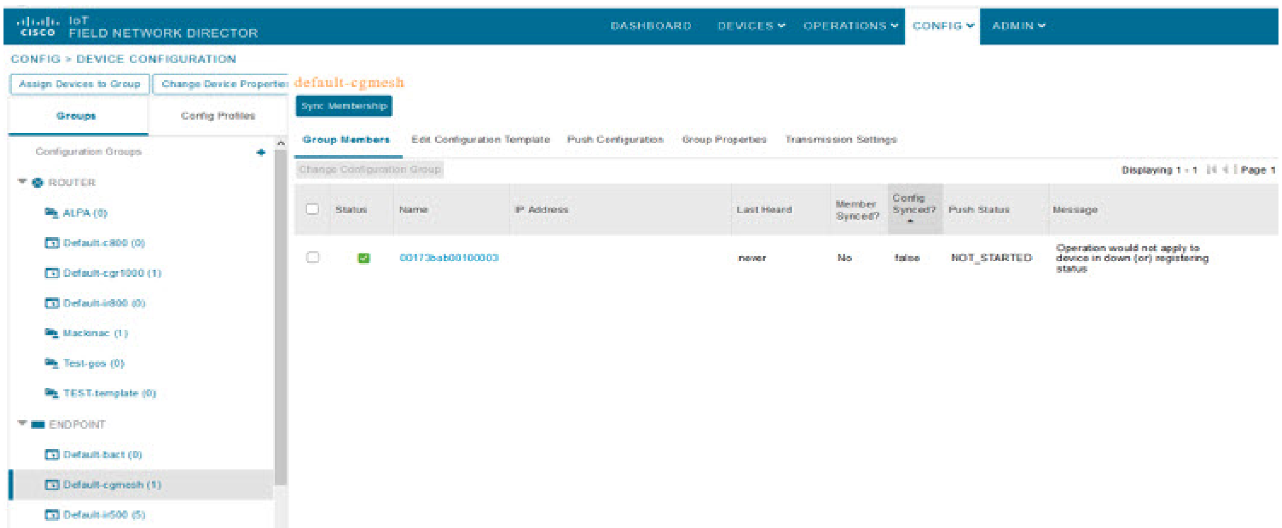
Step 2 Select an ENDPOINT group (left pane) such as Default-cgmesh.

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

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

Step 5 When prompted, click Yes to confirm synchronization.

Step 6 Click **OK**.



Editing the ROUTER Configuration Template

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

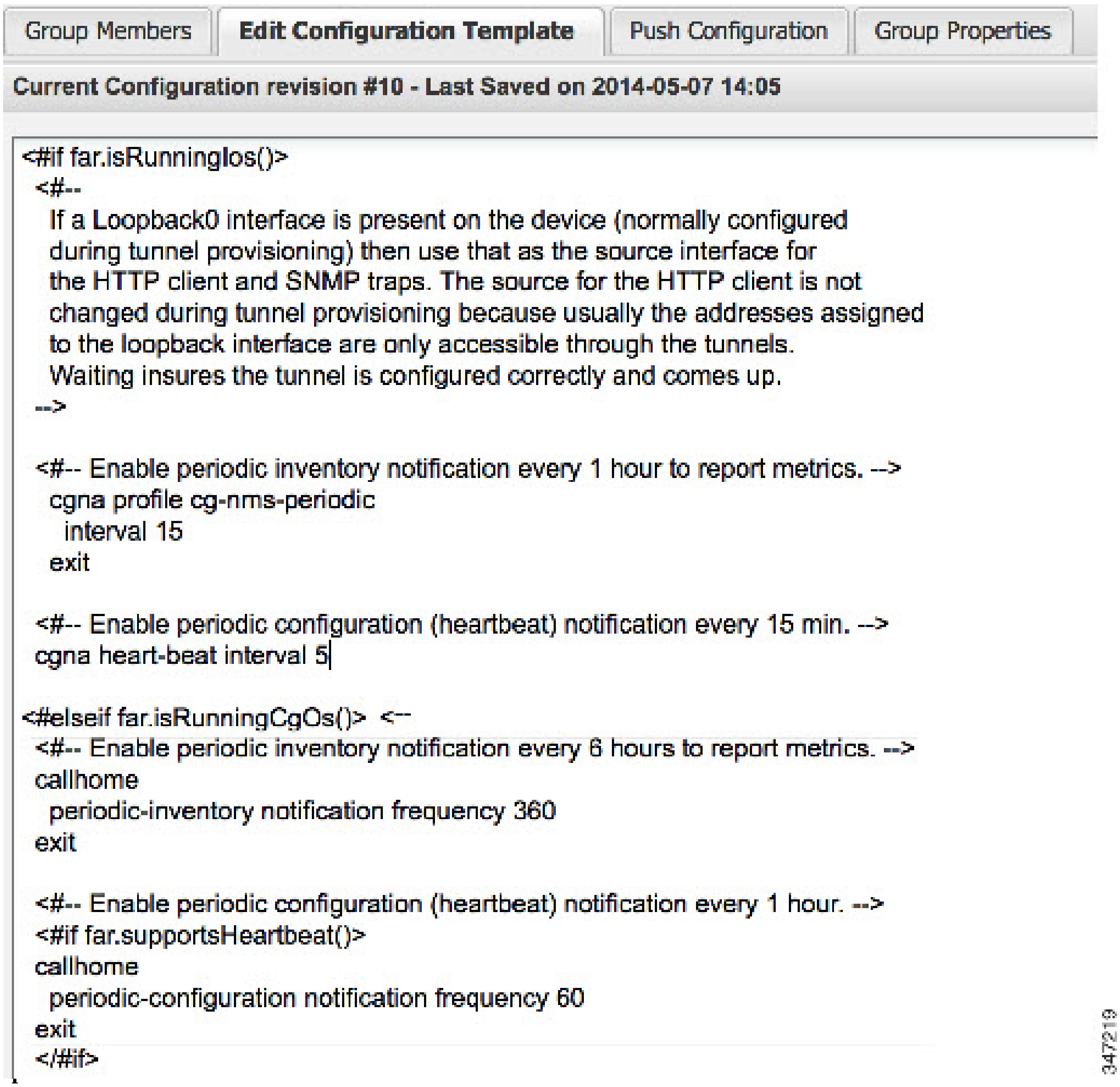
To edit a ROUTER group configuration template:

Procedure

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

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

Step 3 Click **Edit Configuration**



Step 4 Edit the template.

The template is expressed in FreeMarker syntax

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

Step 5 Click **Save Changes**.

What to do next

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

Editing the AP Configuration Template

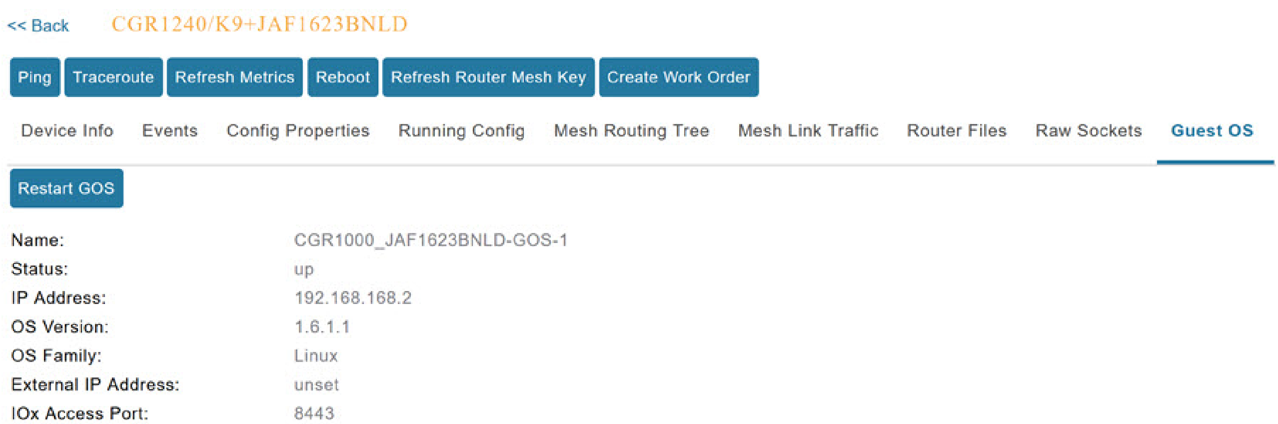
To edit an AP group configuration template:

Procedure

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

Step 2 Under CONFIGURATION GROUPS (left pane), select the 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 257)

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 35: 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.

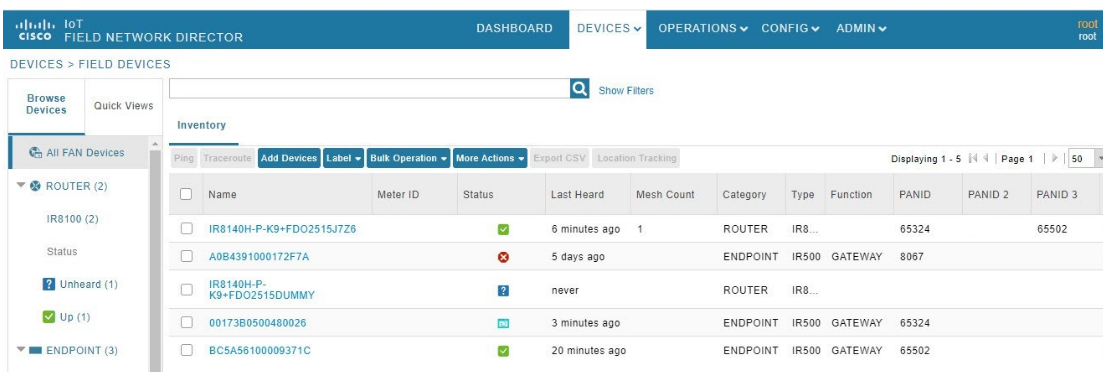
Support of Dual WPAN in Field Device Page

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 232. This displays the respective parameters related to WPAN inserted in either slot 2 or slot 3.

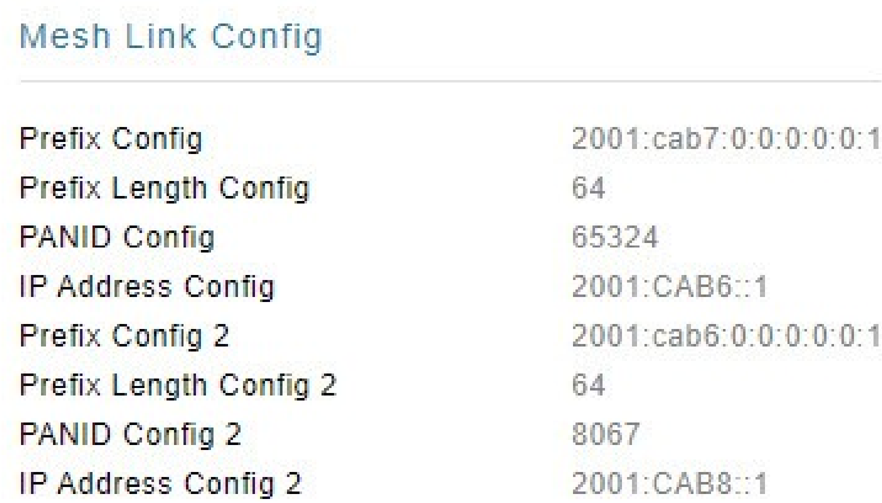
- In the FAN device view, you can view PANID 2 and PANID 3 columns in the Inventory tab that indicates the meshPanID parameter of WPAN that is inserted in either slot 2 or slot 3.

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 255.
  - 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.



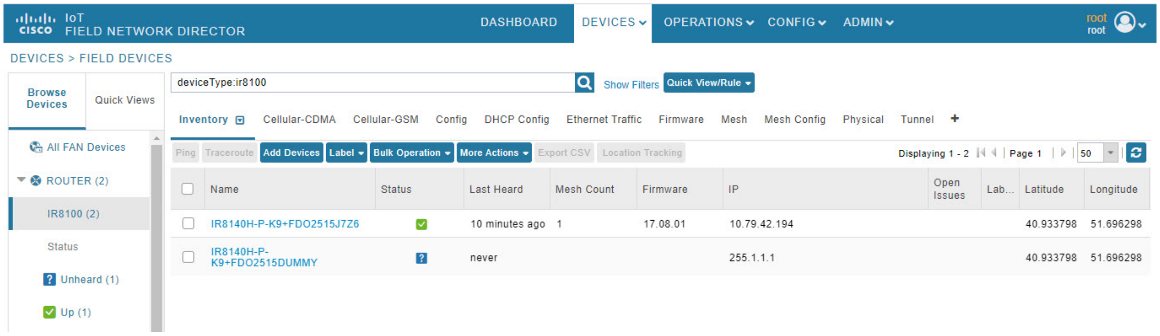
Support of Dual WPAN in Router Device View

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 232.

Support of Dual WPAN in IR8100 Device View

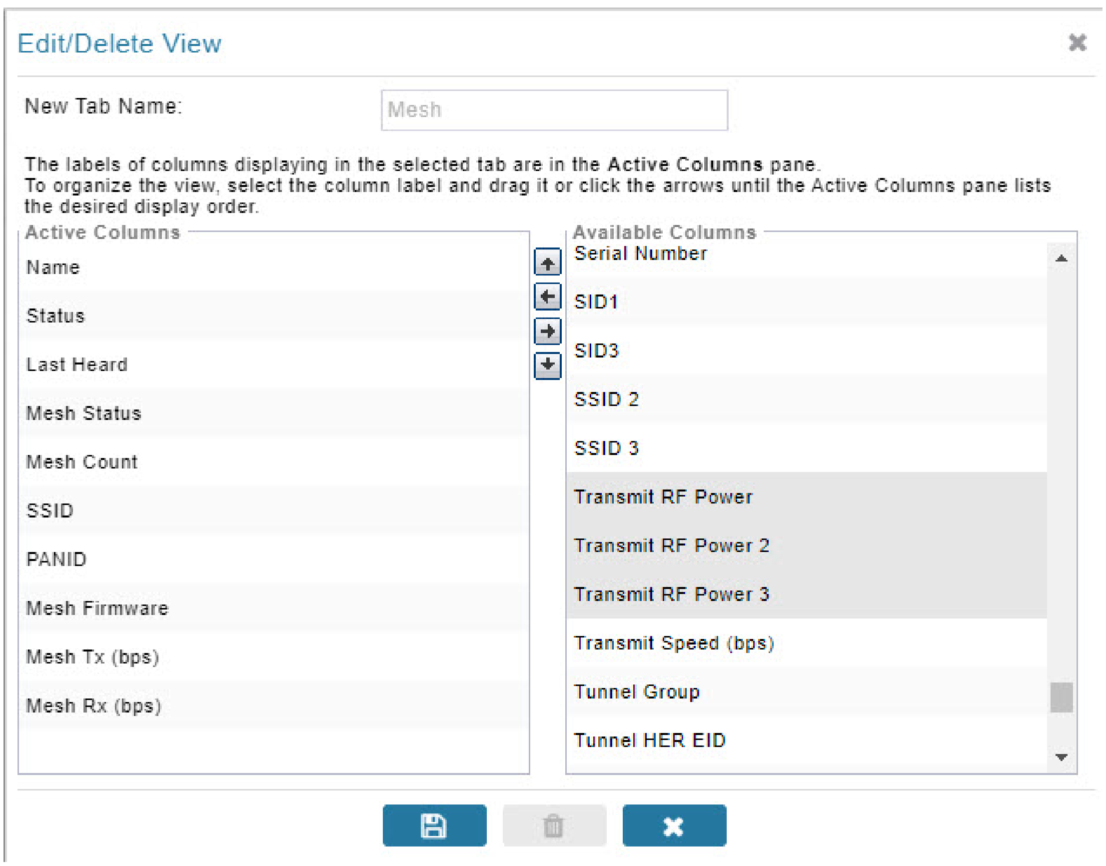
In the **DEVICES** > **FIELD DEVICES** page, select IR8100 under Router category in the Browse Devices tab.

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 232.



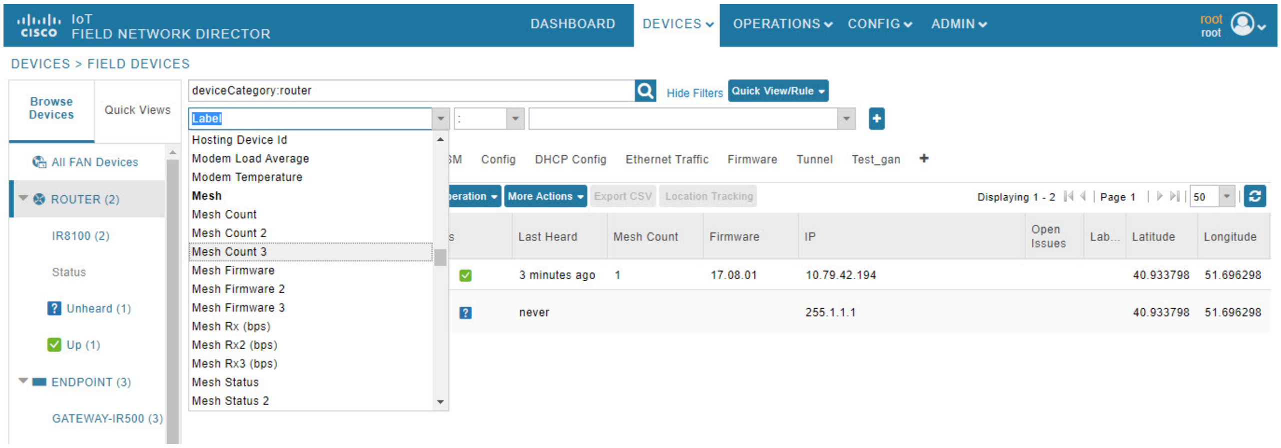
Using Filters to View Additional Dual WPAN Fields

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.

Procedure

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 167.



Support of Dual WPAN on Device Details Page

To view dual WPAN related information associated with IR8100,

Procedure

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

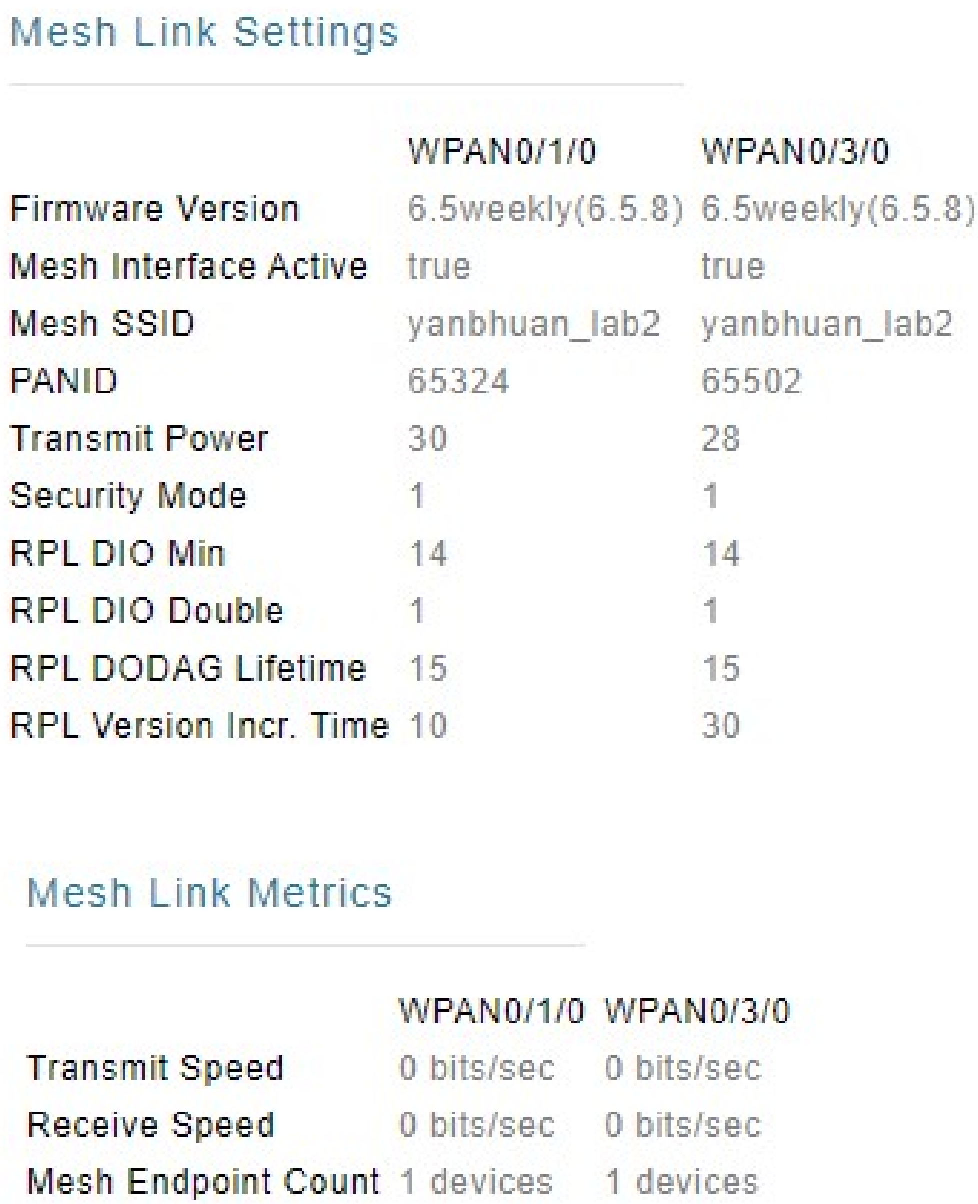
Step 2 Select IR8100 router group on the left pane.

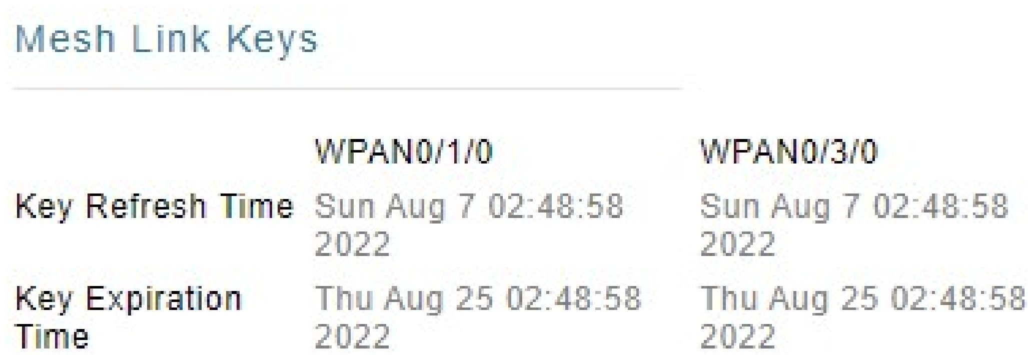
Step 3 Click the IR8100 device on the right pane.

The device details page displays information for the selected device.

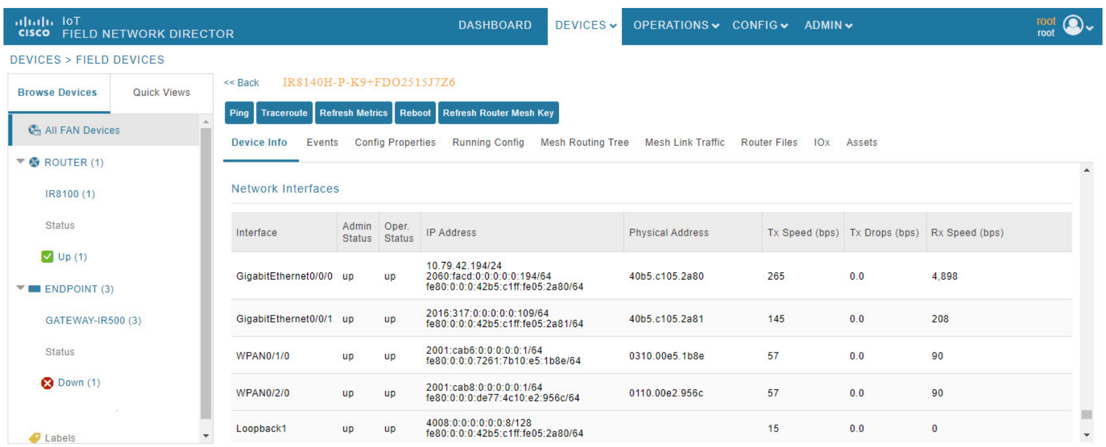
Viewing Device Info Tab

- 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 353. For more information on Mesh Link Metrics, see Link Metrics, on page 352. For more information on Mesh Link Keys, see Mesh Link Keys, on page 355.


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



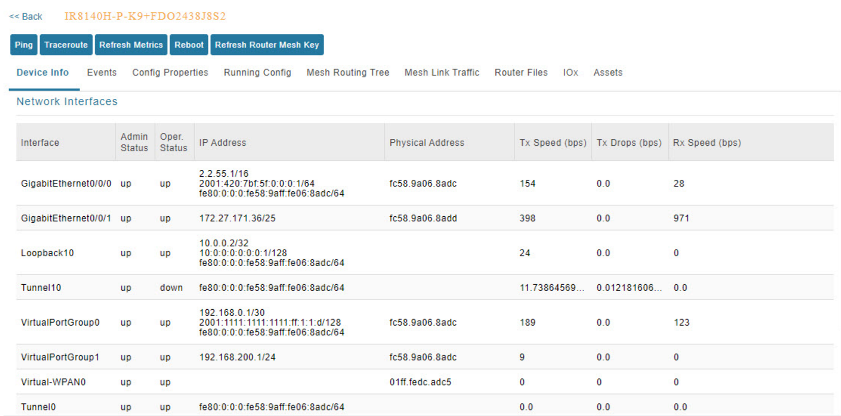
- The Network Interface table in the Device Info page provides the details of both the WPAN interfaces that are connected in any of the three available slots.



The following table describes the Network Interface fields in the Device Info page.

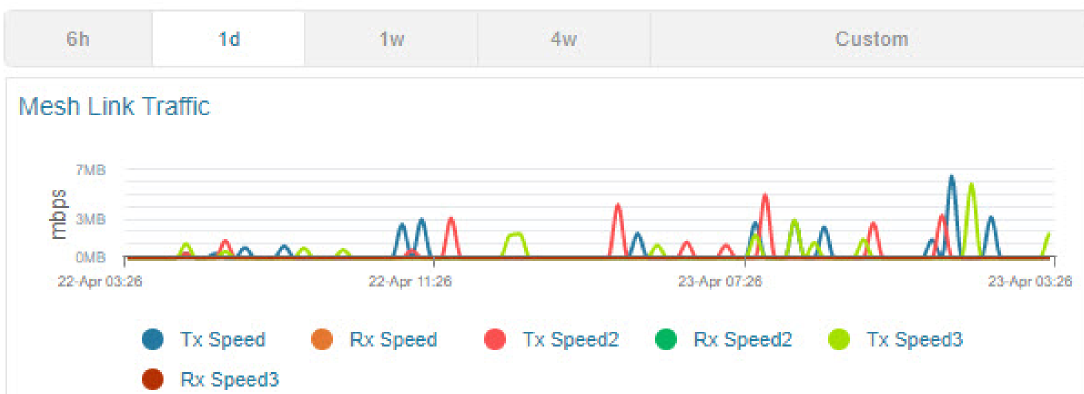
Field	Description
Interface	Indicates the name of the interface
Admin Status	Provides admin status (up/down)
Oper. Status	Provides operational status (up/down)
IP Address	Indicates the IP address of the device
Physical Address	Indicates the latitude and longitude of the device
Tx Speed (bps)	Indicates 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

> **Note** The IR8100 device is connected to CAM module through new virtual port group interface which is processed to retrieve information of the RPL tree. Based on the settings in the RPL tree, the mesh routing tree is displayed.



Interface	Admin Status	Oper. Status	IP Address	Physical Address	Tx Speed (bps)	Tx Drops (bps)	Rx Speed (bps)
GigabitEthernet0/0/0	up	up	2.2.55.1/16 2001:420:7bf:5f:0:0:0:1/64 fe80:0:0:0:fe58:9aff:fe06:8adc/64	fc58.9a06.8adc	154	0.0	28
GigabitEthernet0/0/1	up	up	172.27.171.36/25	fc58.9a06.8add	398	0.0	971
Loopback10	up	up	10.0.0.2/32 10:0:0:0:0:0:0:1/128 fe80:0:0:0:fe58:9aff:fe06:8adc/64		24	0.0	0
Tunnel10	up	down	fe80:0:0:0:fe58:9aff:fe06:8adc/64		11.73864569...	0.012181606...	0.0
VirtualPortGroup0	up	up	192.168.0.1/30 2001:1111:1111:1111:ff:1:1:d/128 fe80:0:0:0:fe58:9aff:fe06:8adc/64	fc58.9a06.8adc	189	0.0	123
VirtualPortGroup1	up	up	192.168.200.1/24	fc58.9a06.8adc	9	0.0	0
Virtual-WPAN0	up	up		01ff.fedc.adc5	0	0	0
Tunnel0	up	up	fe80:0:0:0:fe58:9aff:fe06:8adc/64		0.0	0.0	0.0

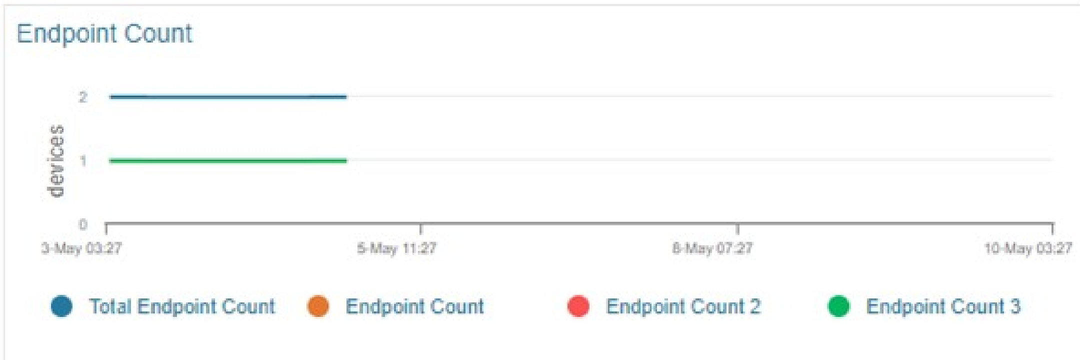
- The Device Info tab displays Mesh Link Traffic chart according to the time period selected on the top-right side of the page. The information given in the chart is colour coded to distinguish the slot in which the WPAN is inserted. For example, the colour used for Tx or Rx speed of WPAN in slot 1 is different from that of WPAN in slot 2.



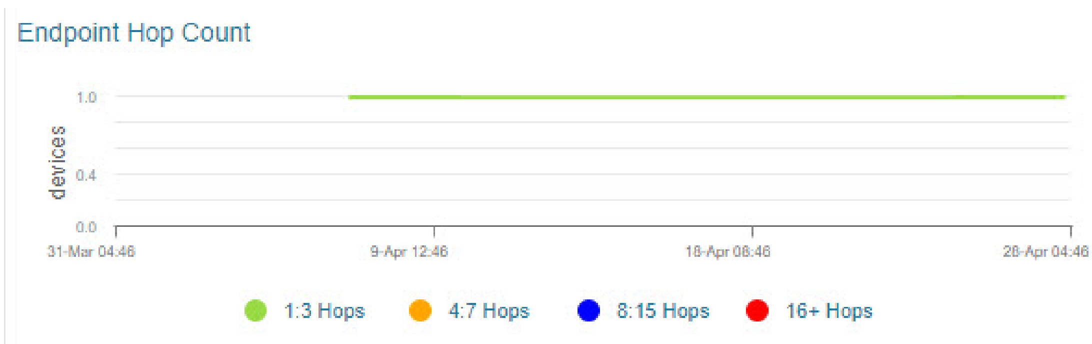
> **Note** Click on colour code and the respective line in the chart is removed from the graph. This applies for all the charts.

- 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.

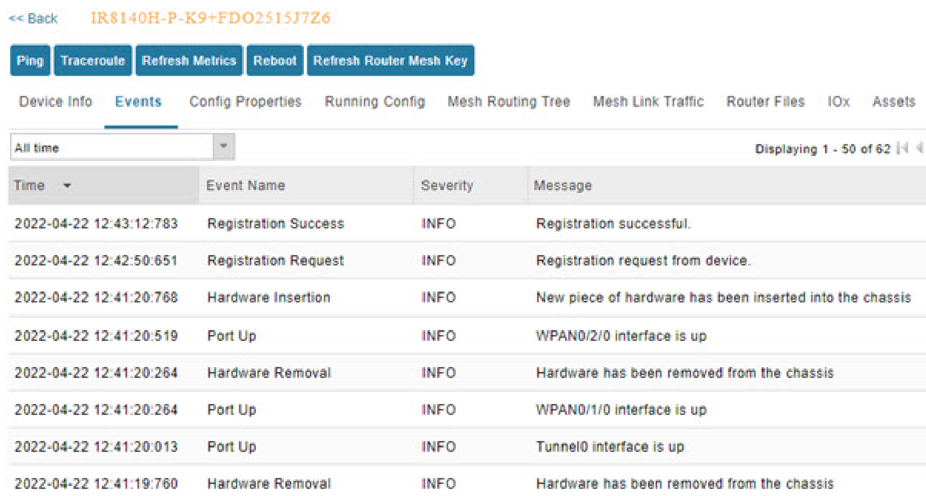


- The endpoint hop count chart shows an aggregated endpoint count between the hops connected to both the WPAN interfaces.



Viewing Dual WPAN Events

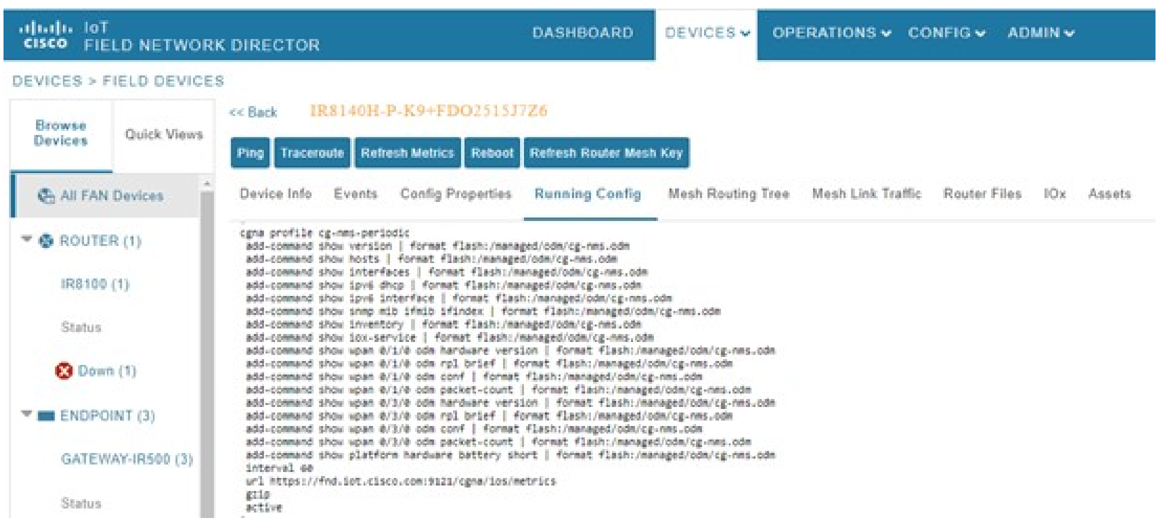
In the device details page, navigate to Events tab. This tab displays the events and alerts for both WPANs.



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.

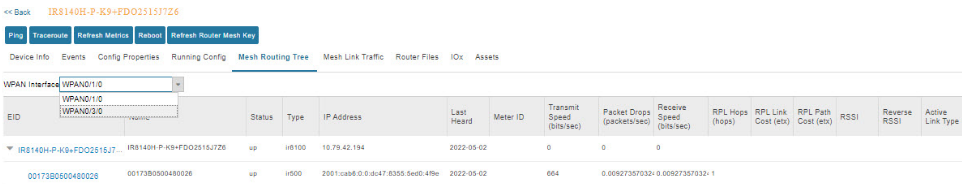
Note By default, the drop-down list displays the WPAN interface inserted in lower slot number. Therefore, the information pertaining to the respective WPAN is displayed. So, you must select the available WPAN from the drop-down list for which you want to view the information.

Procedure

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.



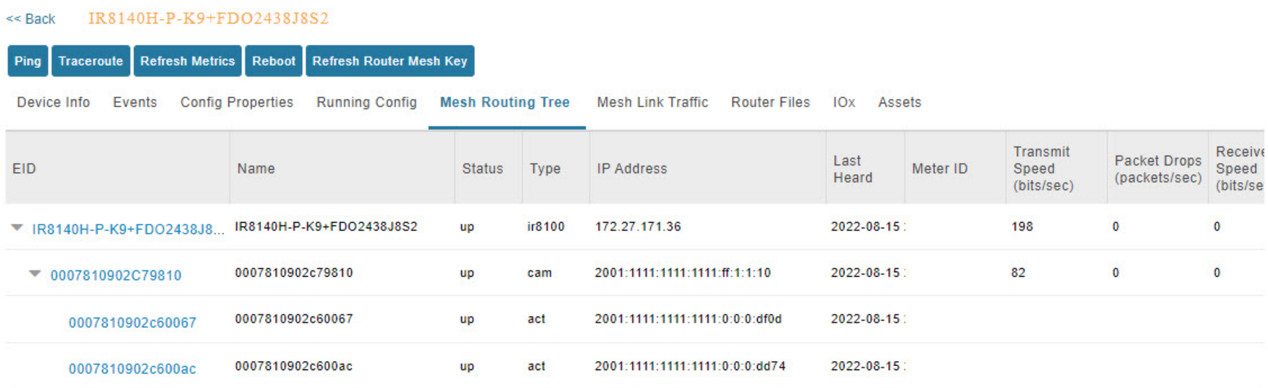
The following table describes the fields under Mesh Routing Tree tab in the Device Info page.

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.
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 143.

Note

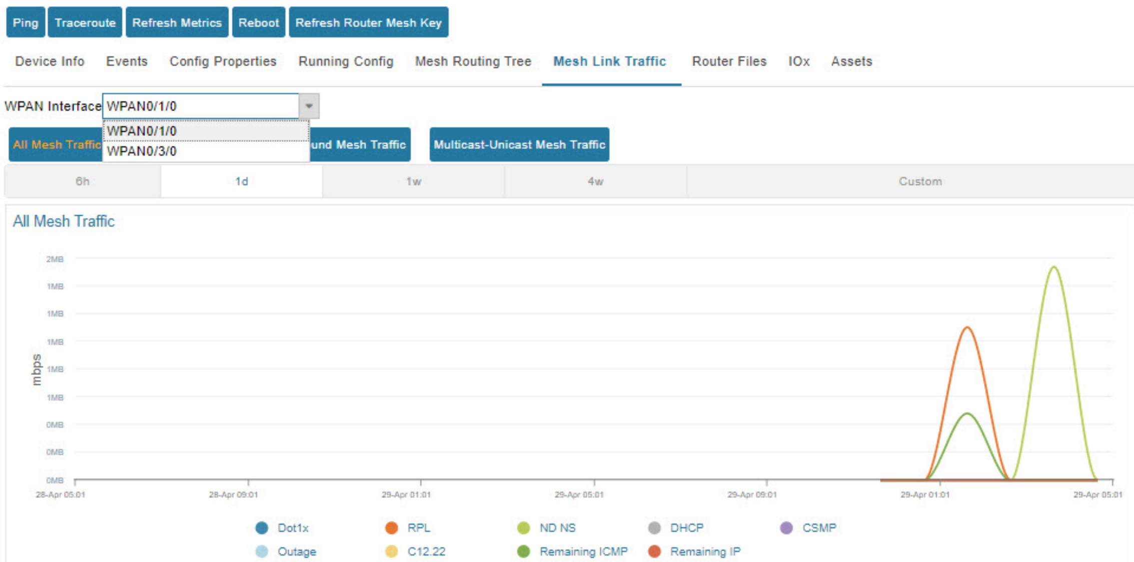
For the IR8100 device with CAM module, the RPL tree information is captured from the respective CAM module and displayed in the Mesh Routing Tree tab. The IR8100 device as the root element and the act devices connected to the CAM module are shown.



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 461.

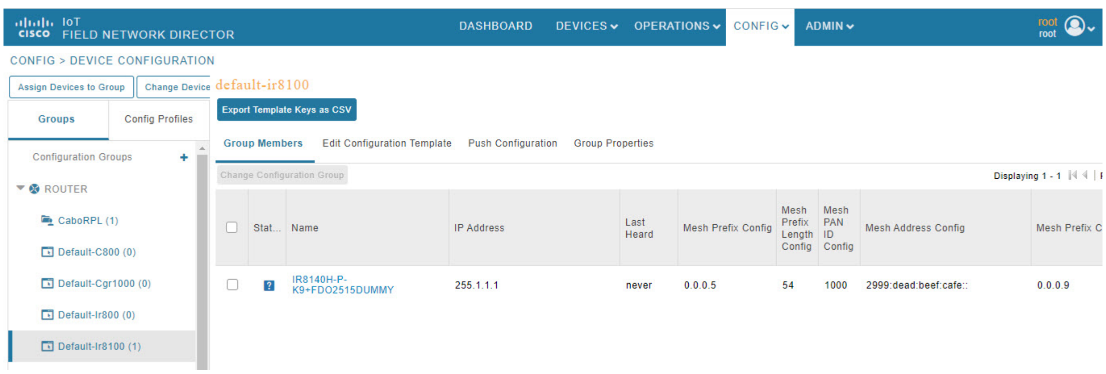
Note By default, the drop-down list displays the WPAN interface inserted in lower slot number. Therefore, the information pertaining to the respective WPAN is displayed. So, you must select the available WPAN from the drop-down list for which you want to view the information.



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.



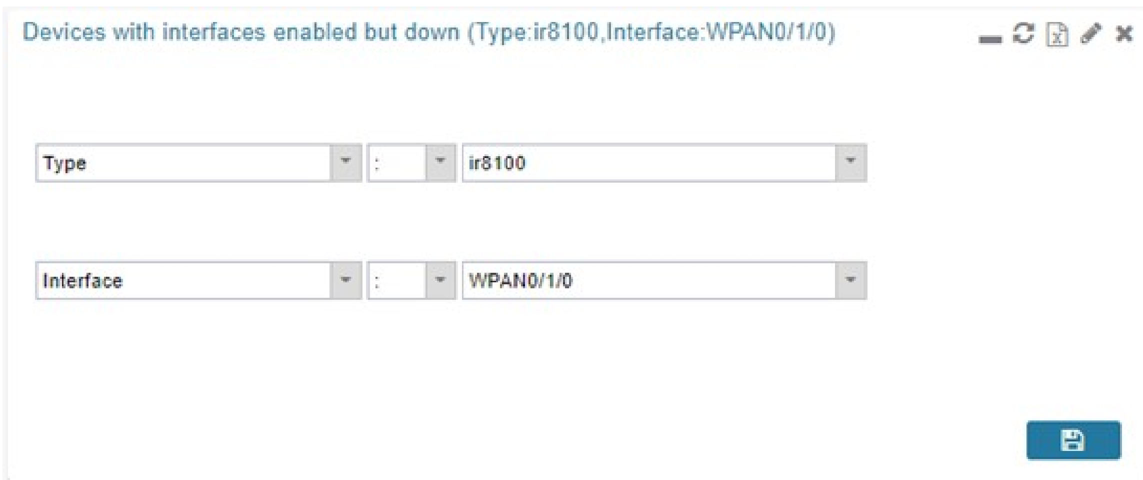
- Edit Configuration Template tab—The page allows you to define user configurable parameters in the template. FND maps the defined parameters to the WPAN parameter value configured through CSV. To configure the user configurable parameters:
    - Navigate to Edit Configuration Template tab.
    - Enter 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.

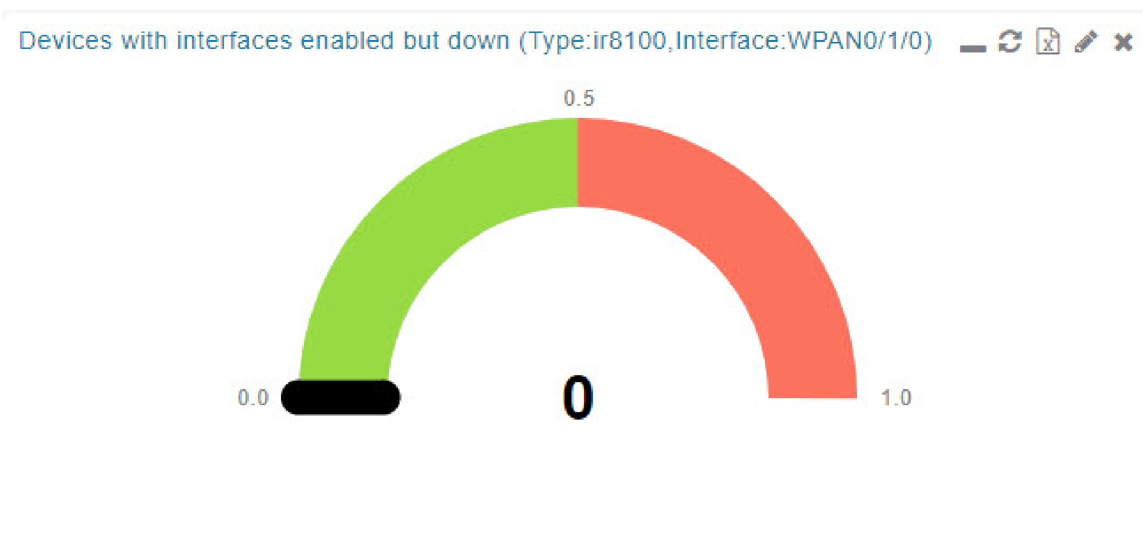
Note You can change device properties by clicking the **Change Device Properties** button above the devices pane.

- 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 453.



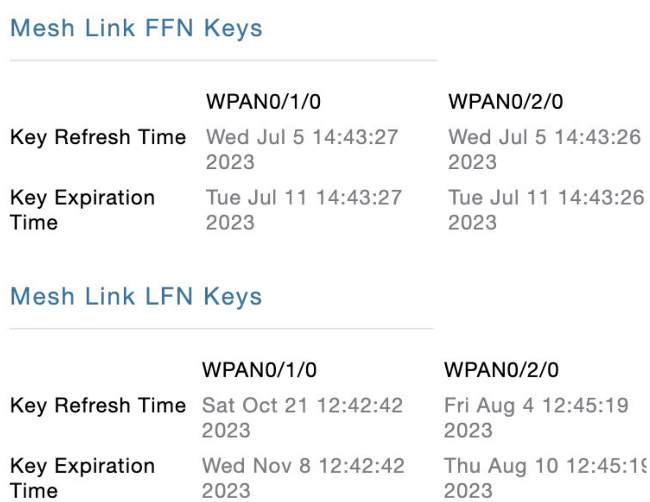


Refreshing Router Mesh Key for Dual WPAN

Refreshing the router mesh key helps to avoid the downtime of devices when they expire. Using the refresh option, you can refresh the IR8100 mesh keys for the following nodes:

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

Figure 11: Refreshing Mesh Keys for Dual WPAN



Note IR8100 also supports single WPAN refresh for LFN and FFN keys.

Figure 12: Refreshing Mesh Keys for Single WPAN

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

To refresh the router mesh LFN or FFN keys:

Procedure

Step 1 Navigate to **DEVICES** > **FIELD DEVICES** > **Browse Devices tab**.

Step 2 Select IR8100 router from the left pane.

Step 3 Go to **More Actions** > **Refresh Router Mesh LFN Key** (or) **Refresh Router Mesh FFN Key**.

Alternatively, you can refresh IR8100 mesh keys from the Devices Details page using the Refresh Router Mesh LFN Key button or Refresh Router Mesh FFN Key button.

Step 4 IoT FND refreshes the mesh key for both the WPANs (with different expiration periods) that are inserted in one of the three available slots. A confirmation message appears.

Figure 13: Confirmation Message - LFN

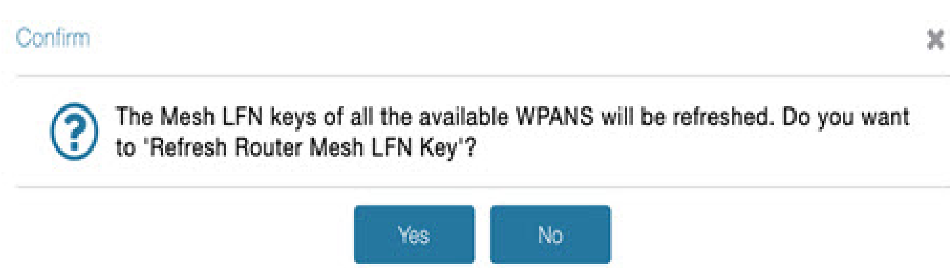
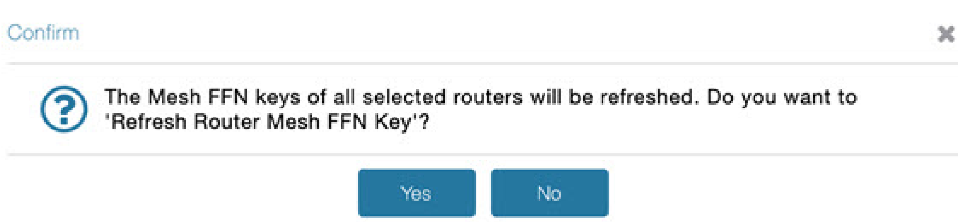


Figure 14: Confirmation Message - FFN



Step 5 Click **Yes** to continue. The following window displays the status of the router refresh.

Figure 15: Router Refresh Status for LFN

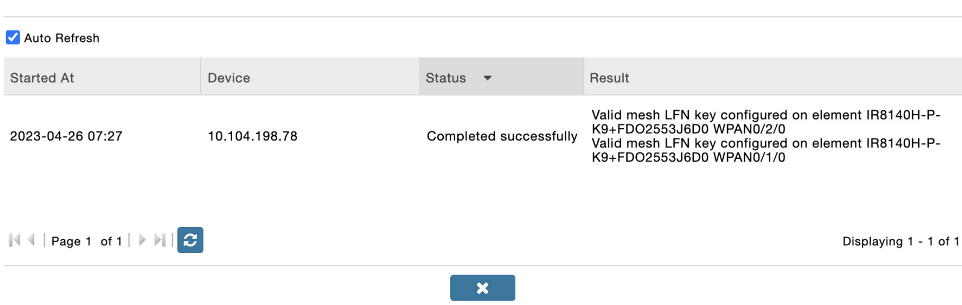
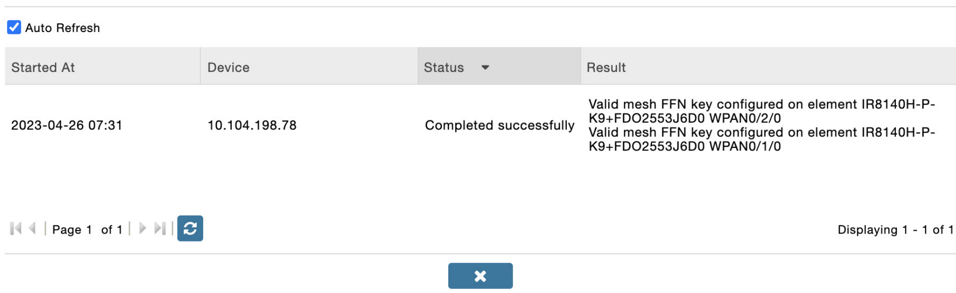


Figure 16: Router Refresh Status for FFN



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

Editing the ENDPOINT Configuration Template

To edit an ENDPOINT configuration template:

Procedure

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

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

Step 3 Click **Edit Configuration Template**.

Step 4 Edit the template.

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

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

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

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

Step 5 Click **Save Changes**.

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

.

Device-Level Configuration Push

Table 36: Feature History

Feature Name	Release Information	Description
Device-Level Configuration Push	Cisco IoT FND Release 5.0	You can push the configurations at the device level using **Push Configuration** tab in the **CONFIG** > **Device Configuration** page using two options: Config push without-rollback or Config push with-rollback. Use the **Running Config** tab to view and differentiate the registration and active running configurations.

The **Push Configuration** tab on the Device Details page enables you to apply configurations at the device level. This tab allows you to define configurations using the FreeMarker template and push them to a device. During reprovisioning, ZTD and re-ZTD the device and group level templates are pushed. The device-level configuration push provides two methods to update the new configuration on the device. The configuration will appear in the registration config.

Methods

- Configuration Push with Rollback: This method allows you to push the configuration to the device by first rolling back to the before-registration-config and then applying the new configuration.

> **Note** During this operation, you cannot perform tunnel provisioning or firmware upgrade.

- Configuration Push Without Rollback: This method allows you to push the configuration to the device without rolling back to the before-registration-config.

Running Config

You can view the new configuration pushed to the device in the **Running Config** tab. This tab has two sections:

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

Note Cisco IoT FND already supports configuration push at the group-level with rollback capabilities. Whenever the configuration is pushed at the group-level, it reverts to the before-registration-config before applying the new configuration to prevent any misconfigurations caused by manual changes.

Configuration Push with Rollback

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

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

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

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

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

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

b. Apply group-level configuration

To push the configuration with rollback:

Procedure

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

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

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

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

Step 5 Define the device configuration in the FreeMarker template.

Step 6 Click **Save**.

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

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

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

- Configuring
- Success
- Error

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

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

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

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

What to do next

- Viewing Config Push Events, on page 302
- Viewing the Audit Trail, on page 304

Configuration Push Without Rollback

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

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

Procedure

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

Step 2 Select Cisco IOS or IOS-XE device type from the left pane. The Inventory page appears.

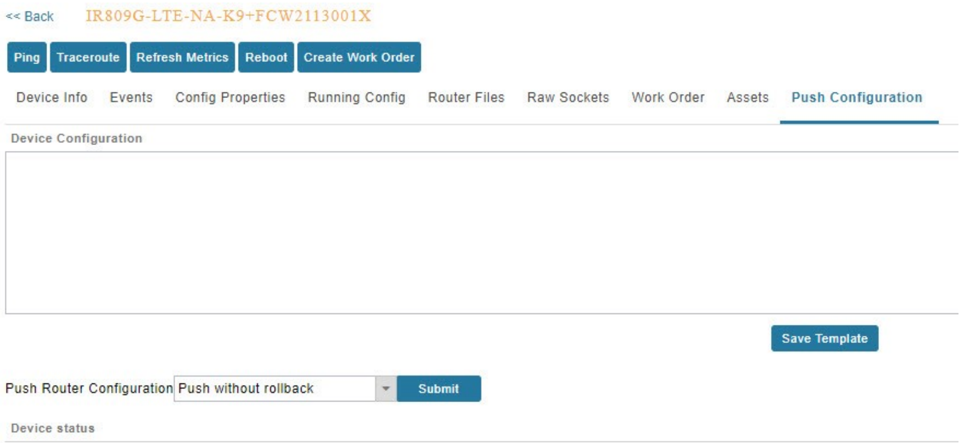
Step 3 In the right pane, click the device for which you want to push the configuration.

Step 4 In the Device Info page, click the **Push Configuration** tab.

Step 5 Define the device configuration in the FreeMarker template.

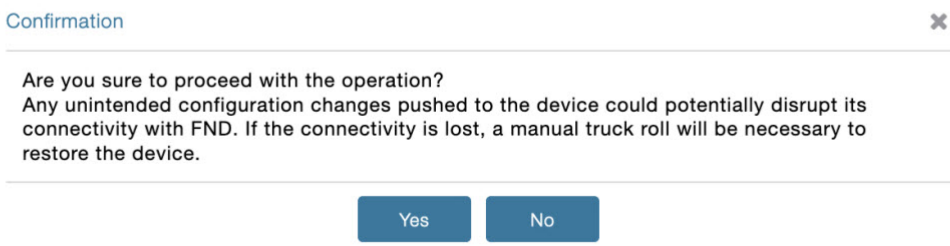
Step 6 Click **Save Template**.

Step 7 Select **Push without rollback** from the **Push Router Configuration** drop-down list.



Step 8 Click **Submit**.

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



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

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

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

What to do next

- Viewing Config Push Events, on page 302
- Viewing the Audit Trail, on page 304

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

Viewing Config Push Events

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

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

Procedure

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

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

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

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

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

Time	Event Name	Severity	Message
2024-08-29 12:19:28:309	Device Configuration Push Failed	MAJOR	java.io.IOException: [invalid configuration commands supplied [BAD_PARAMETER][no shut1]. [PARSE_ERROR_NOMATCH]] Sent [[int loop1234, no shut1]]
2024-08-29 12:19:21:883	Device Configuration Push Initiated Without Rollback	INFO	Configuration push Initiated to Device: CGR1240/K9+FTX2518D00M , Push Type: Push Without Rollback.
2024-08-29 12:15:50:015	Device Configuration Push Successful	INFO	Configuration push successfully applied to Device: CGR1240/K9+FTX2518D00M
2024-08-29 12:15:40:928	Device Configuration Push Initiated Without Rollback	INFO	Configuration push Initiated to Device: CGR1240/K9+FTX2518D00M , Push Type: Push Without Rollback.

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

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

- Registration Request
- Registration Success
- Device Configuration Push Successful

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

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

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

c) Viewing config push events at the group level (for the selected device):

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

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

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

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

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

Viewing the Audit Trail

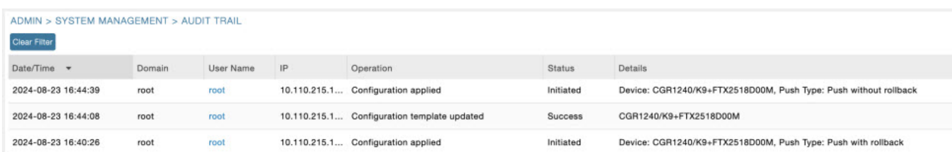
To view the audit trail:

Procedure

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

There are two audit trail statuses:

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



Pushing Configurations to Routers

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

To push the configuration to routers:

Procedure

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

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

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

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

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

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

Step 6 Click **Start**.

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

In the Status column, one of these values appears:

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

What to do next

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

Enabling CGR SD Card Password Protection

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

Note This does not apply to IR800s

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

To enable CGR SD card password protection

Procedure

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

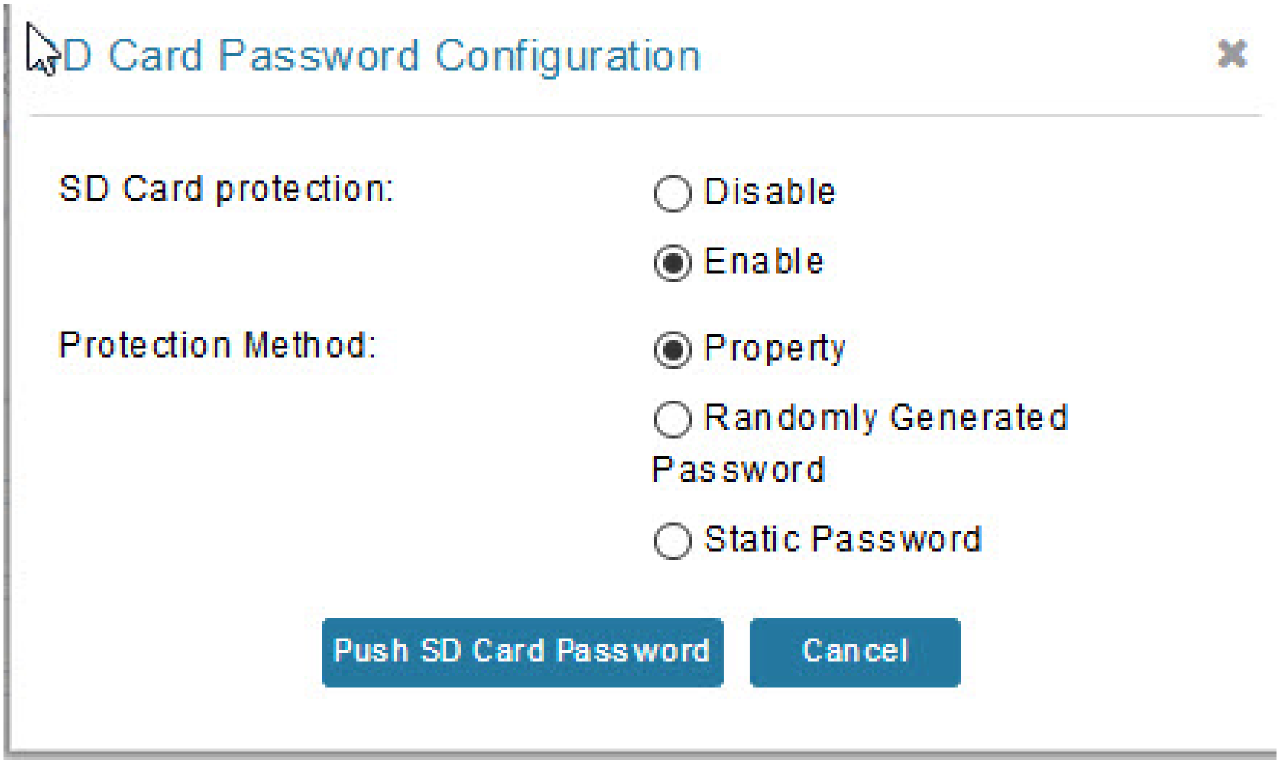
Step 2 Select the CGR group or CGRs to push the configuration to in the Configuration Groups pane

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

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

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

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



Step 7 Select the desired protection method:

• Property: This password is set using a CSV or XML file, or using the Notification Of Shipment file.
• Randomly Generated Password: Enter the password length.
• Static Password: Enter a password.

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

Pushing Configurations to Endpoints

To push configuration to mesh endpoints:

Procedure

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

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

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

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

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

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

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

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

In the Status column, one of these values appears:

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

- PAUSING — The configuration push is in the process of being paused. Active configuration operations complete, but those in the queue are not started.

What to do next

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

Certificate Re-Enrollment for ITRON30 and IR500

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

Supported Devices:

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

Certificates:

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

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

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

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

- Devices page — Figure 17: DEVICES > FIELD DEVICES > Endpoint Re-Enrollment (1 of 2), on page 309
- Device Configuration page — Figure 19: CONFIG > DEVICE CONFIGURATION > Endpoint Certificate Re-enrollment, on page 310
- DTLS Relay Settings — Figure 20: Support for DTLS Relay Settings and Cert Auto-Renew Settings for ITRON30 and IR500 Devices, on page 310
- Additionally, Certificate Information is provided for IR500s — Figure 21: Certificate Information for IR500, on page 310

Figure 17: DEVICES > FIELD DEVICES > Endpoint Re-Enrollment (1 of 2)

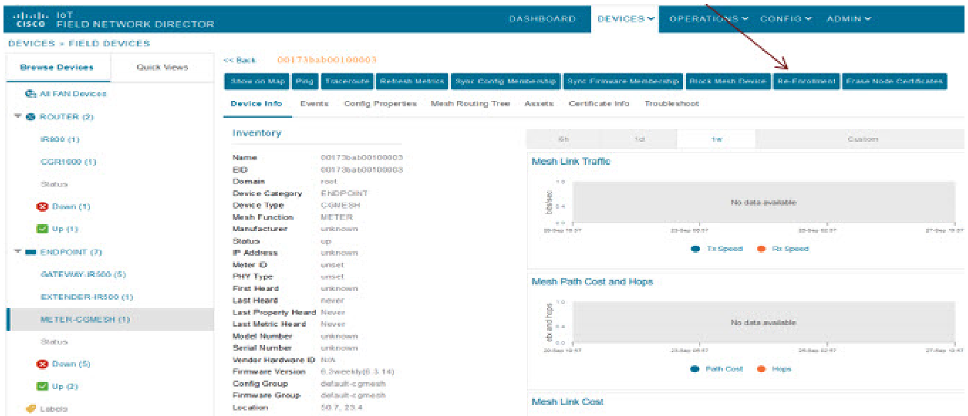


Figure 18: DEVICES > FIELD DEVICES > Endpoint Re-Enrollment (2 of 2)

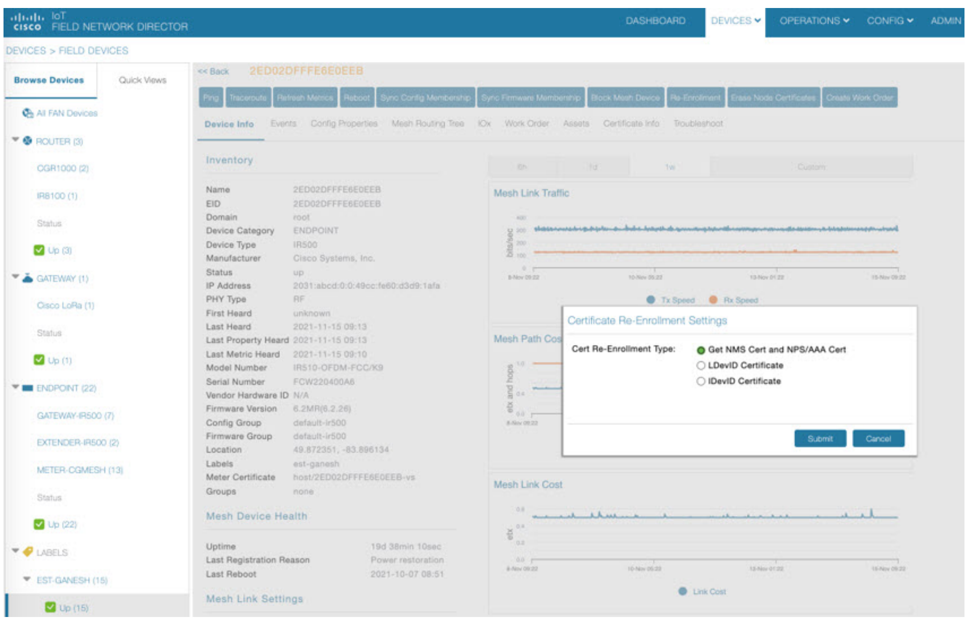


Figure 19: CONFIG > DEVICE CONFIGURATION > Endpoint Certificate Re-enrollment

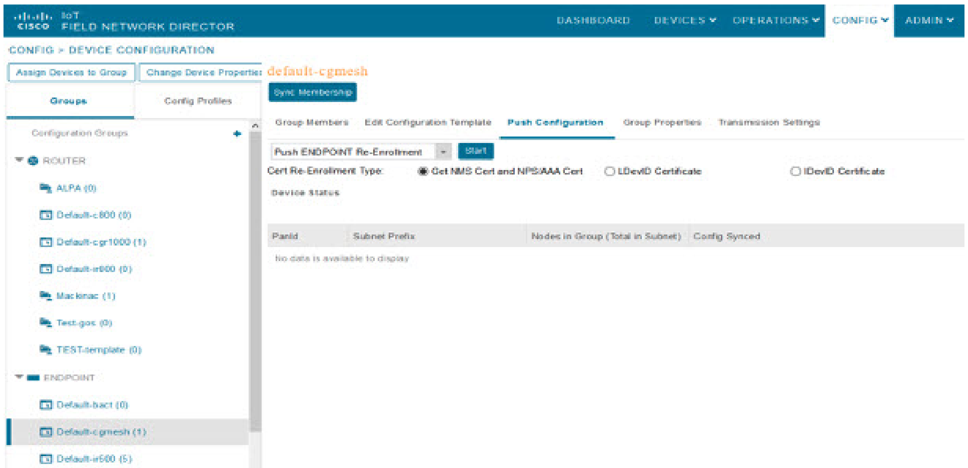
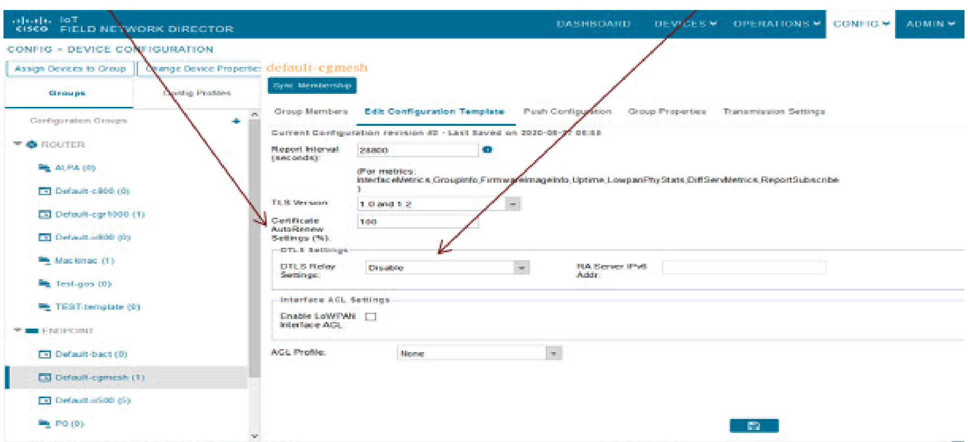
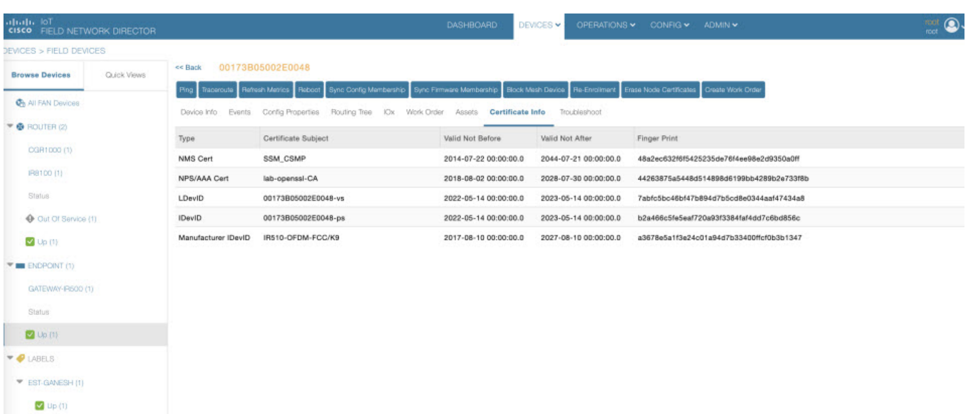


Figure 20: Support for DTLS Relay Settings and Cert Auto-Renew Settings for ITRON30 and IR500 Devices



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.

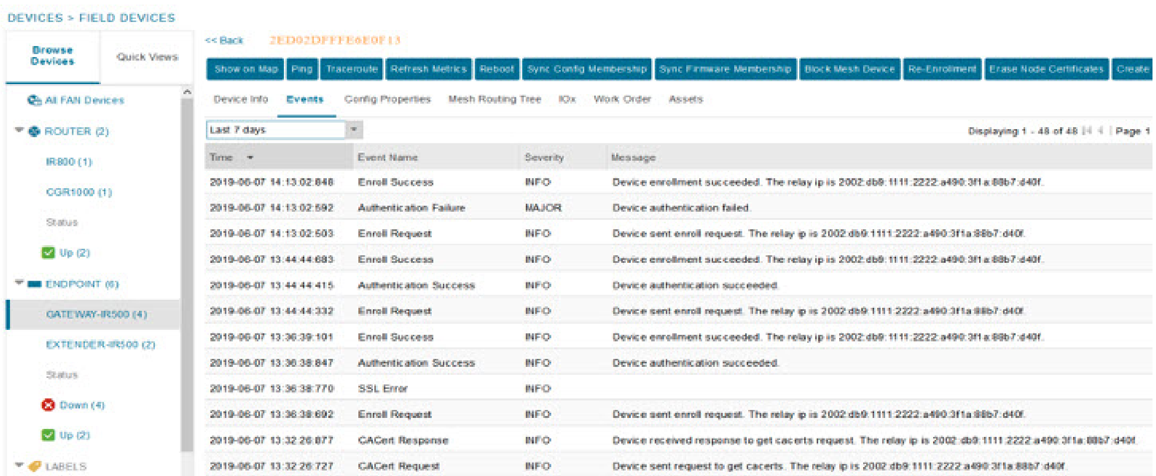
Figure 21: Certificate Information for IR500



New Events for IR500

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

Figure 22: 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:**

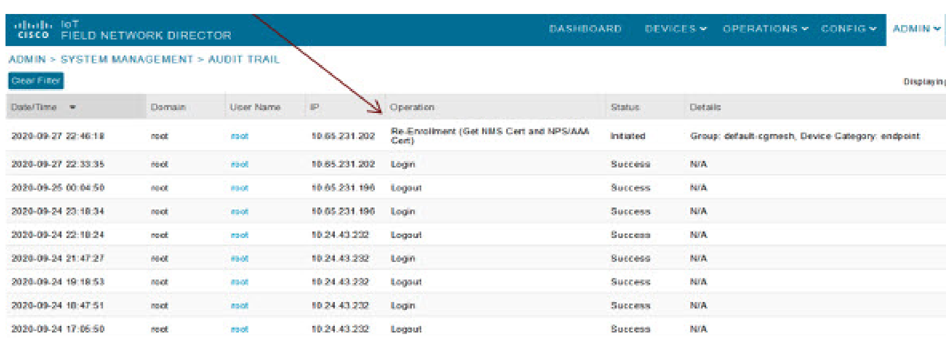
Operation: Re-enrollment (Get NMS Cert and NPS/AAA Cert)

Status: Initiated

Details: Group default-cg-mesh

Device category: endpoint

Figure 23: 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 365). The GOS, Hypervisor, and Cisco IOS all upgrade when you perform a Cisco IOS image bundle installation or update.

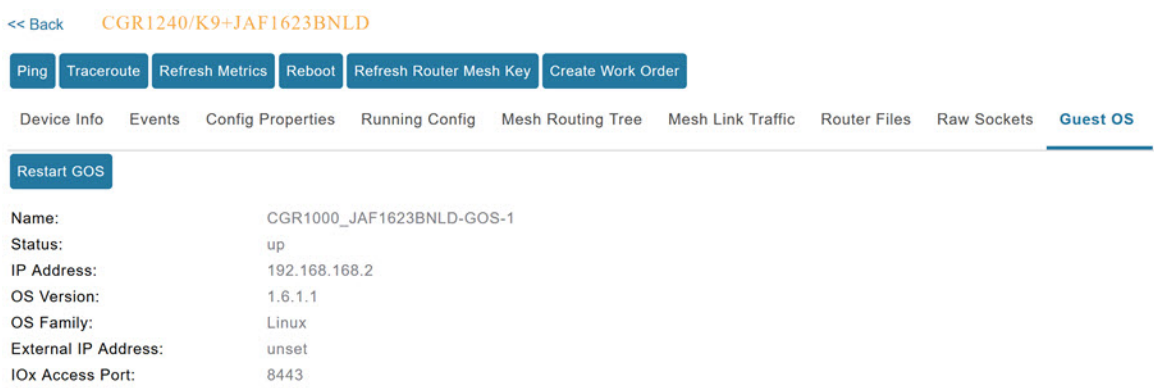
After any Cisco IOS install or upgrade, when IoT FND discovers a GOS, it checks if the initial communications setup is complete before it performs the required setup. The CGR must have a DHCP pool and Gigabit Ethernet 0/1 interface configured to provide an IP address and act as the gateway for the Guest 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 24: DEVICES Field Devices Information Page Showing Guest OS tab and Restart GOS Button



This section includes the following topics:

- Pushing GOS Configurations, on page 313

Pushing GOS Configurations

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

Application Management Support in IoT FND

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

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

Prerequisites

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

  For more configuration related information, see Cisco Catalyst IR1101 Rugged Series Router Software Configuration Guide or Cisco Catalyst IR1800 Rugged Series Router Software Configuration Guide.

- FND and FD Integrated OVA with FD version v1.18.1 and above.

Registering IR1100 or IR1800 Devices with IoT FND through CSV

To register the device:

Procedure

Step 1 Prepare the CSV and add the IOx device to IoT FND. The CSV format is in the following format: **eid,name,status,lastHeard,meshEndpointCount, runningFirmwareversion,ip,openIssues,labels,lat,lng**

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

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

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

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

Starting the IOx Service in Device Details Page

In the device details page:

Procedure

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

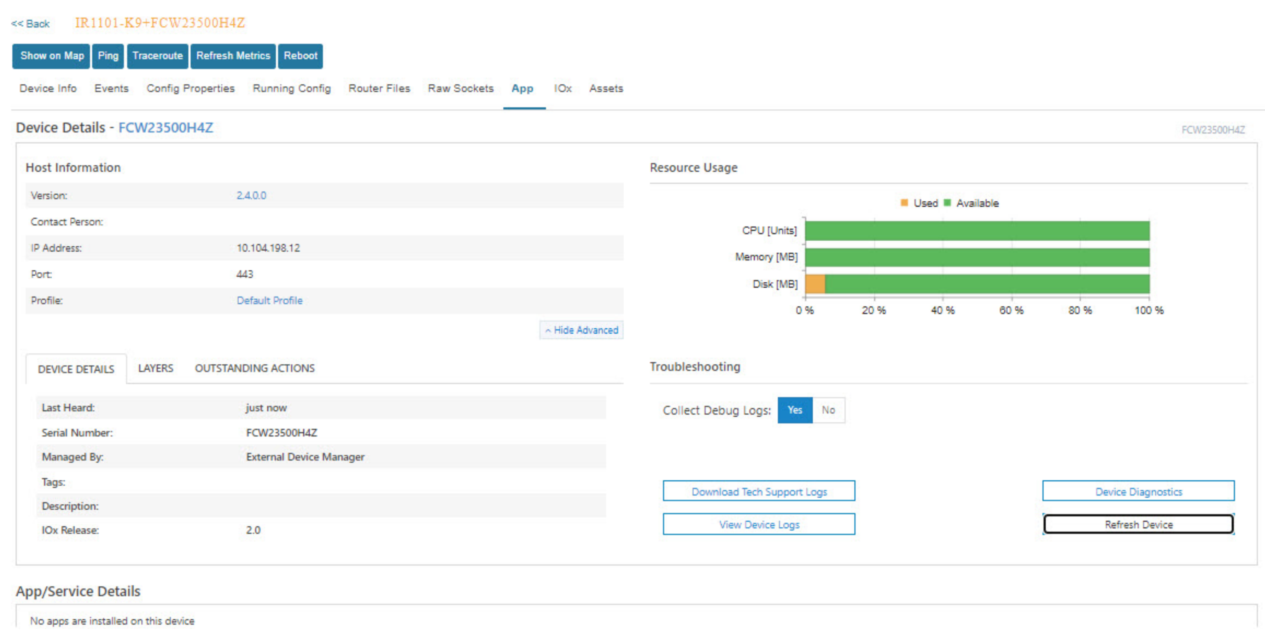
Step 2 Click **Start IOx** button if the service has not started.

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

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

Note

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



Note

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

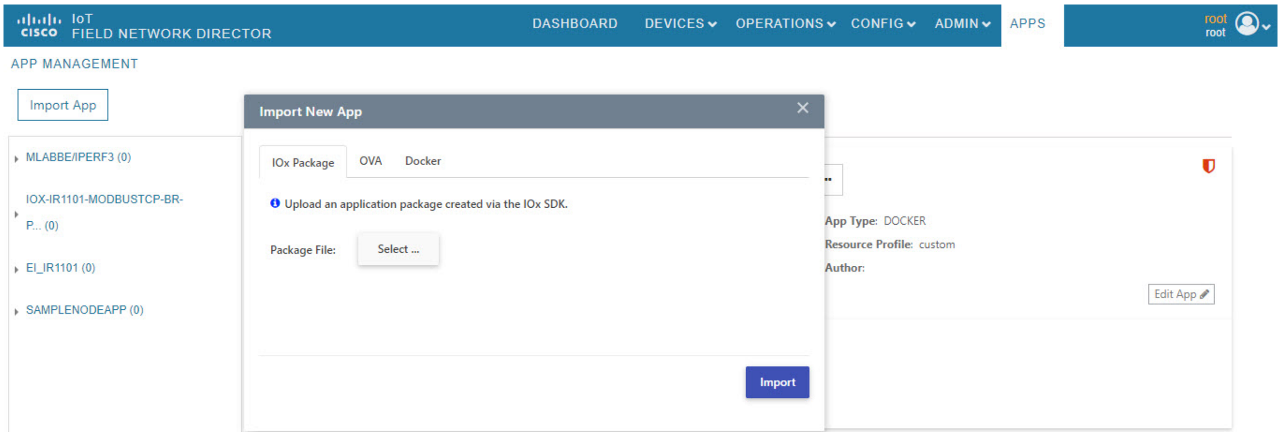
Importing the Application in APPS Main Menu

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

Procedure

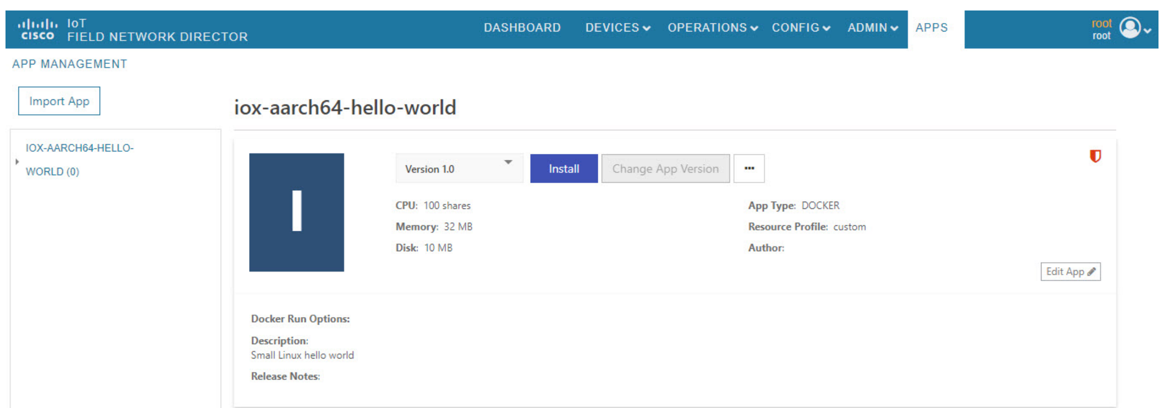
Step 1 Click **Import App**.

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



Installing the Application

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



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

Procedure

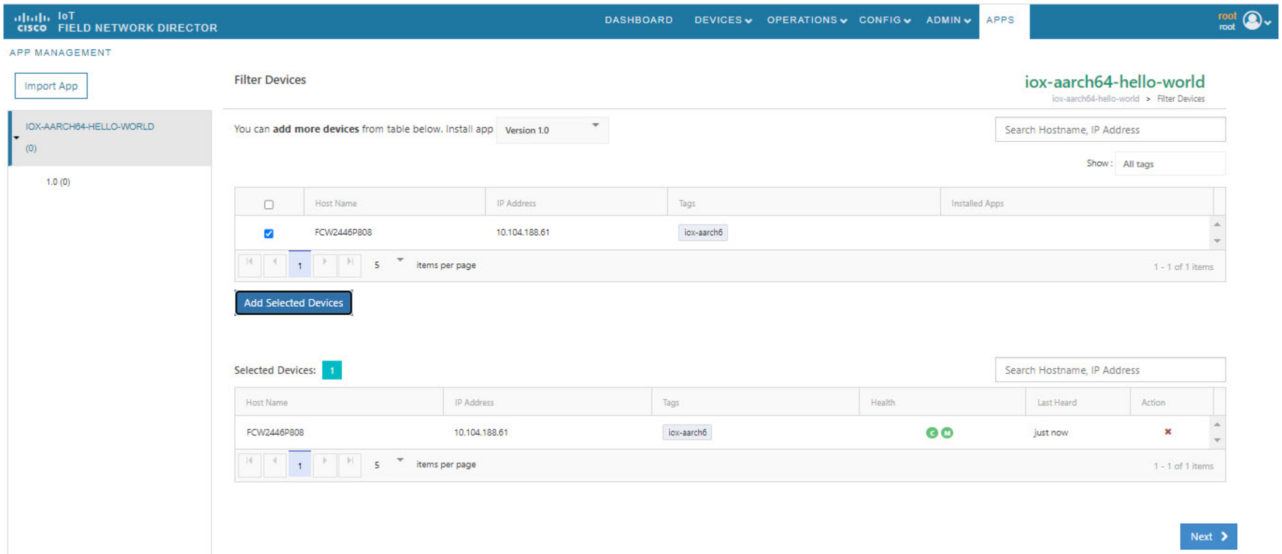
Step 1 Select the device in which the application must be installed.

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

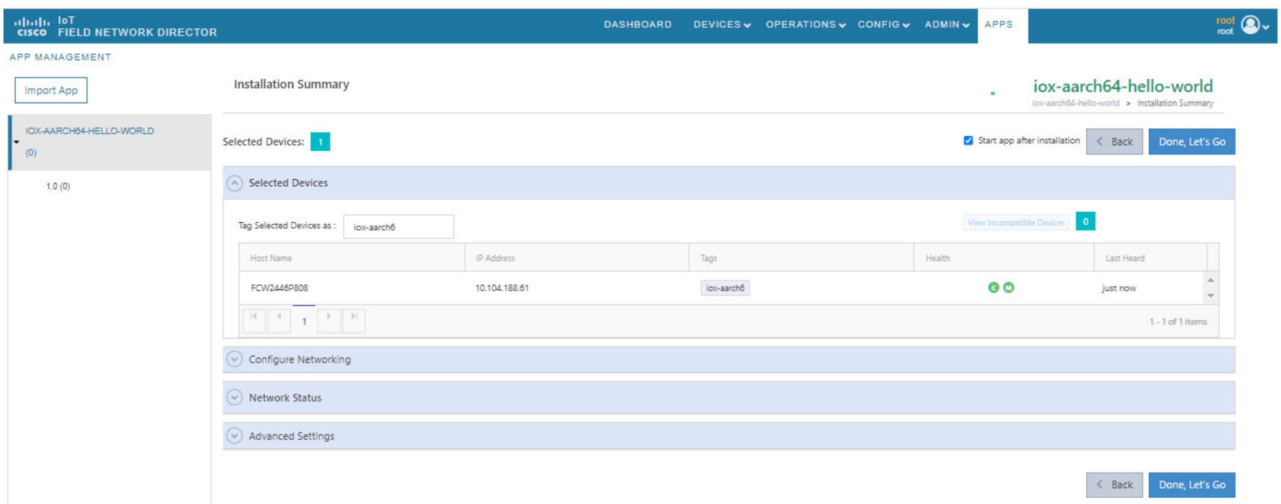
Note

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

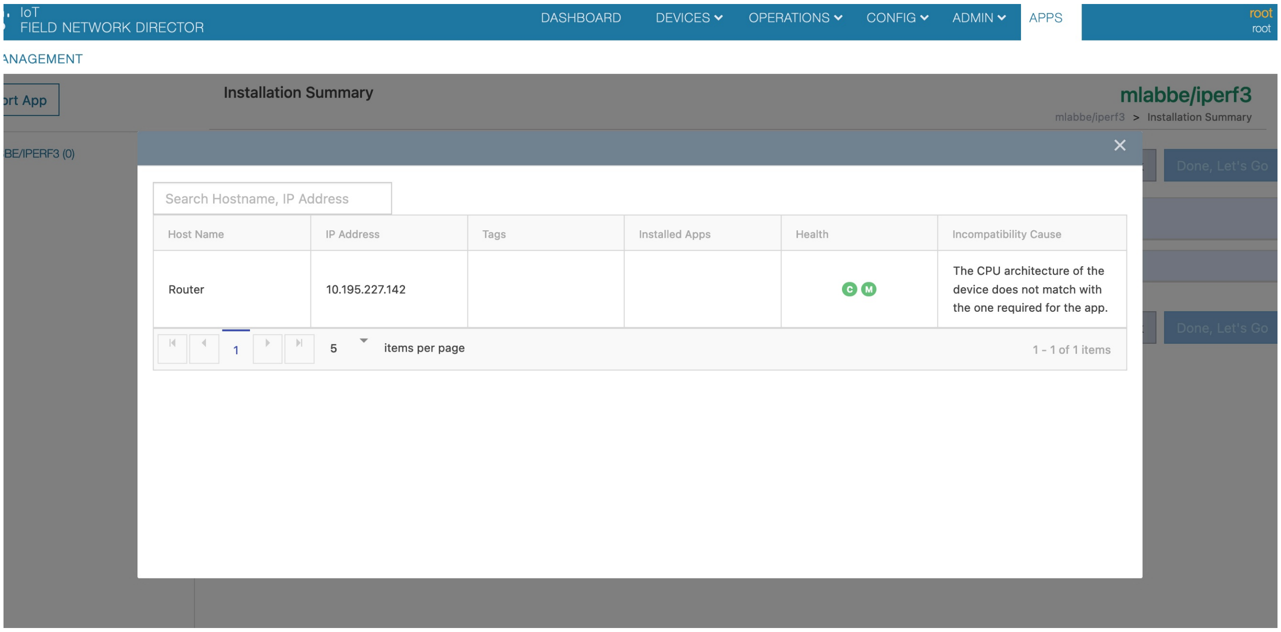
Step 3 Click **Next**.



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

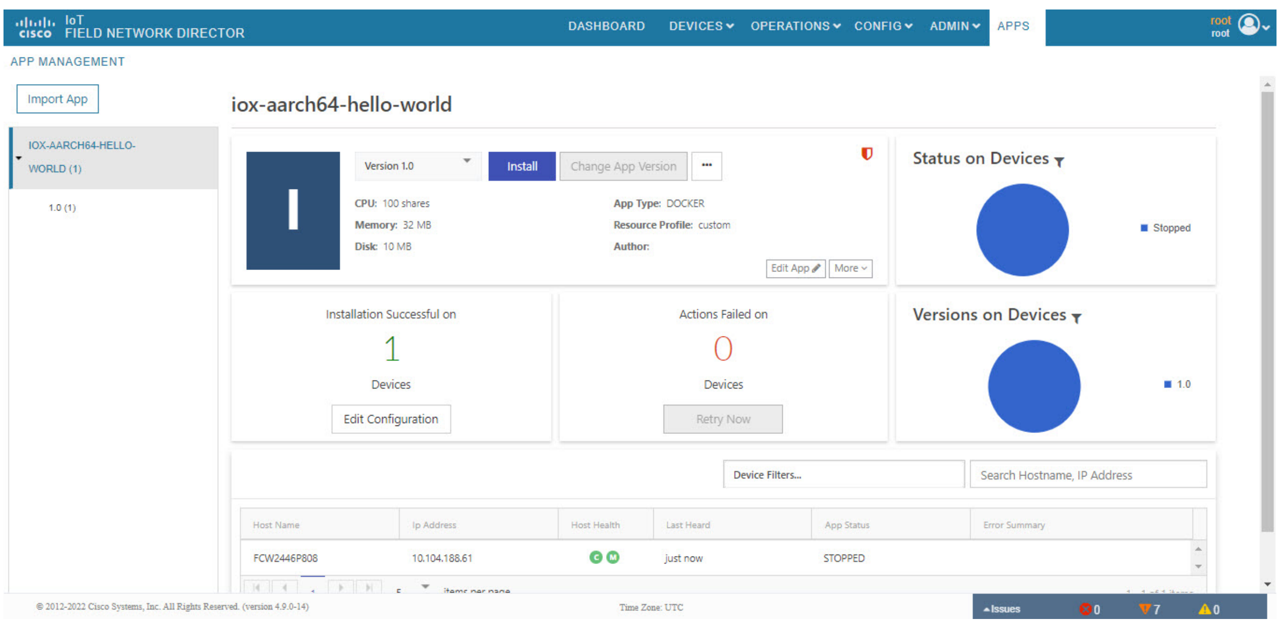


Note
If you install incompatible application, then you will get the following CPU architecture error.



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

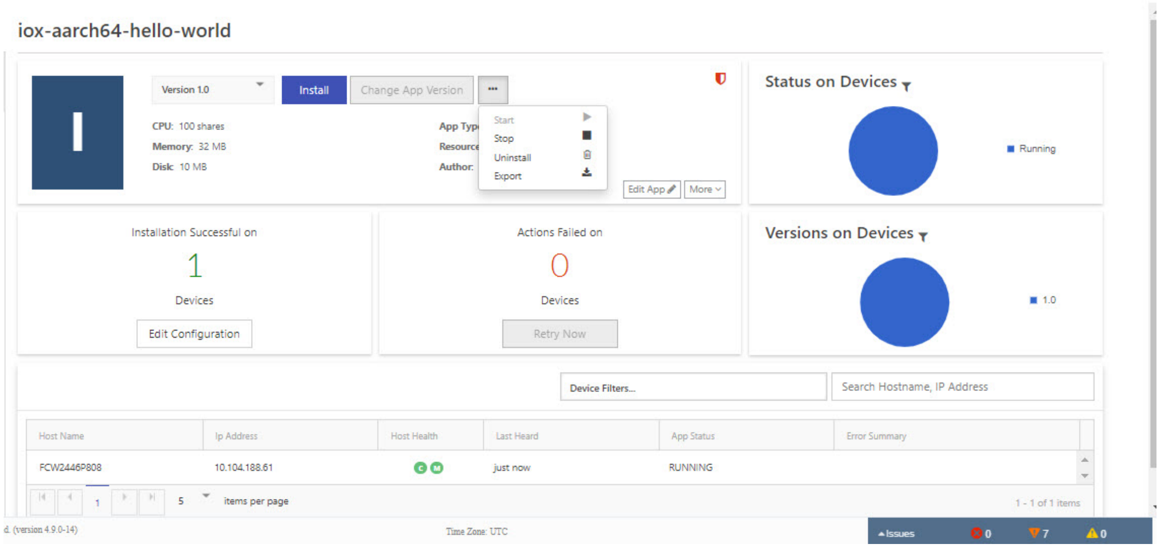
"Installation Successful on device" message appears once installation is complete. The device that is capable of IOx is discovered automatically and the Host Name, Ip Address are properly populated in IoT FND.



Managing the Application

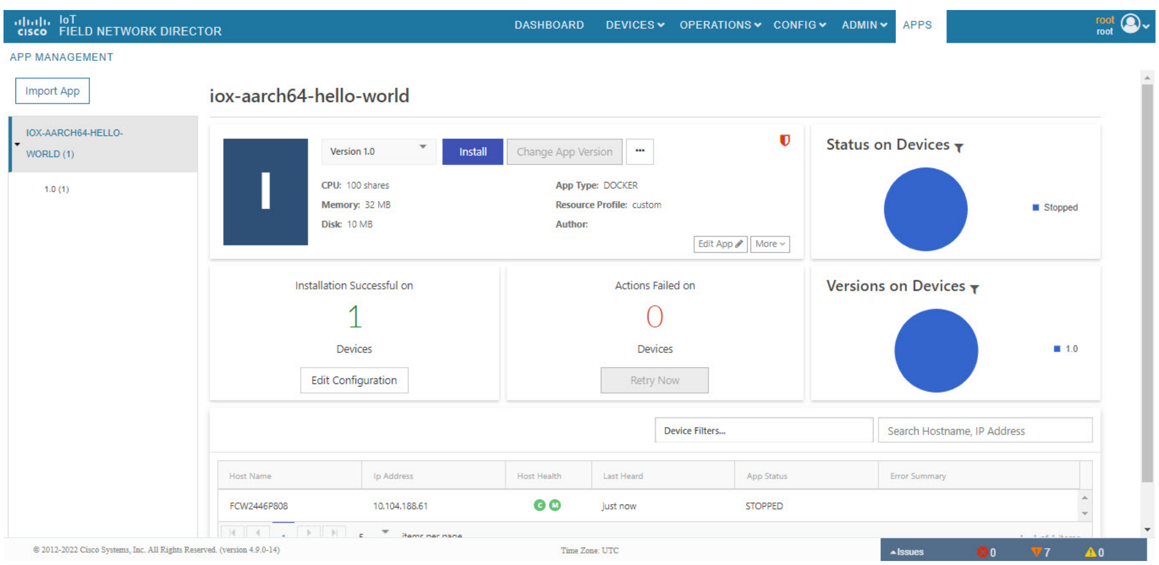
This section describes how to start, stop, and uninstall the application from the APPS menu.

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



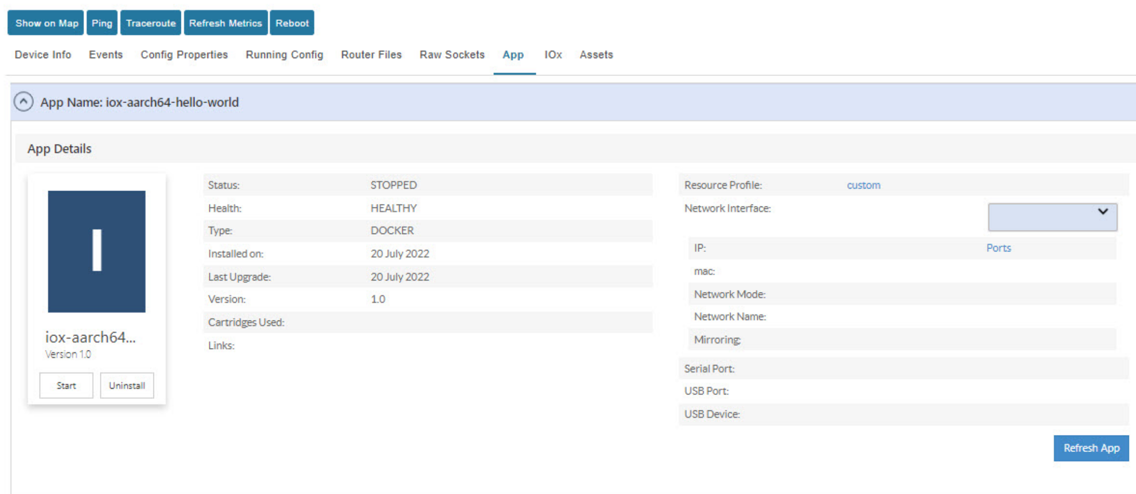
Stopping the Application

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



Note

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



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

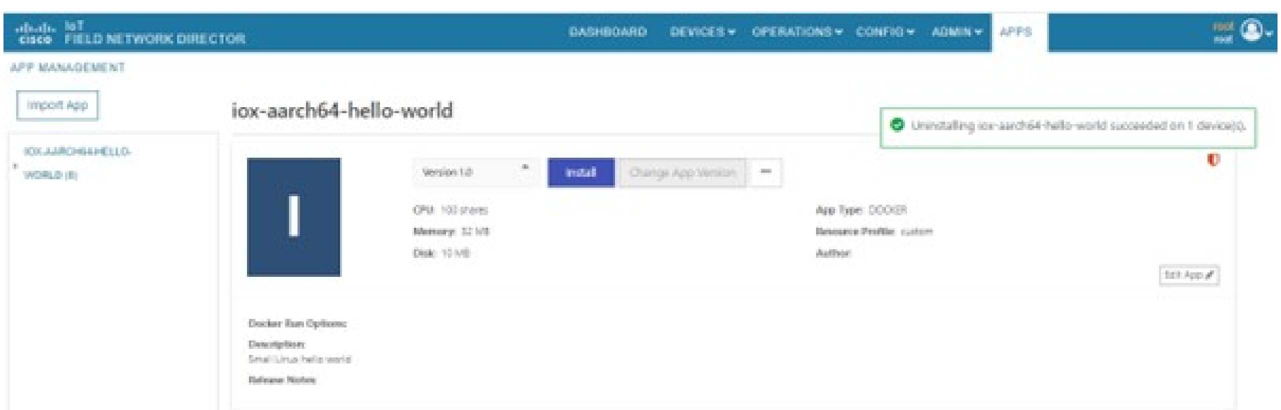
Uninstalling the Application

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

Procedure

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

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



Exporting the Application

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

Support of PIM for IR1100

The P-LTE-450 Pluggable Interface Module (PIM) is a third-party LTE module developed by Cisco and Intelliport for private cellular networks that works on 450 MHz frequency band. PIM is supported since 17.9.3 17.12 and above on IR1101 router. This module requires network-advantage license to work.

PIM has multi-PDN (Public Data Network) support where-in a single SIM slot can be activated with multiple APNs (Access Point Name) with each APN having its own IP and presenting itself as a separate GigabitEthernet interface.

It can be supported on either IR1101 base or compute module, but not on both concurrently. PIM is not supported on IR1100 expansion module slot.

Feature Name	Release Information	Description
PIM Support in IoT FND	IoT FND 4.10	P-LTE-450 Mhz or PIM is a third-party LTE module support for private networks, works with 450Mhz frequency. This module will be part of pluggable module in IR1100.

Display of PIM Module in Field Device Page

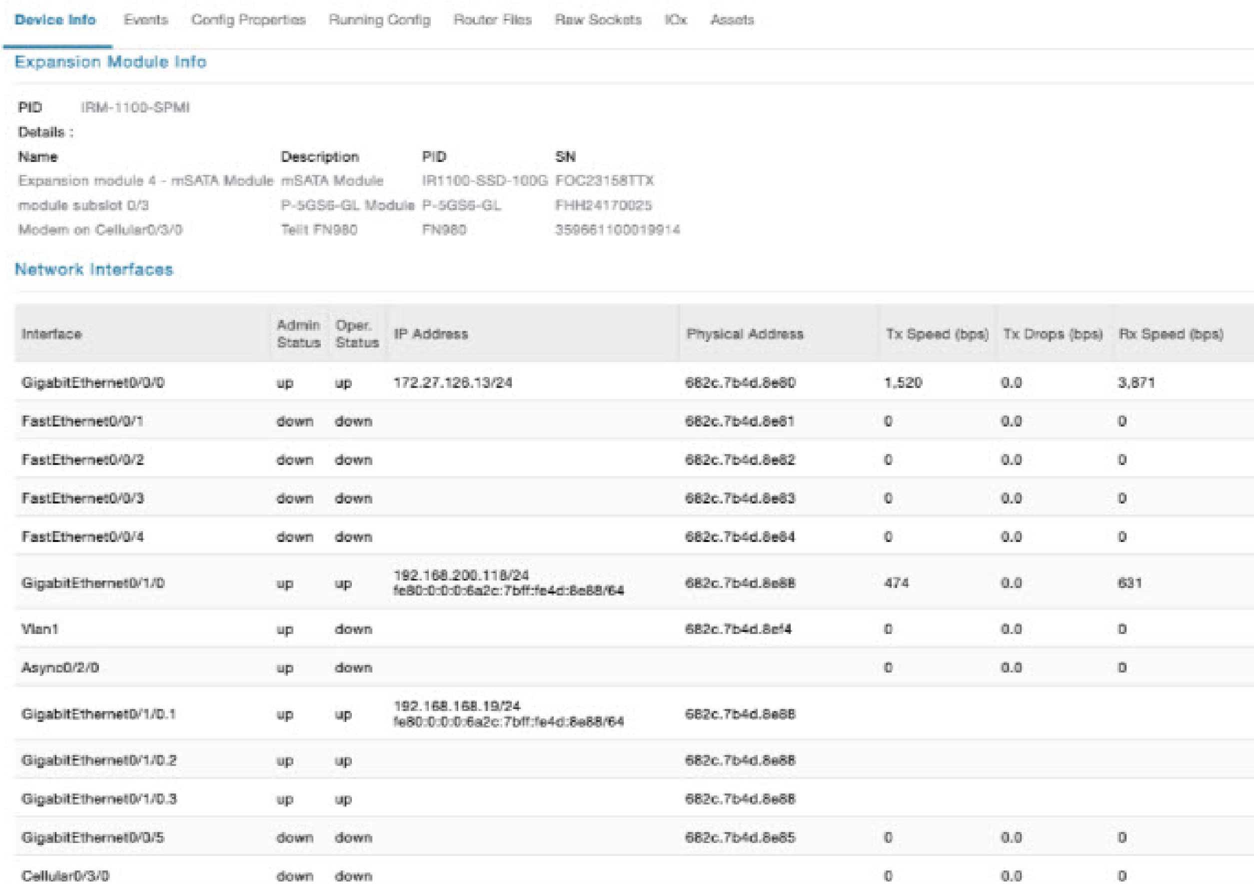
Cisco IoT FND detects the module inserted in IR1101 device during registration of IR1100. To view the module details:

Procedure

Step 1 Select **DEVICES** > **Field Devices** > **Browse Devices tab** > **IR1100**.

Step 2 Click the device on the right pane to view the device information. On the Device Info page, the Pluggable Module Info is displayed.

The Network Interface table in the Device Info page shows the GigabitEthernet interfaces. When P-LTE-450 Mhz module is connected to base module it uses the GigabitEthernet 0/1/0 interface, when connected to compute module it uses GigabitEthernet 0/4/0 interface.



Device Info | Events | Config Properties | Running Config | Router Files | Raw Sockets | IOx | Assets

Expansion Module Info

PID IRM-1100-SPMI

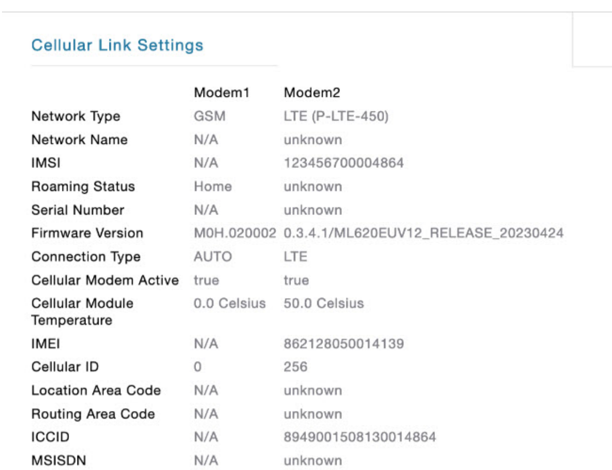
Details :

Name	Description	PID	SN
Expansion module 4 - mSATA Module	mSATA Module	IR1100-SSD-100G	FOC23158TTX
module subslot 0/3	P-5GS6-GL Module	P-5GS6-GL	FHH24170025
Modem on Cellular0/3/0	Telit FN980	FN980	359661100019914

Network Interfaces

Interface	Admin Status	Oper. Status	IP Address	Physical Address	Tx Speed (bps)	Tx Drops (bps)	Rx Speed (bps)
GigabitEthernet0/0/0	up	up	172.27.126.13/24	682c.7b4d.8e80	1,520	0.0	3,871
FastEthernet0/0/1	down	down		682c.7b4d.8e81	0	0.0	0
FastEthernet0/0/2	down	down		682c.7b4d.8e82	0	0.0	0
FastEthernet0/0/3	down	down		682c.7b4d.8e83	0	0.0	0
FastEthernet0/0/4	down	down		682c.7b4d.8e84	0	0.0	0
GigabitEthernet0/1/0	up	up	192.168.200.118/24 fe80:0:0:0:6a2c:7bff:fe4d:8e88/64	682c.7b4d.8e88	474	0.0	631
Vlan1	up	down		682c.7b4d.8ef4	0	0.0	0
Async0/2/0	up	down			0	0.0	0
GigabitEthernet0/1/0.1	up	up	192.168.168.19/24 fe80:0:0:0:6a2c:7bff:fe4d:8e88/64	682c.7b4d.8e88			
GigabitEthernet0/1/0.2	up	up		682c.7b4d.8e88			
GigabitEthernet0/1/0.3	up	up		682c.7b4d.8e88			
GigabitEthernet0/0/5	down	down		682c.7b4d.8e85	0	0.0	0
Cellular0/3/0	down	down			0	0.0	0

The Cellular Link Settings, Cellular Link Info, and Cellular Link section displays PID and descriptive properties for the IR1100 pluggable module in the IoT FND UI at the Device Info page; however, you must refer to the NB API guide for properties and metrics for the pluggable and expansion interfaces, specifically the getMetricHistory and getDeviceDetails. P-LTE-450 can either be connected in the base slot or the expansion CM slot, and it always shows up in Modem2 and APNs hold interface numbers 3,4, and 5.



Cellular Link Settings

	Modem1	Modem2
Network Type	GSM	LTE (P-LTE-450)
Network Name	N/A	unknown
IMSI	N/A	123456700004864
Roaming Status	Home	unknown
Serial Number	N/A	unknown
Firmware Version	M0H.020002	0.3.4.1/ML620EUV12_RELEASE_20230424
Connection Type	AUTO	LTE
Cellular Modem Active	true	true
Cellular Module Temperature	0.0 Celsius	50.0 Celsius
IMEI	N/A	862128050014139
Cellular ID	0	256
Location Area Code	N/A	unknown
Routing Area Code	N/A	unknown
ICCID	N/A	8949001508130014864
MSISDN	N/A	unknown

Cellular Link Metrics

	Interface1	Interface2	Interface3	Interface4	Interface5
Transmit Speed	0.0 bits/sec	0.0 bits/sec	0.0 bits/sec	0.0 bits/sec	0.0 bits/sec
Receive Speed	0.0 bits/sec	0.0 bits/sec	0.0 bits/sec	0.0 bits/sec	0.0 bits/sec
Cellular RSSI	0.0 dBm	0.0 dBm	-64.0 dBm	-64.0 dBm	-64.0 dBm
Bandwidth Usage For Current Billing Cycle	unknown	unknown	unknown	unknown	unknown
Cellular RSRP	-67.0 dBm	-67.0 dBm	-91.0 dBm	-91.0 dBm	-91.0 dBm
Cellular RSRQ	-4.0 dB	-4.0 dB	-13.0 dB	-13.0 dB	-13.0 dB
Cellular SNR	24.0 dB	24.0 dB	30.0 dB	30.0 dB	30.0 dB

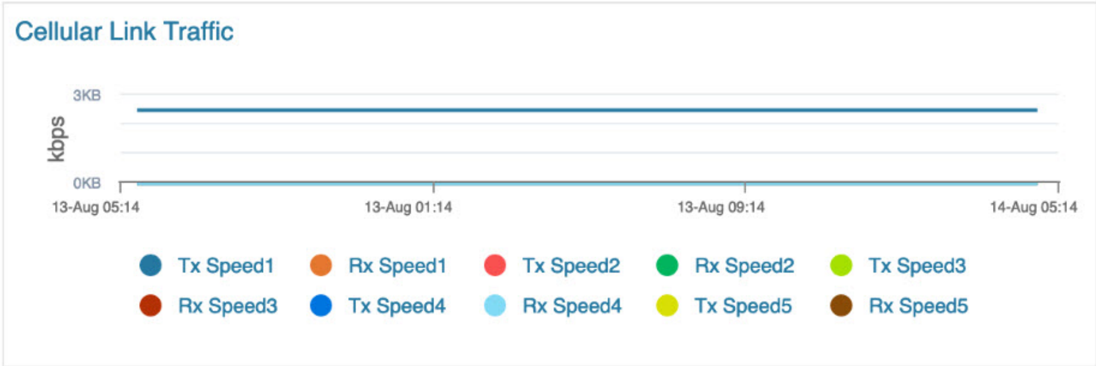
Cellular Link Info

	Interface1	Interface2	Interface3	Interface4	Interface5
Cellular Interface Status	Inactive	unknown	Active	Inactive	Inactive
APN	Inactive	unknown	apn2.mnc001.mcc001.gprs	unknown	unknown

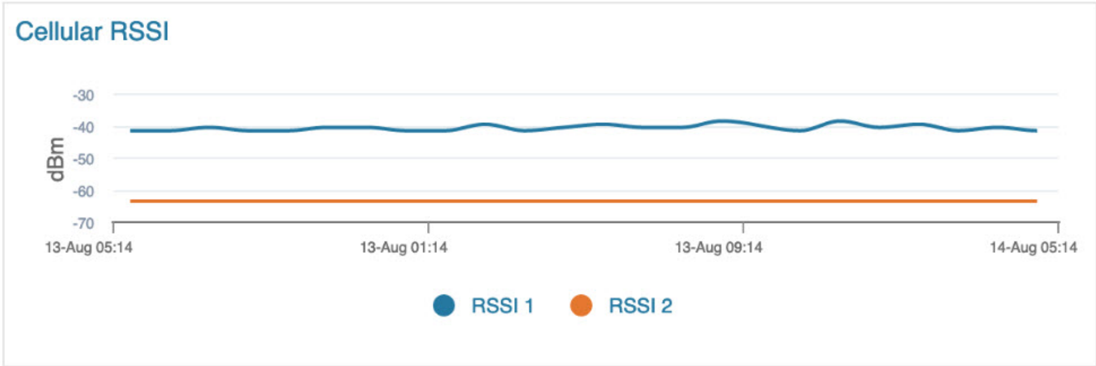
Viewing Cellular Link Traffic and Cellular RSSI Chart for PIM

The Device Info page displays Cellular Link Traffic and Cellular RSSI chart according to the time period selected on the top-right side of the page.

- The Tx speed and Rx speed for the different interfaces display as per the selected period in the Cellular Link Traffic chart. As PIM supports up to 3 interfaces, the Tx Speed5 and Rx Speed5 (for interface 5) can be seen. You can select the Tx or Rx Speed for the interface you wish to see and the active interfaces will display their data.



- The RSSI chart shows RSSI1 and RSSI2 that indicates the radio frequency signal strength of the cellular link. RSSI2 showcases the signal strength of the pluggable module.



Configuring PIM Module

Follow these steps to configure the PIM in IoT FND.

Procedure

Step 1 Choose **CONFIG** > **Device Configuration** > **Groups** > **ROUTER** > **Default-IR1100**.

Step 2 Click **Edit Configuration Template**. The sample CLI commands are as follows:

```
interface GigabitEthernet0/1/0
description Management Interface
ip address dhcp
negotiation auto
ipv6 dhcp client request vendor
ipv6 address autoconfig
ipv6 enable
!
interface GigabitEthernet0/1/0.1
description APN1 Interface
encapsulation dot1Q 2
ip address dhcp
!
interface GigabitEthernet0/1/0.2
```

```
description APN2 Interface
encapsulation dot1Q 3
ip address dhcp
!
interface GigabitEthernet0/1/0.3
description APN3 Interface
encapsulation dot1Q 4
ip address dhcp
```

Support of LTE Cat7 PIMs in IR1100

The Pluggable Interface Module (PIM) that provides LTE (Cat7) capability is supported on Cisco Routers. This PIM is supported since 17.13.1 and above on IR1101 router and can be connected on either IR1101 base module and expansion module (EM). The expansion modules can either be connected on the top of device (Expansion Module) or on the bottom of the device (Compute Module). An expansion module can either be present in expansion or compute slot, but not on both concurrently. The LTE PIMs are supported in all base, EM, and CM slots. The supported LTE Cat7 PIMs are:

- P-LTEA7-NA (EM7411) (for North America)
- P-LTEA7-EAL (EM7421) (for rest of the world)
- P-LTEA7-JP (EM7431) (for Japan)

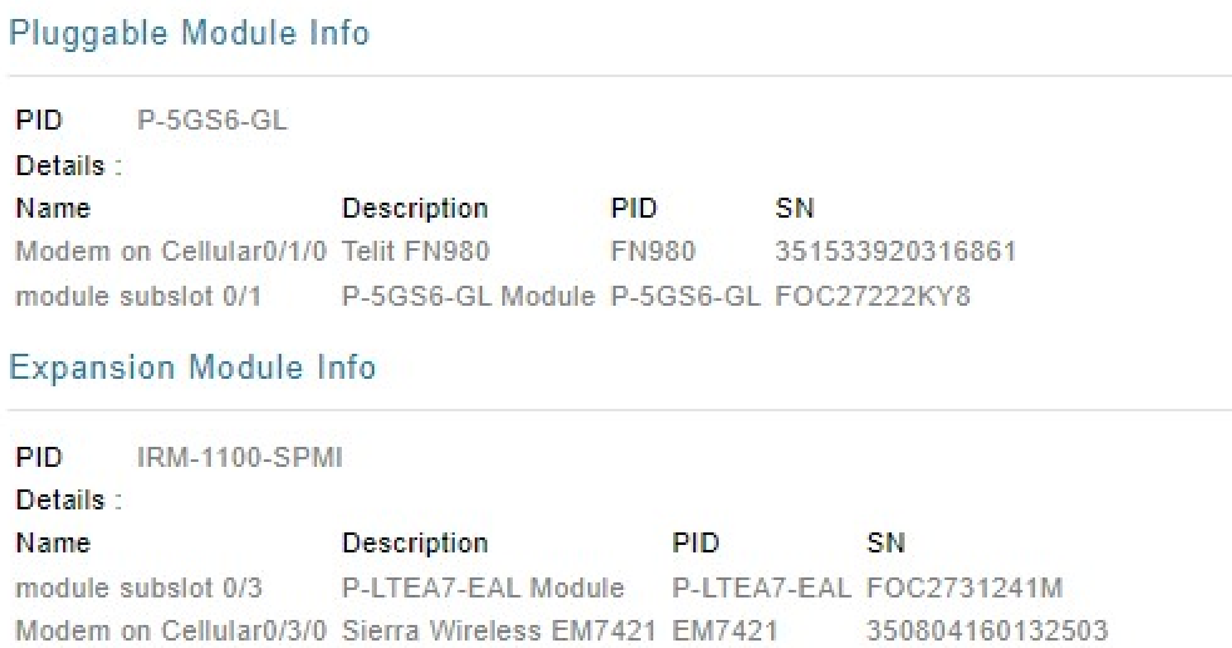
Display of LTE Cat7 PIMs in Field Device Page

Cisco IoT FND detects the modules inserted in IR1101 device during registration. To view the module details:

Procedure

Step 1 Select **DEVICES** > **Field Devices** > **Browse Devices tab** > **IR1100**.

Step 2 Click the device on the right pane to view the device information. On the Device Info page, the Pluggable Module Info is displayed.



Pluggable Module Info

PID P-5GS6-GL

Details :

Name	Description	PID	SN
Modem on Cellular0/1/0	Telit FN980	FN980	351533920316861
module subslot 0/1	P-5GS6-GL Module	P-5GS6-GL	FOC27222KY8

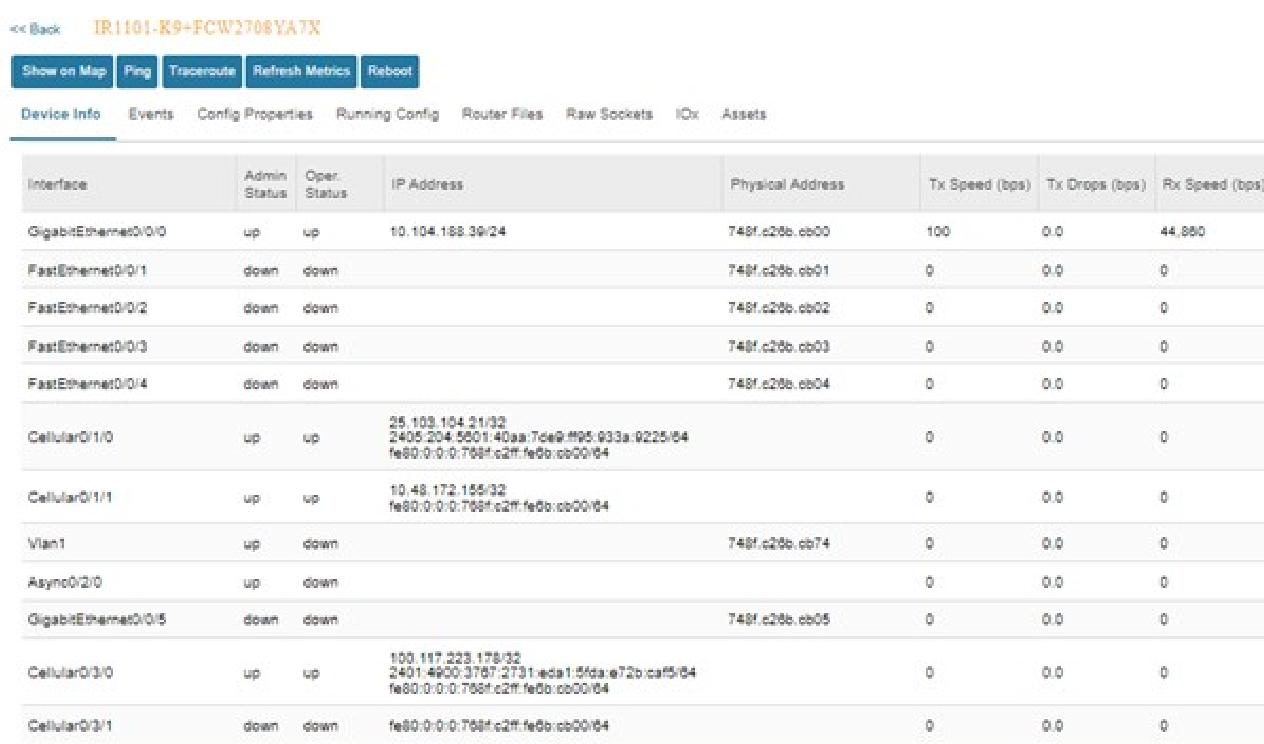
Expansion Module Info

PID IRM-1100-SPMI

Details :

Name	Description	PID	SN
module subslot 0/3	P-LTEA7-EAL Module	P-LTEA7-EAL	FOC2731241M
Modem on Cellular0/3/0	Sierra Wireless EM7421	EM7421	350804160132503

The Network Interface table in the Device Info page shows the Cellular interfaces. The PIMs connected to the base module and compute module use the following interfaces respectively: Cellular 0/1/0, Cellular 0/1/1 in the base module and Cellular 0/3/0, Cellular 0/3/1 in the expansion module.



Interface	Admin Status	Oper. Status	IP Address	Physical Address	Tx Speed (bps)	Tx Drops (bps)	Rx Speed (bps)
GigabitEthernet0/0/0	up	up	10.104.188.39/24	748f.c26b.cb00	100	0.0	44,880
FastEthernet0/0/1	down	down		748f.c26b.cb01	0	0.0	0
FastEthernet0/0/2	down	down		748f.c26b.cb02	0	0.0	0
FastEthernet0/0/3	down	down		748f.c26b.cb03	0	0.0	0
FastEthernet0/0/4	down	down		748f.c26b.cb04	0	0.0	0
Cellular0/1/0	up	up	25.103.104.21/32 2405:204:5601:40aa:7de9:ff95:933a:9225/64 fe80:0:0:0:768f:c2ff:fe6b:cb00/64		0	0.0	0
Cellular0/1/1	up	up	10.48.172.155/32 fe80:0:0:0:768f:c2ff:fe6b:cb00/64		0	0.0	0
Vlan1	up	down		748f.c26b.cb74	0	0.0	0
Async0/2/0	up	down			0	0.0	0
GigabitEthernet0/0/5	down	down		748f.c26b.cb05	0	0.0	0
Cellular0/3/0	up	up	100.117.223.178/32 2401:4900:3767:2731:eda1:5fda:e72b:caf5/64 fe80:0:0:0:768f:c2ff:fe6b:cb00/64		0	0.0	0
Cellular0/3/1	down	down	fe80:0:0:0:768f:c2ff:fe6b:cb00/64		0	0.0	0

On the Device Info page, the cellular link settings, cellular link info, and cellular link metrics section display the values of the modems inside the PIMs.

- **Cellular Link Settings** – A PIM can support two modems. Modem1 corresponds to the primary modem of PIM in base slot and Modem 2 corresponds to the backup modem of PIM in EM or CM slot.

Cellular Link Settings

	Modem1	Modem2
Network Type	LTE	LTE
Network Name	IND-JIO	IND airtel
IMSI	405861098213076	404450631900774
Roaming Status	Home	Home
Serial Number	N/A	8G3186229303B1
Firmware Version	M0H.020202	SWI9X50C_01.14.03.00
Connection Type	LTE	LTE
Cellular Modem Active	true	true
Cellular Module Temperature	42.0 Celsius	40.0 Celsius
IMEI	351533920316861	350804160132503
Cellular ID	101484289	231551755
Location Area Code	N/A	N/A
Routing Area Code	N/A	N/A
ICCID	89918610400464399402	8991000907523490314
MSISDN	916361510527	N/A

- **Cellular Link Info** and **Cellular Link Metrics** – The interfaces 1 and 2 correspond to Modem 1 and interfaces 3 and 4 correspond to Modem 2. Out of each interface per modem, only one of them is in active state. The cellular link metrics is shown for all the interfaces regardless of the state.

Cellular Link Info

	Interface1	Interface2	Interface3	Interface4
Cellular Interface Status	Active	unknown	Active	unknown
APN	jionet	unknown	airtelgprs.com	unknown

Cellular Link Metrics

	Interface1	Interface2	Interface3	Interface4
Transmit Speed	1.571072E7 bits/sec	8736.0 bits/sec	2317312.0 bits/sec	36896.0 bits/sec
Receive Speed	1.4478168E7 bits/sec	0.0 bits/sec	2214528.0 bits/sec	19584.0 bits/sec
Cellular RSSI	-61.0 dBm	-61.0 dBm	-68.0 dBm	-68.0 dBm
Bandwidth Usage For Current Billing Cycle	2 Bytes	0 Bytes	1 Bytes	unknown
Cellular RSRP	-88.0 dBm	-88.0 dBm	-98.0 dBm	-98.0 dBm
Cellular RSRQ	-7.0 dB	-7.0 dB	-12.0 dB	-12.0 dB
Cellular SNR	19.6 dB	19.6 dB	3.4 dB	3.4 dB

Display of Metrics in the Cellular Link Traffic and RSSI Charts

The Device Info page displays the following charts:

- The Cellular Link Traffic chart shows the transmit and receive speeds for each interface according to the time period selected on the top-right side of the page. The series selector is colour coded to distinguish the speed for each interface in the chart.

- The Cellular RSSI chart indicates the quality of the signal strength of each cellular interface for the selected time frame.

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 117 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 271). 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 25: Search for a Specific CGR Device File Name and Upload to FND Router Page, on page 330). 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 26: Upload Multiple CGR Files Within a Given String Search Range to the FND Router Page, on page 330).

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

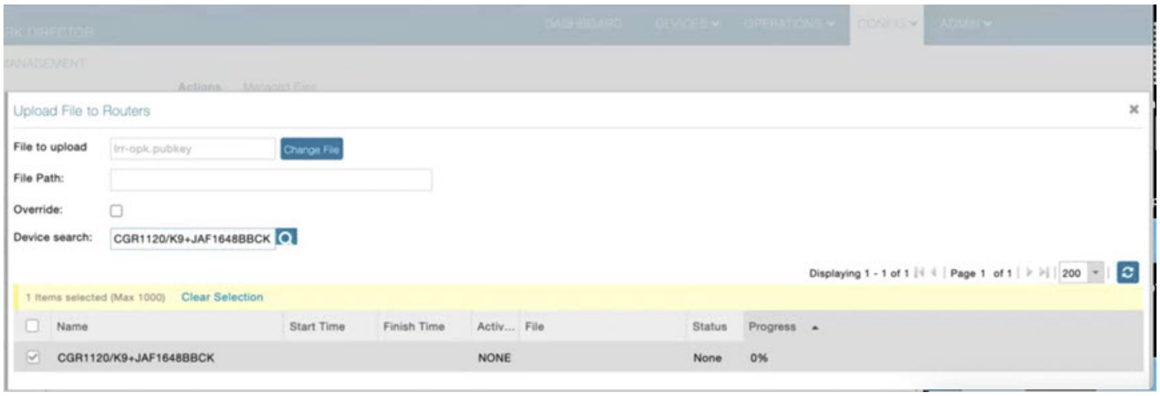
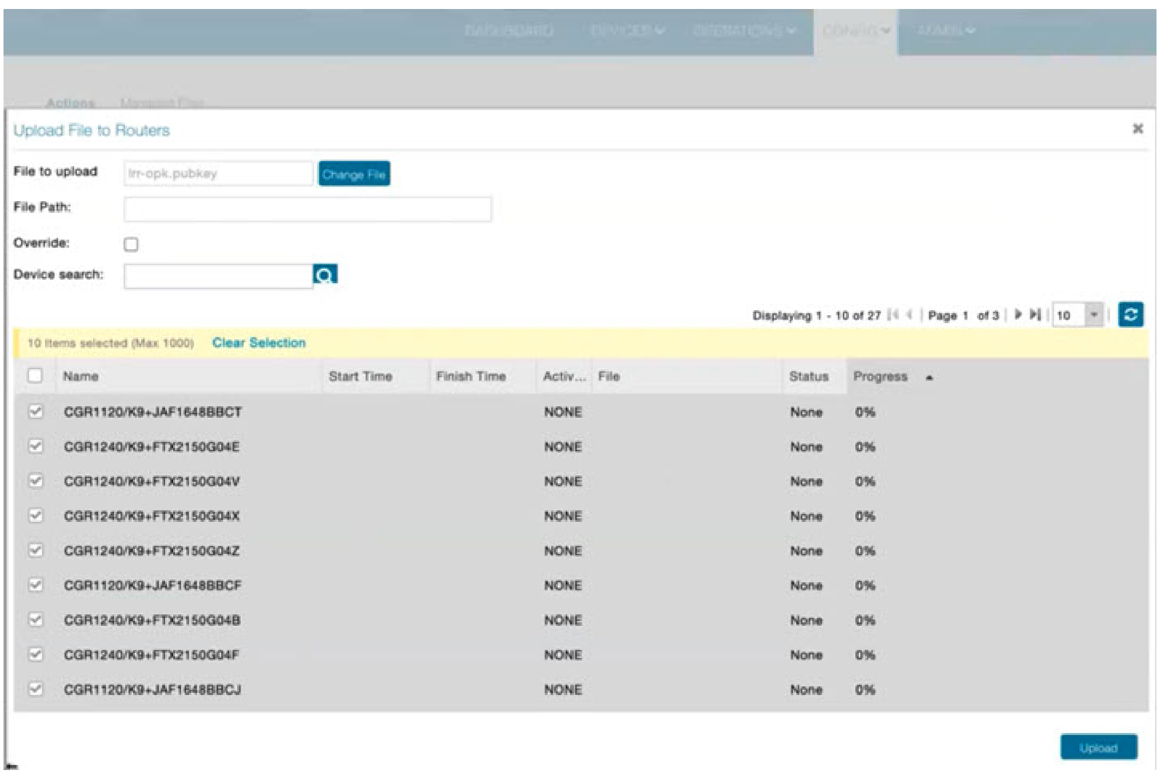


Figure 26: Upload Multiple CGR Files Within a Given String Search Range to the FND Router Page



Deleting a File from IoT FND

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

To delete a file from IoT FND:

Procedure

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

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

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

Transferring Files

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

To perform a file transfer:

Procedure

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

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

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

Step 4 Click **Upload File**.

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

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

Step 6 Click **Upload**.

What to do next

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

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

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

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

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

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

Viewing Files

To view imported text file content:

Procedure

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

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

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

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

What to do next

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

Monitoring Files

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

The following information is included in this list:

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

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

Monitoring Actions

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

The Actions tab lists the following attributes:

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

Deleting Files

To delete files from routers:

Procedure

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

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

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

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

Step 4 Click **Delete File**.

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

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

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

Step 6 Click **Delete**.

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

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

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

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

- File Operation: delete
- Start Date/Time of the last transfer
- End Date/Time
- File name
- Success Count
- Failure Count
- Total Count: The number of CGRs selected for the operation

- Status: UNKNOWN, AWAITING_DELETE, DELETE_IN_PROGRESS, DELETED, CANCELLED
- Percentage Completed
- Error Message
- Error Details

Improved Audit Trail

Download .CSV Files

Table 37: Feature History

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

Information About Improved Audit Trail

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

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

Benefits of Improved Audit Trail

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

Downloading .CSV Files

Here are the steps to download the .csv files:

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

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

Hardware Security Module

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

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

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

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

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

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

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

Verification of FND and HSM Integration After FND and HSM Upgrade

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

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

Procedure

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

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

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

Retrieved public key:

3059301306072a8648ce3d020106082a8648ce3d03010703420004d914167514ec0a110f3170eef74

2a000572cea6f0285a3074db87e43da398ab016e40ca4be5b888c26c4fe91106cbf685a04b0f61d599

826bdbcff25cf065d24

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

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

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

```
lunacm:>exit
[root@fndblr17 bin]#
```

Step 4 Check if the cmu list command is able to retrieve the label of the key and CSMP certificate. This will ask for password. The password is same as the HSM partition. In case of HA, it will be the password of the HSM HAGroup.

```
[root@fndblr17 bin]# cd /usr/safenet/lunaclient/bin
[root@fndblr17 bin]#./cmu list
Certificate Management Utility (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights
reserved.
Please enter password for token in slot 0 : *******
handle=2000001 label=NMS_SOUTHBOUND_KEY
handle=2000002 label=NMS_SOUTHBOUND_KEY--cert0
You have new mail in /var/spool/mail/root
[root@fndblr17 bin]#
```

Step 5 If steps 3 and 4 are successful, it means that the HSM client and HSM communication is good. However, sometimes, there will be an issue with the HSM client API and FND. In such cases, try enabling CK logs as noted below. CK logs are a diagnostic utility of the HSM client. CK logs are resource intensive, so, enable them only when required and disable them after use.

When cklog is enabled, then, the log file will be created in /tmp directory.

This file will generate logs related to FND server access to HSM.

Sometimes it is possible that the HSM client to HSM server is up. However, the FND server is not able to connect to HSM client. In such cases, it will help to find the communication logs between the FND server and also the HSM server.

To enable cklogs:

- Go to directory: **`/usr/safenet/lunaclient/bin`**, then run the command, **`./vtl cklogsupport enable.`**

```
[root@fndserver ~]#cd /usr/safenet/lunaclient/bin
[root@fndserver bin]# pwd
/usr/safenet/lunaclient/bin
[root@fndserver bin]#./vtl cklogsupport enable
vtl (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.
Chrystoki2 LibUNIX = /usr/safenet/lunaclient/lib/libCryptoki2.so
Chrystoki2 LibUNIX64 = /usr/safenet/lunaclient/lib/libCryptoki2_64.so
Cklog not enabled (entry is Null)
Enabling cklog
[root@fndserver bin]#
```

- The location of the cklog file generated is **`/tmp/cklog.txt`**.

```
[root@fndserver bin]# cd /tmp
[root@fndserver tmp]# ls | grep cklog.txt
cklog.txt
[root@fndserver tmp]#
```

Note
HSM does not recommend cklogs to be enabled all the time. Please enable it for troubleshooting and then disable it after use.

To disable:

`[root@fndserver bin]#./vtl cklogsupport disable`

The Linux server will stop logging the FND communications to and from HSM server when **`cklog`** is disabled. The log file, **`/tmp/cklog.txt`** itself is not deleted. When it is enabled again, then, the new logs will be appended to the old logs. If this is not desirable, then after disabling, the cklogs can be renamed if the file is needed or deleted if it is no longer needed.

For example, **`cklog.txt`** is renamed as **`cklog_old_<date>.txt`**

```
[root@fndserver ~]# cd /tmp
[root@fndserver tmp]# ls -al | grep cklog.txt
-rw-r--r--. 1 root root 12643866 Oct 11 00:17 cklog.txt
[root@fndserver tmp]#
[root@fndserver tmp]# mv cklog.txt cklog_old_11oct21.txt
You have new mail in /var/spool/mail/root
[root@fndserver tmp]# ls -al | grep cklog.txt
[root@fndserver tmp]#
[root@fndserver tmp]# ls -al | grep old
-rw-r--r--. 1 root root 12646086 Oct 11 00:20 cklog_old_11oct21.txt
[root@fndserver tmp]#
```

Demo and Bandwidth Operation Modes

The Demo and Bandwidth Operation Modes allow you define the application protocol (HTTP or HTTPS) to use for communication between FND and the router to minimize setup and bandwidth requirements, respectively. The two modes do not affect or change the way that FND communicates with meters or other endpoints. Secure communication between FND and endpoints devices will continue to be secured by using a hardware secure module (HSM) or software secure module (SSM).

- Demo Mode: Allows users to quickly set up a small network with FND for demos by minimizing the setup requirements. It eliminates the need for router certificates or the need to set up SSL.
- Bandwidth optimization mode: Reduces network bandwidth requirements for a network by using HTTP to send periodic metrics between routers and FND while preserving security for other operations. All other router communications will employ HTTPS.

Table 38: Communication Method Given FND Operation Mode

Process	Demo Mode	Bandwidth Optimization Mode	Default Mode
IOS Registration	All communications over HTTP	HTTPS	All communications over HTTPS
AP Registration		HTTPS	
LoRA Registration		HTTPS	
AP Bootstrap		HTTPS	
IOS Tunnel Provisioning		HTTPS	
Configuration Push		HTTPS	
File Transfer		HTTPS	
Metrics		HTTP and HTTPS	

FND Configuration Changes

In order to change FND router Management mode to Demo mode, you must:

Procedure

Step 1 Add the following to the cgms.properties file:

```
fnd-router-mgmt-mode=1 <---where 1
represents Demo Mode
```

Step 2 Add the following to the tpsproxy.properties file:

```
inbound-proxy-destination=
http://<FND-IP/Hostname>:9120 <---where 9120 represents Inbound proxy
tps-proxy-enable-demo-mode=true
<---Enables the TPS proxy to accept HTTP connections
```

Step 3 For the AP registration process, you must add the following two properties to the cgms.properties file:

```
rtr-ap-com-protocol=http
rtr-ap-com-port=80
```

Router Configuration Changes

In order to manage routers in Demo mode:

Procedure

Step 1 Manually change the URL for all the profiles to use HTTP protocol:

```
url http://nms.iot.cisco.com:9121/cgna/ios/registration
url http://nms.iot.cisco.com:9121/cgna/ios/metrics
```

Step 2 Update WSMA profile URL to use HTTP protocol (Only Required in Demo Mode)

```
wsma profile listener config
transport http path /wsma/config
wsma profile listener exec
transport http path /wsma/exec
```

Step 3 Update URL of iot-fnd-register, iot-fnd-metric and iot-fnd-tunnel profiles to use HTTP protocol on Cisco Wireless Gateway for LoRaWAN (IXM-LPWA).

```
configure terminal
igma profile iot-fnd-register
url http://fnd.iok.cisco.com:9121/igma/register
exit
exit
configure terminal
igma profile iot-fnd-metric
url http://fnd.iok.cisco.com:9121/igma/metric
exit
exit
```

```
configure terminal
igma profile iot-fnd-tunnel
url http://fnd.iok.cisco.com:9121/igma/tunnel
exit
exit
```

Configuring Demo Mode in User Interface

Note By default, all communications between FND and the router will be over HTTPS.

To setup Demo Mode for FND and router communications:

Procedure

Step 1 Choose **ADMIN** > **SYSTEM MANAGEMENT** > **Provisioning Settings**.

Step 2 In the Provisioning Process panel, enter the IoT FND URL in the following format: http:// <ip address:9121> in both the IoT FND URL and Periodic Metrics URL.

What to do next

Note The FAR uses the IoT FND URL to communicate with IoT FND after the tunnel is configured and uses the Periodic Metrics URL to report periodic metrics and notifications with IoT FND.

Bandwidth Optimization Mode Configuration

Only periodic metrics will go over HTTP protocol in the Bandwidth Optimization Mode. So, you have to manually change the metric profile URL as follows:

```
url http://nms.iot.cisco.com:9124/cgna/ios/metrics
```

Manually change the URL of metrics profiles to use HTTP protocol, by entering:

```
configure terminal
igma profile iot-fnd-metric
url http://fnd.iok.cisco.com:9124/igma/metrics
exit
exit
```

Note When operating In Bandwidth Optimization Mode, all WSMA requests must go over HTTPS. Therefore, you must ensure that the WSMA profile listener is set to HTTPS at the config and exec command modes.

Configuring Bandwidth Optimization Mode in User Interface

Note By default, all communications between FND and the router will be over HTTPS.

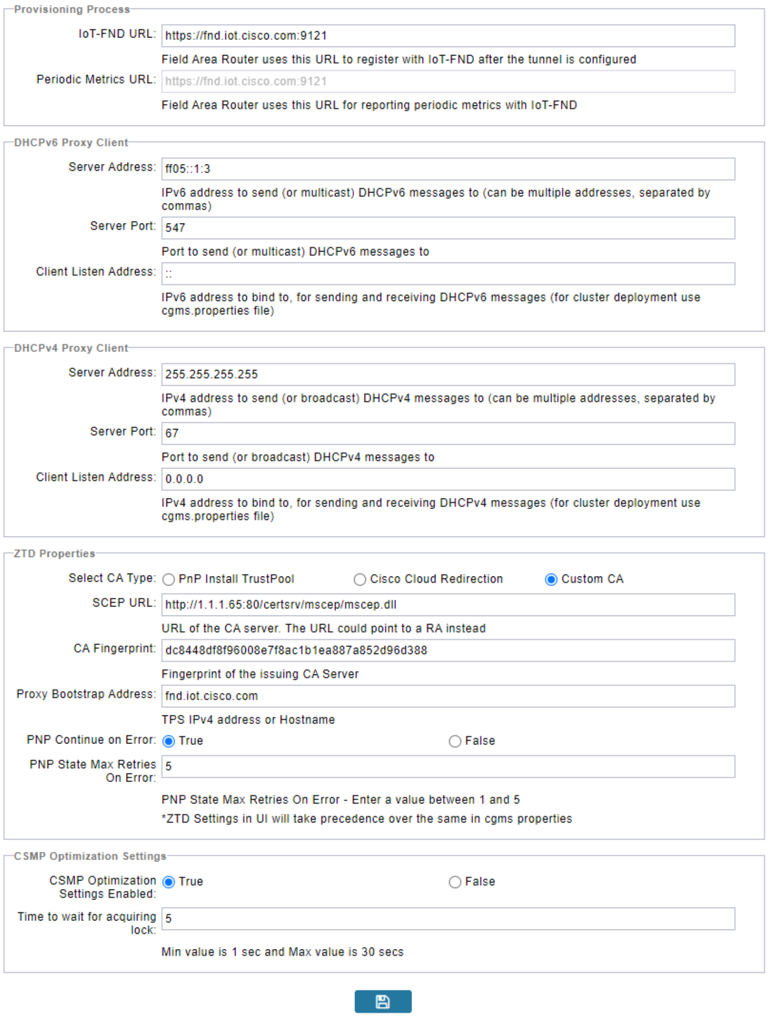
To setup Bandwidth Optimization Mode for FND and router communications:

Procedure

Step 1 Choose **ADMIN** > **SYSTEM MANAGEMENT** > **Provisioning Settings**

Step 2 In the Provisioning Process panel:

- Enter your IoT FND URL in the following format: “https:// FND IP/HostName:9121" in the IoT FND URL field. FAR uses this URL to communicate with IoT FND after the tunnel is configured.
- Enter the following URL in the Periodic Metrics URL field: http:// <ip address:9124>FAR uses this URL to report periodic metrics and notifications with IoT FND.



Device Properties

This section describes the device properties that you can view in IoT FND. Some of these properties are configurable; others are not.

Types of Device Properties

IoT FND stores two types of device properties in its database:

- Actual device properties—These are the properties defined by the device, such as IP Address, Transmit Speed, and SSID.
- IoT FND device properties—These are properties defined by IoT FND for devices, such Latitude and Longitude properties, which IoT FND uses to display device locations on its GIS map.

Note The Key column provides the version of the property name in the IoT FND database that you can use in filters. For example, to search for the device with an IP address of 10.33.0.30, enter **ip:10.33.0.30** in the Search Devices field.

Device Properties by Category

This section presents IoT FND device properties by category.

Every device in IoT FND presents a list of fields, which are used for device searches. The available fields for a device are defined in the **Device Type** field. Fields are either configurable or discovered. Configurable fields are set using XML and CSV files; the device EID is the lookup key. Discovered fields are presented from the device. Fields are also accessible in the device configuration templates for routers.

Cellular Link Metrics for CGRs

Cellular Link Metrics for CGRs describes the fields in the Cellular Link Metrics area of the Device Info view.

Table 39: Cellular Link Metrics for CGRs

Field	Key	Description
Transmit Speed	cellularTxSpeed	Displays the current speed (bits/sec) of data transmitted by the cellular interface over the cellular uplink for a defined period (such as an hour).
Receive Speed	cellularRxSpeed	Displays the average speed (bits/sec) of data received by the cellular uplink network interface for a defined period (such as an hour).
RSSI	cellularRssi	Indicates the radio frequency (RF) signal strength of the cellular uplink. Valid values are 0 to -100. The LED states on the cellular interface and corresponding RSSI values are: • Off: RSSI < = -110 • Solid amber: -100 < RSSI <= -90 • Fast green blink: -90 < RSSI <= -75 • Slow green blink: -75 < RSSI <= -60 • Solid green: RSSI > -60
Bandwidth Usage (Current Billing Cycle)	CellBwPerCycle (bytes)	Displays current bandwidth usage (in bytes) of a particular route for the current billing cycle.
Cell Module Temperature	cellModuleTemp	Internal temperature of 3G module.
Cell ECIO	cellularEcio	Signal strength of CDMA at the individual sector level.

Field	Key	Description
Cell Connect Time	cellConnectTime	Length of time that the current call lasted. This field only applies only to CDMA.
Cellular RSRP	cellularRsrp	Reference Signal Received Power is the average power of resource elements that carry cell specific reference signals over the entire bandwidth.
Cellular RSRQ	cellularRsrq	Indicates the quality of the received reference signal.
Cellular SNR	CellularSnr	The Signal to Noise Ratio is the ratio of signal power to that of all other electrical signals in a location.

Cellular Link Settings

Table 40: Cellular Link Settings Fields lists the fields in the Cellular Link area of the Device Detail page for all Cellular interfaces.

Note Beginning with IoT FND 3.2, Cisco routers IR829, CGR1240, CGR1120, and Cisco 819 4G LTE ISRs (C819) support a new dual-active radio module that supports dual modems and 2 physical interfaces (interfaces 0 and 1, interfaces 2 and 3) per modem. See SKUs below:

- IR829GW-2LTE-K9
- CGM-LTE-LA for CGR 1000 routers
- C819HG-LTE-MNA-K9

Cellular properties supported on the dual modems and their two physical interfaces (and four logical interfaces 0, 1, 2 and 3), display as follows:

Cellular Link Settings	Interface 0 and Interface 1	Interface 2 and Interface 3
—	—	—

Note Starting with IoT FND 4.10, Cisco router IR1100 supports a new dual-active radio module that supports single modem and maximum of 3 APNs. The APNs hold interface numbers 3, 4, and 5 in IoT FND.

Additionally, the 4G LTE dual-active radio module does not support or display all fields summarized in Table 40: Cellular Link Settings Fields

Table 40: Cellular Link Settings Fields

Field	Key	Configurable	Description
Cellular Network Type	N/A	Yes	Defines the type of cellular network for example, GSM or CDMA.

Field	Key	Configurable	Description
Module Status	cellularStatus	No	Displays whether the cellular interface module is active in the network. There is also an unknown state for the module.
Network Name	N/A	Yes	Defines the service provider name, for example, AT&T or Verizon.
Cell ID	cellularID	No	Displays the cell ID for the cellular interface. This value must exist to activate the interface.
Cellular SID	cellularSID	No	Displays the System Identification Number for the CDMA cellular area.
Cellular NID	cellularNID	No	Displays the Network Identification Number for the CDMA cellular area.
Cellular Roaming Status	cellularRoamingStatus	No	Indicates whether the modem is in the Home network or Roaming.
Cellular Modem Serial Number	N/A	No	Displays the serial number of the connected modem.
Cellular Modem Firmware Version	cellularModemFirmwareVersion	No	Displays the version of the modem firmware on the module installed within the CGR.
Connection Type	connectionType	No	Displays the connection type as: • Packet switched • Circuit switched • LTE
Location Area Code	locationAreaCode	No	Displays the Location Area Code (LAC) given by the base station.
Routing Area Code	routingAreaCode	No	Displays the routing area code given by the base station.
APN	cellularAPN	No	Displays the Access Point Name (APN) of the AP to which the cellular interface connects.
Cellular Modem Firmware Version	cellularModemFirmwareVersion	No	Displays the version of the modem firmware on the Cellular module installed within the CGR.
Connection Type	connectionType	No	Displays the connection type as: • Packet switched • Circuit switched

Field	Key	Configurable	Description
IMSI	cellularIMSI	No	The International Mobile Subscriber Identity (IMSI) identifies an individual network user as a 10-digit decimal value within a GSM and CDMA network. Possible values are: • 10-digit decimal value • Unknown
IMEI	cellularIMEI	No	Displays the International Mobile Equipment Identity (IMEI) for the cellular interface within a GSM network only. The IMEI value is a unique number for the cellular interface.
Cellular Module Temperature	cellularModemTemp	—	Displays the modem temperature.
ICCID	cellularICCID	—	The Integrated Circuit Card Identification Number is a unique 18-22 digit code that includes a SIM card's country, home network, and identification number.
MSISDN	cellularMSISDN	—	The Mobile Station International Subscriber Directory Number is an unique number that identifies a mobile subscriber.

DA Gateway Properties

Table 41: DA Gateway Metrics Area Fields describe the fields in the DA Gateway area of the Device Info view.

Table 41: DA Gateway Metrics Area Fields

Field	Key	Description
SSID	N/A	The mesh SSID.
PANID	N/A	The subnet PAN ID.
Transmit Power	N/A	The mesh transmit power.
Security Mode	N/A	Mesh Security mode: • 0 indicates no security mode set • 1 indicates 802.1x with 802.11i key management
Meter Certificate	meterCert	The subject name of the meter certificate.

Field	Key	Description
Mesh Tone Map Forward Modulation	toneMapForwardModulation	Mesh tone map forward modulation: • 0 = Robo • 1 = DBPSK • 2 = DQPSK • 3 = D8PSK
Mesh Tone Map Reverse Modulation	N/A	Mesh tone map reverse modulation: • 0 = Robo • 1 = DBPSK • 2 = DQPSK • 3 = D8PSK
Mesh Device Type	N/A	The primary function of the mesh device (for example, meter, range extender, or DA gateway).
Manufacturer of the Mesh Devices	N/A	Manufacturer of the mesh device as reported by the device.
Basic Mapping Rule End User IPv6 Prefix	N/A	End-user IPv6 address for basic rule mapping for the device.
Basic Mapping Rule End User IPv6 Prefix Length	N/A	Specified prefix length for the end-user IPv6 address.
Map-T IPv6 Address	N/A	IPv6 address for MAP-T settings.
Map-T IPv4 Address	N/A	IPv4 address for MAP-T settings.
Map-T PSID	N/A	MAP-T PSID.
Active Link Type	N/A	Link type of the physical link over which device communicates with other devices including IoT FND.

Device Health

The Table 42: Device Health Fields describes the fields in the Device Health area of the Device Info view.

Table 42: 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 43: Embedded Access Point Credentials Fields describes the fields in the Embedded Access Point Credentials area of the Device Info view.

Table 43: 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 44: Embedded AP Properties describes the fields on the Embedded AP tab of the IR800 Device Info view.

Table 44: Embedded AP Properties

Field	Key	Description
Inventory	NA	Summary of name, EID, domain, status, IP address, hostname, domain name, first heard, last heard, last property heard, last metric heard, model number, serial number, firmware version, and uptime details.
Wi-Fi Clients	NA	Provides client MAC address, SSID, IPv4 address, IPv6 address, device type, state, name, and parent.
Dot11Radio 0 Traffic	NA	Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps), and Rx speed (bps).
Dot11Radio 1 Traffic	NA	Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps,) and Rx speed (bps).
Tunnel3	NA	Provides admin status (up/down), operational status (up/down), Tx speed (bps), Tx drops (bps), and Rx speed (bps).
BVI1	NA	Provides admin status (up/down), operational status (up/down), IP address, physical address, Tx speed (bps), Tx drops (bps) and Rx speed (bps).
GigabitEthernet0	NA	Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps), and Rx speed (bps).

Ethernet Link Metrics

Table 45: Ethernet Link Metrics Area Fields describes the fields in the Ethernet link traffic area of the Device Info view.

Table 45: Ethernet Link Metrics Area Fields

Field	Key	Description
Transmit Speed	ethernetTxSpeed	Indicates the average speed (bits/sec) of traffic transmitted on the Ethernet interface for a defined period of time.

Field	Key	Description
Receive Speed	ethernetRxSpeed	Indicates the average speed (bits/sec) of traffic received on the Ethernet interface for a defined period of time.
Transmit Packet Drops	ethernetTxDrops	Indicates the number of packets dropped (drops/sec) when the transmit queue is full.

IOx Node Properties

Table 46: IOx Node Properties Fields describe the fields in the Iox Node Properties area of the Config Properties page.

Table 46: IOx Node Properties Fields

Field	Key	Description
DHCPv4 Link for IOX Node Gateway	dhcpV4IOxLink	The DHCPv4 gateway address
IOx Node Gateway IPv4 Address	ioxGwyV4Address	The IPv4 gateway address
IOx Node IPv4 Subnet mask	ioxV4Subnetmask	The IPv4 subnet mask address
IOx Node Gateway IPv6 Address	ioxGwyV6Address	The IPv6 gateway address
IOx Node IPv6 Subnet Prefix Length	ioxV6PrefixLength	The IPv6 subnet prefix length
Preferred IOx Node interface on the platform	ioxInterface	The interface on the platform
IOx Node External IP Address	ioxIpAddress	The external IP address
IOx Access Port	ioxAccessPort	The access port

Head-End Routers Netconf Config

Table 47: Head-End Routers Netconf Config Client Fields describes the fields in the Netconf Client area of the **Head-End Routers** > **Config Properties** page.

Table 47: 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 48: 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 48: 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 49: 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 49: Head-End Routers Tunnel 2 Config Device Fields

Field	Key	Configurable	Description
IPsec Tunnel Source 2	ipsecTunnelSrc2	Yes	Identifies the source interface or IP address of IPsec tunnel 2.
IPsec Tunnel Dest Addr 2	ipsecTunnelDestAddr2	Yes	Identifies the destination interface or IP address of IPsec tunnel 2.
GRE Tunnel Source 2	greTunnelSrc2	Yes	Identifies the source interface or IP address of GRE tunnel 2.
GRE Tunnel Dest Addr 2	greTunnelDestAddr2	Yes	Identifies the destination interface or IP address of GRE tunnel 2.

Inventory

The table describes the fields in the Inventory area of the Device Info page for CGR1000.

Table 50: 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.

Field	Key	Configurable	Description
Hardware Version	vid	No	Hardware version of the device.
Hypervisor Version	hypervisor	No	(Cisco IOS CGRs running Guest OS only) The version of the Hypervisor.
Hostname	hostname	No	Hostname of the device.
IP Address	ip	Yes	IP address of the device. Use this address for the IoT FND connection through a tunnel.
Labels	label	Yes	Custom label assigned to the device. A device can have multiple labels. Labels are assigned through the UI or API, but not through an XML or CSV file.
Last Heard	lastHeard	No	Last date and time the device contacted IoT FND.
Last Metric Heard	N/A	No	Time of last polling (periodic notification).
Last Property Heard	N/A	No	The time of last property update for the router.
Last RPL Tree Update	N/A	No	The time of last Routing Protocol for Low power and Lossy Networks (RPL) tree poll update (periodic notification).
Location	N/A	No	Latitude and longitude of the device.
Manufacturer	N/A	No	Manufacturer of the endpoint device.
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 51: Link Metrics Fields describes the fields in the Link Metrics area of the Device Info page.

Table 51: 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.
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 52: Link Settings Fields describes the fields in the Link Settings area of the Device Info view.

Table 52: 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

Field	Key	Description
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 53: 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 54: Mesh Link Config Fields describes the fields in the Mesh Link Config area of the **Routers** > **Config Properties** page.

Table 54: 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.

Field	Key	Configurable	Description
Mesh Address Config	meshAddressConfig	Yes	The IP address of the mesh link.

Mesh Link Keys

Table 55: Mesh Link Keys Fields describes the fields in the Mesh Link Keys area of the Device Info view.

Table 55: 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 56: NAT44 Metrics Fields describes the fields in the NAT44 area of the Device Info page.

Table 56: 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 57: PLC Mesh Info Fields describes the fields in the PLC Mesh Info area of the Device Info view.

Table 57: PLC Mesh Info Fields

Field	Key	Description
Mesh Tone Map Forward Modulation	toneMapForwardModulation	Mesh tone map forward modulation: • 0 = Robo • 1 = DBPSK • 2 = DQPSK • 3 = D8PSK
Mesh Tone Map Forward Map	toneMapForward	Indicates the number of usable subcarriers in the channel, shown as a binary octet (for example, 0011 1111). Ones indicate viable channels. The more ones on the map, the higher the channel capacity.

Field	Key	Description
Mesh Tone Map Reverse Modulation	toneMapRevModulation	Mesh tone map reverse modulation: • 0 = Robo • 1 = DBPSK • 2 = DQPSK • 3 = D8PSK
Mesh Tone Map Reverse Map	toneMapReverse	Indicates the number of usable subcarriers in the channel, shown as a binary octet (for example, 0011 1111). Ones indicate viable channels. The more ones in the map, the higher the channel capacity. The reverse map information and RSSI combine to determine viable channels.
Mesh Absolute Phase of Power	N/A	Mesh absolute phase of power is the relative position of current and voltage waveforms for a PLC node.
LMAC Version	N/A	Version of LMAC firmware in use by the PLC module DSP processor, which provides lower media access functionality for PLC communications compliant with the IEEE P1901.2 PHY standard.

PLC Mesh Info

Table 58: PLC Mesh Info Fields describes the fields in the PLC Mesh Info area of the Device Info view.

Table 58: PLC Mesh Info Fields

Field	Key	Description
Mesh Tone Map Forward Modulation	toneMapForwardModulation	Mesh tone map forward modulation: • 0 = Robo • 1 = DBPSK • 2 = DQPSK • 3 = D8PSK
Mesh Tone Map Forward Map	toneMapForward	Indicates the number of usable subcarriers in the channel, shown as a binary octet (for example, 0011 1111). Ones indicate viable channels. The more ones on the map, the higher the channel capacity.
Mesh Tone Map Reverse Modulation	toneMapRevModulation	Mesh tone map reverse modulation: • 0 = Robo • 1 = DBPSK • 2 = DQPSK • 3 = D8PSK

Field	Key	Description
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 59: Raw Sockets Metrics and Sessions View describes the fields in the TCP Raw Sockets area of the **Field Devices** > **Config Properties** page.

Table 59: Raw Sockets Metrics and Sessions View

Field	Key	Description
Metrics		
Tx Speed (bps)	rawSocketTxSpeedS[portNo]	The transmit speed of packetized streams of serial data in bits per second.
Rx Speed (bps)	rawSocketRxSpeedS[portNo]	The receive speed of packetized streams of serial data in bits per second.
Tx Speed (fps)	rawSocketTxFramesS[portNo]	The transmit speed of packetized streams of serial data in frames per second.
Rx Speed (fps)	rawSocketRxFramesS[portNo]	The receive speed of packetized streams of serial data in frames per second.
Sessions		
Interface Name	N/A	The name of the serial interface configured for Raw Socket encapsulation.
TTY	N/A	The asynchronous serial line on the router associated with the serial interface.
VRF Name	N/A	Virtual Routing and Forwarding instance name.
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.

Field	Key	Description
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 60: Router Battery Device View describes the fields in the Router Battery (Battery Backup Unit (BBU) area of the Device Info page.

Table 60: Router Battery Device View

Field	Key	Configurable	Description
Battery 0 Charge	battery0Charge	No	Shows the battery voltage of BBU 0.
Battery 0 Level (%)	battery0Level	No	Displays the percentage of charge remaining in BBU 0 as a percentage of 100.
Battery 0 Remaining Time	battery0Runtime	No	How many hours remain before the BBU 0 needs to be recharged.
Battery 0 State	battery0State	No	How long BBU 0 has been up and running since its installation or its last reset.
Battery 1 Level (%)	battery1Level	No	Displays the percentage of charge remaining in BBU 1 as a percentage of 100.
Battery 1 Remaining Time	battery1Runtime	No	How many hours remain before BBU 1 needs to be recharged.
Battery 1 State	battery1State	No	How long BBU 1 has been up and running since its installation or its last reset.
Battery 2 Level (%)	battery2Level	No	Displays the percentage of charge remaining in BBU 2 as a percentage of 100.
Battery 2 Remaining Time	battery2Runtime	No	How many hours remain before BBU 2 needs to be recharged.
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 61: Router Config Device View describes the fields in the Router Config area of the **Field Devices** > **Config Properties** page.

Table 61: 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 62: Router Credentials Fields describes the fields in the Router Credentials area of the **Field Devices** > **Config Properties** page.

Table 62: Router Credentials Fields

Field	Key	Configurable	Description
Administrator Username	N/A	Yes	The user name used for root authentication.
Administrator Password	N/A	Yes	The password used for root authentication.
Master key	N/A	Yes	The master key used for device authentication.
SD Card Password	N/A	No	SD card password protection status.
Token Encryption Key	N/A	Yes	The token encryption key.
CGR Username	N/A	Yes	The username set for the CGR.
CGR Password	N/A	Yes	The password set on the CGR for the associated username.

Router DHCP Proxy Config

Table 63: DHCP Proxy Config Fields describes the fields in the DHCP Proxy Config area of the **Field Devices** > **Config Properties** page.

Table 63: 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.

Field	Key	Configurable	Description
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 64: Router Health Device View describes the Router Health fields in the Device Info view.

Table 64: Router Health Device View

Field	Key	Configurable	Description
Uptime	uptime	No	Indicates the length of time (in seconds) that the router has been up and operating since its last reset.
Door Status	doorStatus	No	Options for this field are: • "Open" when the door of the router is open • "Closed" after the door is closed
Chassis Temperature	chassisTemp	No	Displays the operating temperature of the router. You can configure alerts to indicate when the operating temperature falls outside of the customer-defined temperature range.

Router Tunnel 1 Config

Table 65: Router Tunnel 1 Config Device View describes the fields in the Router Tunnel 1 Config area of the **Field Devices** > **Config Properties** page.

Table 65: 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.

Field	Key	Configurable	Description
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 66: Router Tunnel 2 Config Device View describes the fields in the Router Tunnel 2 Config area of the **Field Devices** > **Config Properties** page.

Table 66: Router Tunnel 2 Config Device View

Field	Key	Configurable	Description
Tunnel Source Interface 2	tunnelSrcInterface2	Yes	Defines the interface over which the second tunnel is built to provide WAN redundancy.
OSPF Area 2	ospfArea2	Yes	Defines the OSPFv2 Area 2 in which the router (running IPv4) is a member.
OSPFv3 Area 2	ospfV3Area2	Yes	Defines OSPFv3 Area 2 in which the router (running IPv6) is a member.
IPsec Dest Addr 2	ipsecTunnelDestAddr2	Yes	Defines the destination IP address for IPsec tunnel 2.
GRE Dest Addr 2	greTunnelDestAddr2	Yes	Defines the destination IP address for GRE tunnel 2.

Router Tunnel Config

Table 67: Router Tunnel Config Device View describes the fields in the Router Tunnel Config area of the **Field Devices** > **Config Properties** page.

Table 67: 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 68: SCADA Metrics View describes the fields on the SCADA tab of the Device Info page.

Table 68: SCADA Metrics View

Field	Key	Configurable	Description
Channel Name	channel_name	No	Identifies the channel on which the serial port of the router communicates to the RTU.
Protocol Type	protocol	No	Identifies the Protocol Translation type.
Messages Sent	N/A	No	The number of messages sent by the router.
Messages Received	N/A	No	The number of messages received by the router.
Timeouts	N/A	No	Displays the timeout value for connection establishment.
Aborts	N/A	No	Displays the number of aborted connection attempts.
Rejections	N/A	No	Displays the number of connection attempts rejected by IoT FND.
Protocol Errors	N/A	No	Displays the number of protocol errors generated by the router.
Link Errors	N/A	No	Displays the number of link errors generated by the router.
Address Errors	N/A	No	Displays the number of address errors generated by the router.
Local IP	N/A	No	Displays the local IP address of the router.
Local Port	N/A	No	Displays the local port of the router.
Remote IP	N/A	No	Displays the remote IP address of the router.
Data Socket	N/A	No	Displays the Raw Socket server configured for the router.

WiFi Interface Config

Table 69: WiFi Interface Config Fields describe the fields in the WiFi Interface Config area of the **Field Devices** > **Config Properties** page.

Table 69: 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 70: 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 70: 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 71: WiMAX Link Health Fields describe the fields in the WiMAX Link Health area of the Device Info page.

Table 71: 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 72: WiMAX Link Settings Fields describe the fields in the WiMAX Link Settings area of the Device Info page.

Table 72: 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.

Field	Key	Description
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 7

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, 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:

Procedure

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 383.

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 365). 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 388.

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:

Procedure

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
```

Manage Router Firmware Upgrades

Manage Router Firmware Upgrades

Table 73: Feature History

Feature Name	Release	Description
Manage Router Firmware Upgrades	Cisco IoT FND Release 5.0	Manage router firmware upgrade and install counts using Cisco IoT FND, eliminating the need to manually edit .jboss property files.

Information About Manage Router Firmware Upgrades

Manage router firmware upgrade and install counts directly using Cisco IoT FND. You no longer have to manually edit .jboss property files, simplifying the firmware management process. The router firmware management is now intuitive and accessible. Define the **Maximum Router Firmware Upload Count**, **Maximum Router Firmware Install Count**, and **Router Firmware Upload Retry Count** values globally on Cisco IoT FND. Apply the maximum parallel or concurrent firmware upgrade values to all the group of routers on Cisco IoT FND.

Restrictions For Manage Router Firmware Upgrades

Here are the default counts for the respective fields:

- **Router Firmware Upload Count**: 48
- **Router Fimware Install Count**: 48
- **Router Firmware Upload Retry Count**: 5

Here are some of the maximum counts for the respective fields:

- **Router Firmware Upload Count**: 48
- **Router Fimware Install Count**: 48
- **Router Firmware Upload Retry Count**: 100

Use Cases For Manage Router Firmware Upgrades

- Manage firmware upgrades and installations for a large fleet of routers across multiple locations, ensuring all devices are up to date.
- Minimize configuration errors that might occur with manual property file edits, ensuring smoother and more reliable firmware management.

Configure Router Firmware Upgrades Using Cisco IoT FND

Here are the instructions to configure the router firmware upgrades using Cisco IoT FND:

1. From the Cisco IoT FND Menubar, choose **ADMIN** > **Server Settings** > **Property Settings**.
2. Enter the number of routers in the **Router Firmware Upload Count** field on which a firmware file is uploaded to the device repository. For example, 48
3. Enter the number of routers in the **Router Firmware Install Count** field on which you want to apply the uploaded firmware to the routers for upgrading them. For example, 45
4. Enter the number of attempts that you want Cisco IoT FND to try when there's a failure of firmware uploads in the **Router Firmware Upload Retry Count** field. For example, 5

Manage Firmware Upgrade Properties For A Router Group

Manage Firmware Upgrade Properties For A Router Group

Feature Name	Release	Description
Manage Firmware Upgrade Properties For A Router Group	Cisco IoT FND Release 5.0	Cisco IoT FND includes a **Router Firmware Upload Retry Count** in the **Firmware Update** page. Customize the retry count at the router group level, allowing for tailored firmware update strategies for specific groups of routers.

Information About Manage Firmware Upgrade Properties For A Router Group

Cisco IoT FND introduces a **Router Firmware Upload Retry Count** field in the **Firmware Update** page. You can customize the retry count at the router group level, allowing you to implement tailored firmware upgrade strategies for specific groups of routers. The firmware upload retry count is not defined by default at the group level. In case you don't define the upload retry count, the global value in the **Property Settings** page is applied to the groups as well.

Benefits Of Manage Firmware Upgrade Properties For A Router Group

- You can customize the retry count for firmware uploads at both global and router group levels, providing greater control over the update process.
- You can enhance the reliability of firmware updates, reducing the likelihood of failed uploads due to network issues or other disruptions.
- Different groups of routers can have tailored firmware update strategies, allowing for more efficient management based on specific network conditions or requirements.

Restrictions For Manage Firmware Upgrade Properties For A Router Group

The default value of **Router Firmware Upload Retry Count** is 5 and the maximum value is 100.

Configure Firmware Upgrade Properties For A Router Group

Here are the steps to configure firmware upload retry count using Cisco IoT FND:

1. From the Cisco IoT FND menubar, choose **CONFIG** > **Firmware Update**.
2. Select a router group from the **Firmware Groups** list.
3. Click **Group Properties**.
4. Enter a value between 0 to 100 in the **Router Firmware Upload Retry Count**.

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.

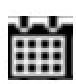
Note RME devices can report BL/Boot Loader image types to IoT FND, but IoT FND cannot upload boot loader images to devices.

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 74: 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: • 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.  • Set as Backup —Set the firmware backup image by selecting the clock icon with reverse arrow.  See Setting the Installation Schedule, on page 373 for complete steps.

Set a Firmware Backup Image

To set an image as a firmware image backup:

Procedure

Step 1 Click the Set as Backup button. (See the icon in the Actions summary in Table 74: Image Information Displayed by IoT FND, on page 372).

Step 2 Click **Yes** to confirm backup.

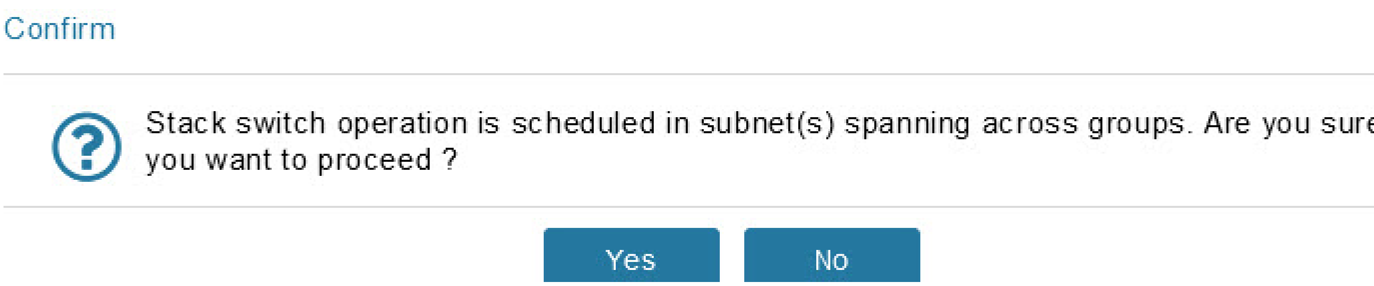
Setting the Installation Schedule

To set the installation schedule for an image:

Procedure

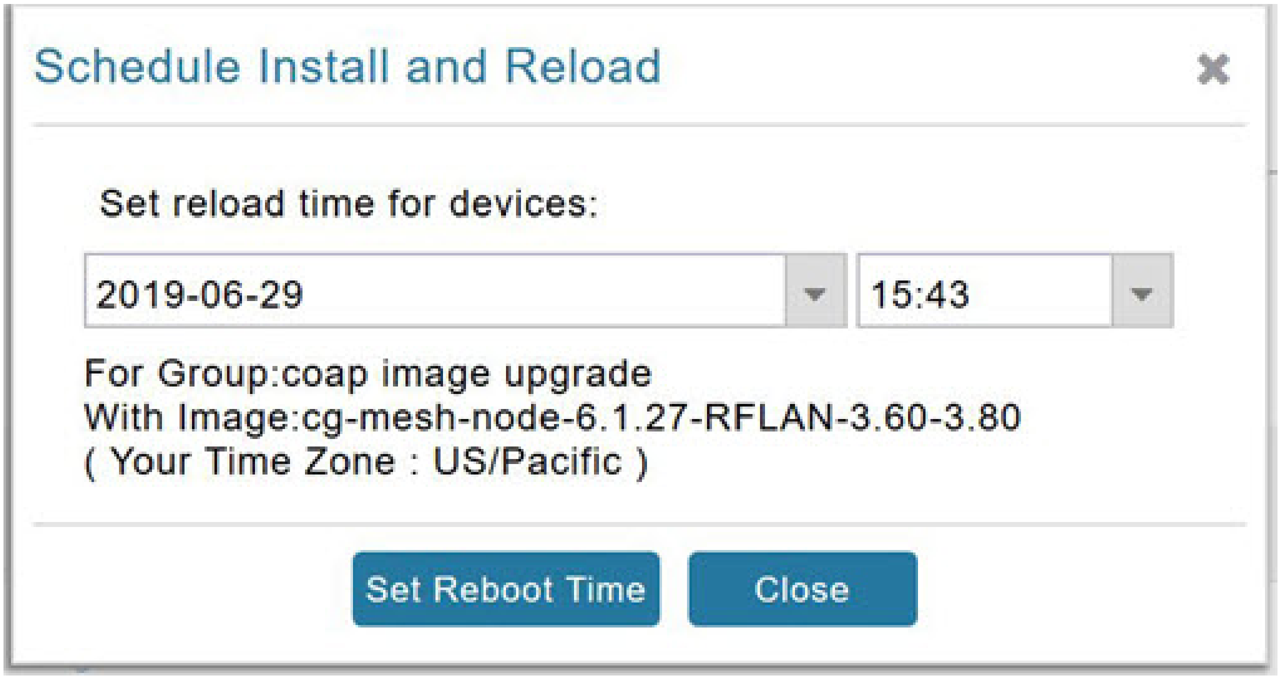
Step 1 Click the **Schedule Install and Reload** button (Calendar icon). For more information, see Table 74: Image Information Displayed by IoT FND, on page 372.

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 27: 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).

Procedure

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 28: CONFIG > FIRMWARE UPDATE

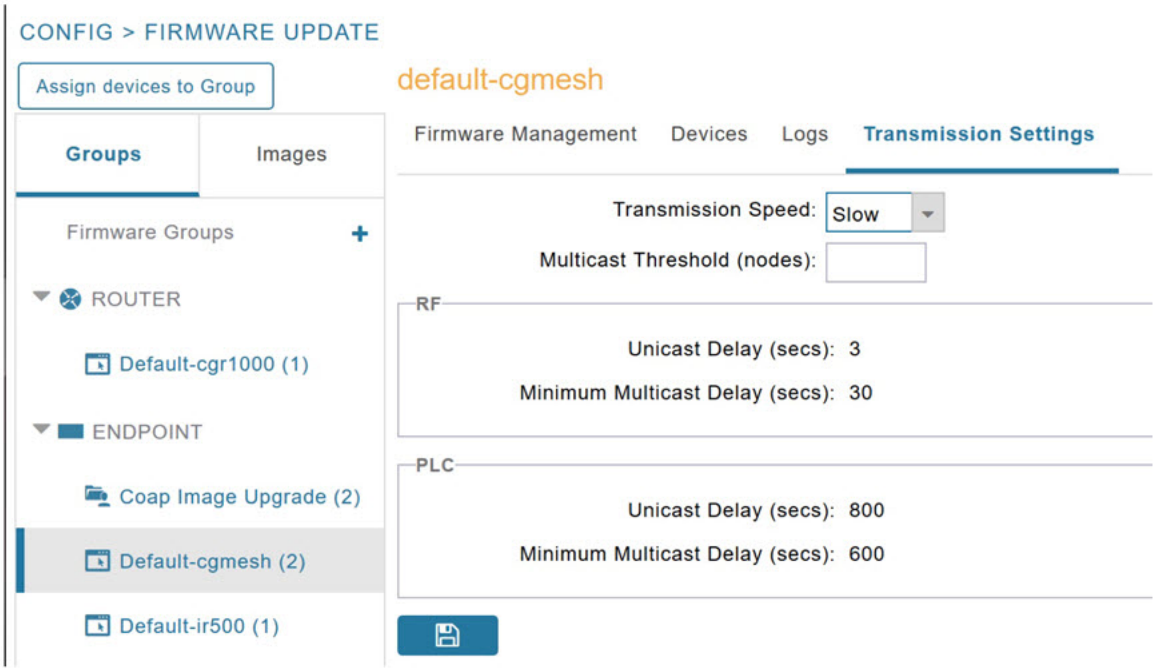


Table 75: Definitions of variables seen on CONFIG > FIRMWARE UPDATE Transmissions Settings page

Item	Description
Minimum Multicast Delay (seconds)	Time between subsequent blocks when sending multi-cast messages/blocks/packets to a node.
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:

Procedure

Step 1 Choose **CONFIG** > **FIRMWARE UPDATE**.

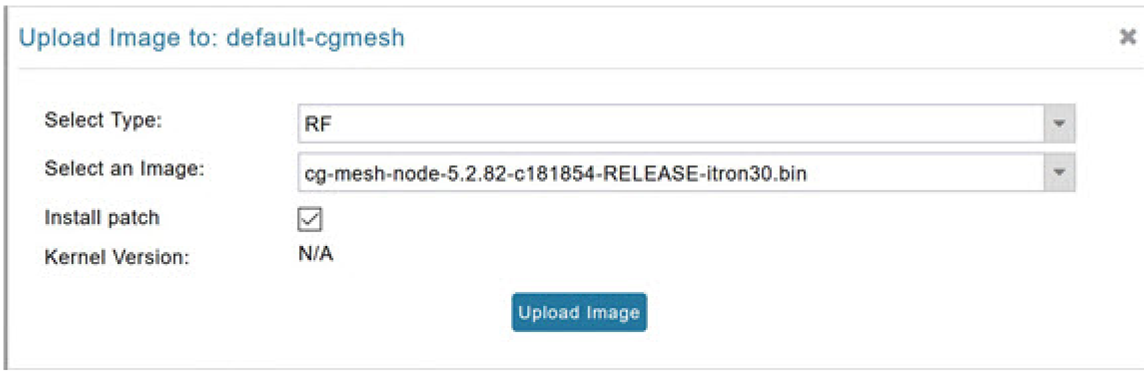
Step 2 Click the **Groups** tab (left-pane).

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 29: Check Install Patch Item to ONLY Install the Patch Rather than the Full Image, on page 376).

Figure 29: 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 30: Firmware Update - Percentage Complete (top-portion of screen), on page 376 and Figure 31: Firmware Update - Upload Summary (bottom-portion of screen), on page 377.

Note
Click the Sync Membership button to ensure that FND and the member endpoint firmware group information are the same.

Figure 30: Firmware Update - Percentage Complete (top-portion of screen)

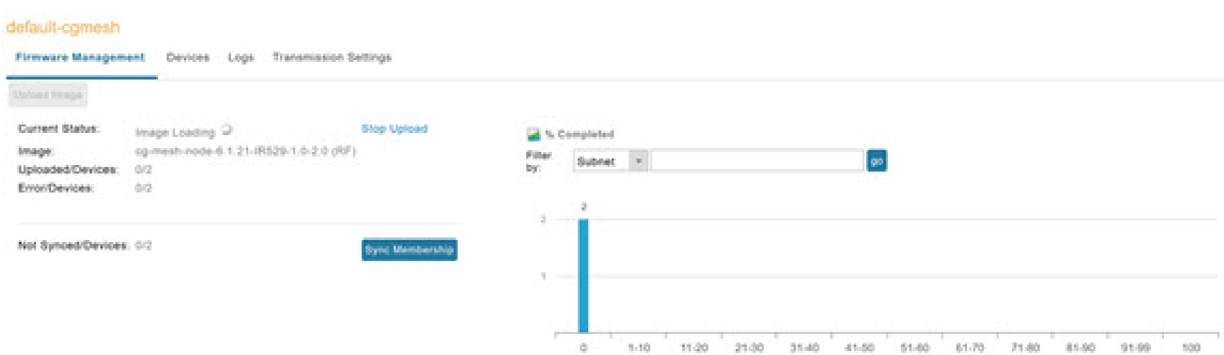
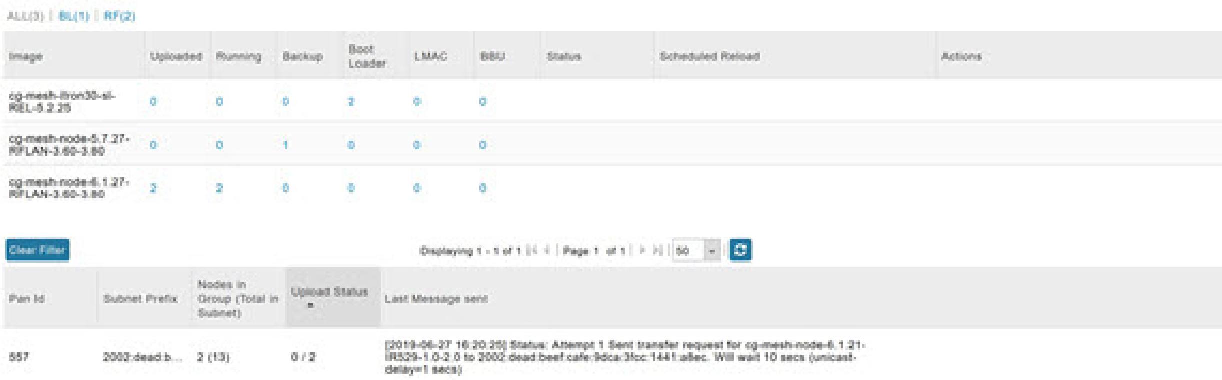


Figure 31: Firmware Update - Upload Summary (bottom-portion of screen)



Uploading a Firmware Image to FND

To upload a firmware image to mesh endpoint group members:

Procedure

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.

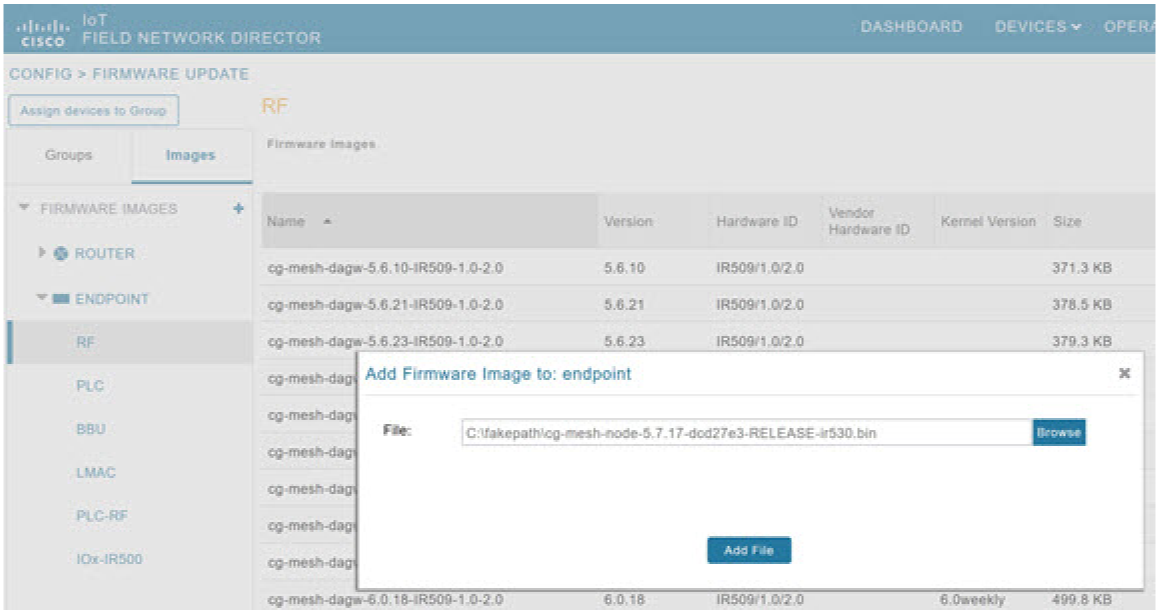
Step 5 Browse and click on **Add file**.

IoT FND can upload the following image types to ENDPOINT devices as shown in the table below:

Table 76: Firmware Images for Endpoints

Image Type	Description
RF	For endpoints with RF radio only.
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 32: 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.

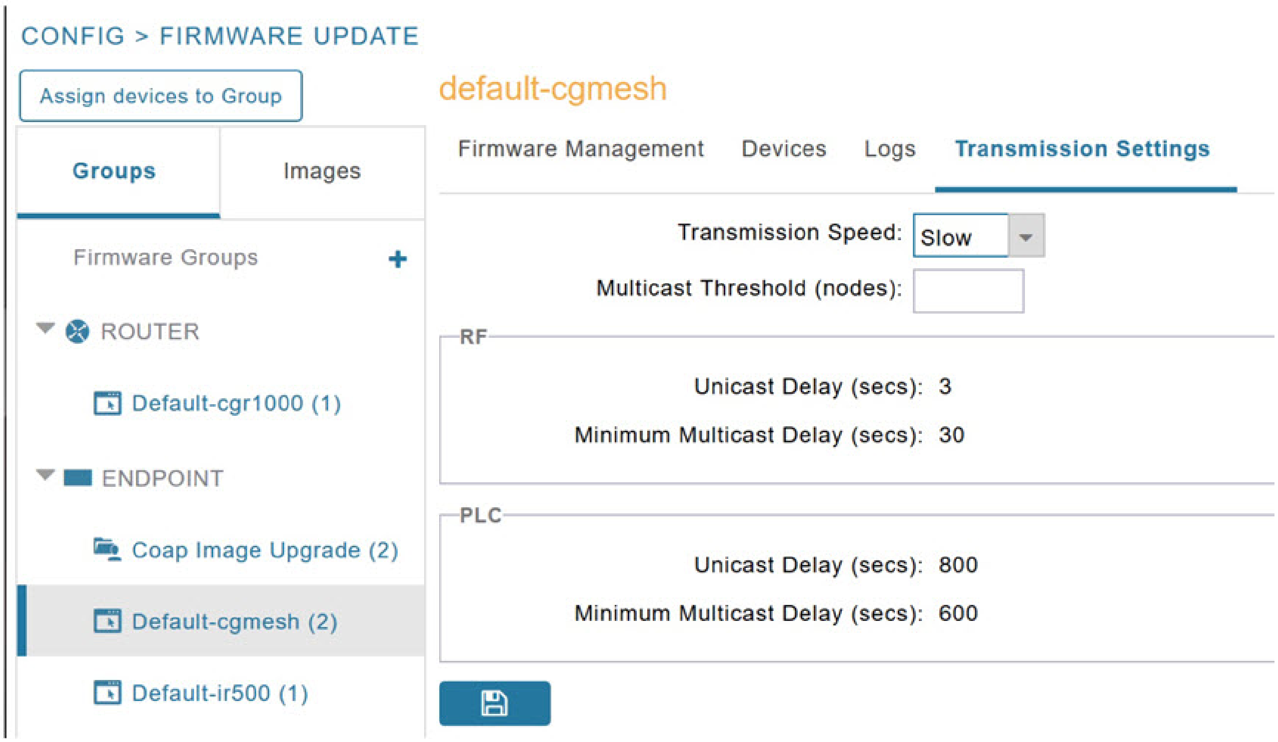
To modify the display of firmware management page:

Procedure

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 33: CONFIG > FIRMWARE UPDATE



Viewing Mesh Device Firmware Image Upload Logs

To view the mesh device firmware image upload logs:

Procedure

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 30: Firmware Update - Percentage Complete (top-portion of screen), on page 376
.

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 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 router will upgrade using the firmware version you define as the autonomous firmware.

To define the Autonomous Firmware for an IR829 router:

Procedure

Step 1 Choose **CONFIG** > **DEVICE CONFIGURATION**.

Step 2 Select the desired router: Default-ir800 (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.

Enhancement to Firmware Update Page for Device Status Types

Table 77: Feature History

Feature Name	Release Information	Description
Enhancement to Firmware Update Page for Device Status Types	Cisco IoT FND Release 5.0	Cisco IoT FND includes two additional device statuses in the **Firmware Update** page: **Down Devices** and **All Devices**. Use the **Down Devices** link to filter the down devices search and **All Devices** displays the count of total devices in the firmware group of routers.

Enhancement to Firmware Update Page for Device Status Types

Starting from Cisco IoT FND 5.0 release, the **Firmware Update** page includes a new device status count link called **Down Devices** which is added for routers. The status field is used in identifying and calculating the count of **All Devices**, **Written Devices**, **Error Devices** and **Down Devices** within a given firmware group.

The **Down Devices** link is used to filter the search for all the down devices in the firmware group of routers. A device is considered down when the status appears with a red cross icon, indicating it is offline. The **All Devices** count displays the total number of devices in the firmware group of routers.

Note The **Down Devices**, **Error Devices** and **Written Devices** status counts are hyperlinked for filtering the search based to the device state.

Benefits of Using Device Status Count Links

Device status count links help in filtering the search for devices based on their status types. These links also help in determining the count of the devices in each state.

Accessing Device Status Links

In the **Firmware Update** page click the link for each device status count to view the devices based on their state.

Avoid Firmware Upgrade Overlap with Certificate Auto Renewal

Problem

As part of the reload process, the cellular modem is powered off during firmware upgrade. If there is an Embedded Event Manager (EEM) script which is in the running configuration, which executes the write memory operation after getting a renewed certificate, then it saves the startup configuration with the cellular modem turned off. This results in an outage after router reload. Once the router reloads and comes up again, due to cellular modem which is in the powered off state, the router cannot register with Cisco IoT FND.

Solution

There are two steps for upgrade:

- Firmware upload.
- Firmware installation.

In case of an overlapping duration between certificate auto renewal and firmware installation, ensure that the firmware installation is initiated only after the certificates are successfully auto renewed for routers. Also, select only those routers which have already completed the certificate auto renewal for the firmware upgrade group.

Note This is applicable only for firmware installation as firmware upload has no such restriction.

Identifying and Avoiding Routers for Firmware Upgrade

To identify and avoid selecting the routers which have certificate expiration, follow the given step:

1. From the Cisco IoT FND menu bar, click **OPERATIONS** > **Issues**.

Note Avoid selecting any router which appears in the **Issues** table with certification expiry message.

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.

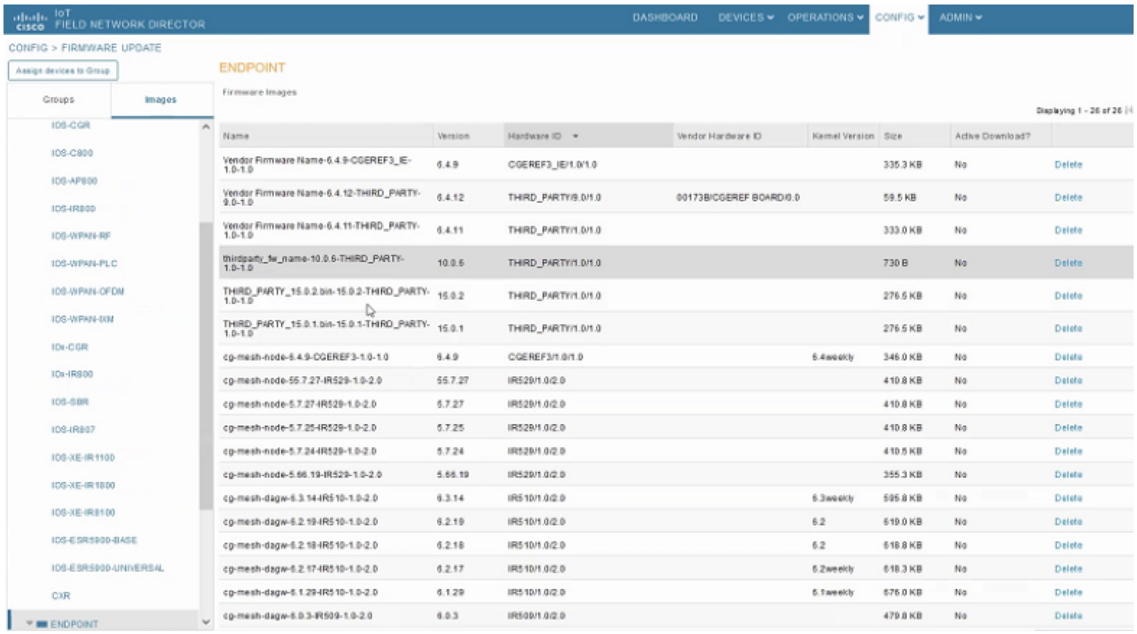
When you add routers or RMEs to IoT FND, the application sorts the devices into the corresponding default firmware group: default-<*router*> or default-cgmesh. Use these groups to upload and install firmware images on member devices. Add firmware groups to manage custom sets of devices. You can assign 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 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 34: CONFIG > FIRMWARE UPDATE



521620

Tip At the Firmware Update page, click the Error/Devices link (not shown) in the **Firmware Update** page to apply a filter.

Click **Clear Filter** to revert to an unfiltered view of the selected device group.

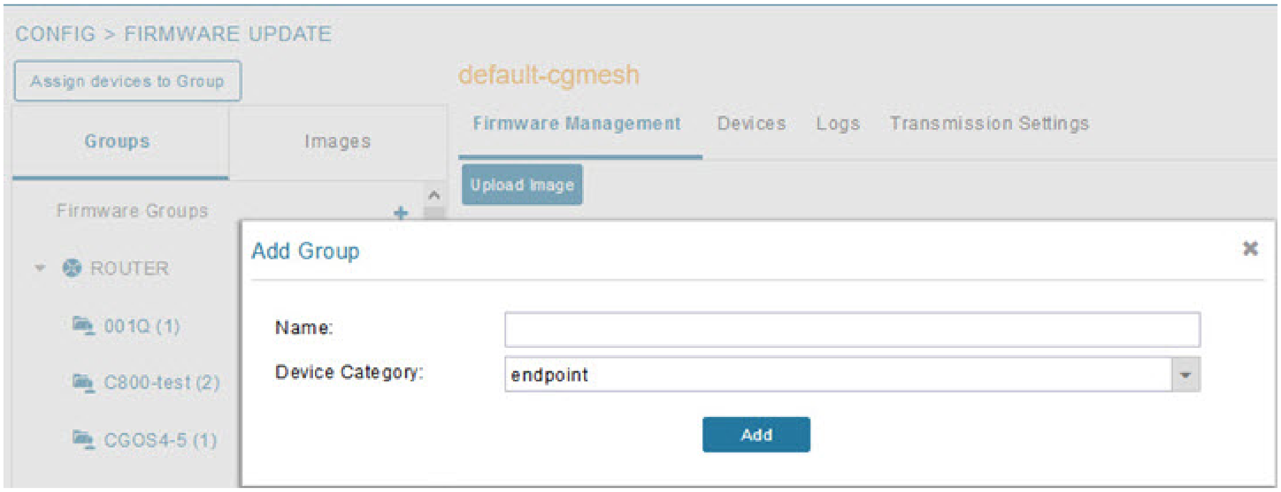
Adding Firmware Groups

To add a firmware group:

Procedure

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-ir500
- Default-ir800
- Default-cgmesh

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 385.

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:

Procedure

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`
`CGR1120/k9+JS1`
`CGR1120/k9+JS2`
`CGR1120/k9+JS3`
	`eid`
	`00078108003c1e07`
	`00078108003C210b`
		`eid`
		`ir800`

***EID* only for ISR 800s:**	***EID* only for IR500s:**	***EID* only for IC3000**

`eid`
`C819HGW-S-A-K9+FTX174685V0`
`C819HGW-S-A-K9+FTX174686V0`
`C819HGW-S-A-K9+FTX174687V0`
	`eid`
	`da1`
	`da2`
	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:

Procedure

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:

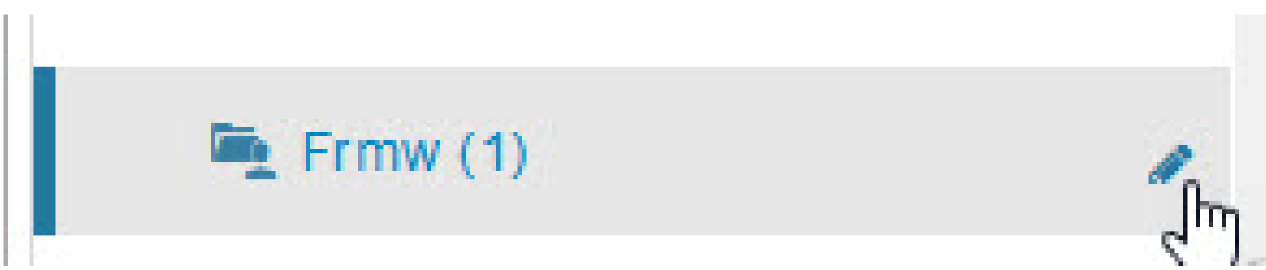
Procedure

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:

Procedure

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:

Procedure

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.

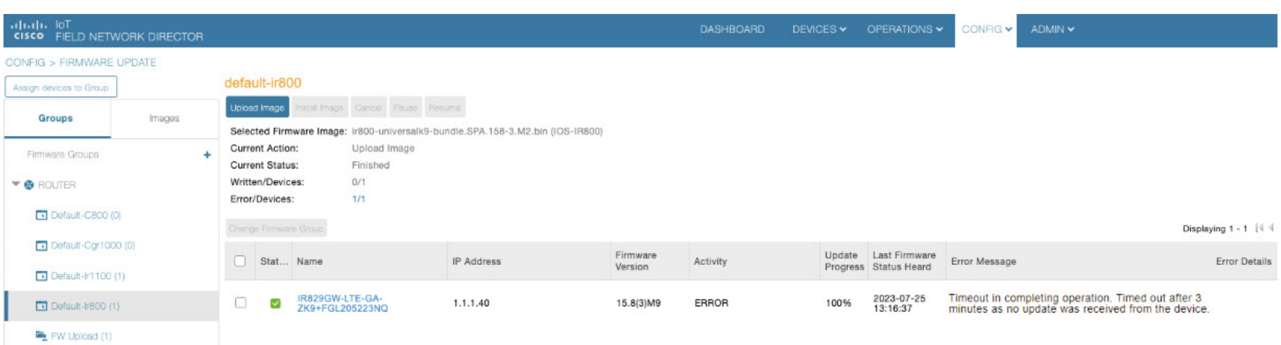
Note
If you restart IoT FND during the image installation process, IoT FND restarts the firmware installation operations that were running prior to IoT FND going offline.

You can pause or stop the installation operation as described in:

- Stopping Firmware Image Installation, on page 395
- Pausing and Resuming Router Firmware Image Installation, on page 394

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 Cisco IoT FND

Before you can upload and install a firmware image on a device, add the image file (as a zip archive) to Cisco IoT FND. Cisco IoT FND stores the image in its database.

Note Do not unzip the image file. Cisco IoT FND unzips the file.

To add a firmware image to Cisco IoT FND, from the Cisco IoT home page:

Procedure

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 391.

Uploading a Firmware Image to a Router Group

Table 78: Feature History

Feature Name	Release Information	Description
Bootflash Space Cleanup	Cisco IoT FND Release 5.0	Check the **Remove unused firmware images from bootflash** check box to remove unused firmware bin files from the bootflash when Cisco IoT FND uploads the image to the router. The check box is enabled for the following devices running Cisco IOS-XE: • Cisco Catalyst IR1100 • Cisco Catalyst IR8100 • Cisco Catalyst IR1800

Uploading a Firmware Image to a Router Group

When you upload a firmware image to router firmware group members, Cisco 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 for IOS devices and 700 MB for IOS-XE devices.

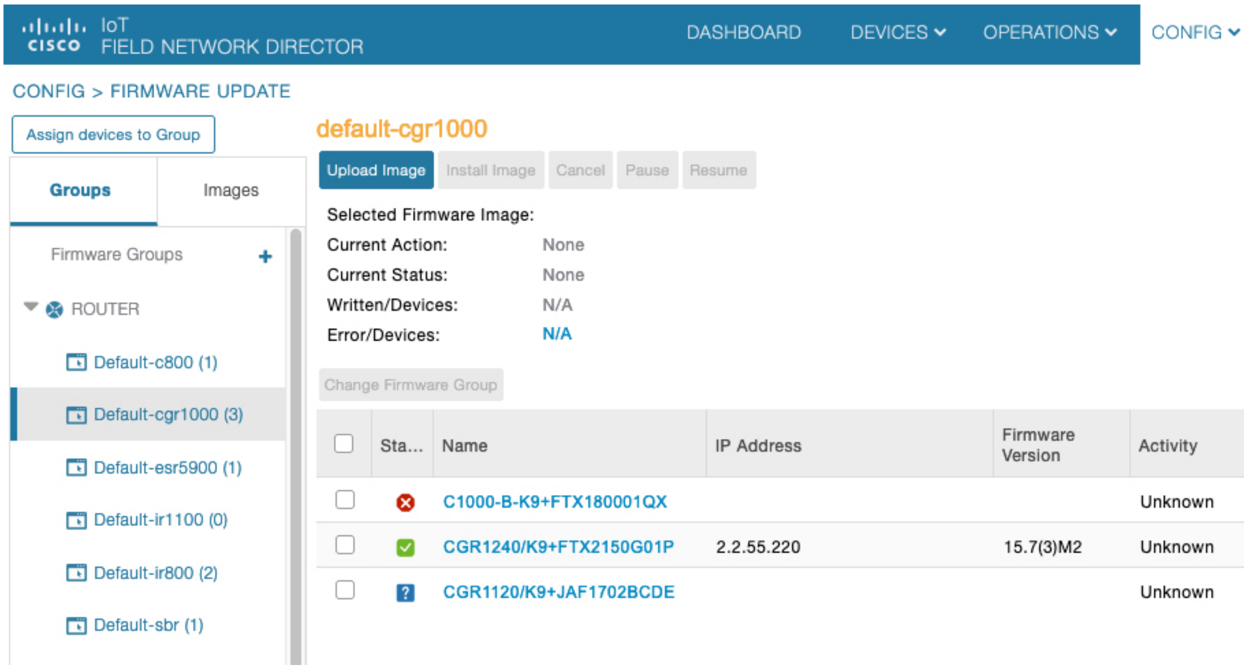
Note If there is not enough disk space on the router for the firmware image, the Cisco IoT FND initiates disk cleanup process on the router and removes unused files in the .../managed/images directory that is not currently running or referenced in the before-tunnel-config, before-registration-config, express-setup-config, and factory-config files for IOS CGRs, sequentially, until there is enough disk space to upload the new image.

To upload a firmware image to router group members from the Cisco IoT home page:

Procedure

Step 1 Select **CONFIG** > **FIRMWARE UPDATE** > **Groups**.

Figure 35: Updating Firmware for a CGR1000



Step 2 In the Groups pane, select the router firmware group that you want to update.

Cisco IoT FND displays the firmware image type applicable to the router.

Step 3 Click **Upload Image** to open the entry panel.

Step 4 From the **Select Type:** drop-down menu, choose the firmware type for your device.

Table 79: Cisco IoT FND displays the firmware image type

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-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.

Image	Type	Applicable Devices
IOx-CGR	cgr1000-ioxvm	Cisco IOS-CGR
IOx-IR800	IR800	Cisco 800 Series ISRs.
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
IOT-FND-IC3000	IC3000	Cisco IC3000 Gateway

Step 5 From the **Select an Image:** drop-down menu, choose the firmware bundle to upload.

Note

- Starting from Cisco IoT FND 5.0 release, for Cisco IOS-XE images, a new checkbox option called **Remove unused firmware images from bootflash** is introduced. While uploading a firmware image to a router, if there is no space left for the image upload, then checking the **Remove unused firmware images from bootflash** checkbox, clears all the .bin files from the bootflash folder, except for those images which are configured in bootparam and bootflash running images. This ensures there is enough disk space left for the new upload.
- Bootflash cleanup is supported by Cisco Catalyst IR1100, IR8100 and IR1800 device types in Cisco IOS-XE.
- Before you upload the image, the system displays a confirmation message before removing firmware images from the bootflash.
- Cisco IoT FND skips cleaning the bootparam image only if it is configured with the bootflash directory. In case the bootparam image is configured with the flash directory, it cleans up the image.

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):

- Remove unused firmware images from bootflash (Cisco IOS-XE Cisco Catalyst IR1100, IR8100 and IR1800).
- 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 6 Click **Upload Image**.

Step 7 Click **OK**.

Cisco IoT FND starts the upload process. After the image uploads, install the image as described in Installing a Firmware Image , on page 388.

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:

Procedure

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:

Procedure

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:

Procedure

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:

Procedure

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:

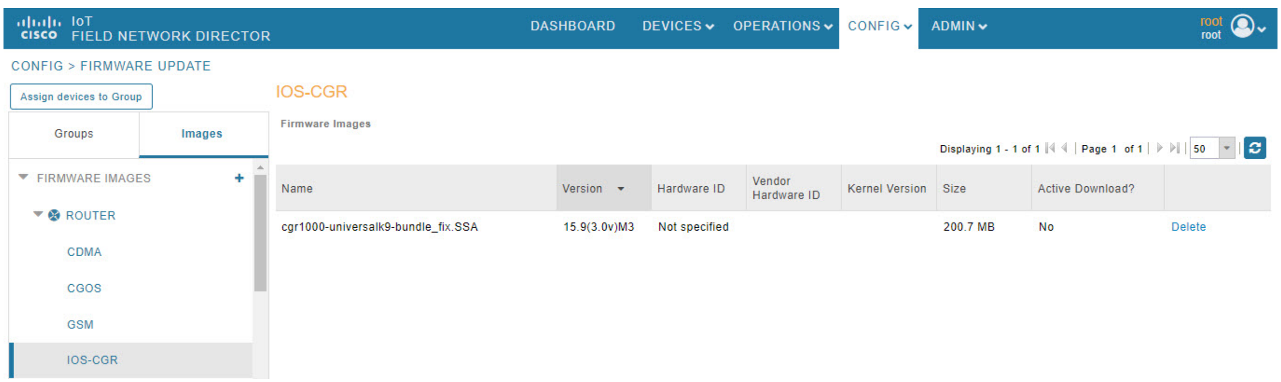
Procedure

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 36: CONFIG > FIRMWARE UPDATE > Image



Search Firmware Updates

Search Firmware Updates

Table 80: Feature History

Feature Name	Release	Description
Search Firmware Updates	Cisco IoT FND Release 5.0	Search through the existing firmware updates using the filters introduced in this release. This feature aims to make the firmware updates page searchable.

Information About Search Firmware Updates

Starting from Cisco IoT FND Release 5.0, search through the firmware updates in the **Firmware Update** page. Use the exhaustive filters provided along with the search option to narrow down your search.

Benefits of Search Firmware Updates

- Quickly locate specific devices, data, or configurations, and reduce the time spent navigating through the system.
- As the network grows, the functionality can help you handle larger datasets, ensuring that performance and usability remain consistent.

Perform a Search Using Search Firmware Updates

1. From the Cisco IoT FND menubar, choose **CONFIG** > **Firmware Updates**.
2. In the default page, perform a search using the search bar. Click **Show Filter**.
3. In the Filters pane, click the first drop-down box and choose from the following options:

Option	Description
Status	Choose Status as a search criteria if you want to filter the devices based on their statuses. Here are the statuses that you can choose from: • blocked • bootstrapped • bootstrapping • down • outage • outofservice • registering • restored • unheard • unmanaged • unsupported • up
Name	Type in the name of the device that you are looking for in the text box.

Option	Description
EID	Type the EID of the device that you are looking for in the text box.
IP Address	Enter the IP address of the device that you are looking for in the text box.
Firmware Version	Use the firmware version of the device to filter the devices running a particular firmware version.
Activity	Choose Activity as a filter if you want to filter out devices based on their activity. Here are some of the device activities: • Unknown • Partially Uploaded • Awaiting Upload • Skipped • Error • Fully Uploaded **Note** You can use any VM on which Cisco IoT FND is installed to monitor all the activities.
Update Progress	You can filter the devices that are going through a firmware update process. Choose **between** in the second drop-down box and enter the firmware upgrade versions in the text boxes provided.
Last Firmware Status Heard	Use this filter if you want to filter devices based on the date and time they broadcasted their firware update status.

4. Click + button to populate the search bar.
5. Click the **Search** icon to perform a search based on the filters.

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 399.

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.

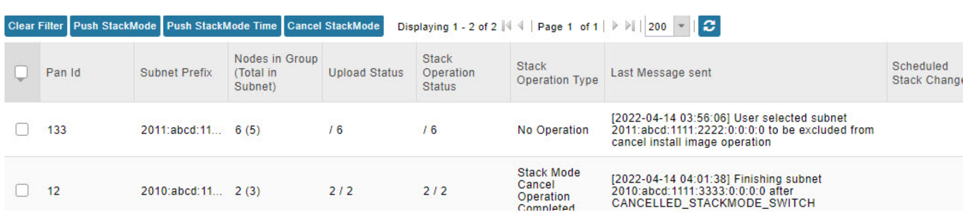
Table 81: Feature History

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 399
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:

Procedure

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 82: PAN ID Status

Field	Description
Stack Operation Type Column	Displays the following states for the push stack mode operation: • **Stack Mode Push Initiated** — Denotes the initiation of the stack mode operation. • **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 404

a) In the **Stack Mode Push Initiated** state, the devices in the selected PAN ID are validated based on the following scenarios:

Table 83: 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.
• If the firmware version is lower than 6.2 MR, then an error message appears.
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.
• 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>
<tr><td rowspan="2">Stack mode configuration.</td><td>Checks if all devices in the selected PAN ID received the stack mode configuration.
• Some devices in the selected PAN ID fail to receive the configuration.</td><td>• Push stack mode again for the selected PAN ID.
or
• Remove the devices that are in Down state from FND and again push stack mode for the remaining devices in the PAN ID.</td></tr>
<tr><td>• 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.</td><td>Scheduling Devices for Wi-SUN Stack Switch, on page 401
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.</td></tr>
</table>

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 399

To schedule devices for Wi-SUN stack switch:

Procedure

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 84: PAN ID Status

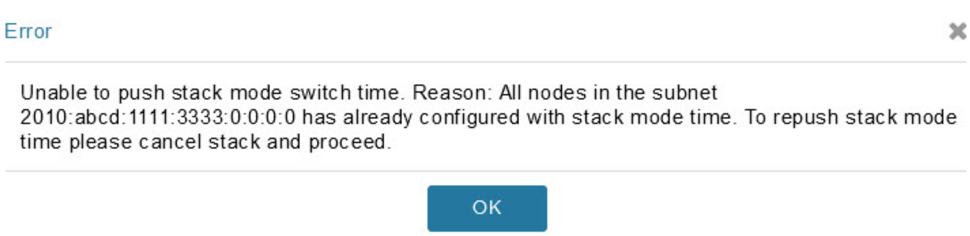
Field	Description
Stack Operation Type Column	Displays the following states for the stack mode time operation: • **Stack Switch Time Push Initiated** — Denotes the scheduling of the stack switch time operation. • **Stack Switch Time Push Completed** — Denotes the completion of the stack switch time operation.
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 404.

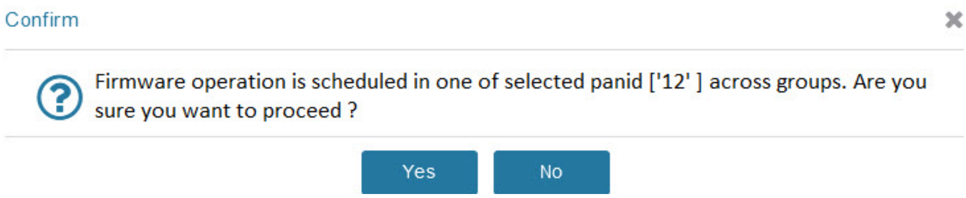
Step 4 Click **Yes** to confirm the stack switching operation.

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:

Procedure

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 85: PAN ID Status

Field	Description
Stack Operation Type Column	Displays the following states for the cancel stack mode operation: • **Stack Mode Cancel Initiated** — Denotes the initiation of the stack mode cancellation process. • **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 404.

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

Procedure

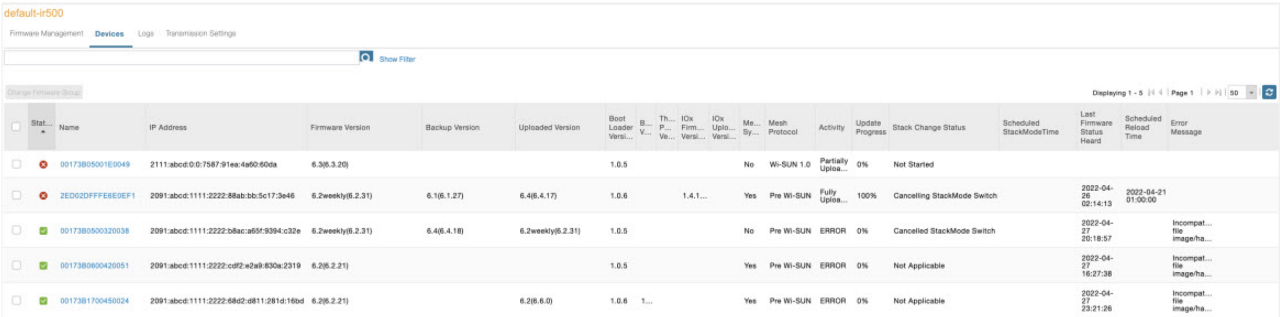
Step 1 Choose **CONFIG** > **FIRMWARE UPDATE** > **Groups** tab.

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 86: 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.
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:

Procedure

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.

Firmware Management Devices **Logs** Transmission Settings

Displaying 1 - 50 of 7987 | Page 1 of 160

	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 :

Procedure

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']

Upgrading Firmware Image during Bootstrapping

During bootstrapping, you can enter a different image if the installed image at manufacturing is inappropriate. This is supported for IR1800 and IR8100 devices from the versions 17.13.01 and above. Plug and Play (PnP) must be supported on these devices.

Note Ensure that IR8100 device has the network-essentials license to register the device to IoT FND.

PnP Device Information service retrieves current firmware version on the device and the PnP ImageInstall service performs the image installation. The CGNA 'image-retrieve' service transfers the image file from IoT FND to router.

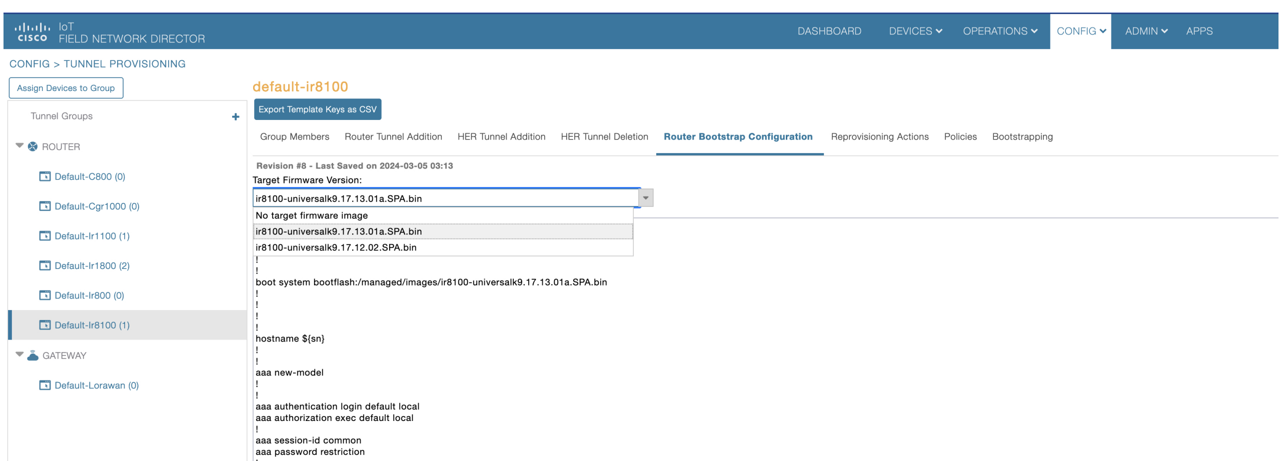
Procedure

Step 1 Set the firmware-update-bootstrap property in cgms.properties to 'true'.

Step 2 On the Tunnel Provisioning Page, navigate to **CONFIG** > **TUNNEL PROVISIONING** > **ROUTER BOOTSTRAP CONFIGURATION**.

Step 3 Select the device group in the left pane, choose the Target Firmware Version from the drop down that lists the images in IoT FND, and click **Save**.

The PnP workflow configures the device to load the new image upon the next reload by executing the boot system command. The configuration changes are saved on the device. The PnP reload happens and sends a message to the PnP server after which an event is generated denoting image installation.



Note
The PnP workflow supports device upgrade only if the target image version is higher than the running (current) image version.

If the target image runs the same or lower version, then the device upgrade is skipped during the PnP workflow.

During PNP, you also have the option to skip the firmware upgrade and proceed with PNP if the source operating system on these devices is found to be unreliable. Enter the image versions as comma separated values in **pnp-skip-update-ios-xe-fw-versions** property in cgms.properties file. This property is applicable for all IR1100, IR1800, and IR8100 devices. For more information, see Skipping Firmware Upgrades during PNP, on page 408.

Skipping Firmware Upgrades during PNP

During Zero Touch Deployment (ZTD), certain scenarios may arise where Plug-and-Play (PNP) devices come bundled with software that exhibits instability or issues. If the source operating system (OS) on these devices is found to be unreliable, it can potentially disrupt the entire registration process. In such instances, during the PNP process, you can skip the firmware upgrade step while allowing PNP to proceed seamlessly. However, you can upgrade the firmware once the PNP process is complete.

To perform a PNP with firmware upgrade skip:

Procedure

Step 1 Set the image versions in pnp-skip-update-ir1100-fw-versions property in cgms.properties file.

Note
The pnp-skip-update-ir1100-fw-versions property is applicable for IOS-XE routers only.

Step 2 Set the image versions in pnp-skip-update-ios-xe-fw-versions property in cgms.properties file.

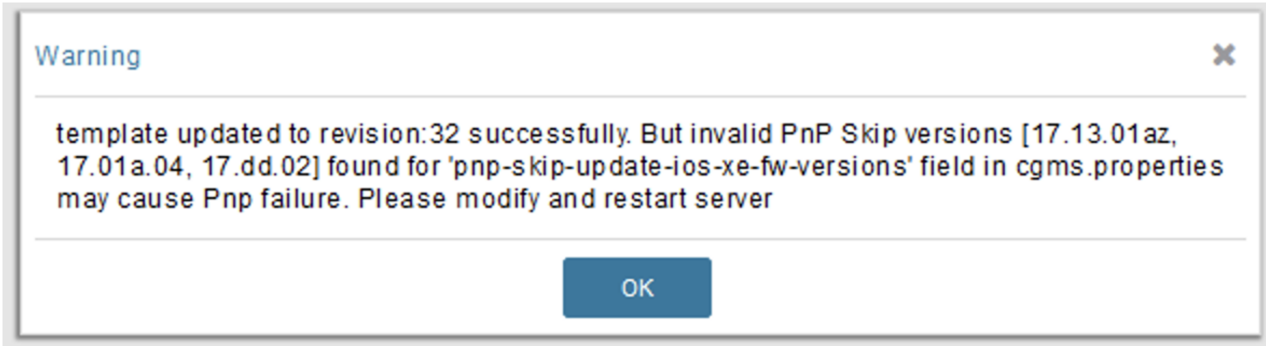
Note
The pnp-skip-update-ios-xe-fw-versions property is applicable for IOS-XE routers only.

Step 3 Choose **CONFIG** > **Tunnel Provisioning**. Select the router group for which you intend to execute the PNP process.

Step 4 Click **Router Bootstrap Configuration** tab.

Step 5 Under Target Firmware Version, specify the image version you want to skip and click **Save**.

The template is saved. However upon performing PNP, during router bootstrap configuration, a warning popup appears if any invalid entry is found. In that case, modify the field and restart server.



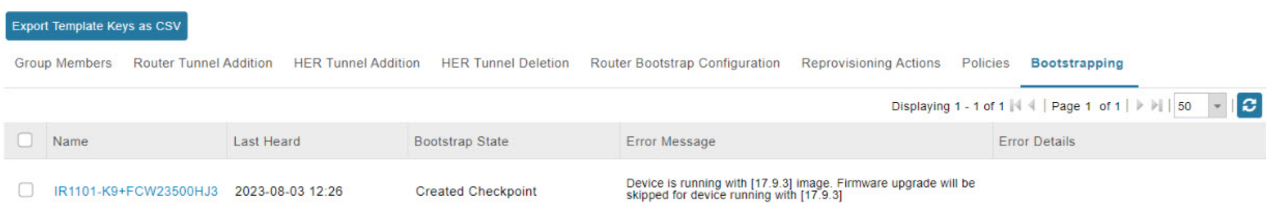
If firmware install is skipped during PnP process, the log details are stored in server.log file. The sample INFO log is shown below:

```
Aug 03 2023 19:24:26.854 +0000: %IOTFND-6-UNSPECIFIED:
 %[ch=WorkResponseHandler][eid=IR1101-K9+FCW23500HJ3][ip=1.1.1.121]
[sev=INFO][tid=tunnelProvJetty-67]: Retrieved device image version
[17.9.3] is present in PnP firmware image skip list. Firmware image update
 during PnP process will be skipped.
```

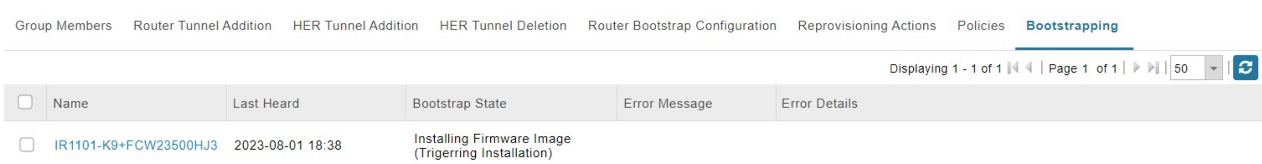
Note

In order to upgrade the device with the latest firmware version, skip entering the current image version in cgms.properties and proceed with PNP.

Step 6 Navigate to the Bootstrapping tab where the Error Message field is updated though the PNP progresses as is.



The Bootstrapping tab shows the status of the PNP under the Bootstrap State field.



Update Target Firmware Versions For All Users

In the Cisco IoT FND Release 4.12.x and earlier releases, when you change the target firmware versions in the **Router Bootstrap Configuration** tab as a root user. The target firmware changes don't reflect in Cisco IoT FND when you're logged in as a different user with specific roles assigned to you by the root user. For more information on managing roles and permissions see, Managing Roles and Permissions.

Starting from Cisco IoT FND Release 5.0, when the root user changes the target firmware version, the changes reflects for all the other associated Cisco IoT FND users.

CHAPTER 8

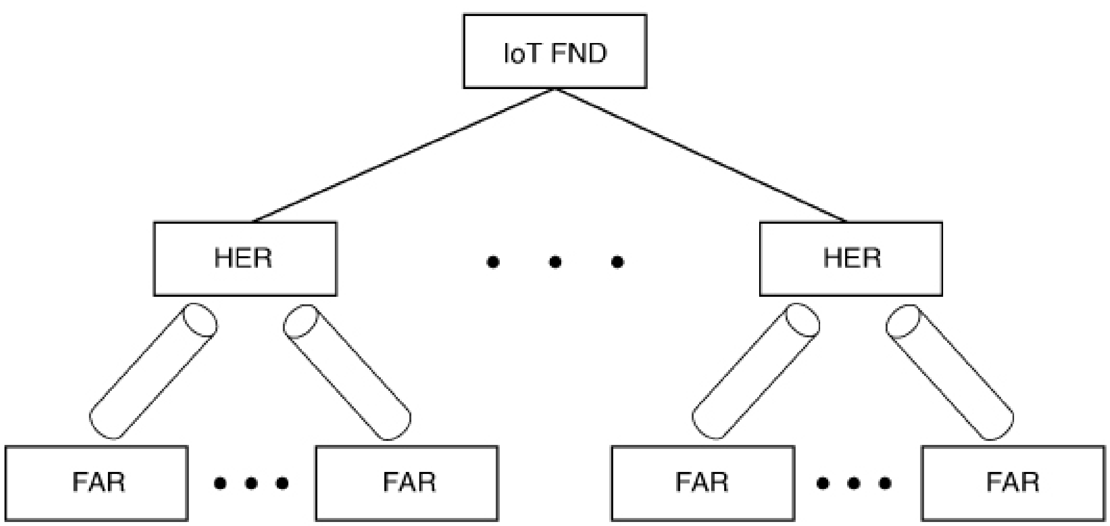
Managing Tunnel Provisioning

This section describes how to configure IoT FND for tunnel provisioning and how to manage and monitor tunnels connecting FARs (CGRs) and 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 37: 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. 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. 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 417 **Note** In IoT FND 4.6.1 release and greater you can use the “Tunnel Provisioning Optimization” feature that allows the following: 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. 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. 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. 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 424
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. 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 412

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>`

Procedure

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.

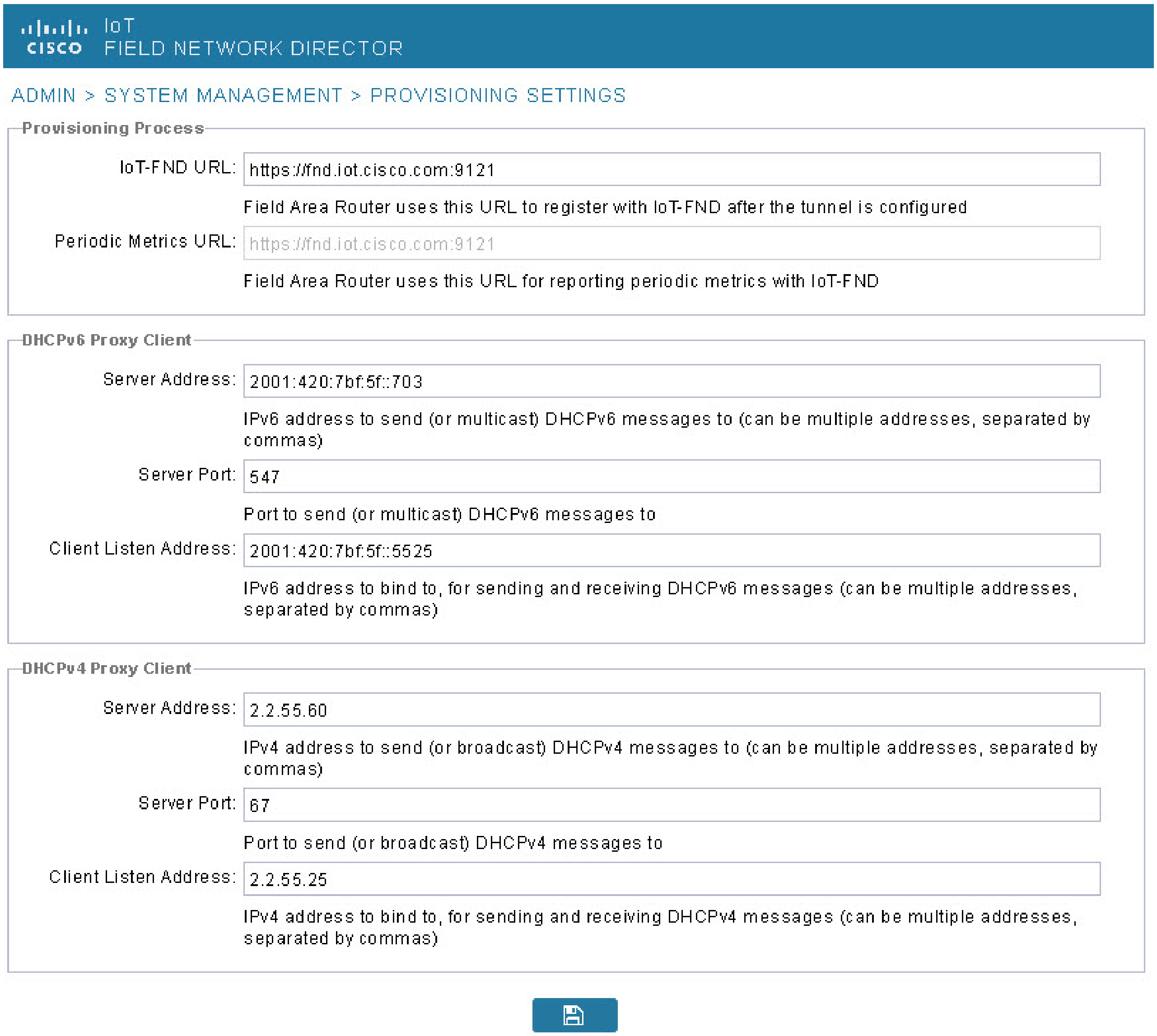
Step 4 For Cisco IOS CGRs, the default templates configure the CGR to use FlexVPN. The FlexVPN client is configured on the CGR that will contact the HER and ask for a FlexVPN tunnel to be dynamically constructed. This is how the HER dynamically adds a new tunnel endpoint interface for the CGR.

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.

Autosync of CGMS Properties Files

Feature Name	Release	Description
Autosync of CGMS Properties Files	Cisco IoT FND Release 5.0	Cisco IoT FND ensures that any changes made to the CGMS properties file, whether inside or outside the container, are automatically mirrored in the corresponding file. This synchronization maintains consistency across configurations, reducing the risk of errors and ensuring seamless application performance.

Information About Autosync of CGMS Properties Files

Cisco IoT FND facilitates the seamless synchronization of the cgms properties files located both inside and outside the container. This feature ensures that any modifications made to one file is auto reflected in the other, maintaining consistency and simplifying configuration management.

Note When you restart the CGMS service or the Cisco IoT FND container, the CGMS property files inside and outside of the docker are in-sync with each other.

Prerequisites of Autosync of CGMS Properties Files

Your Cisco IoT FND should run the release Cisco IoT FND Release 5.0 and later releases.

Benefits of Autosync of CGMS Properties Files

- Autosync of cgms properties files feature ensures that both the internal and external .cgms properties files are always in sync, reducing the risk of configuration mismatches.
- Minimizes the potential for human error by autosyncing changes in the cgms properties files, which helps maintain reliable system performance.
- Enhances the overall reliability of Cisco IoT FND and ensures that all components operate with the same configuration settings.

Configure the CGMS Properties Files

Here are the instructions to making changes to the CGMS properties files:

1. Log in to Cisco IoT FND server using the SSH command.

2. Navigate to /opt/fnd/data directory using the cd command.

```
[root@iot-fnd ~]# cd /opt/fnd/data/
```

3. Use `ls -lrth` command to view all the properties.

```
[root@iot-fnd data]# ls -lrth
```

Here's an example output:

```
total 24K
-rw-------. 1 root root 1.3K Nov  7 05:15 userPropertyTypes.xml
-rw-r--r--. 1 root root  518 Nov  7 06:22 fnd_psk.keystore
-rw-------. 1 root root 1.5K Nov  8 05:06 cisco-sudi-ca.pem
-rw-------. 1 root root 4.3K Nov  8 05:06 cgms_keystore.selfsigned
-rwxrwxrwx. 1 root root  278 Nov 11 10:40 cgms.properties
[root@iot-fnd data]# docker exec -i -t fnd-container /bin/bash
[root@fnd-server /]# cd /opt/cgms/server/cgms/conf/
[root@fnd-server conf]# ls -lrth
total 664K
-rw-r--r--. 1 root root  518 Nov  7 06:22 fnd_psk.keystore
```

4. Edit the CGMS properties file using the `vi` command.

```
[root@fnd-server conf]# vi cgms.properties
```

Make the necessary changes to the cgms properties file and save the changes.

5. Log in to the docker using the `docker exec -it fnd-container /bin/bash` command.

```
[root@iot-fnd data]# docker exec -it fnd-container /bin/bash
```

6. Navigate to the docker's directory using the cd command.

```
[root@fnd-server /]# cd /opt/cgms/server/cgms/conf/
```

7. Use `ls -lrth` command to view all the properties.

Here's an example output:

```
total 664K
-rw-r--r--. 1 root root  518 Nov  7 06:22 fnd_psk.keystore
-rw-r--r--. 1 root root 115K Nov  8 01:00 standardjbosscmp-jdbc.xml
-rw-r--r--. 1 root root  65K Nov  8 01:00 standardjboss.xml
-rw-r--r--. 1 root root  41K Nov  8 01:00 standalone.xml.template
-rw-r--r--. 1 root root  41K Nov  8 01:00 standalone-postgres.xml.template
-rw-r--r--. 1 root root  42K Nov  8 01:00 standalone-postgres-cluster.xml.template
-rw-r--r--. 1 root root  43K Nov  8 01:00 standalone-cluster.xml.template
-rw-r--r--. 1 root root 7.6K Nov  8 01:00 login-config.xml.template
-rw-r--r--. 1 root root 7.6K Nov  8 01:00 login-config.xml
-rw-r--r--. 1 root root 2.0K Nov  8 01:00 logging.properties
-rw-r--r--. 1 root root  194 Nov  8 01:00 jndi.properties
-rw-r--r--. 1 root root  15K Nov  8 01:00 jbossts-properties.xml
-rw-r--r--. 1 root root  840 Nov  8 01:00 jbossas_server.cer
-rw-r--r--. 1 root root   52 Nov  8 01:00 jbossas.keystore.password
-rw-r--r--. 1 root root  15K Nov  8 01:00 jboss-service.xml
-rw-r--r--. 1 root root  15K Nov  8 01:00 jboss-log4j.xml
-rw-r--r--. 1 root root 7.8K Nov  8 01:00 jax-ws-catalog.xml
-rw-r--r--. 1 root root   95 Nov  8 01:00 java.policy
-rw-r--r--. 1 root root 143K Nov  8 01:00 ios.p7b
-rw-r--r--. 1 root root   20 Nov  8 01:00 cgmsdb_master.password
-rw-r--r--. 1 root root  485 Nov  8 01:00 bootstrap.xml
-rw-r--r--. 1 root root   19 Nov  8 01:00 cgnms_schema_version.txt
-rw-r--r--. 1 root root  572 Nov  8 01:00 cgnms_aggr_metadata.xml
drwxr-xr-x. 2 root root 4.0K Nov  8 04:35 xmdesc
drwxr-xr-x. 2 root root 4.0K Nov  8 04:35 props
drwxr-xr-x. 2 root root  135 Nov  8 04:35 migration
```

```
-rw-r--r--. 1 root root  689 Nov  8 04:35 fnd_psk.tgz
drwxr-xr-x. 2 root root 4.0K Nov  8 04:35 endpoint-meta-templates
drwxr-xr-x. 2 root root   51 Nov  8 04:35 ciscosudi
drwxr-xr-x. 2 root root  133 Nov  8 04:35 bootstrap
drwxr-xr-x. 3 root root   54 Nov  8 04:35 bindingservice.beans
drwxr-xr-x. 2 root root    6 Nov  8 10:45 device_licenses
-rwxrwxrwx. 1 root root  278 Nov 11 10:40 cgms.properties
-rw-------. 1 root root 4.3K Nov 11 10:41 cgms_keystore
-rw-------. 1 root root 1.3K Nov 11 10:41 userPropertyTypes.xml
-rw-r--r--. 1 root root 2.2K Nov 11 10:41 jbossas.keystore
```

8. When you edit the `cgms.properties` using the `vi` command. You'll see the changes you made to the cgms properties file outside the container reflected here as well.

Note

- When you make changes to the CGMS properties file values inside the docker, the changes are replicated in the CGMS properties file outside the docker as well.
- Restart the Cisco IoT FND container or the CGMS service for the properties to take effect. The CGMS properties file is in-sync with both inside and outside the docker.

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 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 can be in the same tunnel provisioning group if your custom templates are applicable to both router types.

To create a tunnel group:

Procedure

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 422.

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:

Procedure

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:

Procedure

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 87: Tunnel Group Fields

Field	Description
Name	Router EID (device identifier).
Status	Status of the router: • Unheard—The router has not contacted IoT FND yet. • Unsupported—The router is not supported by IoT FND. • Up—The router is in operation. • 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 OSPF Area 2	Open shortest path first (OSPF) areas 1 and 2.
OSPFv3 Area 1 OSPFv3 Area 1	OSPFv3 area 1 OSPFv3 area 2.
IPsec Dest Addr 1 IPsec Dest Addr 2	IPv4 destination address of the tunnel.
GRE Tunnel Dest Addr 1 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:

Procedure

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:

Procedure

Step 1 Choose **CONFIG** > **Tunnel Provisioning**.

Step 2 Click the **Group Members** tab.

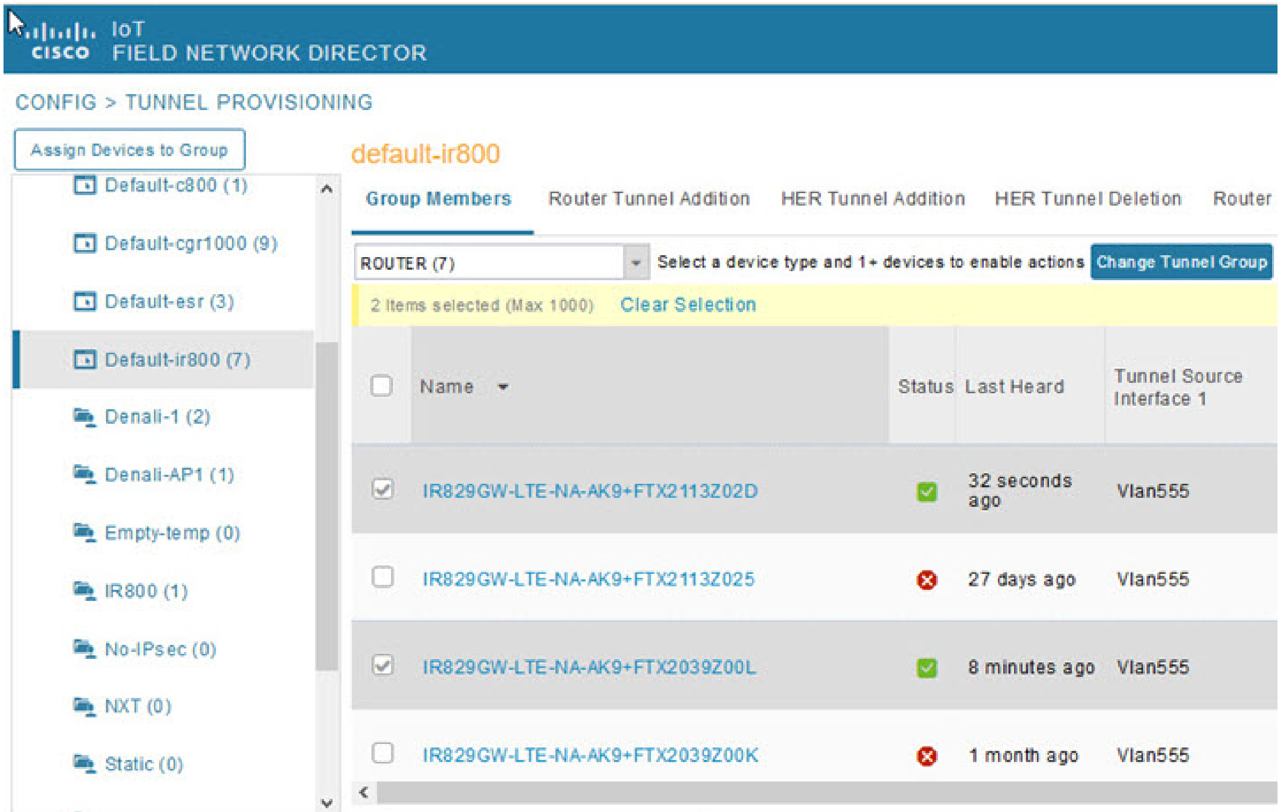
Step 3 In the TUNNEL GROUPS pane, select the tunnel group with the routers to move.

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).

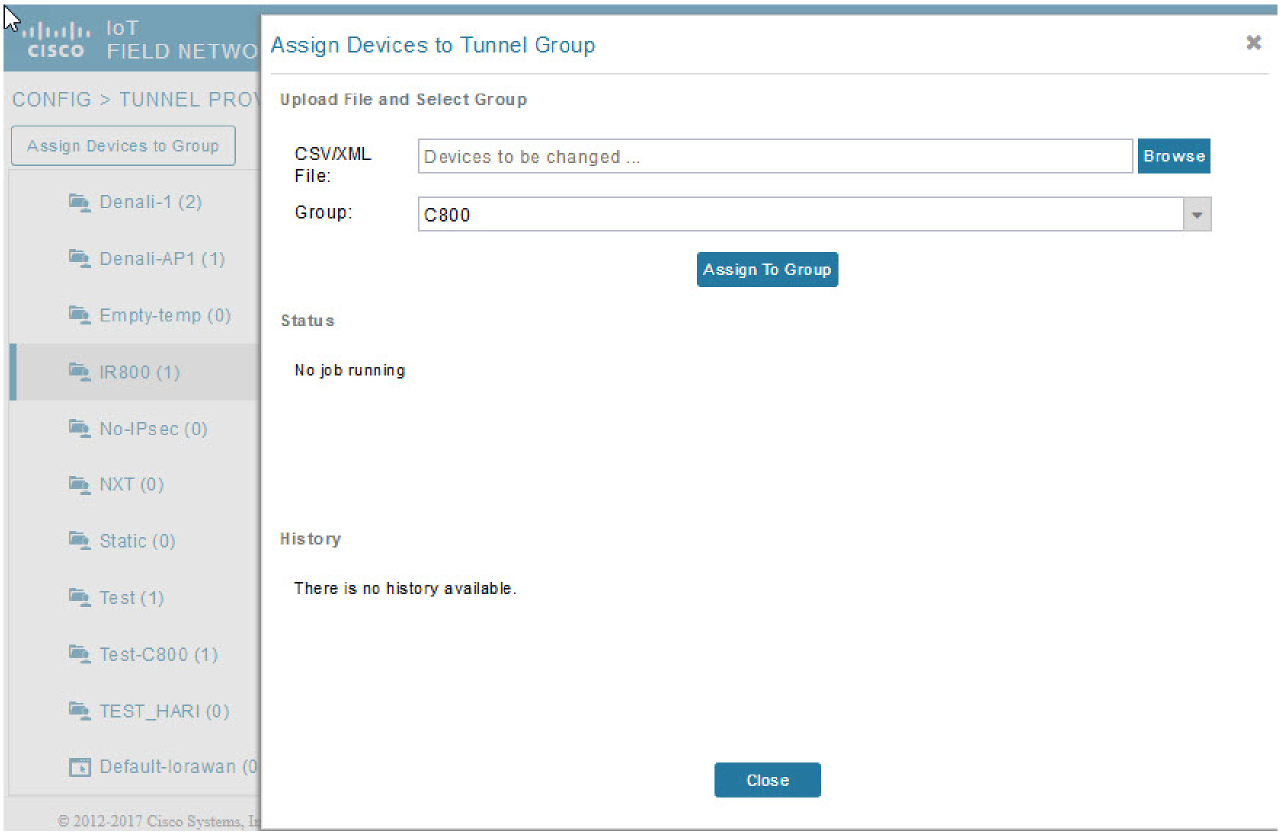
To move FARs to another group in bulk:

Procedure

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

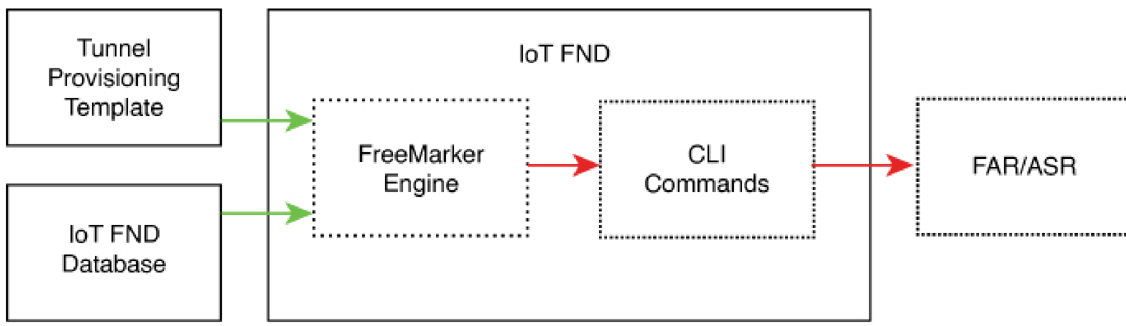
IoT FND has three default tunnel provisioning templates:

- 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 38: 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

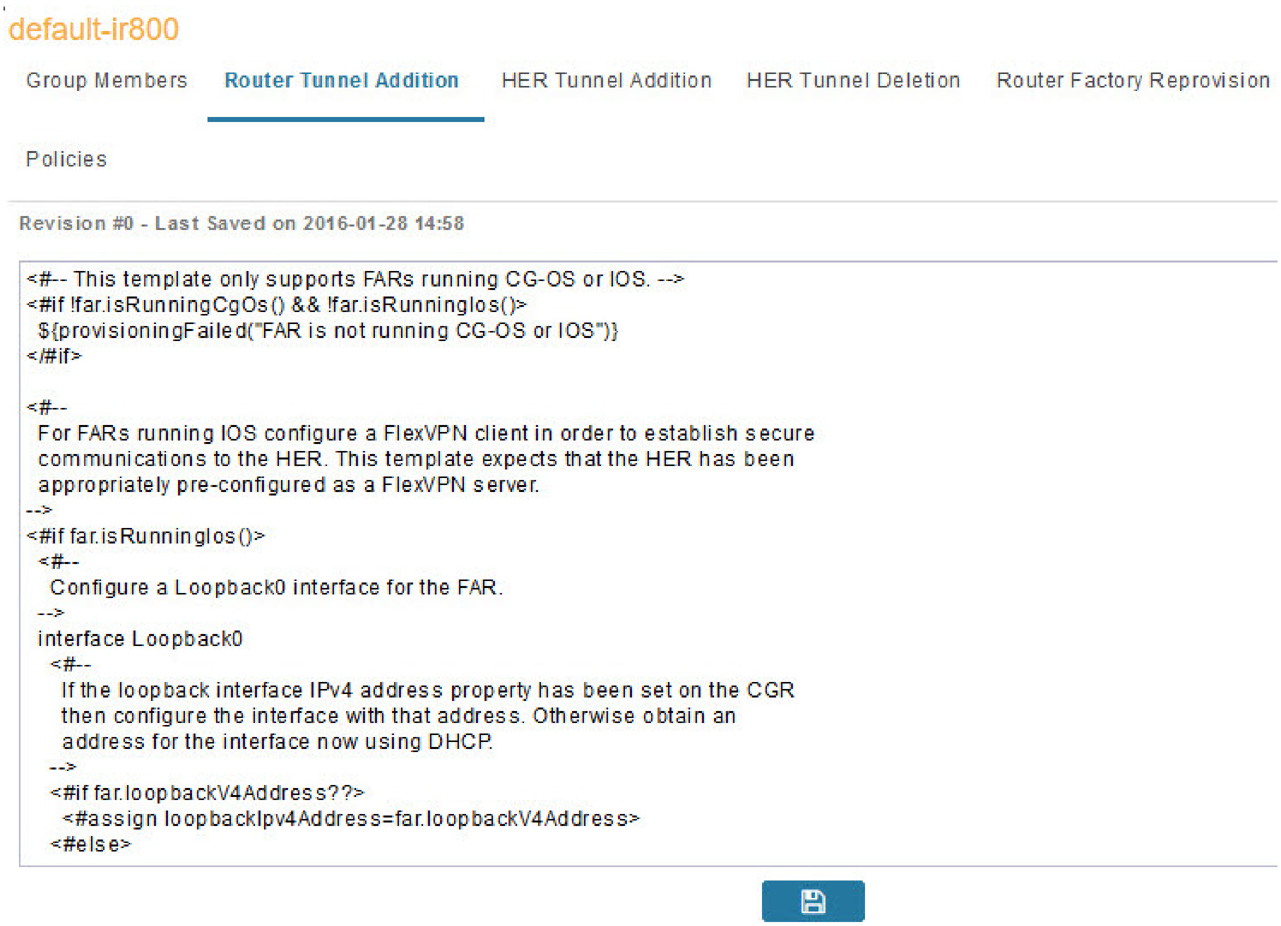
To edit the FAR Tunnel Addition template to provide one end of an IPsec tunnel on FARs in the group:

Procedure

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 425.

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:

Procedure

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:

Procedure

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.

Procedure

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.

Procedure

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.

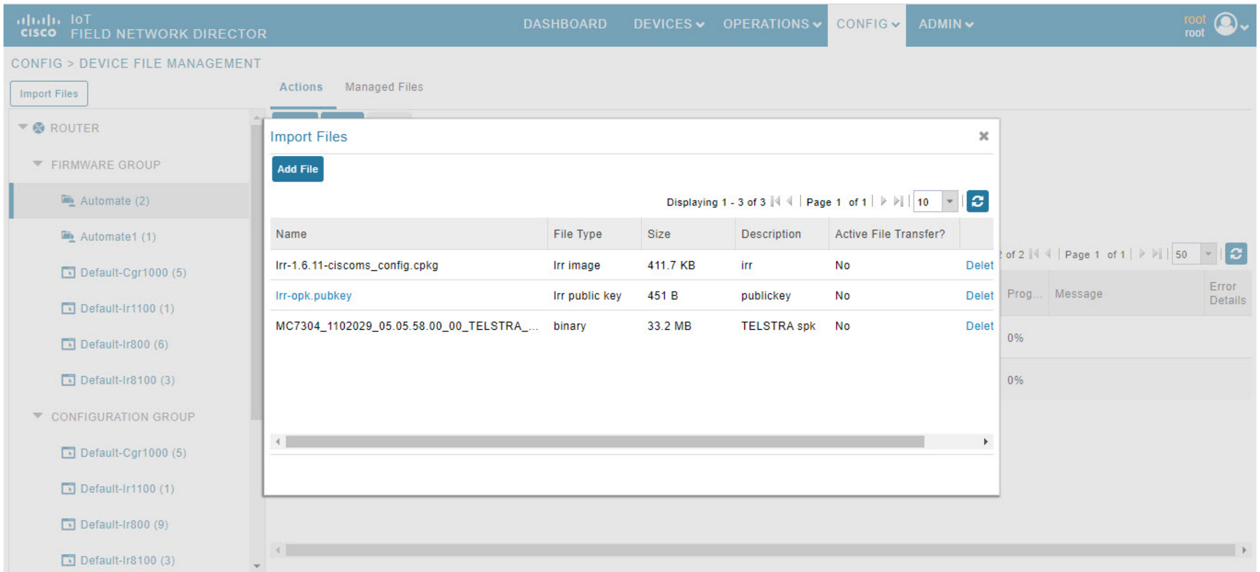
Note
If you are using Rivest-Shamir-Adleman (RSA), ignore this step.

The userPropertyTypes.xml is shown below.

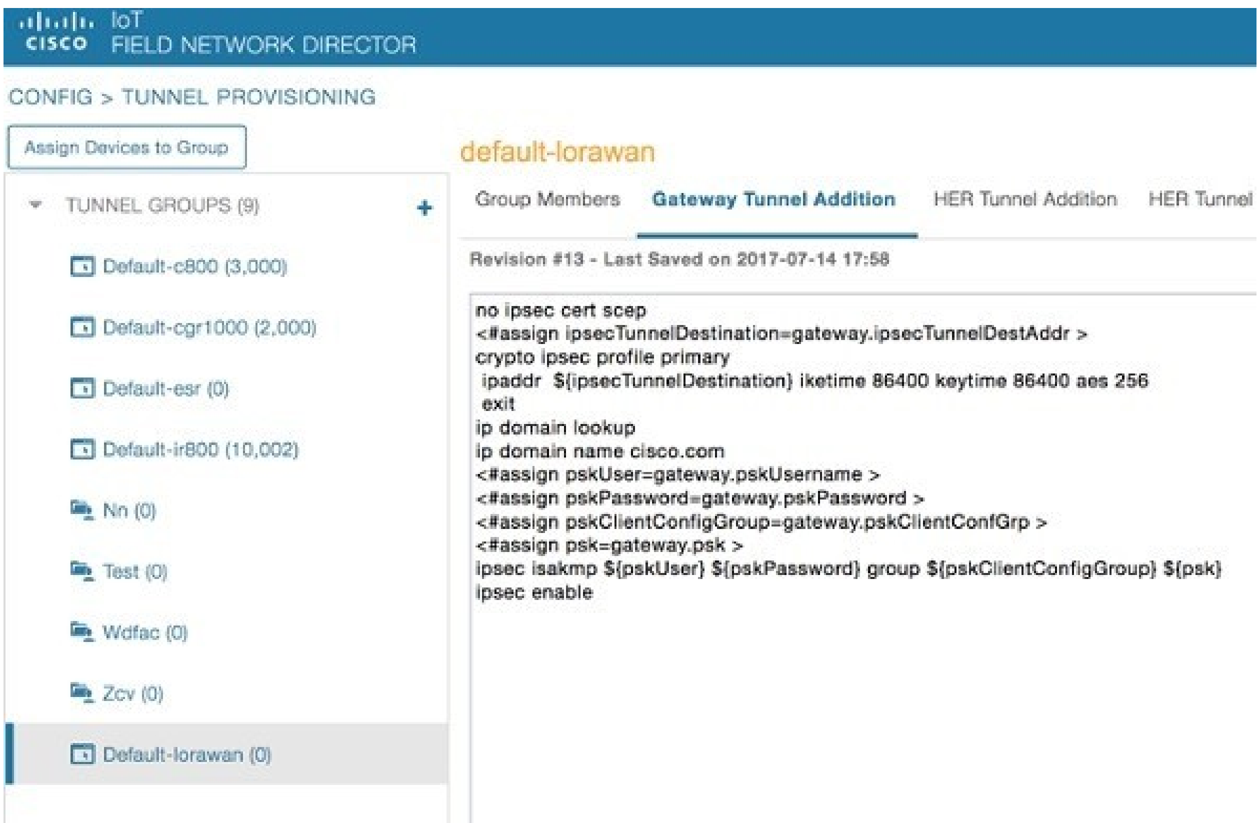
```xml
<?xml version="1.0" encoding="UTF-8"?>
<cgms xmlns="http://www.w3schools.com"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://www.w3schools.com propertyTypes.xsd">
  <propertyTypes kind="lorawan">
  <!--Psk Properties -->
   <propertyType>
      <name>pskUsername</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**.

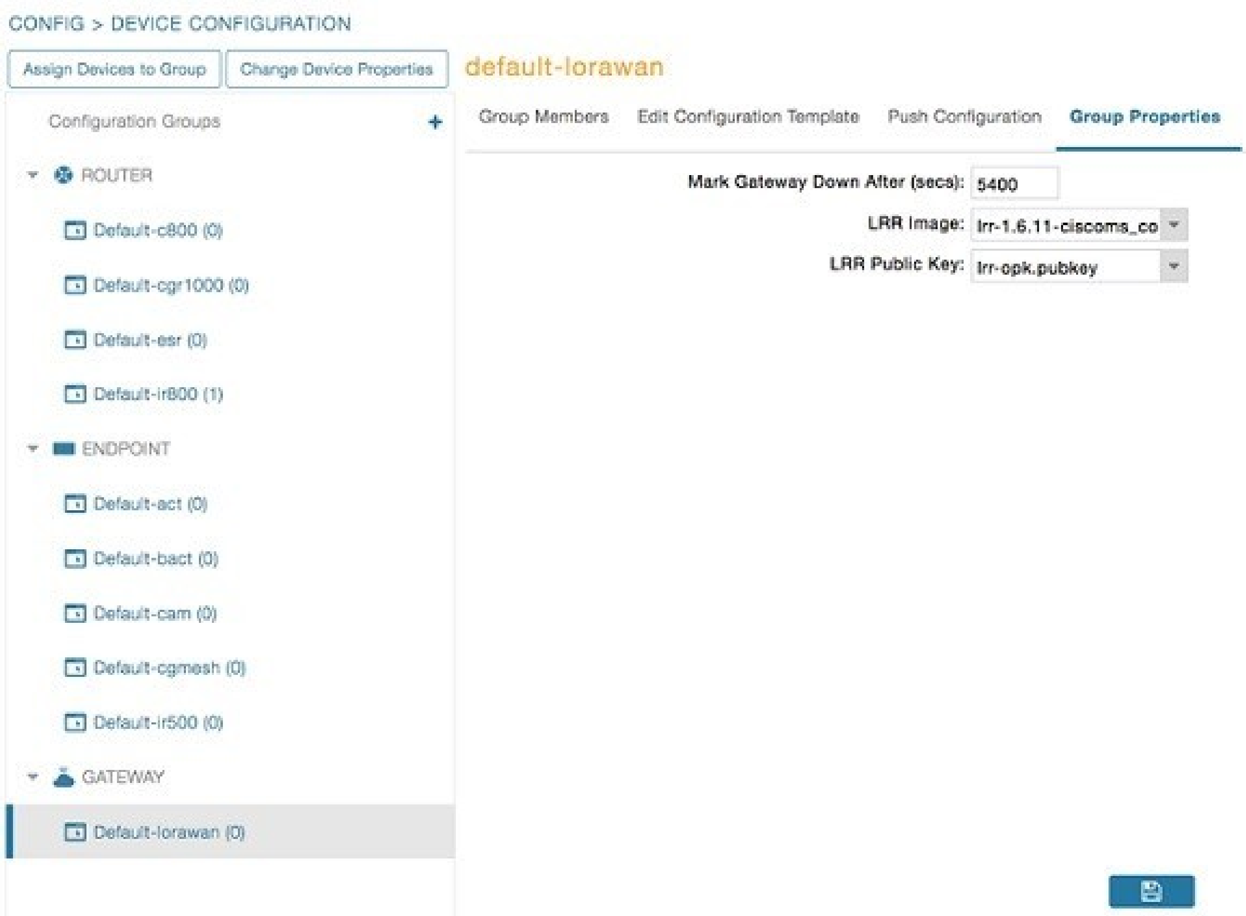
Step 4 Click **Add File** to add the Actility LRR and public key to IoT FND.



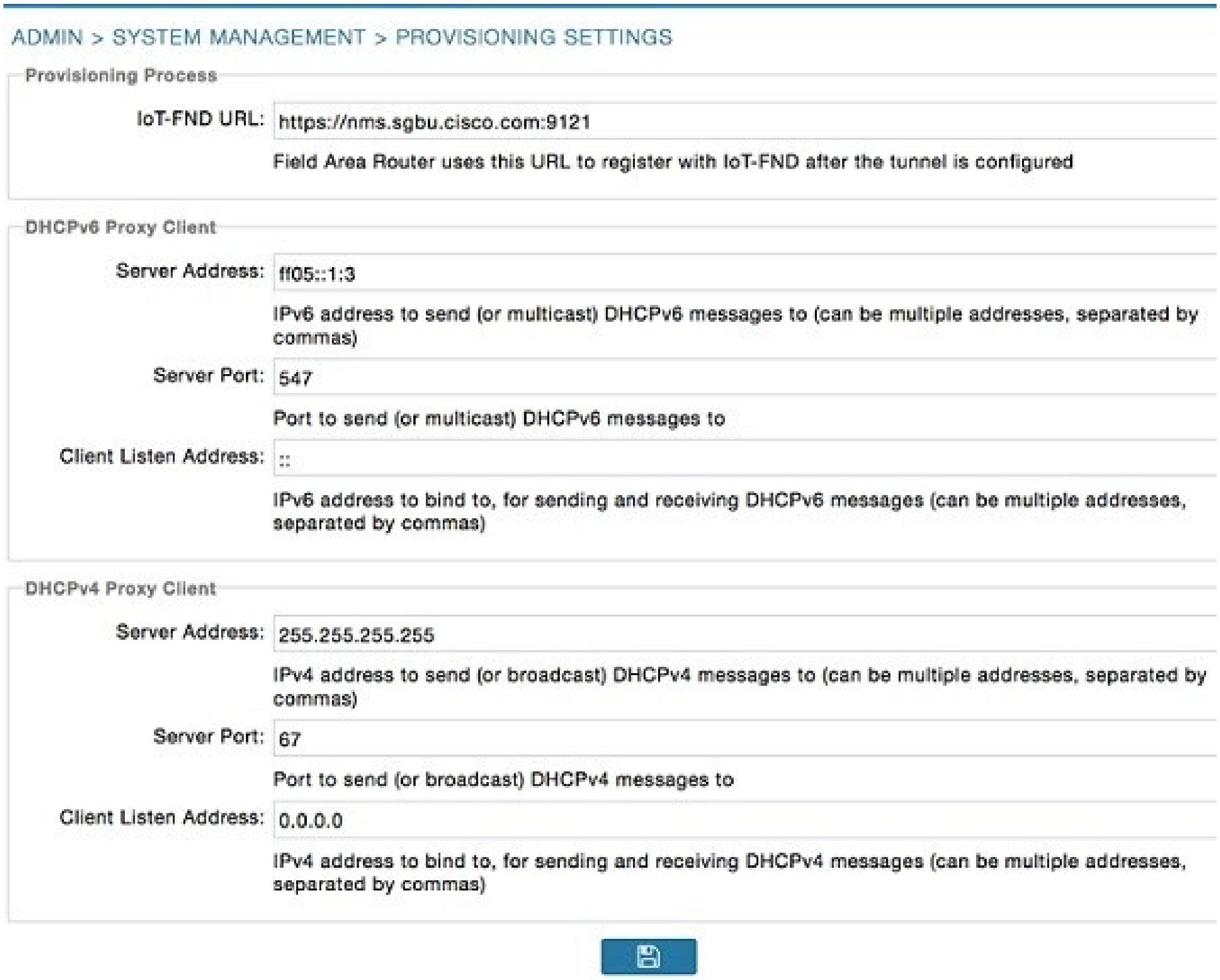
Step 5 In the **Config** > **Tunnel Provisioning** page, update the tunnel configuration group with the following parameters in the Gateway Tunnel Addition tab and click **Save**.



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,,,,,,,,
```

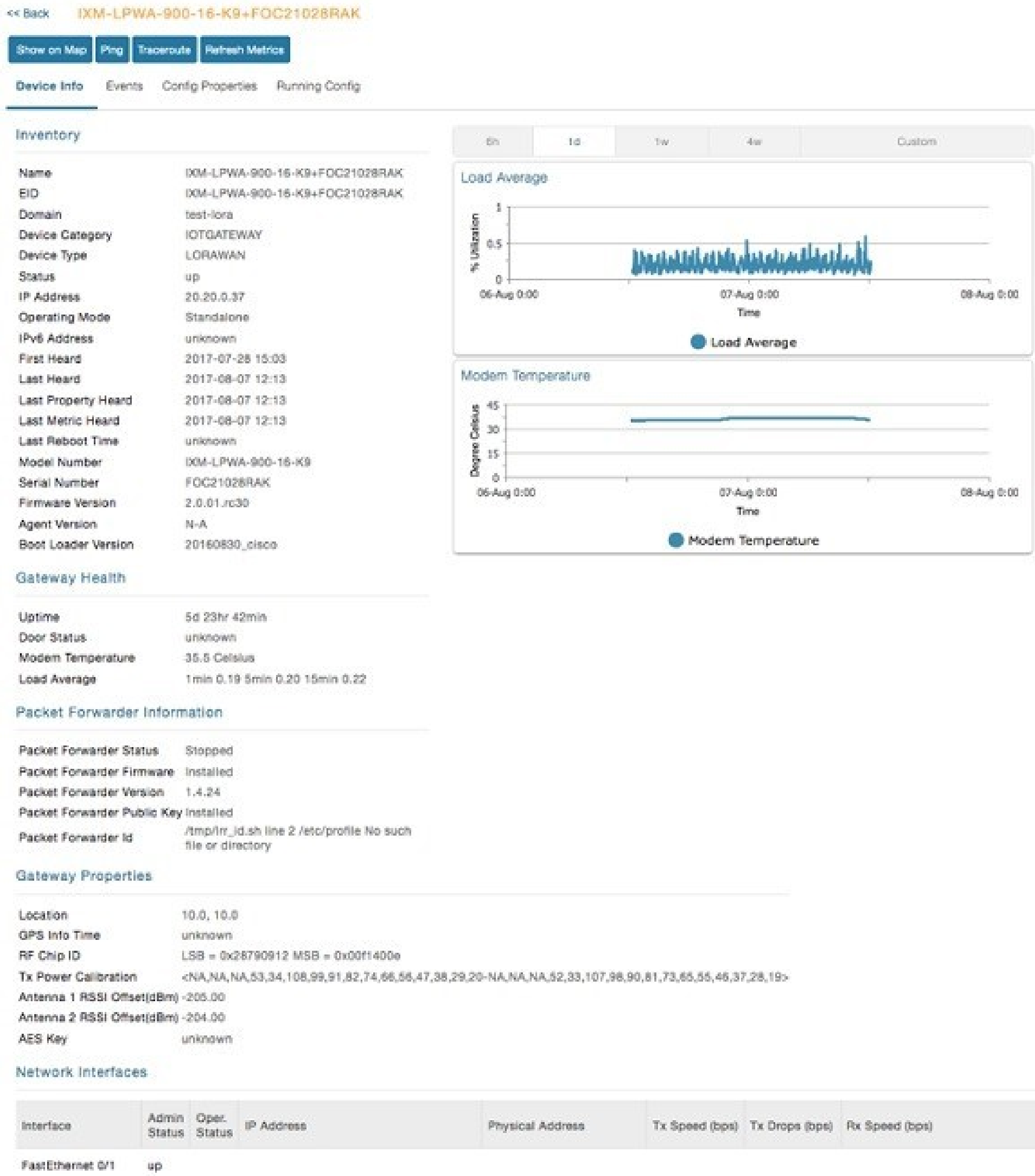
Note

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
```

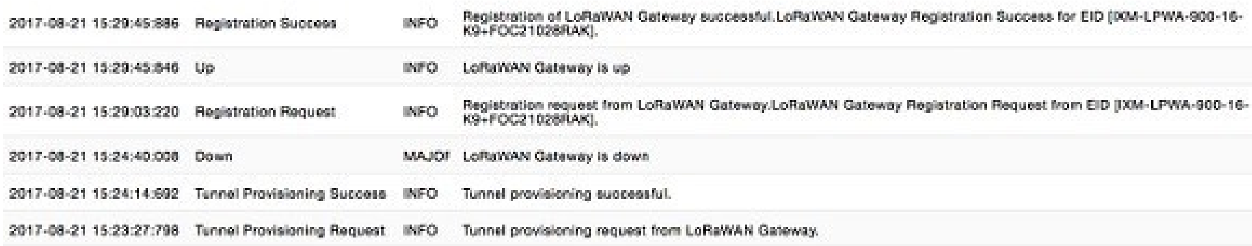
```
ki8OjEO5Pr+krJTtUooUMD0GoqmOAznc2JObiUUr4ismXyP0uXs8JRuSPOfo
jMDavGIHiO8unUUJm3zdxv0LP8b6fe5G+oshy76A6IqX1jk7ymSFOaVPQBT8fUS6onjsuSThi
LERS0B6Brn2gRx/KpQMk9IdYQMOSsHh4khvtxbqBZy6j++pIjeG4+
dPz/v52DmJR+DOrE7ZQpfvS9PSHkJoaqC2o6PrKN5YZ50G9+Tm+diPmbyv/
PdHKtXn1ny3qBAdbfDwOjlA+NtJPld3/
06vq6WhHsgujYwMJWs7Cuu3rR0/FVHF/5wFxarakJsfo/zd69EpzrI8Hsic/QmMzA==,19,
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.



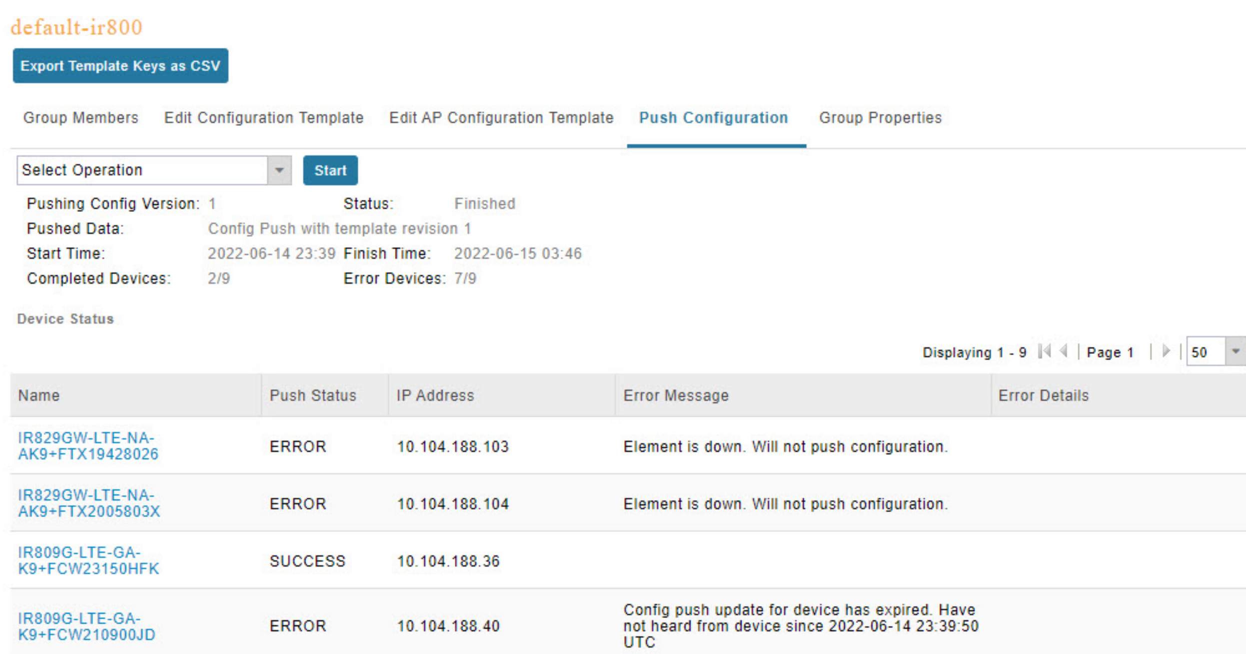
Note

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**.



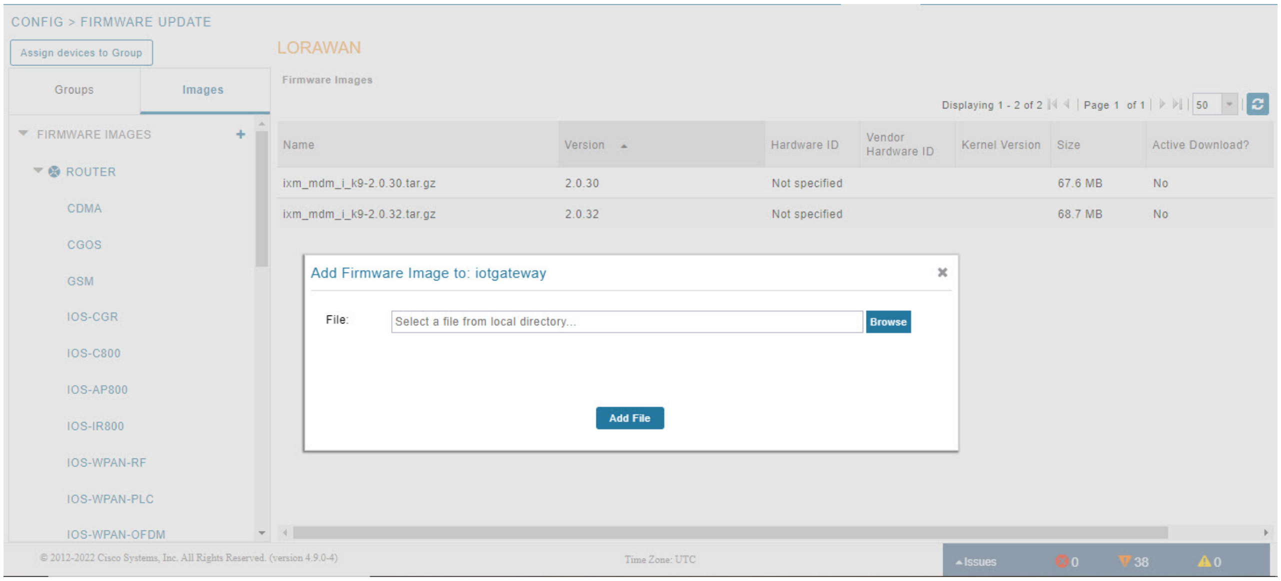
IXM Firmware Update

Follow the steps for upgrading the firmware.

Procedure

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.

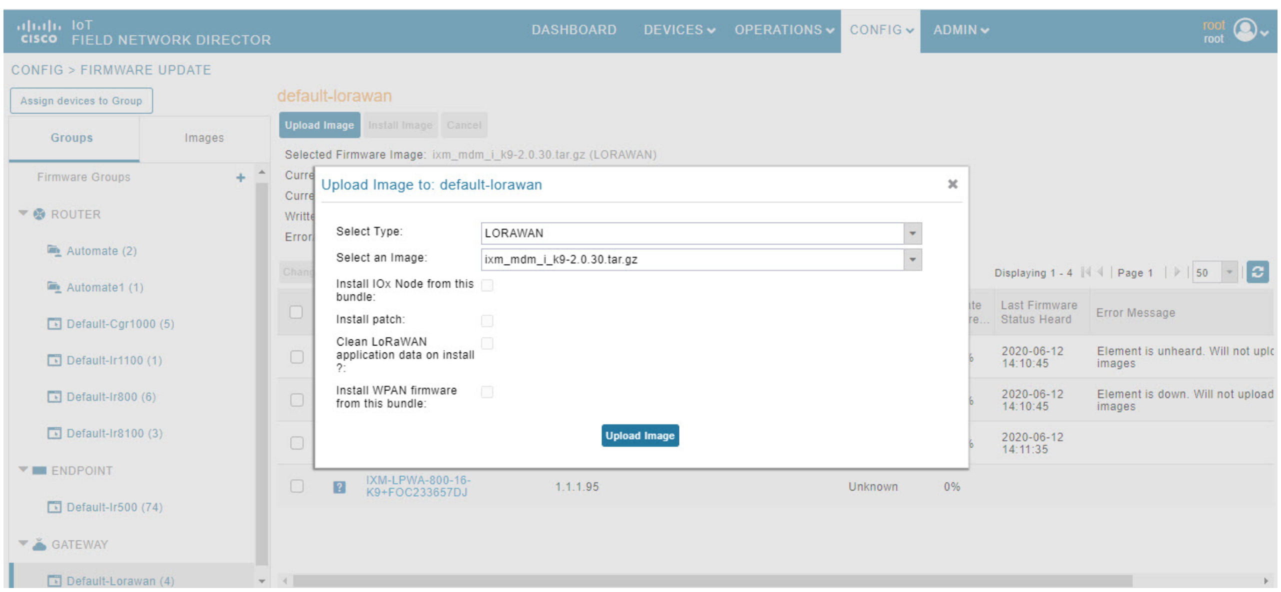
Step 4 Click **Upload Image** to push the firmware to the IXM modem. For more information, see Uploading a Firmware Image to a Router Group, on page 391.

Note

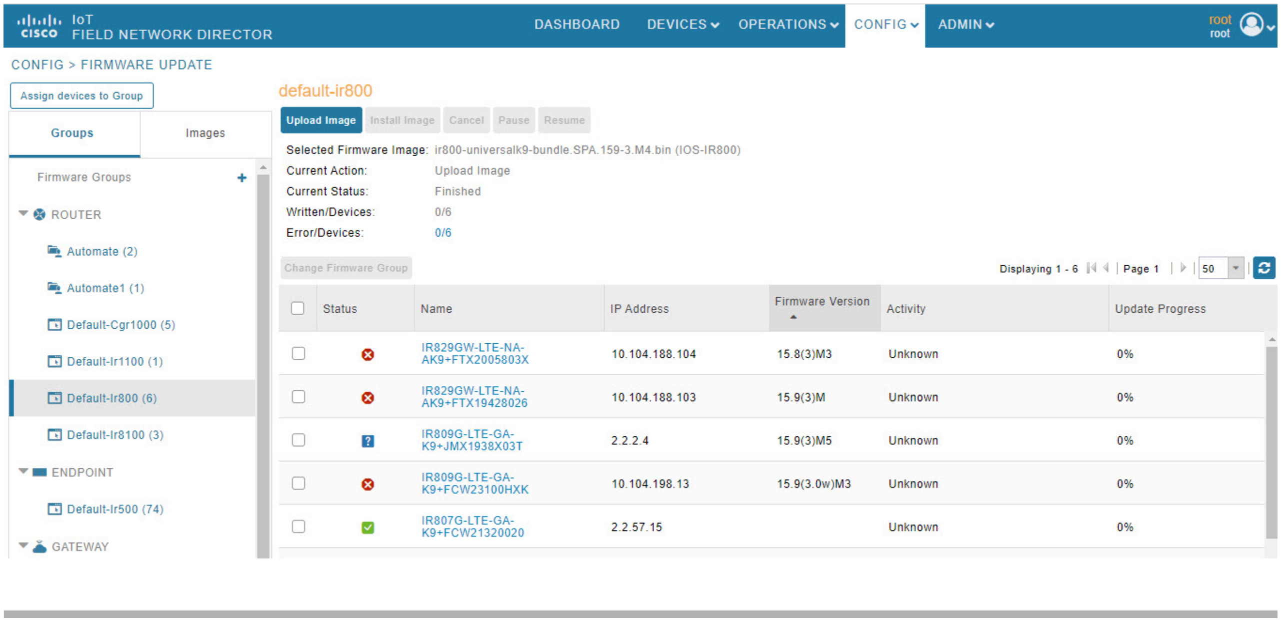
If you want to erase the LRR or public key, select **Clean LoRaWAN application data on install ?** option.

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.

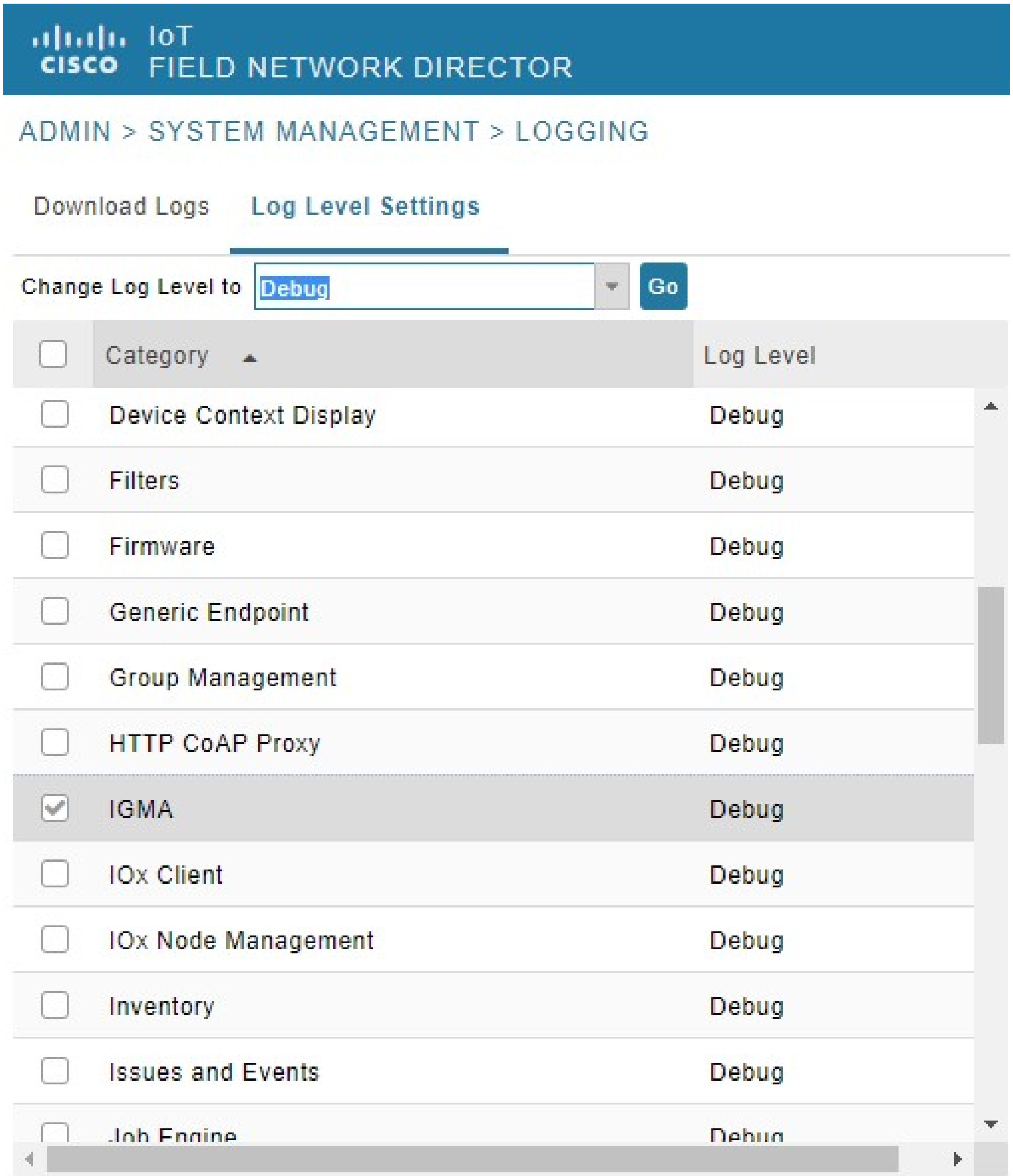


Step 5 Click **Install Image** button to install the image once the upload is complete.



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 88: 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 88: 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 88: 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. **Note** Because one HER can serve up to 500 FARs, there may be multiple tunnels in the list with the same HER EID. 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. **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. 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.

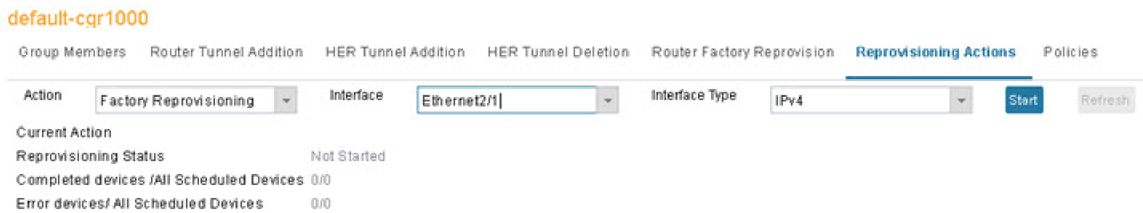
CGR Reprovisioning Sequence

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 89:

Reprovisioning Actions	Description
Factory Reprovisioning	Drop-down menu allows you to change the express-setup-config file loaded on the CGR during factory configuration. 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 90: Reprovisioning Actions Pane Fields describes the fields on the Reprovisioning Actions pane.

Table 90: 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:

Procedure

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 412).

To configure and trigger factory reprovisioning:

Procedure

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.

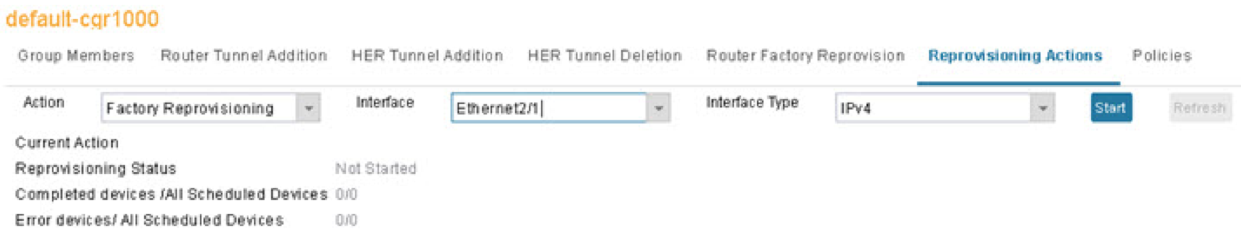
Note
The Router Factory Reprovision template is processed twice during factory reprovisioning; once when pushing the configuration and again before saving the configuration in express-setup-config. Because of this, when making your own template, use the specific if/else condition model defined in the 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 9

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:

Procedure

Step 1 At first login, as a root user, click **Dashboard**. A No Devices or Dashlets panel appears, which displays the following options:

- ADD LICENSE
- ADD DEVICES
- ADD DASHLET
- 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

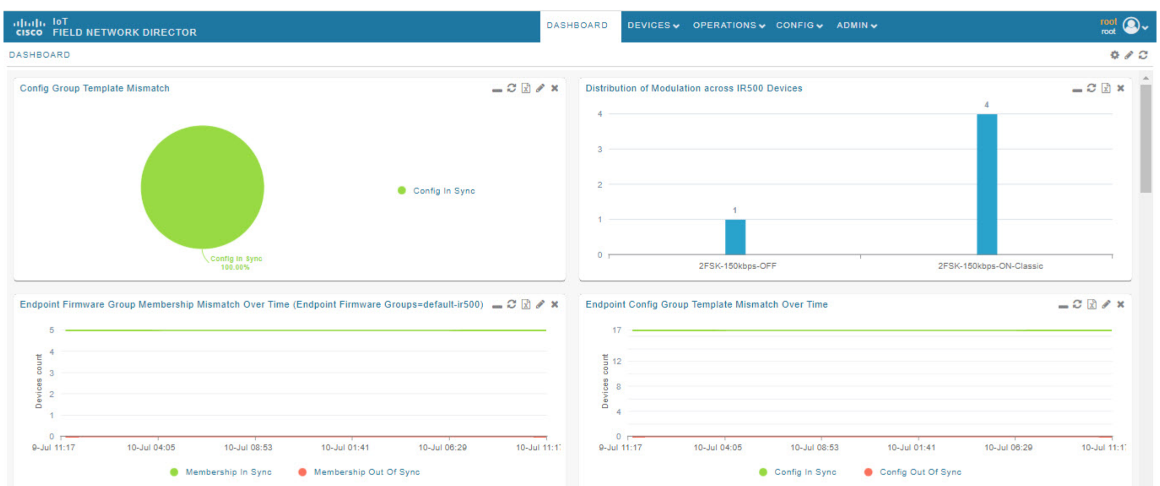
Step 4 After you select one of the Guided Tours, you will be redirected to that configuration page and windows appear to step you through the configuration steps and let you Add or Update Values as necessary.

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.

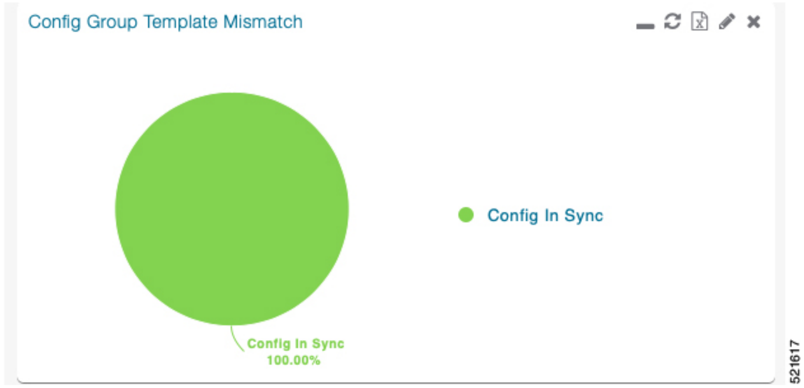
Figure 39: DASHBOARD



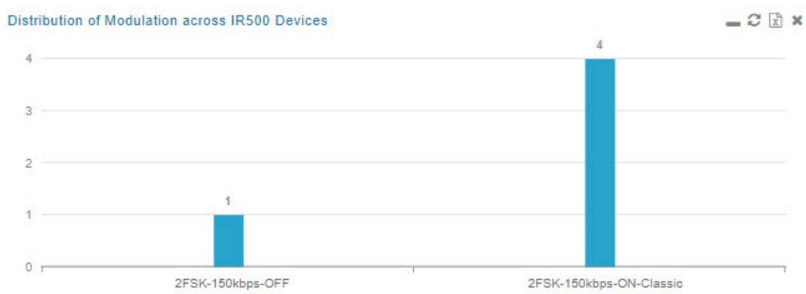
Types of Dashlets

The Dashboard displays three types of dashlets for a selected device:

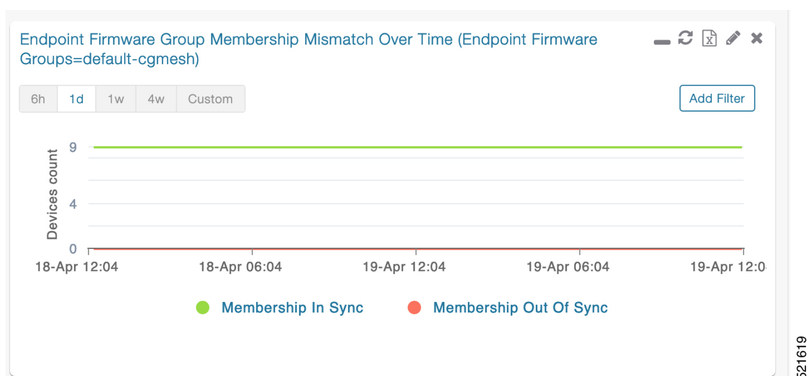
- Pie-chart dashlets display a ratio of the device properties as a pie chart.



- 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:

Procedure

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

Table 91: Feature History

Feature Name	Release Information	Description
User Experience Enhancements	Cisco IoT FND Release 5.0	The Cisco IoT FND dashboard includes pre-defined dashlets, where an additional **Name** field is added along with the Element Identifier (**EID**). You can delete the default views of the devices you select in the **Devices** > **Field Devices** page. You can also add the user-defined properties in the customized tab in the **Field Devices** page.

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).
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.

Dashlet	Description
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. Use the Add Filter button to track: • Specific router (Type) • Router Configuration Groups • Router Firmware Groups
Routers With Top Cellular Bandwidth Usage	This bandwidth chart displays the following information for the top *n* routers: EID, NAME, 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. **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, NAME, 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. **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, NAME, Interface, Cellular RSSI and Cellular RSSI (in dBm) for a router.

Dashlet	Description
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). This dashlet displays the aggregated maximum Down Routers for device types CGR1000 and IR800 for single modem routers. **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). This dashlet displays the aggregated maximum Down Routers for device types CGR1000 and IR800 for dual modem routers. **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.

Procedure

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

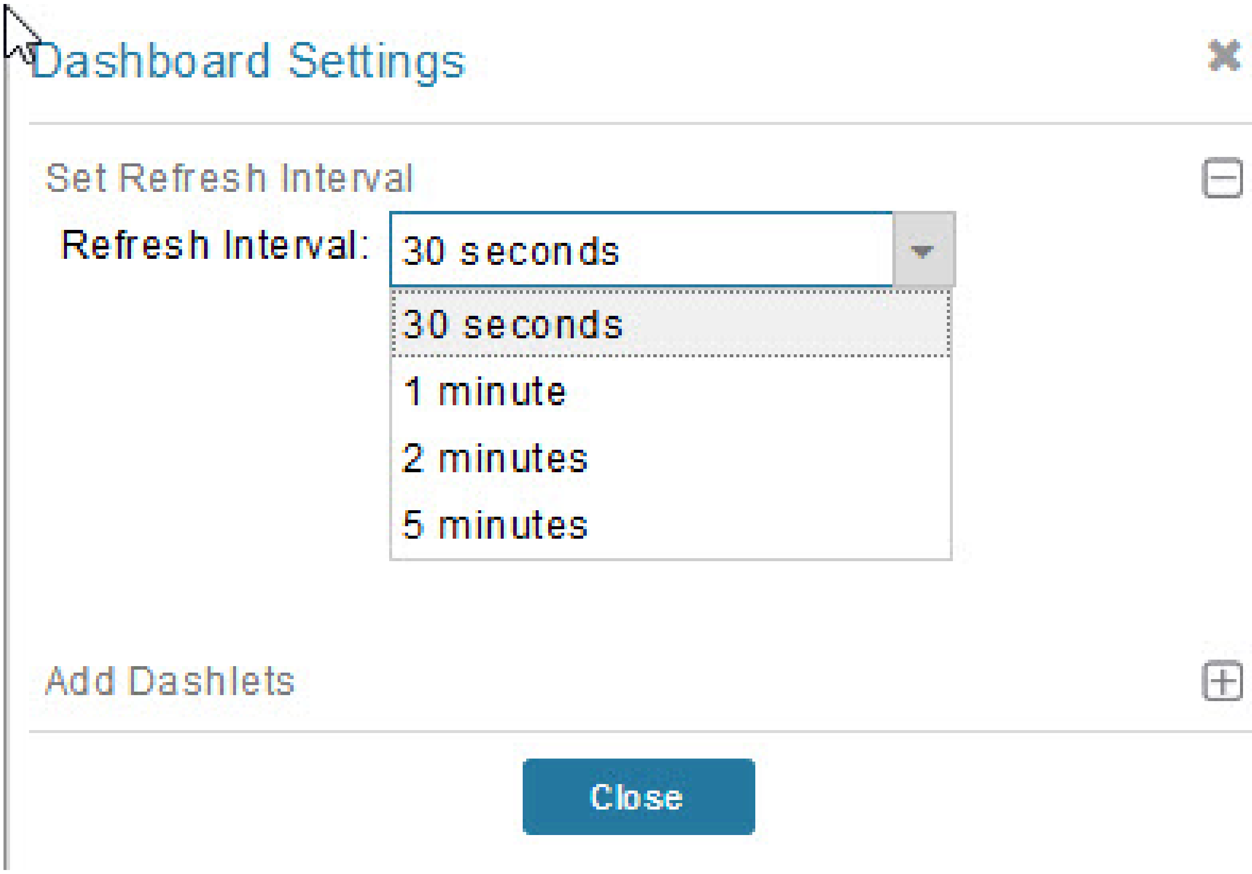
To set the refresh interval for dashlets:

Procedure

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:

Procedure

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 92: 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.
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.

Field Name	Key	Description
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.
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 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 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.

Field Name	Key	Description
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).
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.

Field Name	Key	Description
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).
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 93: 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.

Field Name	Key	Description
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:

Procedure

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:

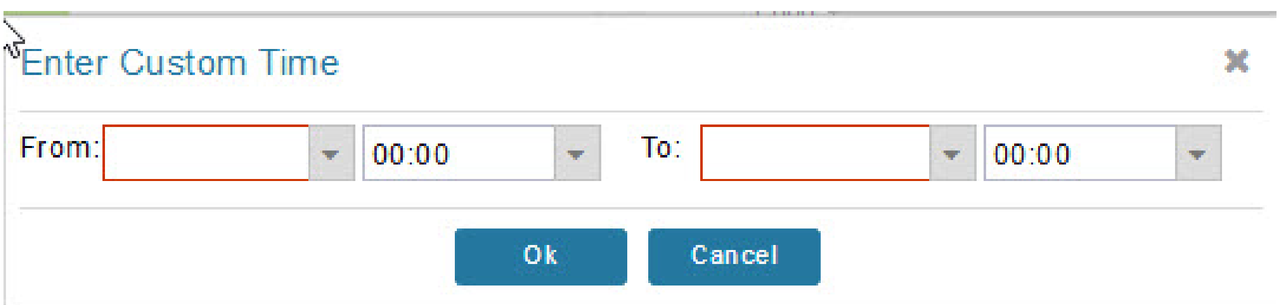
Procedure

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:

Procedure

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

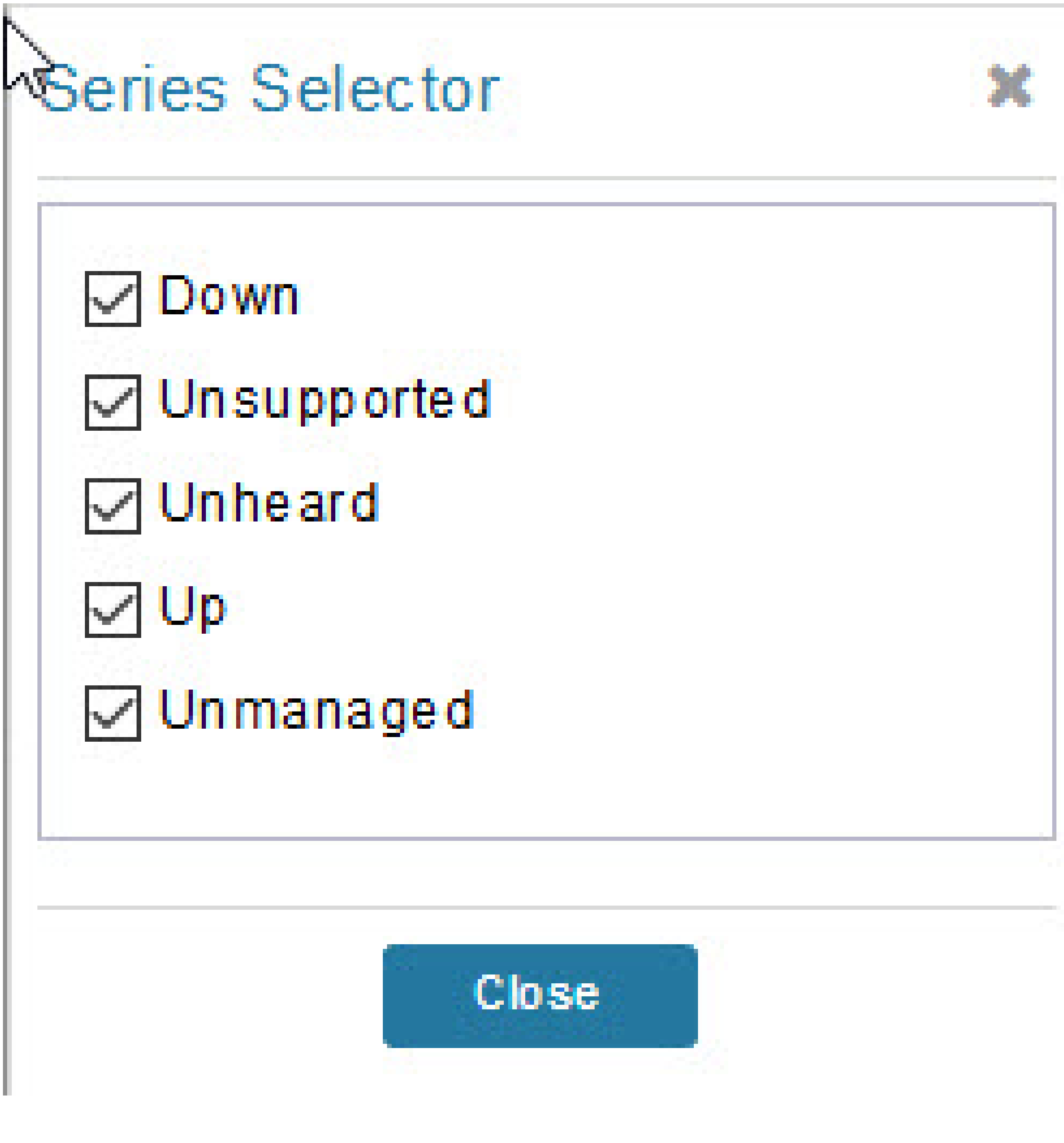
To use the Series Selector:

Procedure

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:

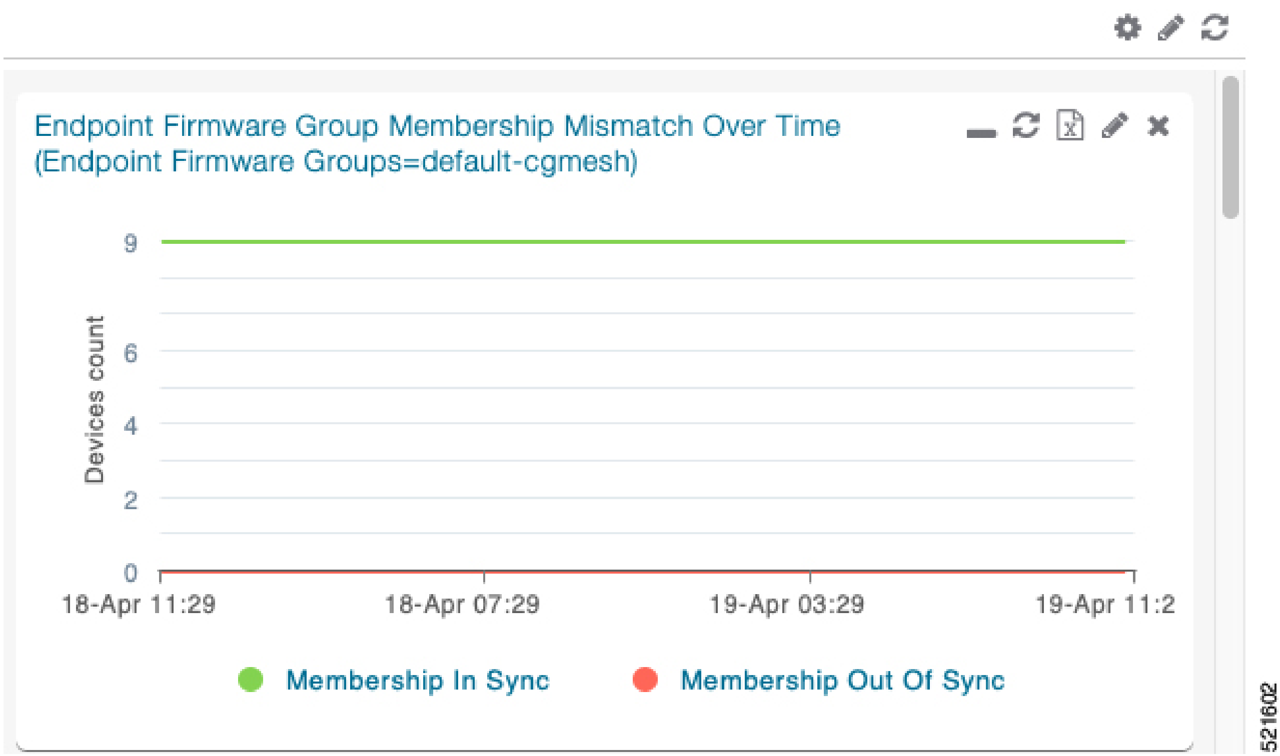
Procedure

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 40: 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:

Procedure

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.

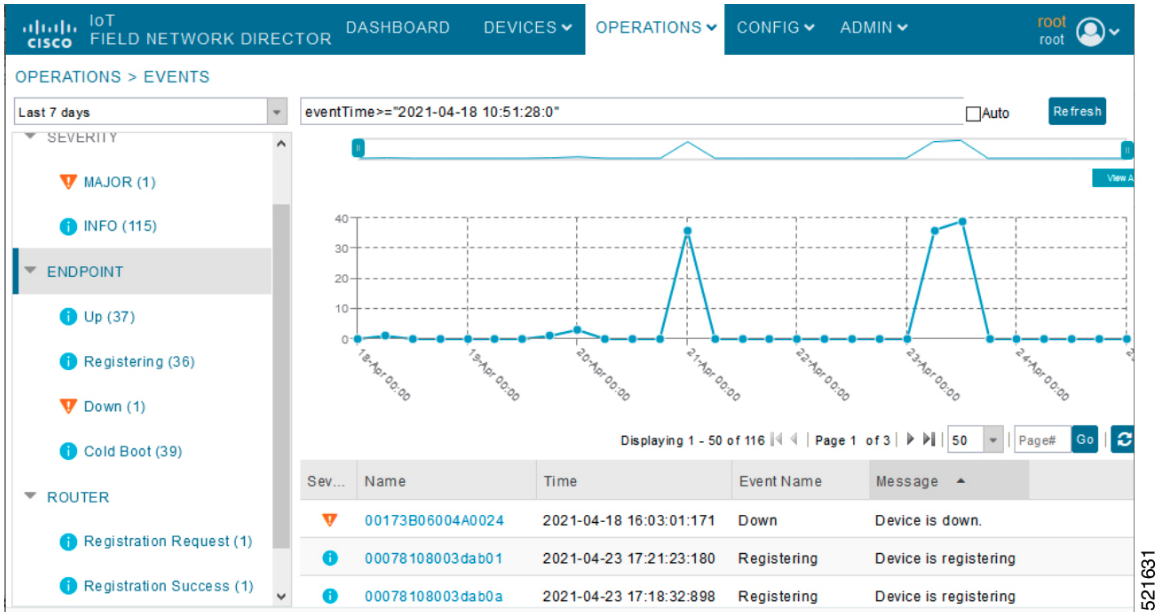
Set Time Range and Page View Preferences for Operations > Events

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 41: 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 461.

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**.

Procedure

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:

Procedure

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.

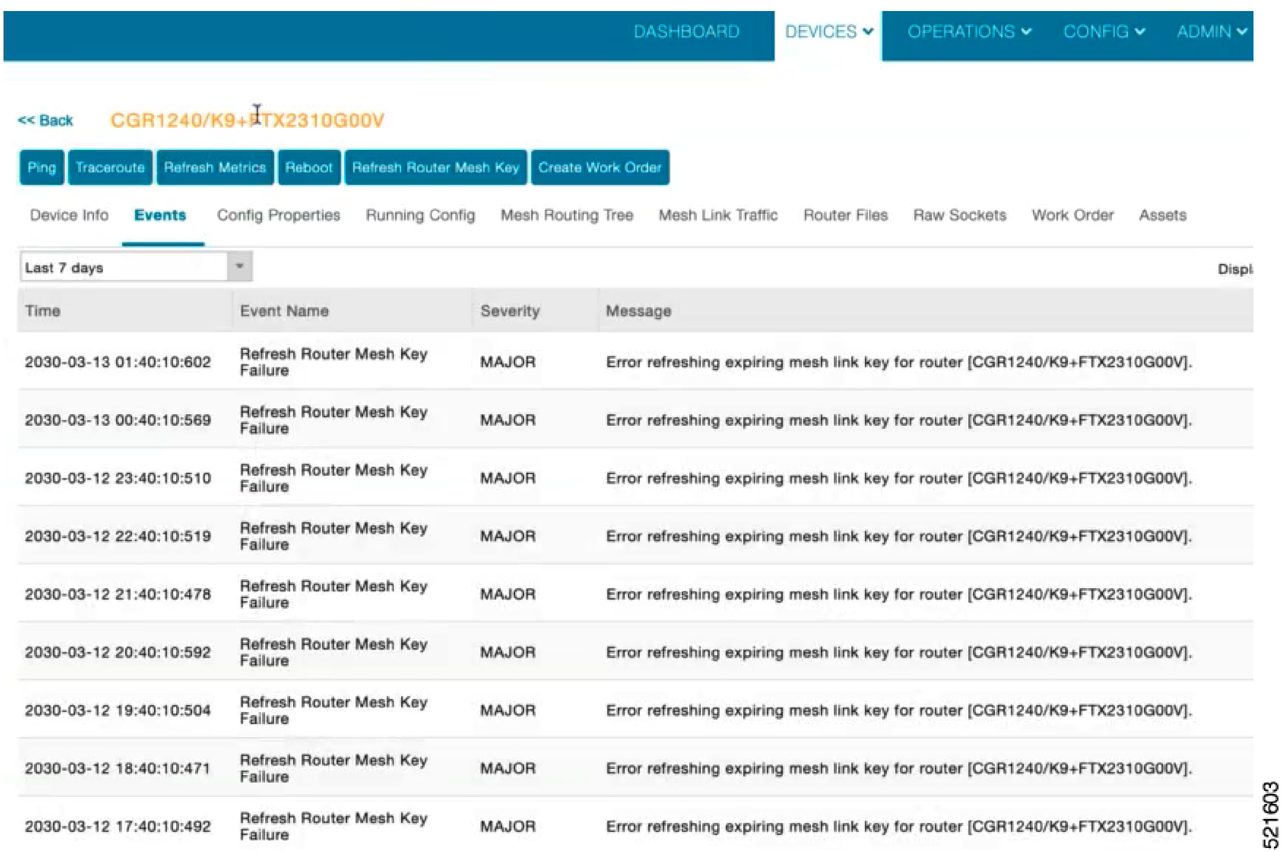
Advanced Event Search

To use the filter to search for events:

Procedure

Step 1 Choose **OPERATIONS** > **Events**.

Figure 42: 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.

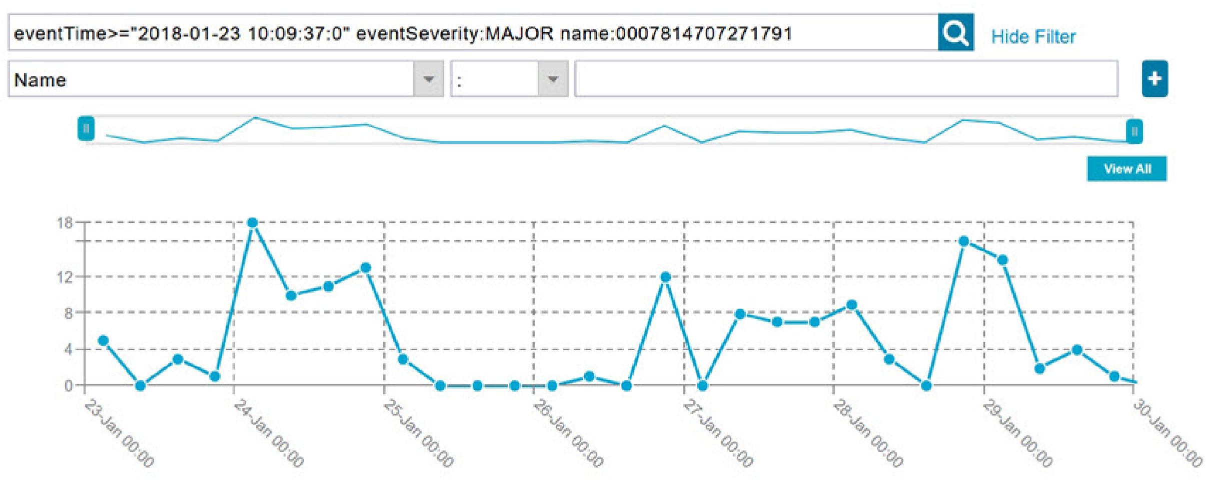
Repeat the process of adding search strings to the Search field as needed.

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:

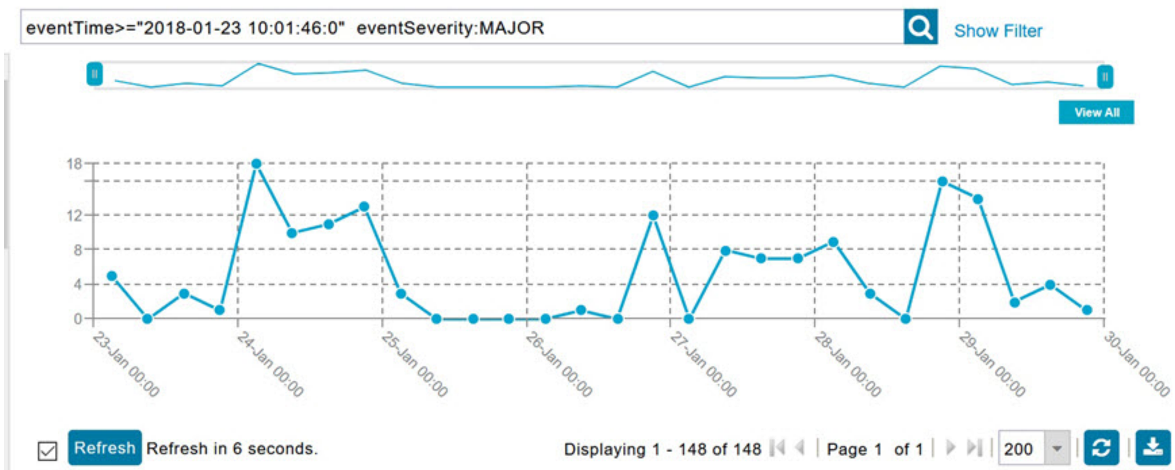
- To filter events by Name (EID), enter the following string in the Search Events field:
  - **name:** *router eid string*
  - Search Events by Name Filter



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):

Procedure

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:

Procedure

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:

Procedure

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 94: Events Reported

Events	Devices	Severity
CRITICAL EVENTS		
Certificate Expired	AP800, CGR1000, 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	CGR1000, IR800	Major
ACT2L Failure	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
BBU Power Off	IR500	Major
Block Mesh Device Operation Failed	CGR1000	Major
Certificate Expiration	AP800, CGR1000, FND, IR800	Major
DB FRA Space Very Low	Database	Major
Default Route Lost	CGMESH, IR500	Major
Device Unknown	FND	Major
Door Open	CGR1000, IR800, LORA	Major

Events	Devices	Severity
Dot1X Authentication Failure	CGR1000	Major
Dot1X Authentication Flood	CGR1000, IR800	Major
Down	AP800, ASR, C8000, Cellular, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900, LORA	Major
Element Configuration Failed	CGR1000, IR800	Major
High CPU Usage	LORA	Major
High Flash Usage	LORA	Major
High Temperature	LORA	Major
HSM Down	FND	Major
Interface Down	ASR, C8000, ISR3900	Major
Linecard Failure	CGR1000, IR800	Major
Line Power Failure	CGR1000, IR800	Major
Link Down	IR500	Major
Low Flash Space	CGR1000, IR800	Major
Low Memory/Memory Low	CGR1000, FND, IR800, LORA (Memory Low)	Major
Low Temperature	LORA	Major
Mesh Connectivity Lost/ Node Connectivity Lost	CGMESH, IR500	Major
Mesh Link Key Timeout/ Node Link Key Timeout	CGMESH, IR500	Major
Metric Retrieval Failure	ASR, C8000, CGR1000, IR800, ISR3900	Major
Modem Temperature Cold Alarm	CGR1000, IR800	Major
Modem Temperature Warm Alarm	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, CGR1000, IR800	Major

Events	Devices	Severity
Port Failure	AP800, CGR1000, IR800	Major
Refresh Router Mesh Key Failure	CGR1000, IR8100	Major
Refresh Router Mesh LFN Key Failure	IR8100	Major
RPL Tree Size Warning	CGR1000	Major
Software Crash	CGR1000, IR800	Major
SSM Down	FND	Major
System Software Inconsistent	CGR1000, IR800	Major
Temperature Major Alarm	CGR1000, IR800	Major
Time Mismatch	CGMESH, IR500	Major
Tunnel Down	CGR1000, IR800	Major
Tunnel Provisioning Failure	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	CGR1000, IR800	Minor
Temperature Low Minor Alarm	CGR1000, IR800	Minor
RPL Tree Reset	CGR1000	Minor
INFORMATION EVENTS		
Archive Log Mode Enabled	Database	Information
Battery Normal	CGR1000	Information
Battery Power	CGR1000	Information
BBU Firmware Download Passed	CGR1000	Information
Certificate Expiration Recovery	AP800, CGR1000, FND, IR800	Information
Cold Boot	AP800, CGMESH, CGR1000, IR500, IR800	Information
Configuration is Pushed	FND	Information
Configuration Rollback	AP800, CGR1000, IR800	Information

Events	Devices	Severity
DB FRA Space Normal	Database	Information
DB Table Space Normal	Database	Information
Device Added	Cellular, CGMESH, CGR1000, IR500, IR800	Information
Device Location Changed	CGR1000, IR800	Information
Device Removed	Cellular, CGMESH, CGR1000, IR500, IR800	Information
Door Close	CGR1000, IR800, LORA	Information
Dot11 Deauthenticate Send	CGR1000, IR800	Information
Dot11 Disassociate Send	CGR1000, IR800	Information
Dot11 Authentication Failed	CGR1000, IR800	Information
Hardware Insertion	CGR1000, IR800	Information
Hardware Removal	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, C8000, ISR3900	Information
Line Power	CGR1000, IR800	Information
Line Power Restored	CGR1000, IR800	Information
Link Up	IR500	Information
Low Flash Space OK	CGR1000, IR800	Information
Low Memory OK/Low Memory Recovery	CGR1000, IR800, LORA (Low Memory Recovery)	Information
Manual Close	ASR, C8000, Cellular, 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

Events	Devices	Severity
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	CGR1000, IR800	Information
Modem Temperature Warm Alarm Recovery	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, CGR1000, IR800	Information
Power Source OK	CGR1000, IR800	Information
Power Source Warning	CGR1000, IR800	Information
Registered	ASR, C8000, ISR3900	Information
Registration Failure	AP800, Cellular, CGR1000, IR800, LORA	Information
Registration Request	AP800, CGR1000, IR800, LORA	Information
Registration Success	AP800, Cellular, 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

Events	Devices	Severity
Rule Event	ASR, C8000, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900	Information
SSM Up	FND	Information
Temperature Low Recovery	LORA	Information
Temperature Low Minor Alarm Recovery	CGR1000, IR800	Information
Temperature Major Recovery	CGR1000, IR800	Information
Temperature Low Major Alarm Recovery	CGR1000, IR800	Information
Temperature Minor Recovery	CGR1000, IR800	Information
Time Mismatch Resolved	CGMESH, IR500	Information
Tunnel Provisioning Request	CGR1000, IR800	Information
Tunnel Provisioning Success	CGR1000, IR800	Information
Tunnel Up	CGR1000, IR800	Information
Unknown Event	AP800, ASR, C8000,Cellular, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900, LORA	Information
Unknown Registration Reason	CGMESH, IR500	Information
Unsupported	AP800, CGR1000, IR800, LORA	Information
Up	AP800, ASR, C8000,Cellular, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900, LORA,	Information
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 461.

The Figure 44: Issues Status Bar, on page 479 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 43: OPERATIONS ISSUES

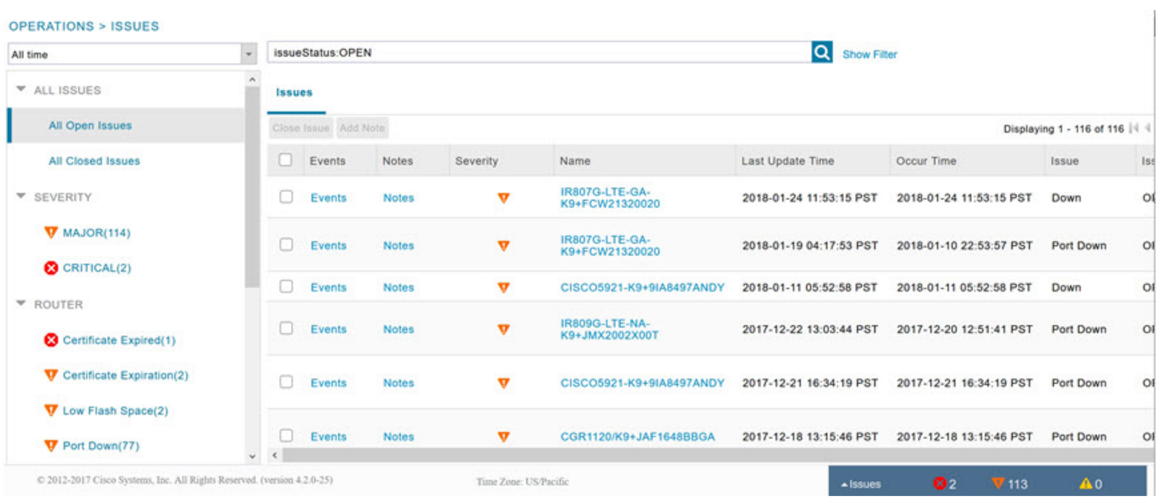


Figure 44: Issues Status Bar

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.

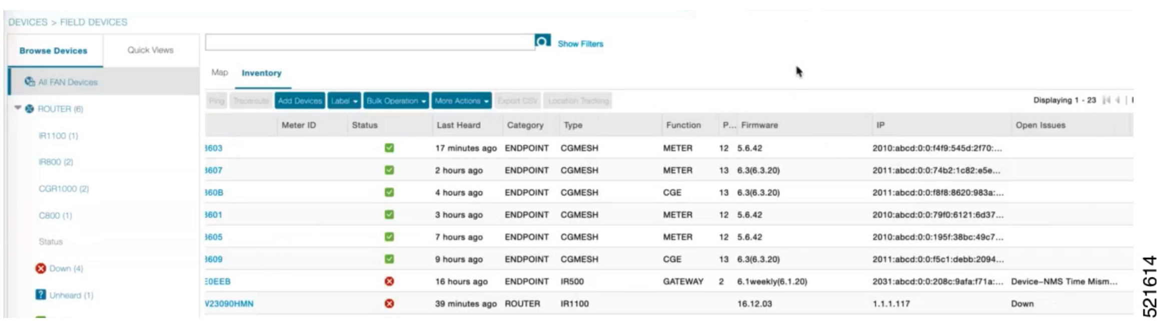
Click the Issues status bar to view the Issues Summary pane, which displays issues listed by the selected device category. Click count links in the Issues Summary pane to view complete issue criteria filtered by severity on the **OPERATIONS** > **Issues** page.

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

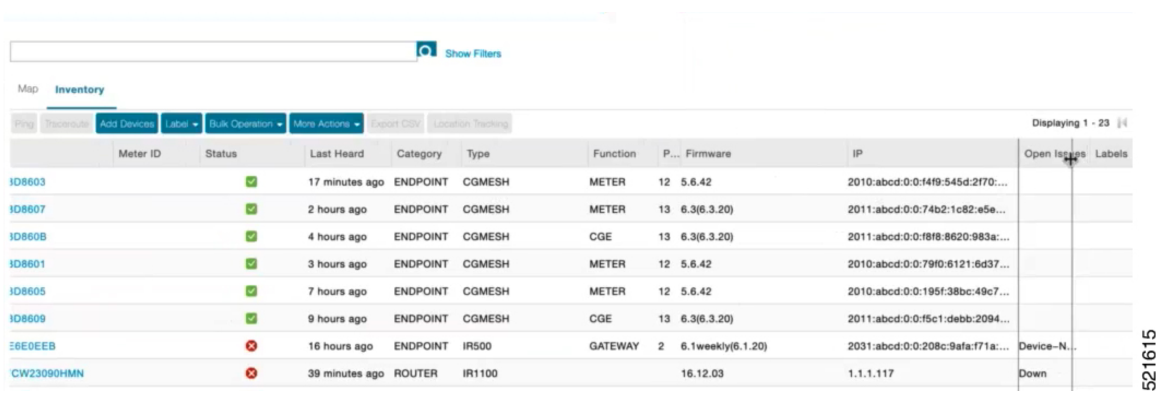
At the **DEVICES** > **FIELD DEVICES** > **Browse Devices** > **Inventory** page, multiple entries of the same Open Issue (such as Device-NMS Time Mismatch, Down) for a given device will display as one entry only. This reduces multiple entries of the same Open Issue for a Field Device from filling up the display window.

Figure 45: DEVICES > FIELD DEVICES > Browse Devices > Inventory



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 46: DEVICES > FIELD DEVICES > Browse Devices > Inventory page with Open Issues Column Resized, on page 480 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 46: 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 47: Issues Status Bar

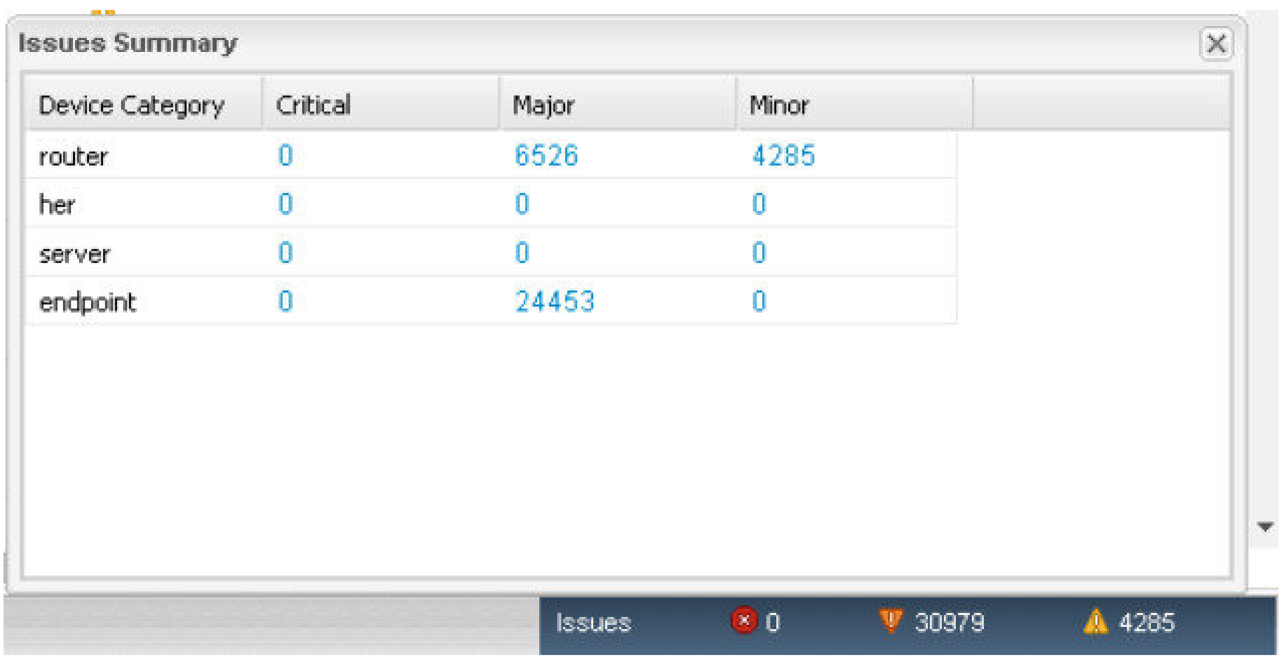
To view the device severity status on the issue status bar:

Procedure

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 48: Issues Summary Pane

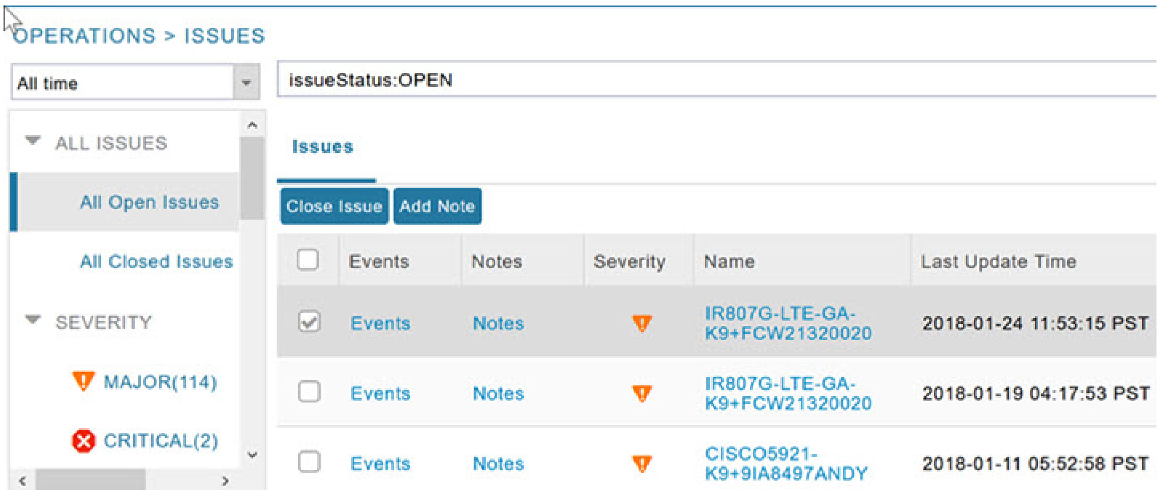


Adding Notes to Issues

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:

Procedure

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:

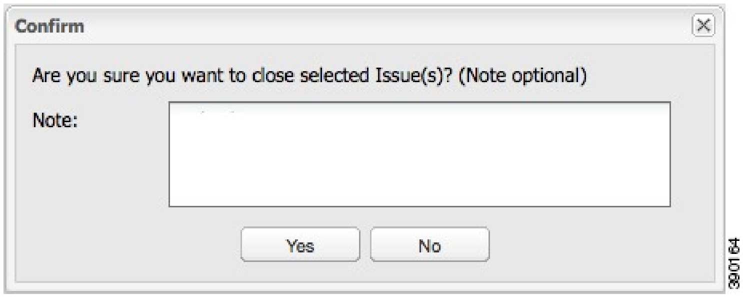
a) Click the **Notes** link inline with the issue.

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:

Procedure

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 130):

- 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:

Procedure

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):

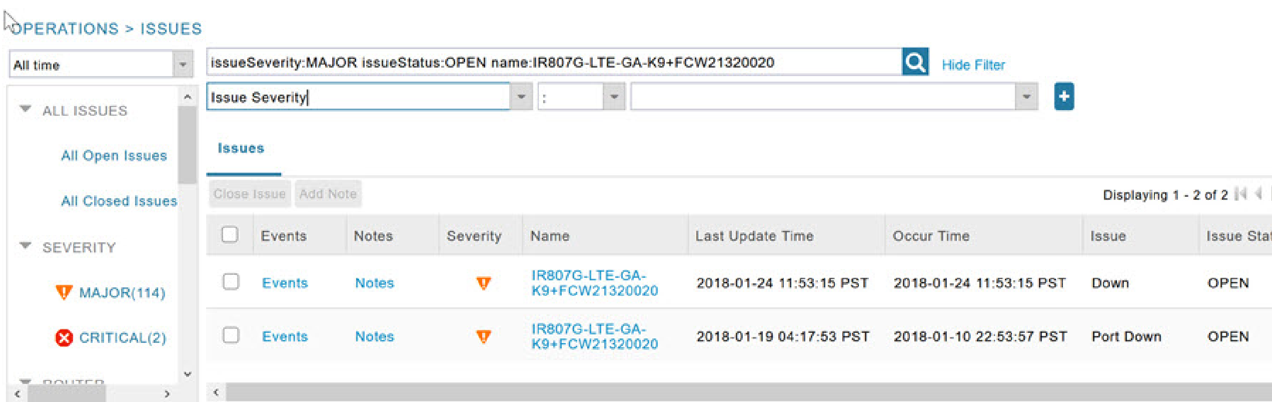
- In the left pane, select a Severity level (such as Major). The filter name populates the first field (top) of the Filter.
- From the second Filter drop-down menu on the left, choose **Name**.
- In the third Filter field, enter the EID of the device to discover issues about.
- Click the search icon (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

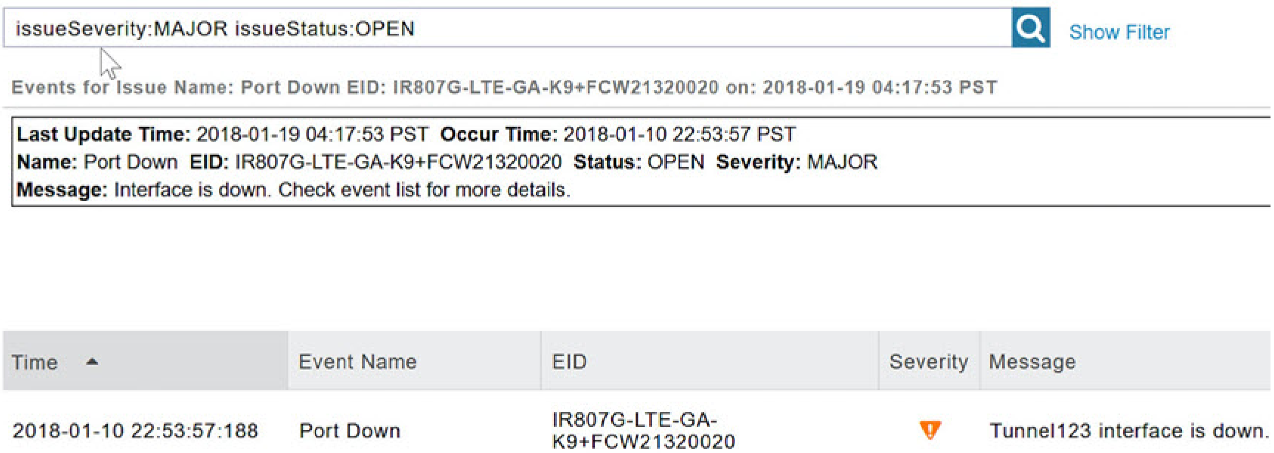
Step 4 Click **Search Issues**.

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:

Procedure

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 483 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

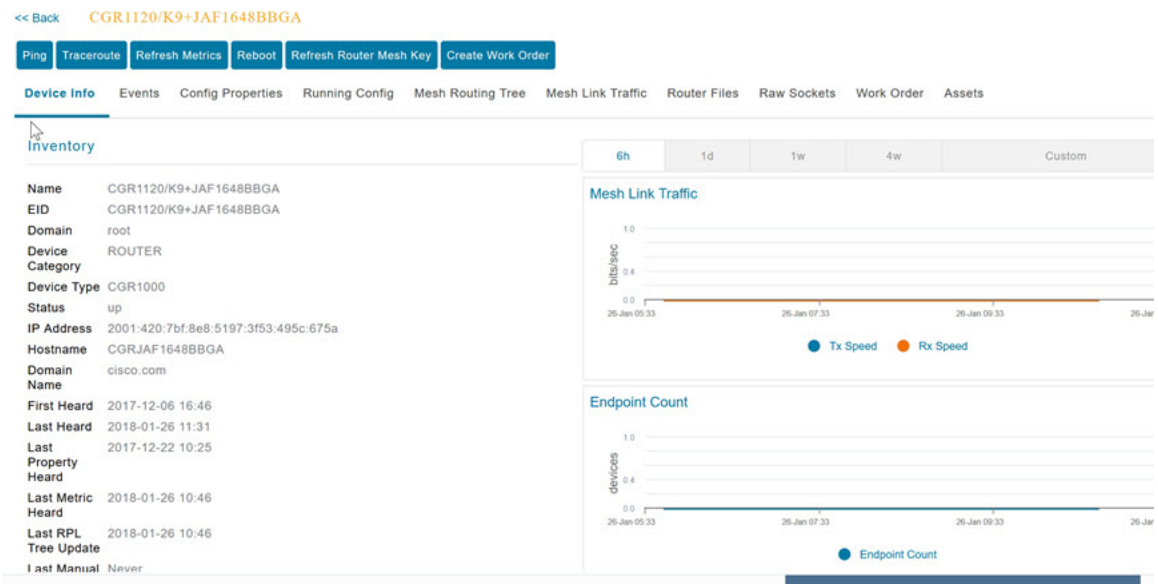
IoT FND provides these charts in the Device Info pane on the Device Details page for any router:

Table 95: Device Detail Charts

Chart	Description
Link Traffic	Shows the aggregated WPAN rate for a router over time. To view the chart for default or custom-defined time intervals, refer to Setting Time Filters To View Charts, on page 461.
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 49: 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 96: Device Detail Charts

Chart	Description
Link Traffic	Shows the aggregated WPAN rate for an endpoint over time. To view the chart for default or custom-defined time intervals, refer to Setting Time Filters To View Charts, on page 461
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 50: Mesh Endpoint Device Info Page (partial view)

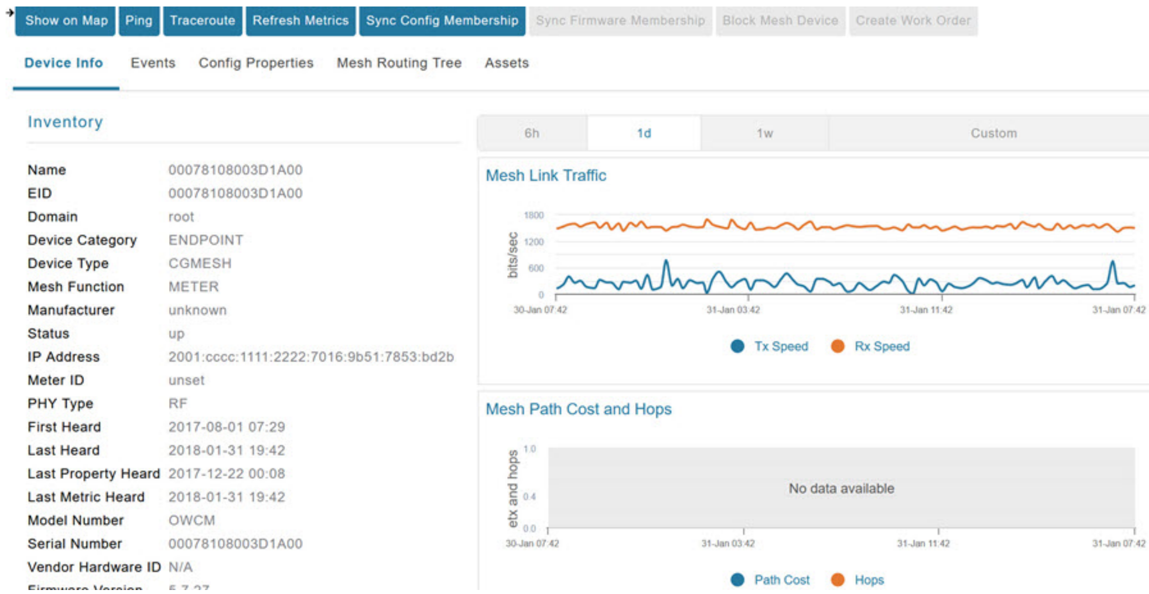
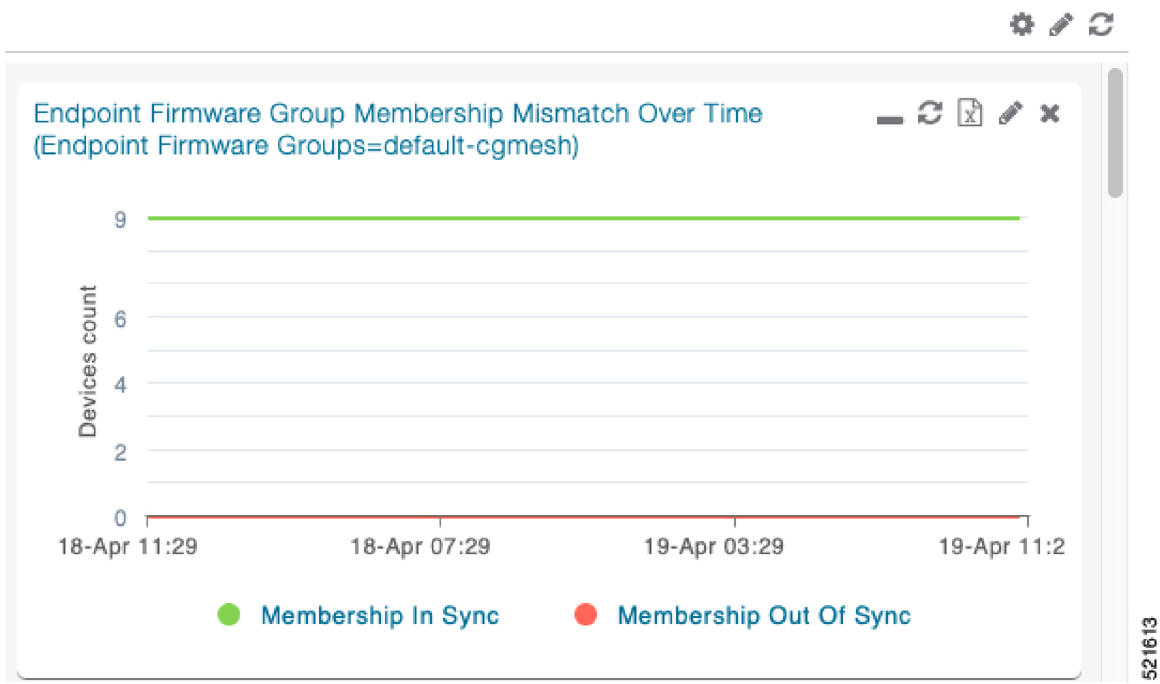


Figure 51: Mesh Endpoint Firmware Group Mismatch Over Time Page



CHAPTER 10

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.

Table 97: Feature History

Feature Name	Release Information	Description
Full Open CoAP Simple Management Protocol Support	Cisco IoT FND Release 5.0	A Vendor TLV 127 value support is added to the Full Open CoAP Simple Management Protocol (CSMP) for the Cisco IoT FND devices. A new tab **Vendor TLV Info** is introduced where you can add the TLV details for a selected device. You can modify and retrieve Vendor TLV details and push the modified configuration to new endpoints. You can also upgrade and manage the firmware with supported TLVs.

- Signing CSMP Message, on page 526
- Firmware Upgrade, on page 526

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.

Procedure

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": [ ] ,
 "vendorId": " ",
 "vendorName": " ",
 "device_actions": [
 "reboot",
  "ping",
 "traceroute",
 "inventory",
     ]
"configure_vendortlv": "",
 "hw_info": " "
   }
}
```

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").
vendorId	Enter the vendorId which is used in Vendor TLV 127
vendorName	Enter the vendor name which corresponds to the vendorId.
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.
configure_vendortlv	By default, it is set to false. Enter true for FND to support config push of vendor TLV 127.

Field	Description
hw_info	Enter the hardware info for the device type which is present in the firmware image header.

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:

Procedure

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>
```

```
      &lt;displayName&gt;Protocol&lt;/displayName&gt;
      &lt;description&gt;Protocol for Low Pan Interface&lt;/description&gt;
    &lt;/propertyType&gt;
    &lt;propertyType&gt;
      &lt;name&gt;aclDirectionLp&lt;/name&gt;
      &lt;displayName&gt;Direction&lt;/displayName&gt;
      &lt;description&gt;Direction for Low Pan Interface&lt;/description&gt;
    &lt;/propertyType&gt;
    &lt;propertyType&gt;
      &lt;name&gt;aclSrcPortLp&lt;/name&gt;
      &lt;displayName&gt;Source Port&lt;/displayName&gt;
      &lt;description&gt;Source Port for Low Pan Interface&lt;/description&gt;
    &lt;/propertyType&gt;
    &lt;propertyType&gt;
      &lt;name&gt;aclDstPortLp&lt;/name&gt;
      &lt;displayName&gt;Destination Port&lt;/displayName&gt;
      &lt;description&gt;Destination Port for Low Pan Interface&lt;/description&gt;
    &lt;/propertyType&gt;
    &lt;propertyType&gt;
      &lt;name&gt;aclMaxRateLimit&lt;/name&gt;
      &lt;displayName&gt;ACL Max Rate Limit (kb/s)&lt;/displayName&gt;
      &lt;description&gt;ACL Max Rate Limit used for Rate Limit validation&lt;/description&gt;
    &lt;/propertyType&gt;
  &lt;/propertyTypes&gt;
&lt;/cgms&gt;
```

Mesh Metric Types

The following is a sample list of mesh metric types for the end point device.

```
&lt;?xml version="1.0" encoding="UTF-8" ?&gt;
<cgms xmlns="http://www.w3.org"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  &lt;metricTypes kind="cgmesh"&gt;
    &lt;metricType&gt;
      &lt;name&gt;uptime&lt;/name&gt;
      &lt;valueType&gt;gauge&lt;/valueType&gt;
      &lt;displayName&gt;Uptime&lt;/displayName&gt;
      &lt;unit&gt;sec&lt;/unit&gt;
      &lt;description&gt;The amount of time in seconds that the element has been running since
last boot&lt;/description&gt;
      &lt;lowerBound&gt;0&lt;/lowerBound&gt;
      &lt;upperBound&gt;31536000&lt;/upperBound&gt;
      &lt;displayFormat&gt;secondsToTime&lt;/displayFormat&gt;
    &lt;/metricType&gt;
    &lt;metricType&gt;
      &lt;name&gt;meshTxSpeed&lt;/name&gt;
      &lt;valueType&gt;gauge&lt;/valueType&gt;
      &lt;displayName&gt;Mesh Link Transmit Speed&lt;/displayName&gt;
      &lt;unit&gt;bits/sec&lt;/unit&gt;
     &lt;description&gt;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)&lt;/description&gt;
      &lt;lowerBound&gt;0&lt;/lowerBound&gt;
      &lt;upperBound&gt;76800&lt;/upperBound&gt;
      &lt;displayFormat&gt;###,###&lt;/displayFormat&gt;
    &lt;/metricType&gt;
    &lt;metricType&gt;
      &lt;name&gt;meshTxDrops&lt;/name&gt;
      &lt;valueType&gt;gauge&lt;/valueType&gt;
      &lt;displayName&gt;Mesh Link Transmit Packet Drops&lt;/displayName&gt;
      &lt;unit&gt;drops/sec&lt;/unit&gt;
      &lt;description&gt;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>
```

```
      &lt;name&gt;rfFsk2Dr150WtFecLU&lt;/name&gt;
      &lt;valueType&gt;cumulative&lt;/valueType&gt;
      &lt;displayName&gt;Modulation 2FSK 150 without FEC link usage&lt;/displayName&gt;
      &lt;unit&gt;&lt;/unit&gt;
      &lt;description&gt;Cumulative link usage of modulation 2FSK 150 without FEC&lt;/description&gt;
      &lt;lowerBound&gt;0&lt;/lowerBound&gt;
    &lt;/metricType&gt;
    &lt;metricType&gt;
      &lt;deviceType&gt;wpan&lt;/deviceType&gt;
      &lt;name&gt;rfFsk2Dr150WFecLU&lt;/name&gt;
      &lt;valueType&gt;cumulative&lt;/valueType&gt;
      &lt;displayName&gt;Modulation 2FSK 150 with FEC link usage&lt;/displayName&gt;
      &lt;unit&gt;&lt;/unit&gt;
      &lt;description&gt;Cumulative link usage of modulation 2FSK 150 with FEC&lt;/description&gt;
      &lt;lowerBound&gt;0&lt;/lowerBound&gt;
    &lt;/metricType&gt;
    &lt;metricType&gt;
      &lt;deviceType&gt;wpan&lt;/deviceType&gt;
      &lt;name&gt;phyTxSpeed&lt;/name&gt;
      &lt;valueType&gt;counter&lt;/valueType&gt;
      &lt;displayName&gt;Transmit Speed on PHY layer(PLC and RF combined)&lt;/displayName&gt;
      &lt;unit&gt;bits/sec&lt;/unit&gt;
      &lt;description&gt;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)&lt;/description&gt;
      &lt;lowerBound&gt;0&lt;/lowerBound&gt;
      &lt;upperBound&gt;76800&lt;/upperBound&gt;
    &lt;/metricType&gt;
    &lt;metricType&gt;
      &lt;deviceType&gt;wpan&lt;/deviceType&gt;
      &lt;name&gt;phyRxSpeed&lt;/name&gt;
      &lt;valueType&gt;counter&lt;/valueType&gt;
      &lt;displayName&gt;Receive Speed on PHY layer(PLC and RF combined)&lt;/displayName&gt;
      &lt;unit&gt;bits/sec&lt;/unit&gt;
      &lt;description&gt;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)&lt;/description&gt;
      &lt;lowerBound&gt;0&lt;/lowerBound&gt;
      &lt;upperBound&gt;76800&lt;/upperBound&gt;
    &lt;/metricType&gt;
    &lt;metricType&gt;
      &lt;deviceType&gt;ppp&lt;/deviceType&gt;
      &lt;name&gt;txSpeed&lt;/name&gt;
      &lt;valueType&gt;counter&lt;/valueType&gt;
      &lt;displayName&gt;Transmit Speed&lt;/displayName&gt;
      &lt;unit&gt;bits/sec&lt;/unit&gt;
      &lt;description&gt;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)&lt;/description&gt;
      &lt;lowerBound&gt;0&lt;/lowerBound&gt;
      &lt;upperBound&gt;76800&lt;/upperBound&gt;
    &lt;/metricType&gt;
    &lt;metricType&gt;
      &lt;deviceType&gt;ppp&lt;/deviceType&gt;
      &lt;name&gt;txDrops&lt;/name&gt;
      &lt;valueType&gt;counter&lt;/valueType&gt;
      &lt;displayName&gt;Transmit Packet Drops&lt;/displayName&gt;
      &lt;unit&gt;drops/sec&lt;/unit&gt;
      &lt;description&gt;The rate of packets that were dropped while trying to transmit on the
interface because the outbound queue was full&lt;/description&gt;
      &lt;lowerBound&gt;0&lt;/lowerBound&gt;
      &lt;upperBound&gt;1&lt;/upperBound&gt;
    &lt;/metricType&gt;
    &lt;metricType&gt;
```

```
      <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>
```

```
    &lt;displayName&gt;Mesh Tone Map Forward Tone Quality&lt;/displayName&gt;
    &lt;unit&gt;&lt;/unit&gt;
    &lt;description&gt;The number of bits set in the tone map vector&lt;/description&gt;
    &lt;lowerBound&gt;0&lt;/lowerBound&gt;
    &lt;upperBound&gt;24&lt;/upperBound&gt;
  &lt;/metricType&gt;
  &lt;metricType&gt;
    &lt;deviceType&gt;RPL&lt;/deviceType&gt;
    &lt;name&gt;tmRevTxResRaw&lt;/name&gt;
    &lt;valueType&gt;gauge&lt;/valueType&gt;
    &lt;displayName&gt;Mesh Tone Map Reverse Tx Res Raw&lt;/displayName&gt;
    &lt;unit&gt;&lt;/unit&gt;
    &lt;description&gt;The txres field integer value in tone map reverse message&lt;/description&gt;
    &lt;lowerBound&gt;-1000&lt;/lowerBound&gt;
    &lt;upperBound&gt;1000&lt;/upperBound&gt;
  &lt;/metricType&gt;
  &lt;metricType&gt;
    &lt;deviceType&gt;RPL&lt;/deviceType&gt;
    &lt;name&gt;tmRevTxGainRaw&lt;/name&gt;
    &lt;valueType&gt;gauge&lt;/valueType&gt;
    &lt;displayName&gt;Mesh Tone Map Reverse Tx Gain Raw&lt;/displayName&gt;
    &lt;unit&gt;&lt;/unit&gt;
    &lt;description&gt;The txres gain integer value in tone map reverse message&lt;/description&gt;
    &lt;lowerBound&gt;-1000&lt;/lowerBound&gt;
    &lt;upperBound&gt;1000&lt;/upperBound&gt;
  &lt;/metricType&gt;
  &lt;metricType&gt;
    &lt;deviceType&gt;RPL&lt;/deviceType&gt;
    &lt;name&gt;tmRevTxGain&lt;/name&gt;
    &lt;valueType&gt;gauge&lt;/valueType&gt;
    &lt;displayName&gt;Mesh Tone Map Reverse Tx Gain&lt;/displayName&gt;
    &lt;unit&gt;&lt;/unit&gt;
    &lt;description&gt;Equals to txResRaw * txResGain&lt;/description&gt;
    &lt;lowerBound&gt;-1000000&lt;/lowerBound&gt;
    &lt;upperBound&gt;1000000&lt;/upperBound&gt;
  &lt;/metricType&gt;
  &lt;metricType&gt;
    &lt;deviceType&gt;RPL&lt;/deviceType&gt;
    &lt;name&gt;tmRevToneQuality&lt;/name&gt;
    &lt;valueType&gt;gauge&lt;/valueType&gt;
    &lt;displayName&gt;Mesh Tone Map Reverse Tone Quality&lt;/displayName&gt;
    &lt;unit&gt;&lt;/unit&gt;
    &lt;description&gt;The number of bits set in the tone map reverse vector&lt;/description&gt;
    &lt;lowerBound&gt;0&lt;/lowerBound&gt;
    &lt;upperBound&gt;24&lt;/upperBound&gt;
  &lt;/metricType&gt;
  &lt;metricType&gt;
    &lt;deviceType&gt;RPL&lt;/deviceType&gt;
    &lt;name&gt;absolutePhase&lt;/name&gt;
    &lt;valueType&gt;gauge&lt;/valueType&gt;
    &lt;displayName&gt;Mesh absolute phase of power&lt;/displayName&gt;
    &lt;unit&gt;&lt;/unit&gt;
    &lt;description&gt;Relative position of current and voltage waveforms for a PLC
Node&lt;/description&gt;
    &lt;lowerBound&gt;0&lt;/lowerBound&gt;
    &lt;upperBound&gt;76800&lt;/upperBound&gt;
  &lt;/metricType&gt;
  &lt;metricType&gt;
    &lt;deviceType&gt;RPL&lt;/deviceType&gt;
    &lt;name&gt;rank&lt;/name&gt;
    &lt;valueType&gt;gauge&lt;/valueType&gt;
    &lt;displayName&gt;Mesh Route RPL Rank&lt;/displayName&gt;
    &lt;unit&gt;&lt;/unit&gt;
    &lt;description&gt;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>
```

License Support

The registered devices utilize the current endpoint license for lifecycle management in FND.

Viewing Endpoints on Dashboard

On the FND dashboard, the endpoints dashlets display the following properties for the registered devices:

- Endpoint States Over Time
- Endpoint Config Group Template Mismatch Over Time
- Endpoint Firmware Group Template Mismatch Over Time
- Endpoint Inventory
- Hop Count Distribution
- Config Group Template Mismatch
- Firmware Group Template Mismatch
- RF and PLC Media utilization over time

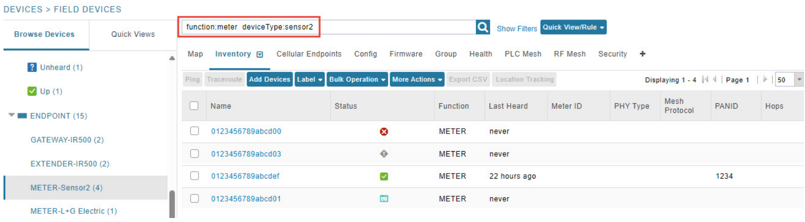
Viewing Endpoints on Field Devices Page

The registered endpoint devices appear on the Field Devices page, with the device type and function as defined in the meta data file; their function is similar to the existing endpoints in FND.

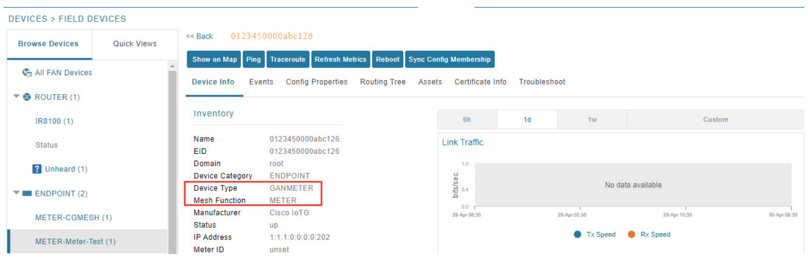
To view the registered devices:

Procedure

Step 1 Choose **DEVICES** > **Field Devices** > **ENDPOINTS** to view the inventory of the registered device.



Step 2 Click the registered endpoint device to view the device information.



Both the Device Inventory and the Device Details pages display the tabs, buttons, filter options similar to the existing endpoints in FND.

Viewing VendorTLV on Field Devices Page

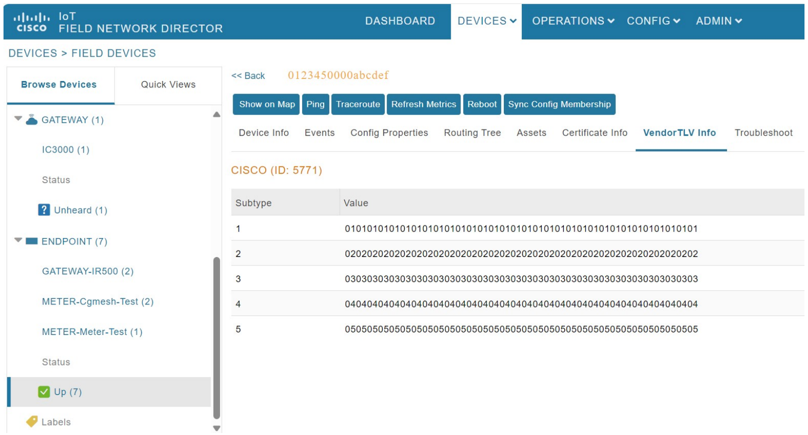
The vendor TLV details are added in the inventory page. It also displays vendor name in the following format as vendor name (vendor-id). For example, Cisco (ID: 5771) , where ID refers IANA PEN of the vendor received by FND during device registration.

To view the vendor details:

Procedure

Step 1 Choose **DEVICES** > **Field Devices** > **ENDPOINTS** to view the inventory of the registered device.

Step 2 In the Device Details page, navigate to **VendorTLV info** tab to view the vendor name, vendor ID and the list of **Subtype** and its **Value**.



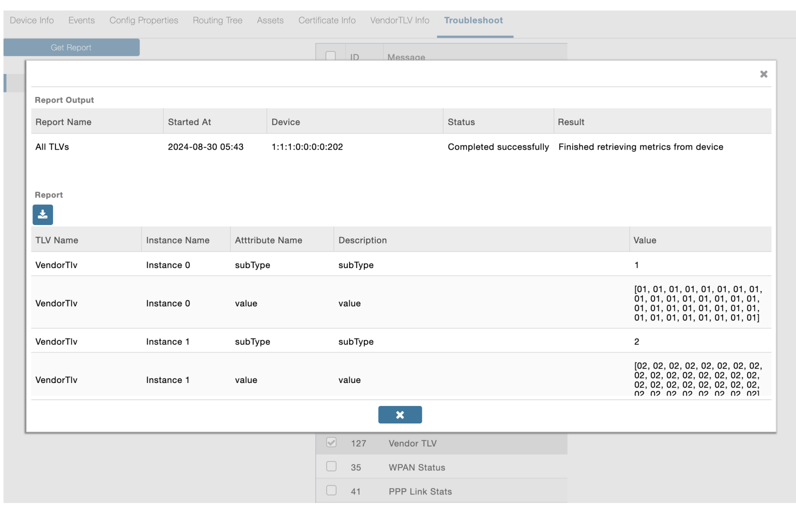
Viewing Response from the Endpoint for the VendorTLV

To view the response from the endpoint for the VendorTLV:

Procedure

Step 1 Choose **DEVICES** > **Field Devices** > **ENDPOINTS** to view the inventory of the registered device.

Step 2 In the Device Details page, navigate to **Troubleshoot** tab to view the response from the endpoint for the VendorTLV 127.



Configuring Markdown Timer

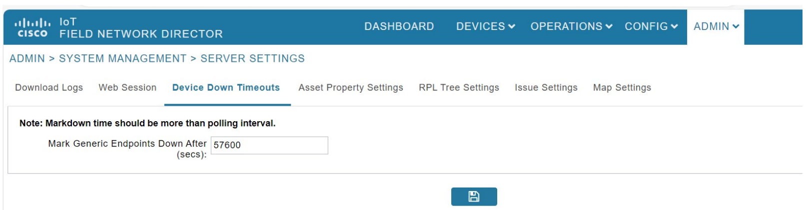
Once the endpoint is added with the generic device type, the **Mark Generic Endpoints Down After** option is enabled in **Device Down Timeouts** tab.

To configure the Markdown timer:

Procedure

Step 1 Choose **ADMIN** > **System Management** > **Server Settings**.

Step 2 Click the **Device Down Timeouts** tab.



Step 3 Enter the time in the **Mark Generic Endpoints Down After** field.

Step 4 Click the disk icon to save the configuration.

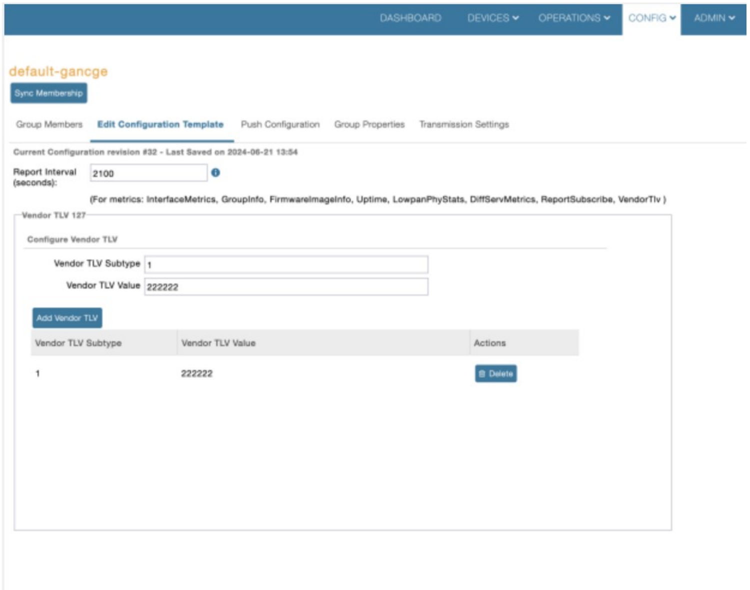
Supported Periodic Metric TLVs

FND supports the following TLVs for periodic metrics.

TLV ID	TLV Name
23	Interface Metrics
17	IP Route
25	IP Route RPL Metrics
58	Group Info
75	Firmware Image Info
22	Uptime
61	LoWPAN PHY Stats
88	DiffServ Metrics
13	Report Subscribe
127	Vendor TLV

Procedure

Step 1 Choose **CONFIG** > **Device Configuration** > **Edit Configuration Template** tab.



Step 2 Select the **Vendor TLV Subtype** from the drop-down list and click **Add Vendor TLV** to configure the Vendor TLV.

Pushing Configuration

The registered endpoint devices appear in the UI with the default configuration group name (default-deviceType). The configuration defined for the devices is read from the meta data file and is reflected in the default configuration group. The Cisco IoT FND release 4.12 allows you to configure and process only the report interval TLV metrics for the new endpoint devices.

Cisco IoT FND release 5.0 allows you to change and retrieve the Vendor TLV details and push the configuration to the new endpoint devices.

The default template configuration is:

```
[{
    "name": "ReportSubscribe",
    "value": {
        "interval": 28800,
        "tlvid": ["InterfaceMetrics", "IPRoute", "IPRouteRPLMetrics", "GroupInfo",
"FirmwareImageInfo", "Uptime", "LowpanPhyStats", "DiffServMetrics", "ReportSubscribe",
"VendorTlv"]
    } }]
```

When you select the **RPL Tree Settings** as **Mesh Nodes**, add the VendorTLV in the metadata file `default[devicetype]Template.json`.

When you select the **RPL Tree Settings** as **Router**, add the VendorTLV in the metadata file `default[devicetype]NoIPRouteTemplate.json file`.

The events defined in the `deviceTypeEventTypes.xml` are applicable for the new endpoint devices.

Procedure

Step 1 Choose **CONFIG** > **Device Configuration** > **Push Configuration** tab.

Step 2 Select Push ENDPOINT Configuration from the drop-down list and click **Submit** to push the configuration to the devices from FND.

Signing CSMP Message

To enable the CSMP signing in FND the following configuration is required:

- Ensure that the CSMP certificate, present in FND, is installed in the endpoint.
- Enable the CSMP signing setting in the endpoints.

Firmware Upgrade

Starting from Cisco IoT FND release 5.0 the following TLVs are supported as a part of Firmware upgrade and management.

TLV ID	TLV Name
65	Transfer Request
67	Image Block
68	Load Request
69	Cancel Load Request
70	Set Backup Request
71	Transfer Response
72	Load Response
73	Cancel Load Response
74	Set Backup Response
75	Firmware Image Info

Cisco IoT FND reads the following fields in the firmware image header:

```
hdrVersion - mandatory
hdrLen - mandatory
appRevMajor - mandatory
appRevMinor - mandatory
appBuild - mandatory
appLen - mandatory
appName - mandatory
appGitBranch - not mandatory
appGitCommit - not mandatory
appGitFlag - not mandatory
appBuildDate - mandatory
hw_info - mandatory
kernelVersion - not mandatory
```

Update the hw_info field in the `deviceTypeMeta.json` file with the same hw_info present in the firmware image header. FND maps the hw_info with the device type internally.

Navigate to **CONFIG** > **Firmware Update** > **Images** tab and select the endpoint **PLC-RF** to upload the firmware images.

CHAPTER 11

Troubleshooting IoT FND

This chapter is moved to the Troubleshooting Guide for Cisco IoT Field Network Director.