



Cisco IoT Field Network Director Configuration Guide, Release 4.3.x

First Published: September 2018



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](#)
- [How to Use This Guide](#)
- [Interface Overview](#)

Cisco IoT Connected Grid Network

This section provides an overview of:

- [Cisco IoT FND Features and Capabilities](#)
- [IoT FND Architecture](#)
- [Resilient Mesh Endpoints](#)
- [Grid Security](#)
- [Related Software](#)

The Cisco IoT Field Network Director (IoT FND) is a software platform that manages a 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 (for example, C800 or C819) 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 upgradeable, so you can add new services without changing equipment.
- Cisco 800 Series Industrial Integrated Services Routers (IR800s) are compact, ruggedized, Cisco IOS Software routers. They offer support for integrated 4G LTE wireless WAN (IR807, IR809 and IR829 models) and wireless LAN capabilities (IR829 only). These devices are referred to as routers in this document; and identified by product ID (for example, IR800) on the Field Devices page. You can use IoT FND to manage the following IR800 models:
 - IR807: Highly compact, low-power industrial router. Well-suited for industrial applications (distribution automation for utilities, transportation, manufacturing) and remote asset management across the extended enterprise.
 - IR809: Very compact, cellular (3G,4G/LTE) industrial routers that enable reliable and secure cellular connectivity for remote asset monitoring and machine-to-machine (M2M) applications such as distribution automation, pipeline monitoring and roadside infrastructure monitoring.
 - IR829: Highly ruggedized compact cellular (3G and 4G LTE with GPS and dual SIM) and WLAN (2.4/5GHz) industrial routers supporting scalable, reliable and secure management of those IoT applications requiring mobile connectivity such as fleet vehicles and mass transit.

- Cisco 5921 Embedded Services Router (ESR) is designed to operate on small, low-power, Linux-based platforms. It helps integration partners extend the use of Cisco IOS into extremely mobile and portable communications systems. It also provides highly secure data, voice, and video communications to stationary and mobile network nodes across wired and wireless links.
- Cisco Industrial Compute (IC3000) Gateway supports edge computing and communicates with IoT FND through the IOx application, Cisco Fog Director (FD). A subset of FD is provided. With built-in interfaces that support a wide range of industrial standards and a simple development toolkit, the IC3000 enables application developers to create apps to harness IoT data.
- 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 supported, which are differentiated by their band support (863-870 MHz ISM or 902-928 MHz ISM). The module is identified by product ID (for example, IXM-LORA-800-H-V2).
- Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR500) supply RF mesh connectivity to IPv4 and serial IoT devices (for example, recloser control, cap bank control, voltage regulator controls, and other remote terminal units).

Note: CGRs, C800s, IR800s, IR500s and other types of Cisco Resilient Mesh endpoints (RMEs) can coexist on a network, but cannot be in the same device group (see [Creating Device Groups](#) and [Working with Resilient Mesh Endpoint Firmware Images](#)) or firmware management group (see [Configuring Firmware Group Settings](#)).

- Cisco 800 Series Access Points are integrated with IR800s and C800s. These devices are referred to as routers in this document; and identified by product ID (for example, AP800). You can use IoT FND to manage the following AP800 models:
 - AP802 embedded in C800
 - AP803 embedded in IR829
- Cisco ASR 1000 Series Aggregation Services Routers (ASRs), Cisco ISR 3900 Series Integrated Service Routers (ISRs), and ISR 4300 and ISR 4400 routers are referred to as *head-end routers* or HERs in this document.
- Cisco IPv6 RF (radio frequency), PLC (power line communications), and Dual PHY (RF and PLC) mesh endpoints (smart meters and range extenders).

Note: In this document, *mesh endpoints* refers to Cisco range extenders and Cisco-compatible smart meters.

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 *Cisco IoT FND NMS North Bound API Programming Guide* 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 published by the NB API client (the event consumer) while making the secure connection.

Cisco IoT FND Features and Capabilities

- **Configuration Management** – Cisco IoT FND facilitates configuration of a large number of Cisco CGRs, Cisco C800s, Cisco ISRs, Cisco IRs, Cisco ASRs, and mesh endpoints. Use Cisco IoT FND to bulk-configure devices by placing them into configuration groups, editing settings in a configuration template, and then pushing the configuration to all devices in the group.
- **Device and Event Monitoring** – Cisco IoT FND displays easy-to-read tabular views of extensive information generated by devices, allowing you to monitor your network for errors. Cisco IoT FND provides integrated Geographic Information System (GIS) map-based visualization of FAN devices such as routers and smart meters. Use IoT FND to create CGR-specific work orders that include the required certificates to access the router.
- **Firmware Management** – Cisco IoT FND serves as a repository for Cisco CGR, Cisco C800, Cisco ISR, Cisco IR, and mesh endpoint firmware images. Use Cisco IoT FND to upgrade the firmware running on groups of devices by loading the firmware image file onto the Cisco IoT FND server, and then uploading the image to the devices in the group. Once uploaded, use IoT FND to install the firmware image directly on the devices. In release 3.0.1-36 and later, a Subnet List view on the Firmware Upgrade page for Mesh Endpoints lets you filter and view subnets by PAN identifier (PAN ID) and Group (details include number of nodes within a group, hops away from the router and operational status). A subnet progress histogram has also been added.
- **OS Migration** – For Cisco CGR 1000, IoT FND allows you to migrate CGRs running CG-OS to IOS.
- **Zero Touch Deployment** – This ease-of-use feature automatically registers (enrolls) and distributes X.509 certificates and provisioning information over secure connections within a connected grid network.
- **Tunnel Provisioning** – Protects data exchanged between Cisco ASRs and Cisco CGRs, C800s, Cisco ISRs and Cisco IRs, and prevents unauthorized access to Cisco CGRs, to provide secure communication between devices. Cisco IoT FND can execute CLI commands to provision secure tunnels between Cisco CGRs, C800s, Cisco ISRs and Cisco IRs and Cisco ASRs. Use IoT FND to bulk-configure tunnel provisioning using groups.
- **IPv6 RPL Tree Polling** – The IPv6 Routing Protocol for Low-power and Lossy Networks (RPL) finds its neighbors and establishes routes using ICMPv6 message exchanges. RPL manages routes based on the relative position of the mesh endpoints to the CGR that is the root of the routing tree. RPL tree polling is available through the mesh nodes and CGR periodic updates. The RPL tree represents the mesh topology, which is useful for troubleshooting. For example, the hop count information received from the RPL tree can determine the use of unicast or multicast for the firmware download process. IoT FND maintains a periodically updated snapshot of the RPL tree.
- **Dynamic Multipoint VPN and FlexVPN** – For Cisco C800 devices and Cisco IR800 devices, DMVPN and FlexVPN do not require IoT FND to apply device-specific tunnel configuration to the HER during tunnel provisioning. HER tunnel provisioning is only required for site-to-site VPN tunnels.
- **Embedded Access Point (AP) Management** – IoT FND provides management of embedded APs on C819 and IR829 routers.
- **Dual PHY Support** – IoT FND can communicate with devices that support Dual PHY (RF and PLC) traffic. IoT FND identifies CGRs running Dual PHY, enables configuration to masters and slaves, and collects metrics from masters. IoT FND also manages security keys for Dual PHY CGRs. On the mesh side, IoT FND identifies Dual PHY nodes using unique hardware IDs, enables configuration pushes and firmware updates, and collects metrics, including RF and PLC traffic ratios.
- **Guest OS (GOS) Support** – For Cisco IOS CGR 1000 and IR800 devices that support Guest OS, IoT FND allows approved users to manage applications running on the supported operating systems. IoT FND supports all phases of application deployment, and displays application status and the Hypervisor version running on the device.
- **Device Location Tracking** – For CGR 1000, C800, and IR800 devices, IoT FND displays real-time location and device location history. This feature requires enabling the GPS feature.

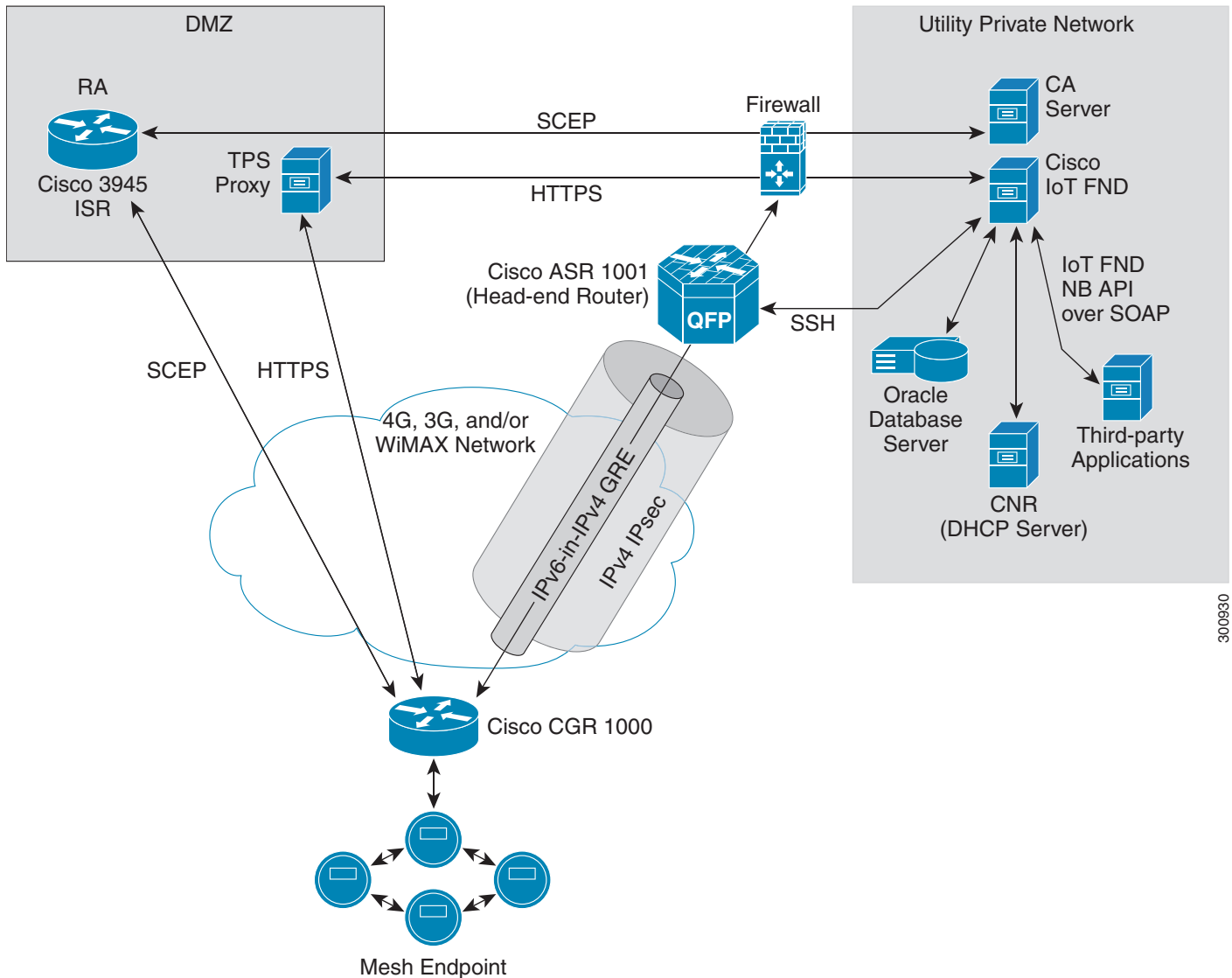
- **Software Security Module (SSM)** – This is a low-cost alternative to the Hardware Security Module (HSM), and is used for signing CSMP messages sent to meters and IR500 devices.
- **Customer Certificates** – Cisco IoT FND allows you to use your own CA and ECC-based certificates to sign smart meter messages.
- **Diagnostics and Troubleshooting** – The IoT FND rule engine infrastructure provides effective monitoring of triage-based troubleshooting. Device troubleshooting runs on-demand device path trace and ping on any CGR 1000, IR800, Cisco Series Integrated Services Routers (C800), Cisco 5921 Embedded Services Router (C5921), range extender, gateway or meter (mesh endpoints).
- **High Availability** – To ensure uninterrupted network management and monitoring, you can deploy the Cisco IoT FND solution in a High Availability (HA) configuration. By using clusters of load-balanced IoT FND servers and primary and standby IoT FND databases, Cisco IoT FND constantly monitors the health of the system, including connectivity within clusters and server resource usage. If a server cluster member or database becomes unavailable or a tunnel fails, another takes its place seamlessly. Additionally, you can add reliability to your IoT FND solution by configuring redundant tunnels between a Cisco CGR and multiple Cisco ASRs.
- **Power Outage Notifications** – Mesh Endpoints (MEs) implement a power outage notification service to support timely and efficient reporting of power outages. In the event of a power outage, MEs perform the necessary functions to conserve energy and notify neighboring nodes of the outage. Routers relay the power outage notification to IoT FND, which then issues push notifications to customers to relate information on the outage.
- **Resilient Mesh Upgrade Support** – Over-the-air software and firmware upgrades to field devices such as Cisco CGRs and Resilient Mesh Endpoints (RMEs) (for example, AMI meter endpoints).
- **Audit Logging** – Logs access information for user activity for audit, regulatory compliance, and Security Event and Incident Management (SEIM) integration. This simplifies management and enhances compliance by integrated monitoring, reporting, and troubleshooting capabilities.
- **North Bound APIs** – Eases integration of existing utility applications such as outage management system (OMS), meter data management (MDM), trouble-ticketing systems, and manager-of-managers.
- **Work Orders for Device Manager** – Credentialed field technicians can remotely access and update work orders.
- **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 provides a high-level view of the systems and communication paths that exist in a typical utility company operating on a Cisco CGR connected grid network in which Zero Touch Deployment is in use.

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

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

Figure 1 Zero Touch Deployment Architecture

300930

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 RA (Cisco 3945 ISR in Figure 1), functioning as a CA proxy, obtains certificates for the Cisco CGR from the CA. 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 ASR 1001 in Figure 1). For CG-OS CGR installations, we recommend a network configuration with an outer IPsec tunnel over IPv4 inside which is an IPv6-in-IPv4 GRE tunnel. All traffic from the MEs is over IPv6. The GRE tunnel provides a path for IPv6 traffic to reach the data center. The outer IPsec tunnel secures that traffic. When the tunnel is active, the Cisco CGR (after configuration) connects to the utility company network like a Virtual Private Network (VPN).

Main Components of a IoT FND Solution

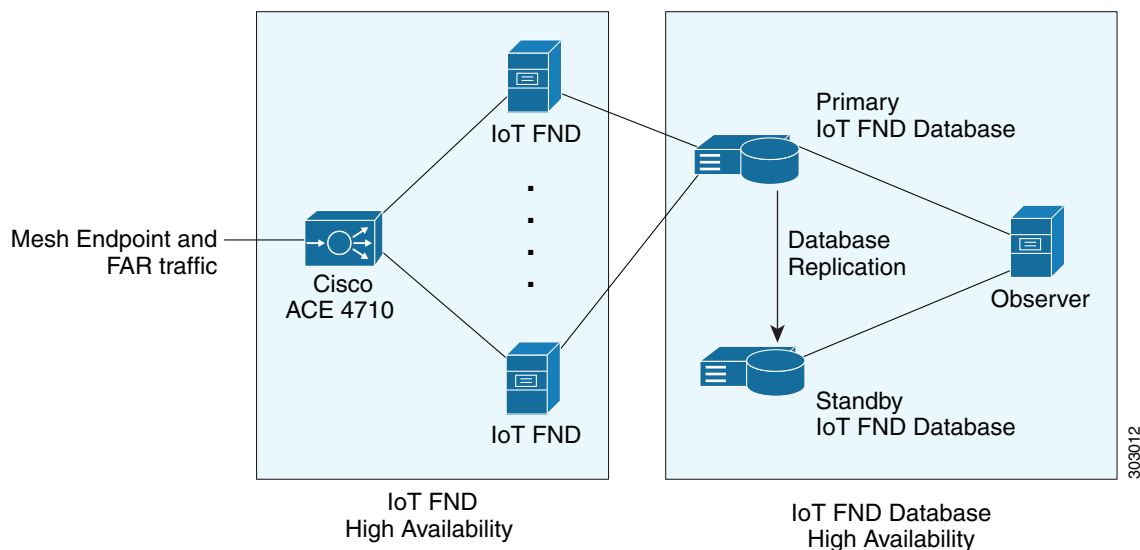
Component	Description
IoT FND Application Server	This is the heart of IoT FND deployments. It runs on an RHEL server and allows administrators to control different aspects of the IoT FND deployment using its browser-based graphical user interface. IoT FND HA deployments include two or more IoT FND servers connected to a load balancer.
NMS Database	This Oracle database stores all information 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 ASRs, the routers communicate with IoT FND directly.
Load Balancer	(Optional) IoT FND uses the Cisco ACE 4710 in Figure 1 to provide HA. The load balancer distributes the traffic among the IoT FND servers in the server cluster in your solution.

High Availability and Tunnel Redundancy

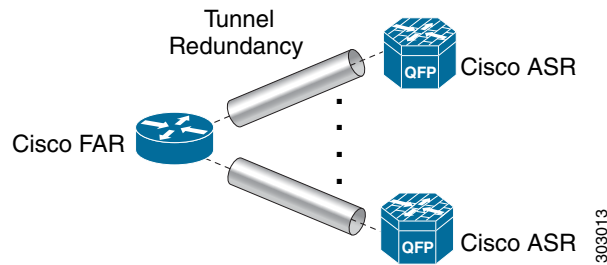
The example in [Figure 1](#) is of a single-server deployment with one database and no tunnel redundancy. However, you could take advantage of Cisco IoT FND HA support to deploy a cluster of Cisco IoT FND servers connected to a Cisco ACE 4710 load balancer, as shown in [Figure 2](#). The load balancer sends requests to the servers in a round-robin fashion. If a server fails, the load balancer keeps servicing requests by sending them to the other servers in the cluster.

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

Figure 2 IoT FND Server and Database HA



To provide tunnel redundancy, IoT FND allows you to create multiple tunnels to connect a CGR to multiple ASRs, as shown in [Figure 3](#).

Figure 3 IoT FND Tunnel Redundancy

For more information about HA, see Database High Availability.

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 AML, 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.

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.
- **Thread 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.

Related Software

The following software packages assist in deploying and managing your Cisco IoT Network solution.

Cisco IoT Device Manager

The [Cisco IoT Device Manager \(Device Manager or IoT-DM\)](#) is a Windows-based application used by field technicians to remotely manage Cisco CGRs. For some activities, the IoT-DM retrieves information from IoT FND.

Cisco Industrial Operations Kit

The Cisco Industrial Operations Kit (IOK) incorporates multiple virtual appliances for management, network, and IOK security-related head-end network services for the Cisco IoT Network solution. Talk to your Cisco representative for more information.

How to Use This Guide

This section has the following topics to help you quickly find information:

- [Common Tasks](#)
- [CGR Tasks](#)
- [Mesh Endpoint Tasks](#)
- [Administration Tasks](#)
- [Document Conventions](#)

Common Tasks

Table 1 lists tasks that users perform on both routers and mesh endpoints. The ability to perform tasks is role-based. For information about user roles, see [System-Defined User Roles](#).

Table 1 Common Tasks

Task	Use
Device Viewing Tasks	
View devices	Working with Router Views, Viewing Endpoints in Default View
View detailed device information	Displaying Detailed Device Information
Device Labeling Tasks	
Add labels	Adding Labels in Bulk
Remove labels	Removing Labels in Bulk
Search and Device Filtering Tasks	
Use filters	Using Filters to Control the Display of Devices
Diagnostics and Troubleshooting Tasks	
Ping	Pinging Devices
Traceroute	Tracing Routes to Devices
Download logs	Downloading Logs
Monitoring Tasks	
View and search events	Monitoring Events
View and search issues	Monitoring Issues, Viewing Device Severity Status on the Issues Status Bar
View tunnel status	Monitoring Tunnel Status in the Managing Tunnel Provisioning chapter of the Cisco IoT Field Network Director Installation Guide, Release 4.x
General Tasks	
Change password	Resetting Passwords
Set time zone	“Configuring the Time Zone” in the Cisco IoT Field Network Director User Guide, Release 4.x.
Set user preferences	“Setting User Preferences” in the Cisco IoT Field Network Director User Guide, Release 4.x.

CGR Tasks

Table 2 lists CGR tasks. For information about user roles, see [System-Defined User Roles](#).

Table 2 CGR Tasks

Task	Use
Router Configuration Group Tasks	
Add CGRs to configuration groups	Creating Device Groups
Delete a configuration group	Deleting Device Groups
List devices in a configuration group	Listing Devices in a Configuration Group
Assign devices to groups	Adding Routers to IoT FND Adding HERs to IoT FND Moving Devices to Another Configuration Group Manually Moving Devices to Another Configuration Group in Bulk
Rename configuration groups	Renaming a Device Configuration Group
Router Configuration Tasks	
Change device configuration properties	Changing Device Configuration Properties
Edit configuration templates	Editing the ROUTER Configuration Template Editing the AP Configuration Template
Push configurations	Pushing Configurations to Endpoints
Migrate from CG-OS to IOS	Performing CG-OS to Cisco IOS Migrations
Monitoring a Guest OS	"Monitoring a Guest OS" in the Cisco IoT Field Network Director User Guide, Release 4.x.
Tunnel Provisioning Tasks	
Configure tunnel provisioning	"Configuring Tunnel Provisioning" in the Cisco IoT Field Network Director User Guide, Release 4.x.
Edit tunnel provisioning templates	"Configuring Tunnel Provisioning Template in the Cisco IoT Field Network Director Installation Guide, Release 4.x
Reprovisioning tunnels	"\"Tunnel Reprovisioning Template\" in the Cisco IoT Field Network Director Installation Guide, Release 4.x "\"Factory Reprovisioning Template\" in the Cisco IoT Field Network Director Installation Guide, Release 4.x
Firmware Management Tasks	
Assign devices to firmware groups	Assigning Devices to a Firmware Group
Upload images to firmware groups	Uploading a Firmware Image to a Router Group
Work Order Tasks	
Create work orders	Creating Work Orders

Mesh Endpoint Tasks

[Table 3](#) lists ME tasks. For information about user roles, see [System-Defined User Roles](#).

Table 3 Mesh Endpoint Tasks

Task	Use
ME Configuration Group Tasks	
Add mesh endpoint configuration groups	Creating Device Groups
Delete mesh endpoint configuration groups	Deleting Device Groups
Rename mesh endpoint configuration groups	Renaming a Device Configuration Group
Assign mesh endpoint devices to a configuration group	Moving Devices to Another Group
List devices in a configuration group	Listing Devices in a Configuration Group
ME Configuration Tasks	
Change mesh endpoint configuration properties	Changing Device Configuration Properties
Edit mesh endpoint configuration templates	Editing the ENDPOINT Configuration Template
Push configuration to mesh endpoints	Pushing Configurations to Endpoints
Add mesh endpoint firmware groups	Creating Device Groups
Assign devices to firmware groups	Moving Devices to Another Group
Upload images to firmware groups	Uploading a Firmware Image to a Resilient Mesh Endpoint Group

Administration Tasks

[Table 4](#) lists administration tasks.

Table 4 Administration Tasks

Task	Use
System Management Tasks	
Set password policies	Managing the Password Policy
Define roles	Managing Roles and Permissions
Manage user accounts	Managing Users
Access Management Tasks	
Manage active sessions	Managing Active Sessions
Display the audit trail	Displaying the Audit Trail
Manage certificates	Managing Certificates
Configure data retention	Configuring Data Retention
Manage licenses	Managing Licenses
Manage logging	Managing Logs
Configure server settings	Configuring Server Settings
Manage the syslog	Managing System Settings
Configure tunnel settings	Configuring Provisioning Settings

Document Conventions

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in bold font .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	Elements in square brackets are optional.
{x y z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution: Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning: IMPORTANT SAFETY INSTRUCTIONS

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

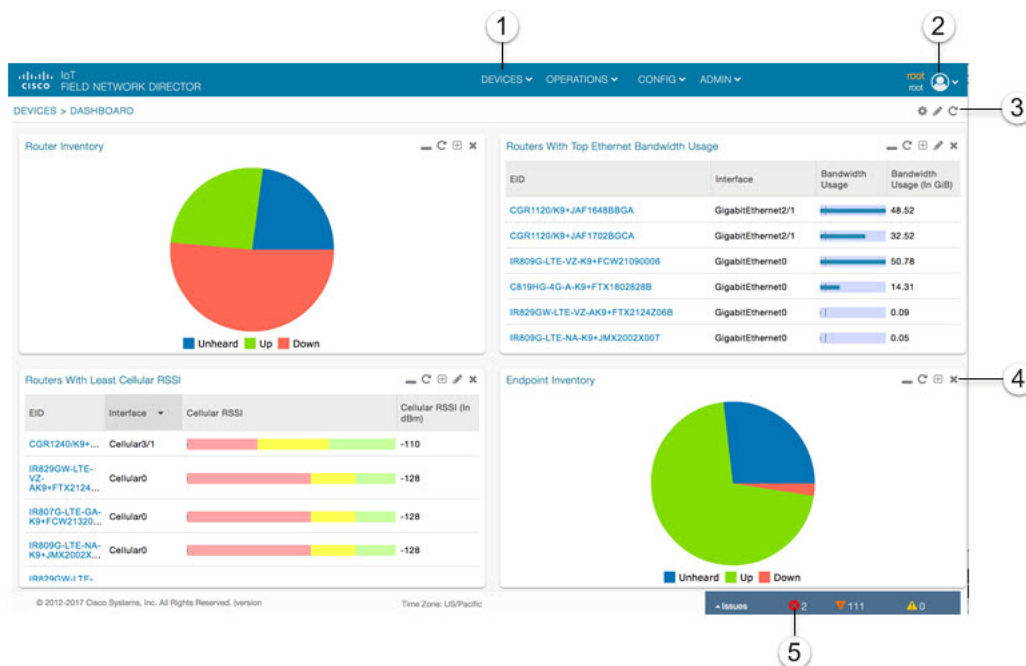
Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Interface Overview

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

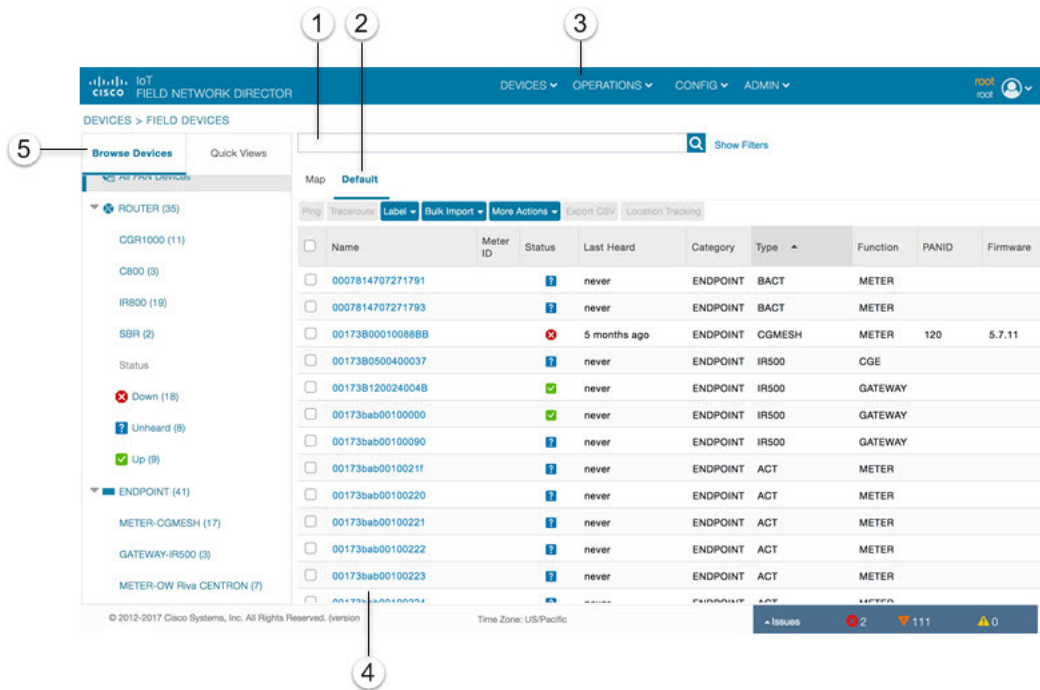
- [Icons](#)
- [Main Menus](#)

The IoT FND displays the dashboard after you log in ([Figure 4](#)). See [Using the Dashboard](#).

Figure 4 IoT FND Dashboard

<p>1 Menu and Submenu tabs.</p> <p>Roll over the Menus to display Submenus, which display as tabs below the main menus.</p>	<p>4 Dashlet action buttons (left to right):</p> <ul style="list-style-type: none"> ■ Minimize (close) dashlet window ■ Refresh dashlet ■ Export data ■ Filter (not available on all pages) ■ Close dashlet
<p>2 <user name> menu</p> <ul style="list-style-type: none"> ■ Preferences: Sets display settings of the user interface. ■ Switch Domain ■ Change Password ■ Time Zone ■ Log Out 	<p>5 Issues Status bar</p> <p>Summary of issues by devices (routers, head-end routers, servers, endpoints) and their severity (critical, major, minor)</p> <p>Viewing Device Severity Status on the Issues Status Bar</p>
<p>3</p> <ul style="list-style-type: none"> ■ 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	Filters	4	Device EID links to Device Info page
2	Define labels, define bulk imports, and More Actions (such as create work orders and block or remove mesh devices)	5	Browse Devices pane
3	Main menu		

Working with Views

Use the Browse Devices pane (5) 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 (1). See [Using Filters to Control the Display of Devices](#). 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 (4) to display a device information page. You can generate work orders directly from the Device Info page, and perform some device-specific tests such as pinging the device to determine if it responds in your network. 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, the Default tab in [Figure 5](#)).

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 (5) to display devices on a GIS map (see [Viewing Routers in Map View](#) and [Viewing Mesh Endpoints in Map View](#)).

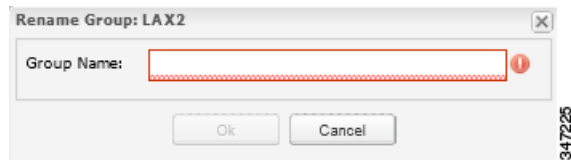
Working with Filters

Create custom filters by clicking the Show Filters link (the Hide Filters link displays in the same place in [Figure 5](#)) and using the provided filter parameters (1) to build the appropriate syntax in the Search Devices field (4). Click the Quick Views tab to display saved custom filters (see [Creating and Editing Quick View Filters](#)).

Completing User-entry Fields

[Figure 6](#) 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

[Table 5](#) lists the icons that display in the UI

Table 5 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.

Table 5 IoT FND Icons (continued)


















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.
	<p>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.</p> <p>The RPL tree connection displays as blue or orange lines.</p> <ul style="list-style-type: none"> ■ Orange lines indicate that the link is up. ■ Blue lines indicate that the link is down.

Table 5 IoT FND Icons (continued)

Icon	Description
	In Map view, this is a device group icon. The colors reflect the device status: Up, Down, and Unheard.
	<p>On the Events and Issues pages, and on the Issues Status bar, these icons indicate the event severity level, top-to-bottom, as follows:</p> <ul style="list-style-type: none"> ■ Critical ■ Major ■ Minor ■ Info <p>Each event type has a preset severity level. For example, a Router Down event is a Major severity level event.</p>
	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 Menu

This section describes the IoT FND menus available in the title bar at the top of the page.

Devices Menu

The Devices menu provides access to the Dashboard and the device management pages:

- Dashboard—This user-configurable page displays information about the connected grid.
- 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—Use this page to create and monitor work orders.

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.
 - Remote Authentication—Use this page to configure remote 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.



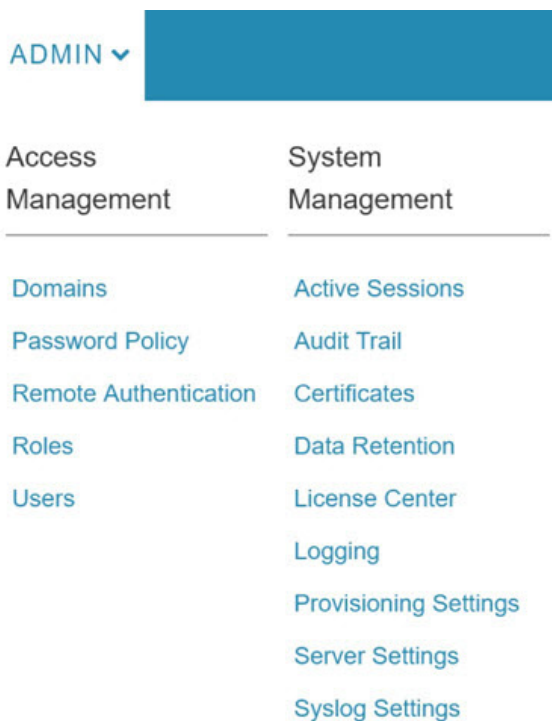
Managing User Access

This section has the following topics for managing users and roles in IoT FND:

- [Managing the Password Policy](#)
- [Configuring Remote Authentication](#)
- [Managing Roles and Permissions](#)
- [Managing Users](#)

All user management actions are accessed through the **Admin > Access Management** menu ([Figure 1](#)).

Figure 1 Admin Menu



Managing the 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:

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

Policy	Value	Status	Terminate Session and Reset Password
Password minimum length	6	Enabled	Yes, if minimum password length is increased.
Password history size	4	Disabled	
Max unsuccessful login attempts	5	Enabled	
Password expire interval (days)	180	Disabled	Yes, if password expire interval is reduced.
Password cannot contain username or reverse of username		Disabled	Yes, if changed to Enabled state.
Password cannot be cisco or ocsic (cisco reversed)		Disabled	Yes, if changed to Enabled state.
No character can be repeated more than three times consecutively in the password		Disabled	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)		Disabled	Yes, if changed to Enabled state.

2. To enable or disable a policy, choose the appropriate option (**Enabled** or **Disabled**) from the Status drop-down menu.
3. To modify the value of a policy, if applicable, enter the new value in the Value field.

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

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.

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.

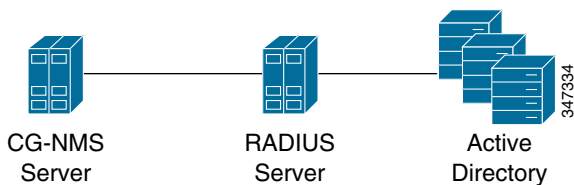
- [Support for Remote Authentication](#)
- [Configuring Remote Authentication in AD](#)
- [Configuring Security Policies on the RADIUS Server](#)

- [Configuring Remote Authentication in IoT FND](#)
- [Enabling and Disabling Remote User Accounts](#)
- [Deleting Remote User Accounts](#)
- [Logging In to IoT FND Using a Remote User Account](#)

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.

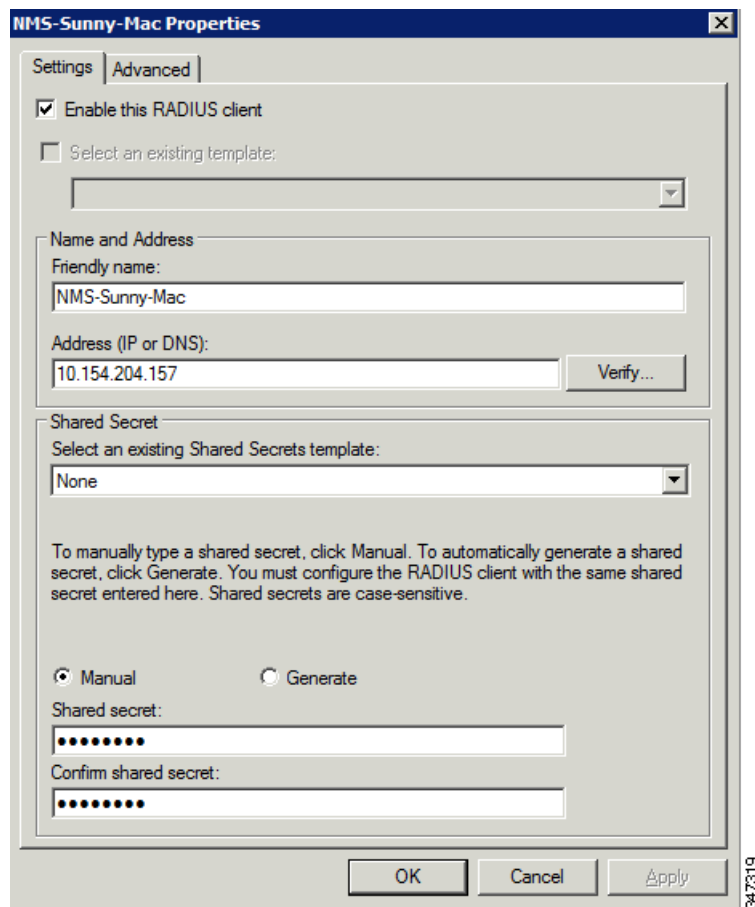
Note: When remote authentication is enabled, user management is done in AD. If an AD user logs in who was deleted from IoT FND, their profile is added back to IoT FND. To prevent access to IoT FND, their AD user profiles must first be deleted from AD.

Configuring Remote Authentication in AD

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

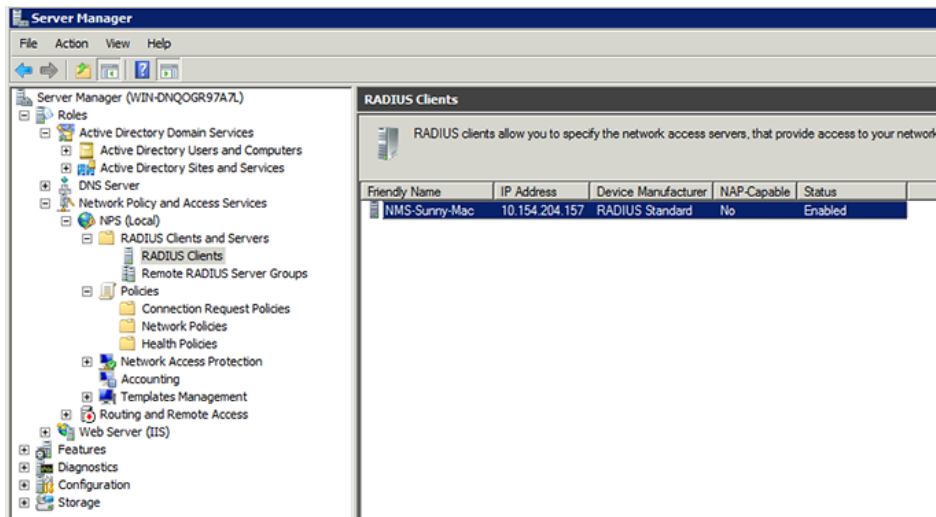
1. Log in to NPS.
2. Add IoT FND as a radius client on the RADIUS server.

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.



347319

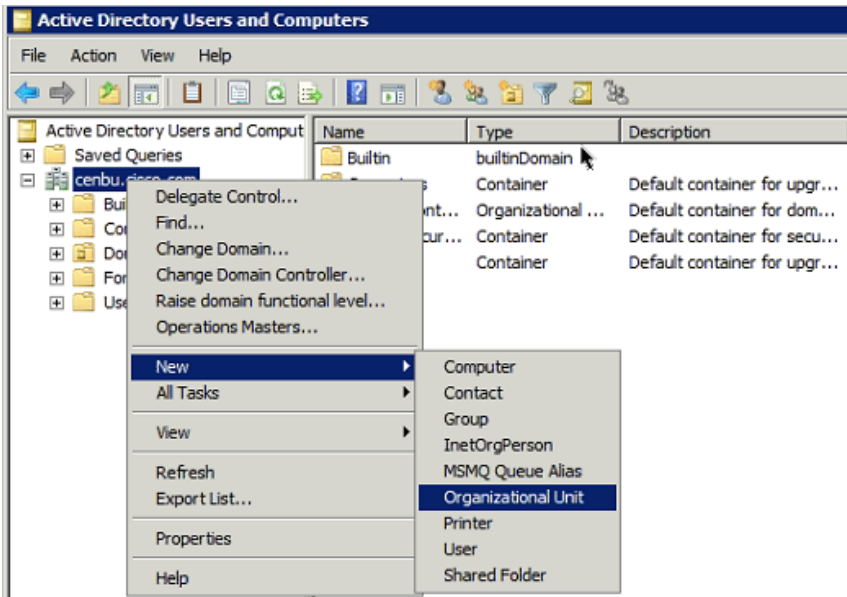
An entry for the RADIUS client appears under RADIUS Clients and Servers.



347318

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

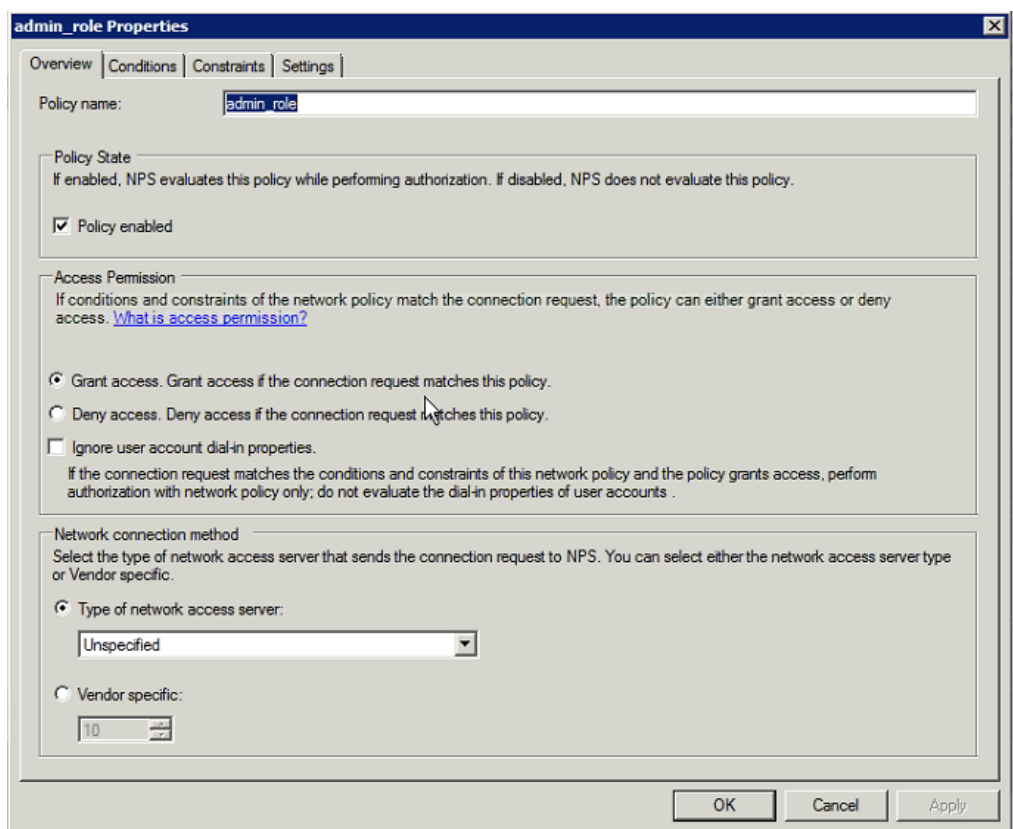
Cisco recommends that you create all security groups (IoT FND roles) within this Organizational Unit.



347328

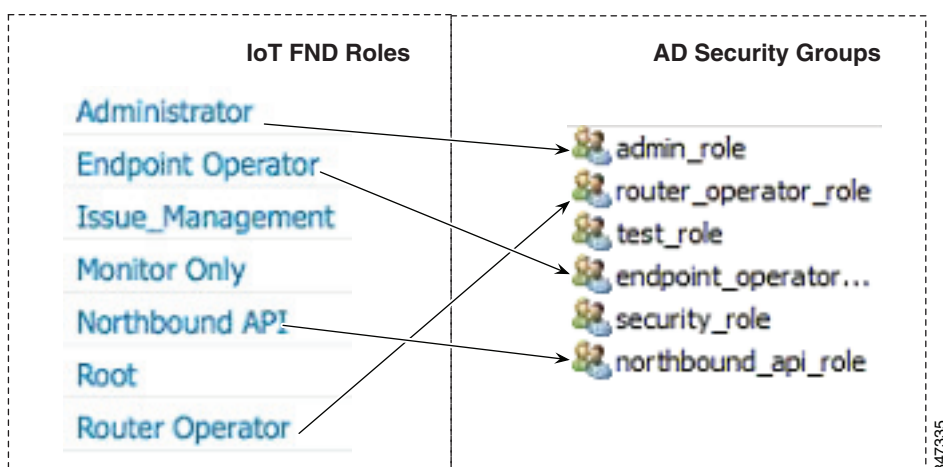
4. Add security groups corresponding to IoT FND roles to the Organizational Unit.

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.

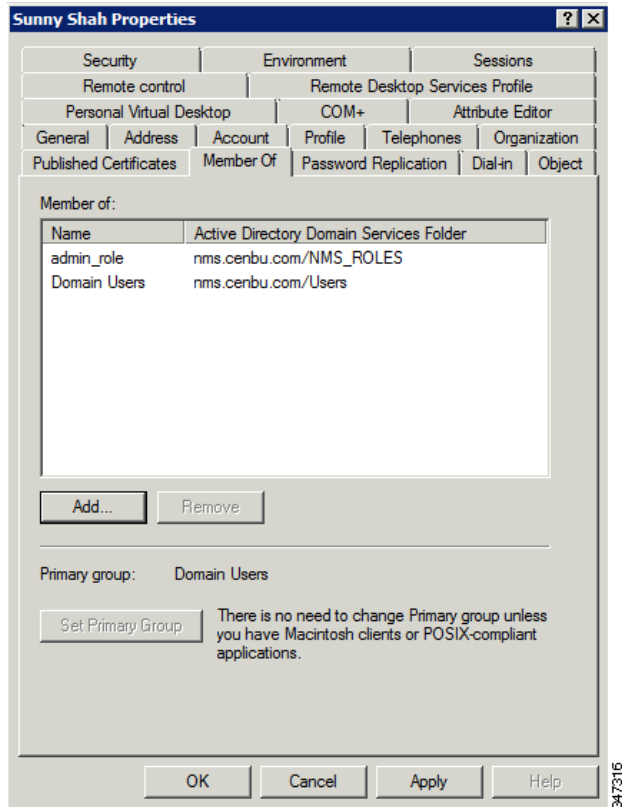
Note: You cannot create or assign the IoT FND root role in AD.



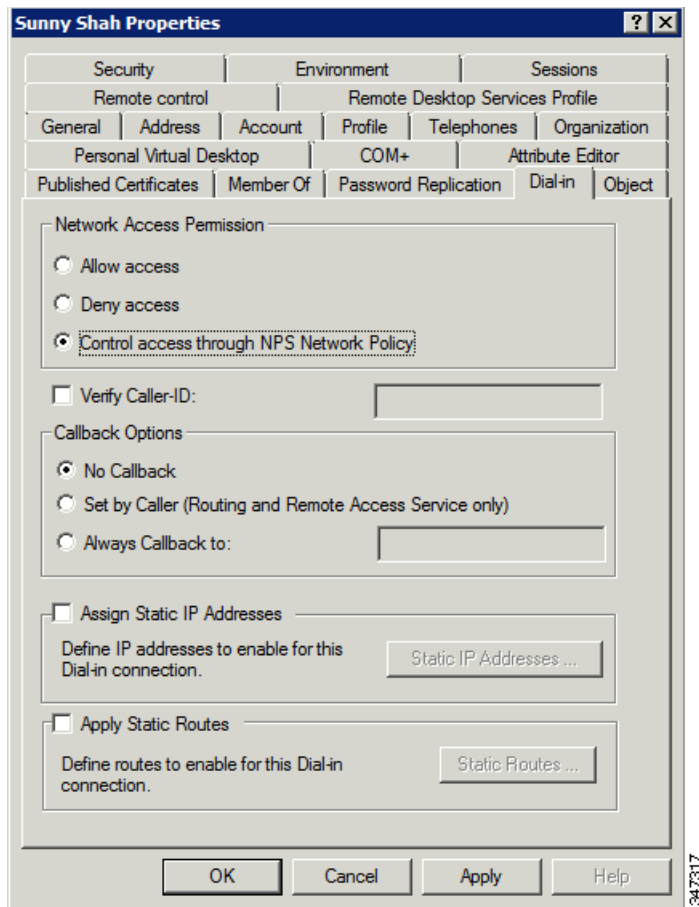
5. Assign AD users a role by adding them to the security group mapping to that role.

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 create the corresponding AD security group. Users in this new group can then carry out the tasks allowed by this role.



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

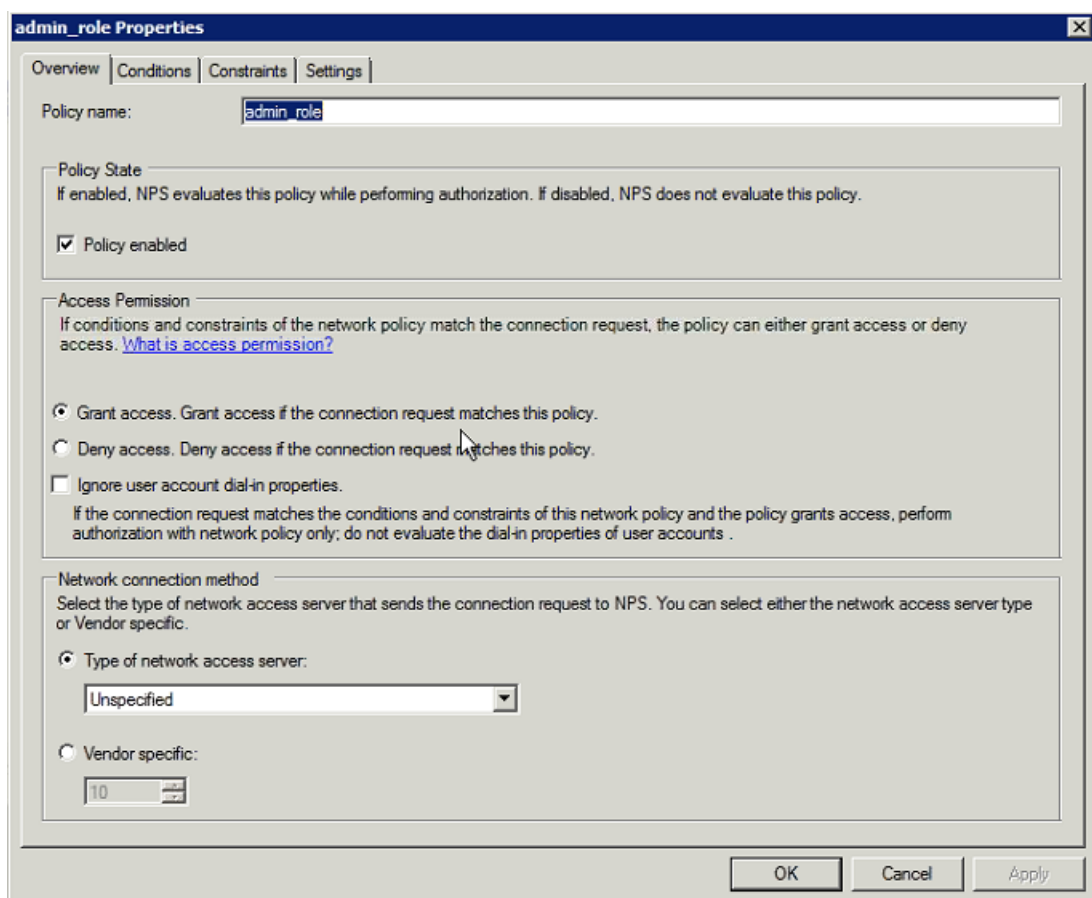


Configuring Security Policies on the RADIUS Server

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

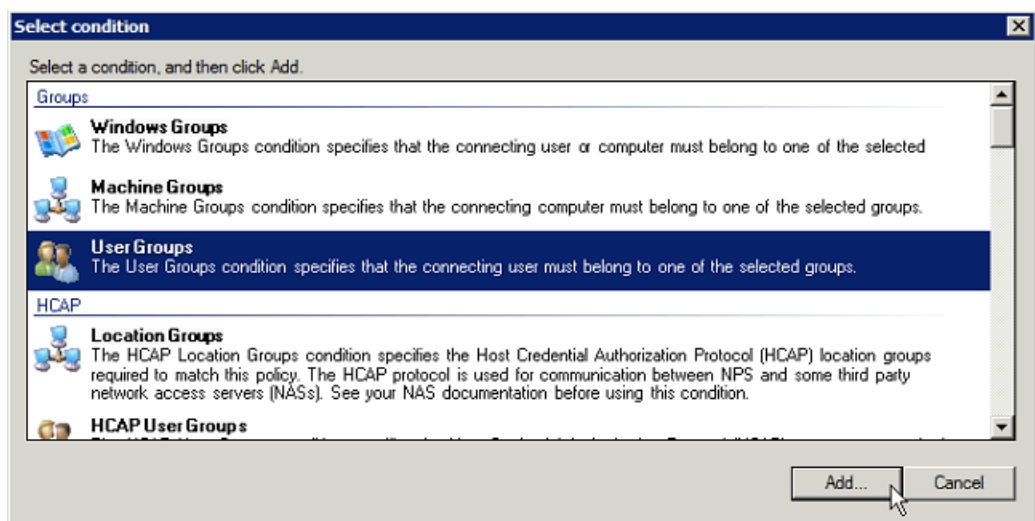
To configure security policies on the RADIUS server, follow these steps:

1. Create a network policy for each security group you created in AD.
2. Configure the policy as follows:
 - a. In the Overview pane, define the policy name, enable it, and grant access permissions.



347320

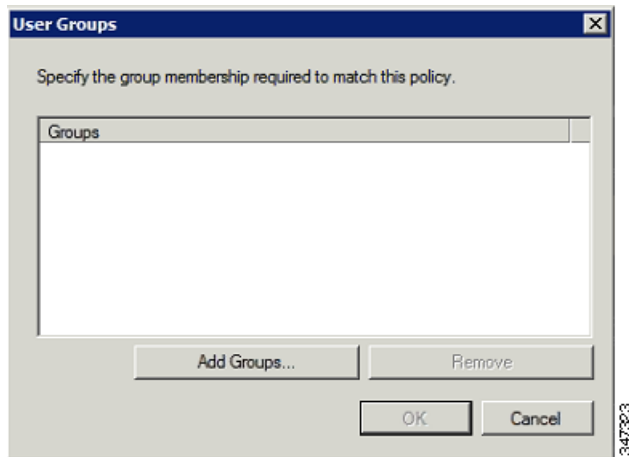
- b. Click the **Conditions** tab, select the **User Groups** condition, and click **Add**.



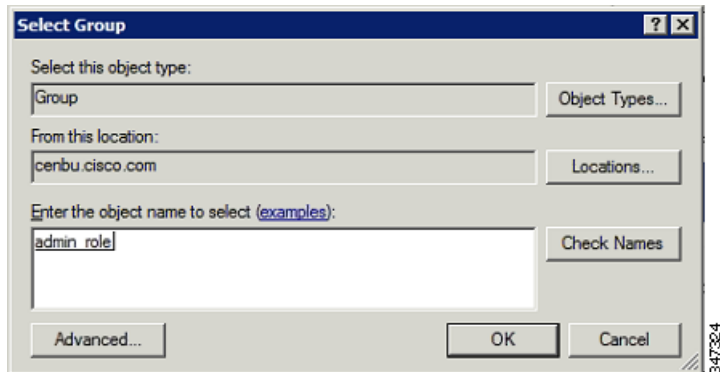
347322

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**.

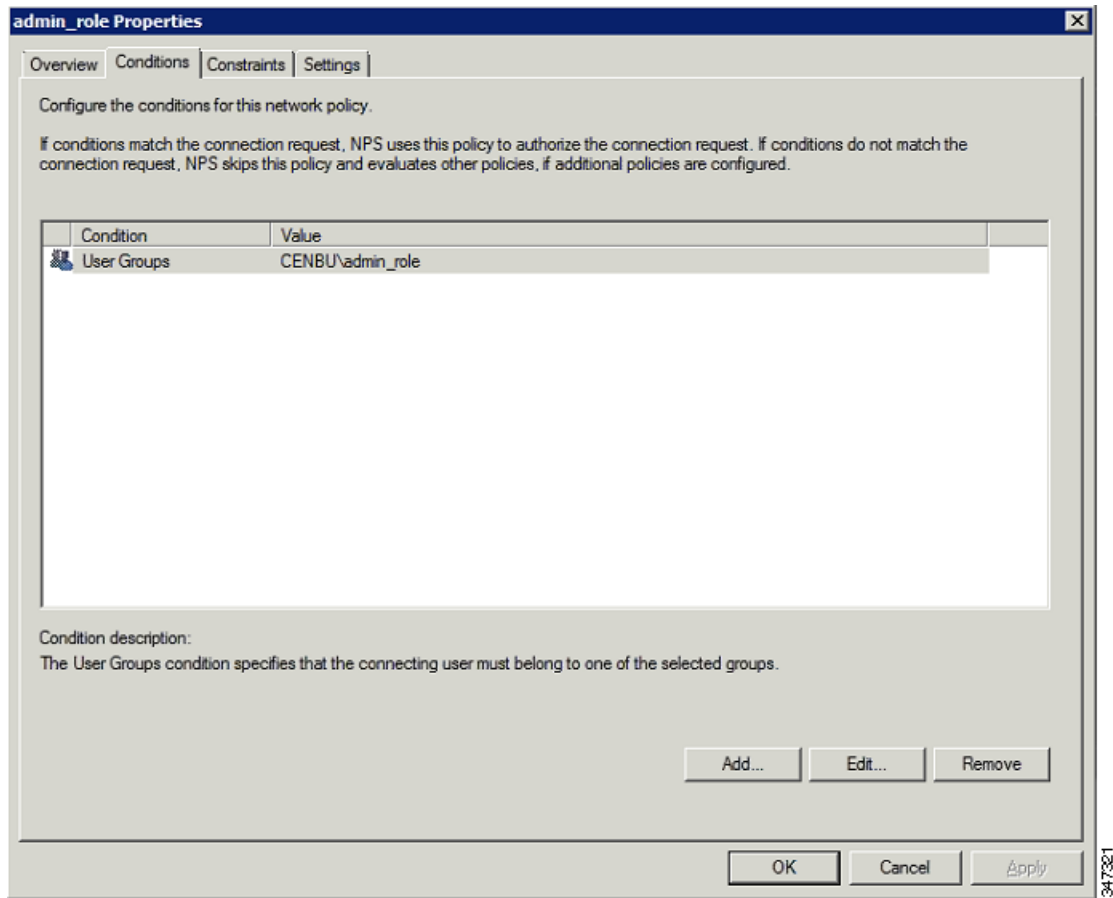


- d. In the Select Group window, enter the name of the group
- e. Click **OK** to close the Select Group dialog box, and then click **OK** to close the User dialog box.

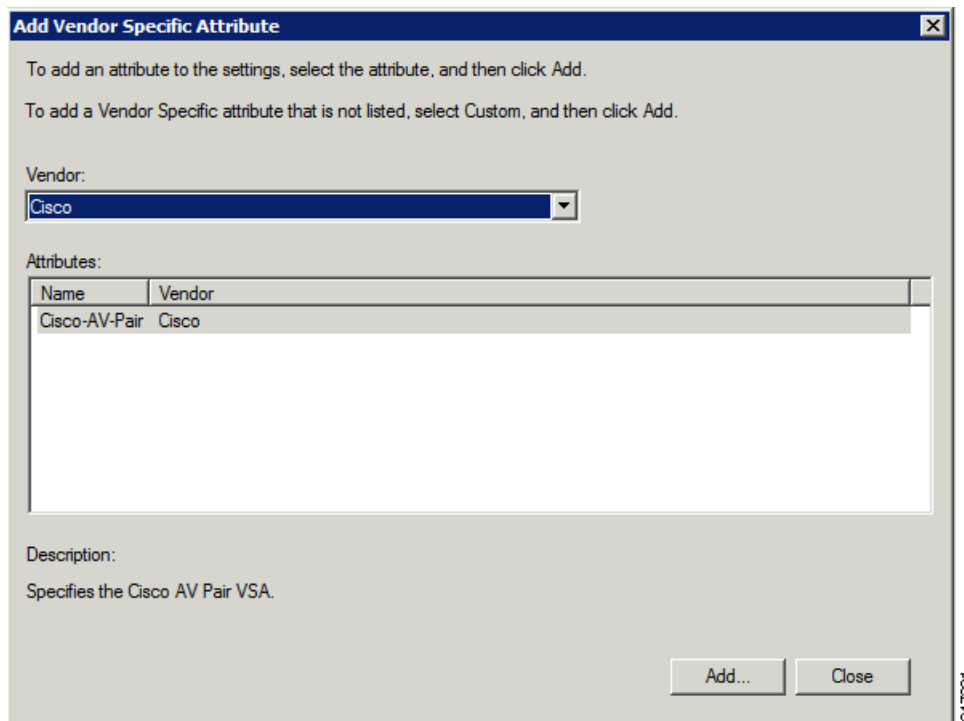


- f. Click **Cancel** to close the Select condition window.

The condition appears in the Conditions pane.



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



Add Vendor Specific Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor:
Cisco

Attributes:

Name	Vendor
Cisco-AV-Pair	Cisco

Description:
Specifies the Cisco AV Pair VSA.

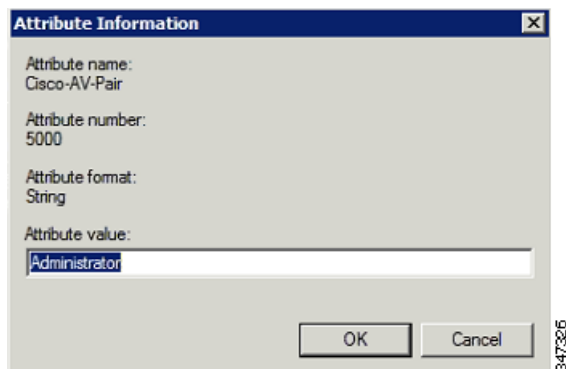
Add... Close

347331

- 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:

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



Attribute Information

Attribute name:
Cisco-AV-Pair

Attribute number:
5000

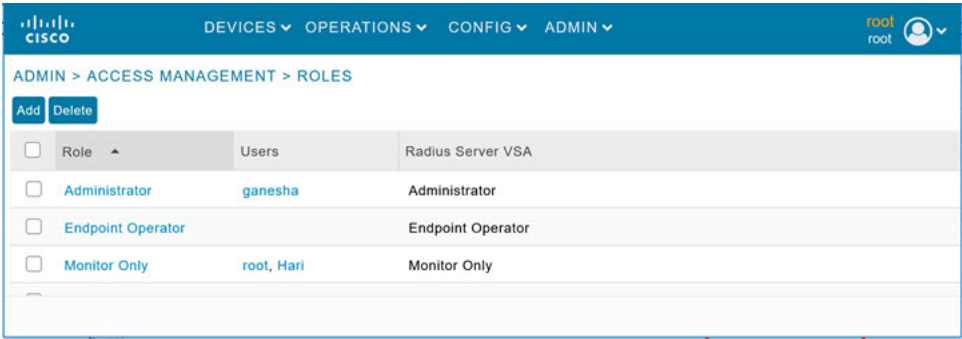
Attribute format:
String

Attribute value:
Administrator

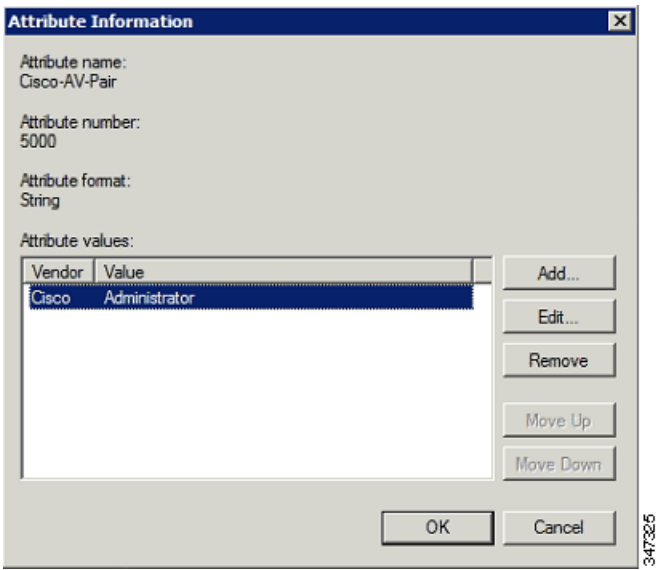
OK Cancel

347326

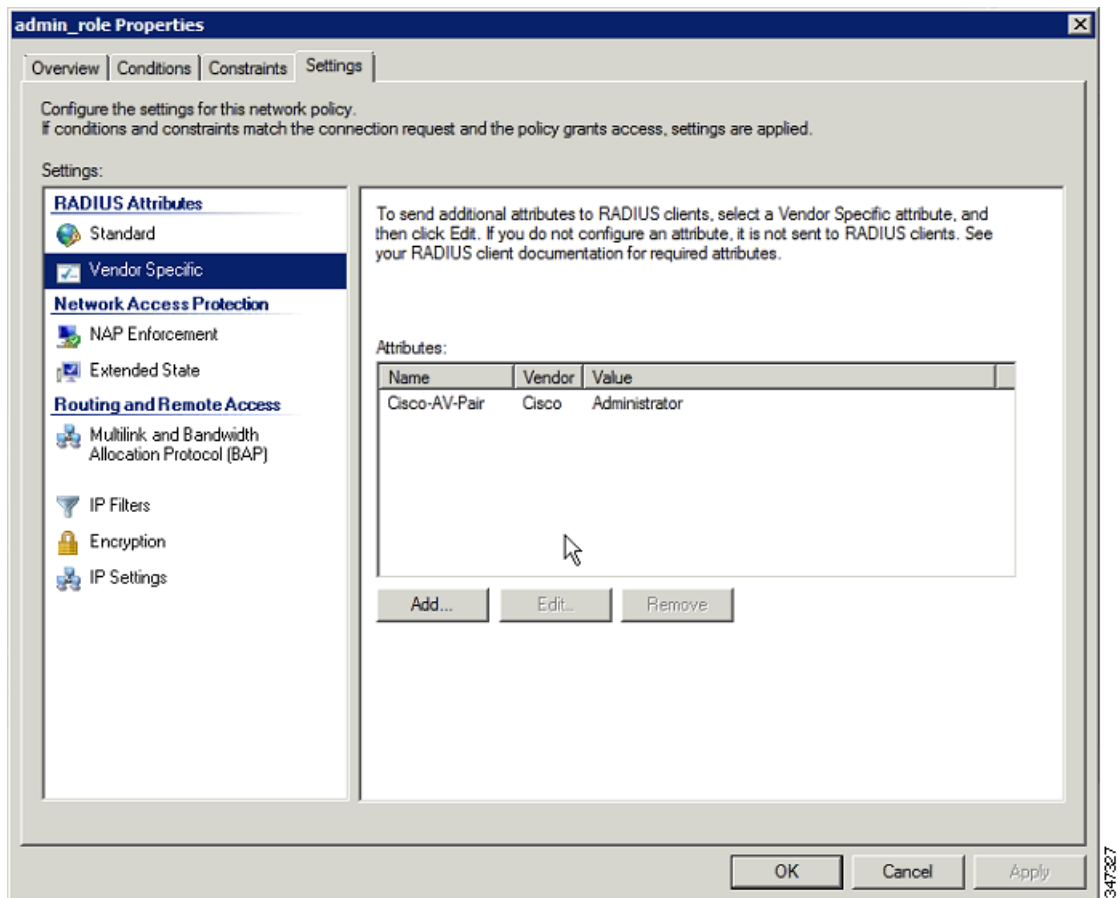
Note: The string entered in the Attribute value field must be the exact string listed in the Radius Server VSA column on the Roles page in IoT FND (**ADMIN > Access Management > Roles**).



i. Click **OK**.



The VSA attribute appears in the Settings pane.



j. Click **OK**.

Configuring Remote Authentication in IoT FND

You enable remote user authentication and configure RADIUS server settings on the Remote Authentication page (**Admin > Access Management > Remote Authentication**).

To configure remote authentication:

1. Choose **ADMIN > Access Management > Remote Authentication**.
2. Check the **Enable Remote Authentication** check box.
3. Enter this information about the RADIUS server:

Field	Description
IP	The IP address of the RADIUS server.
Radius Server Description	A descriptive name of the RADIUS server.
Shared Secret	The shared secret you configured on the RADIUS server.
Confirm Shared Secret	
Authentication Port	The RADIUS server port that IoT FND uses to send request to. The default port is 1812.

Field	Description
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.

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**.

5. Click **Save** when done.

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.

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 This section has the following topics:

- [Adding Roles](#)
- [Deleting Roles](#)
- [Editing Roles](#)

■ Viewing Roles

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. The following topics are discussed in this section:

- Basic User Permissions
- System-Defined User Roles
- Custom User Roles

Basic User Permissions

Table 1 describes basic IoT FND permissions.

Table 1 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.
BACT Operations	Special Battery powered meters managed by CAM. The interaction with these endpoints should be kept to a minimum in order to reduce draw down of battery within the endpoints.
Device Manager User	Permission for IoT-DM user (field technician) to retrieve a Work Order from FND through the Work Order NB APIs.
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 WiFi pre-shared key, admin user password, and master key.
Manage Head-End Devices Credentials	Allows users to view the ASR admin NETCONF password.
NBAPI Audit Trail	Allows users to query and delete audit trails using IoT FND NB API.
NBAPI Device Management	Allows users to add, remove, export, and change router and endpoint devices using IoT FND NB API.
NBAPI Endpoint Group Management	Permission for accessing the Group Management NB API.
NBAPI 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.

Table 1 IoT FND User Permissions (continued)

Permission	Description
NBAPI Issues	Allows users to search issues.
NBAPI Orchestration Services	Permission for IOK Orchestration Service to access the Orchestration NB APIs.
NBAPI Reprovision	Allows users to reprovision devices using IoT FND NB API.
NBAPI Rules	Allows users to search, create, delete, activate, and deactivate rules using IoT FND NB API.
NBAPI Search	Allows users to search devices, get device details, group information, and metric history using IoT FND NB API.
NB API Tunnels	Permission for accessing the Tunnel Status NB APIs.
Password Policy	Provides a flexible password policy system to manage user passwords. It contains configurable properties for password expiration, failed login attempts, password strength and other aspects of password maintenance.
Router Configuration	Allows users to edit router configuration templates and push configuration to routers.
Router File Management	Permission for managing router files on the Device File Management GUI page.
Router Firmware Update	Allows users to add and delete firmware images and perform firmware update operations for routers.
Router Group Management	Allows users to assign, remove, and change device assignments to router configuration and firmware groups.
Router Reboot	Allows users to reboot the router.
Rules Management	Allows users to add, edit, activate, and deactivate rules.
Security Policy	Allows users to block mesh devices, refresh mesh keys, and so on.
Tunnel Provisioning Management	Allows users to manage tunnel groups, edit/apply tunnel-related templates, and perform factory reprovisioning.
View Device Configuration	Allows users to view field device configuration.
View Head-end	Allows users to view ASR configuration, tunnel provisioning, and HER events.
View Work Orders	Allows users to view work orders.
Work Order Management	Allows users to manage work orders for IoT-Device Manager (IoT-DM).

System-Defined User Roles

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

[Table 2](#) lists system-defined roles. These roles cannot be modified.

Table 2 System-defined User Roles

Role	Description
Administrator	<p>This role combines these basic permissions:</p> <ul style="list-style-type: none"> ■ Administrative Operations ■ Label Management ■ Rules Management
Endpoint Operator	<p>This role combines these basic permissions:</p> <ul style="list-style-type: none"> ■ 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	<p>This role combines these basic permissions:</p> <ul style="list-style-type: none"> ■ 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	<p>This role combines these basic permissions:</p> <ul style="list-style-type: none"> ■ 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 [Table 1](#)). These permissions specify the type of actions users with this role can perform.

Adding Roles

To add IoT FND user roles:

1. Choose **ADMIN > Access Management > Roles**.
2. Click **Add**.
3. Enter the name of the role.
4. Check the appropriate check boxes to assign permissions.
5. Click **Save**.
6. To continue to add roles, click **Yes**; otherwise, click **No** to return to the Roles page.

Deleting Roles

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

To delete IoT FND user roles:

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

Editing Roles

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

To edit IoT FND custom roles:

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

Viewing Roles

To view IoT FND user roles:

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

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

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

Managing Users

This section has the following topics on managing users:

- [Resetting Passwords](#)
- [Viewing Users](#)
- [Adding Users](#)
- [Deleting Users](#)
- [Enabling Users](#)
- [Disabling Users](#)
- [Editing Users](#)

Resetting Passwords

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

To reset a password, enter this command:

```
[root@yourname-lnx1 bin]#./password_admin.sh root
```

IoT FND manages its own user account database; therefore, you must add all new local users from the IoT FND user interface at the **Admin > Access Management > Users** page. Remote users are automatically added to the database. You can also enable, disable, edit, or delete users on this page.

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.

Viewing Users

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

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 > Remote Authentication).

Adding Users

To add users to IoT FND:

1. Choose **ADMIN > Access Management > Users**.
2. Click **+** icon to **Add User**.
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.

4. Click **Assign Domain** to open the configuration panel:
 - Select the domain name from the drop-down menu
 - Assign Role(s) and its associated Permission for the user by selecting the role check box.

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

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

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.

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:

1. Choose **ADMIN > Access Management > Users**.
2. Check the box next to the User Name entry that you want to remove from the User Account list.
3. To delete the entry, click the **trash can** icon.
4. To confirm action, click **Yes**.

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:

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

2. Check the check boxes for the user account(s) to enable.
3. Click the **solid person** icon.
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:

1. Choose **Admin > Access Management > Users**.
2. Check the check boxes for the user account(s) to disable.
3. Click the **outlined person** icon.
Note: If you disable a user account, IoT FND resets the user password.
4. To confirm action, click **Yes**.

Editing Users

To edit user settings in IoT FND:

1. Choose **Admin > Access Management > Users**.
2. To edit user credentials:
 - a. Click the user name link.
 - b. Edit the role assignments.
 - c. Click **Save**.



Managing System Settings

This section describes how to manage system settings, and includes the following sections:

- [Managing Active Sessions](#)
- [Displaying the Audit Trail](#)
- [Managing Certificates](#)
- [Configuring Data Retention](#)
- [Managing Licenses](#)
- [Managing Logs](#)
- [Configuring Provisioning Settings](#)
- [Configuring Server Settings](#)
- [Managing the Syslog](#)

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 ([Figure 1](#))

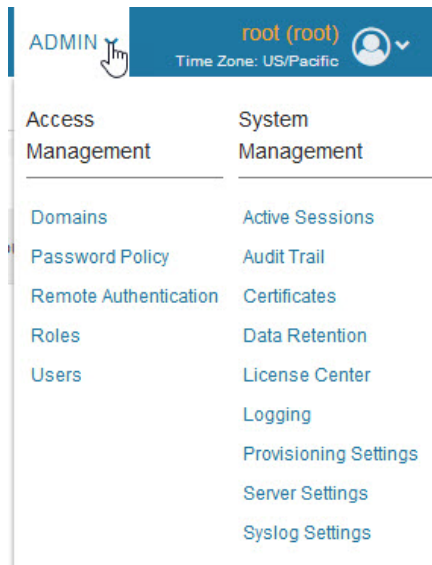
default-cqr1000

Group Members Router Tunnel Addition HER Tunnel Addition HER Tunnel Deletion Router Factory Reprovision **Reprovisioning Actions** Policies

Action Interface Interface Type

Current Action
Reprovisioning Status Not Started
Completed devices / All Scheduled Devices 0/0
Error devices / All Scheduled Devices 0/0

Figure 1 Admin Menu



Managing Active Sessions

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

- [Viewing Active Sessions](#)
- [Logging Users Out](#)
- [Filtering the Active Sessions List](#)

Viewing Active Sessions

To view active user sessions, choose **ADMIN > System Management > Active Sessions**. IoT FND displays the Active Sessions page ([Figure 2](#)).

Figure 2 Active Sessions Page

<input type="checkbox"/> User Name	IP	Login Time	Last Access Time
<input type="checkbox"/> root	10.118.30.215	2017-06-29 11:29	2017-06-29 11:34
<input type="checkbox"/> root	10.41.50.86	2017-06-29 10:51	2017-06-29 11:33

Table 1 describes the Active Session fields.

Table 1 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 Users Out

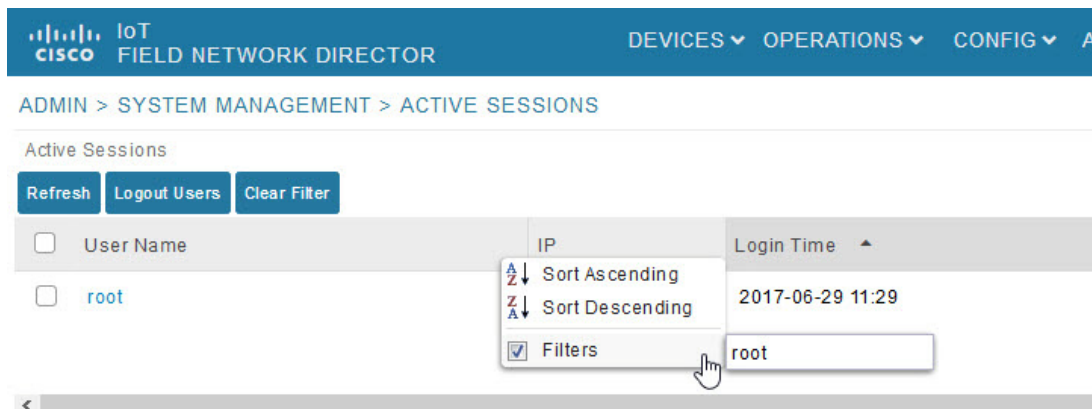
To log out an IoT FND user:

1. Choose **ADMIN > System Management > Active Sessions**.
2. Select the check boxes for those users you want to log out.
3. Click **Logout Users**.
4. Click **Yes** to confirm logout of the users.

Filtering the Active Sessions List

To filter the Active Sessions list using column filtering:

1. Choose **ADMIN > System Management > Active Sessions**.
2. Hover the mouse over the User Name column heading to expose the filter icon (triangle). Enter the user name or the first characters of the user name to filter the list.



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

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

Displaying the Audit Trail

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

To display the Audit Trail, choose **ADMIN > System Management > Audit Trail**

Date/Time	User Name	IP	Operation	Status	Details
2017-06-29 11:48	root	10.41.50.86	Logout	Success	N/A
2017-06-29 11:29	root	10.118.30.215	Login	Success	N/A
2017-06-29 10:53	root	10.41.50.86	Devices added	Initiated	N/A

Table 2 describes the Audit Trail fields.

Table 2 Audit Trail Fields

Field	Description
Date/Time	Date and time of the operation.
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:

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

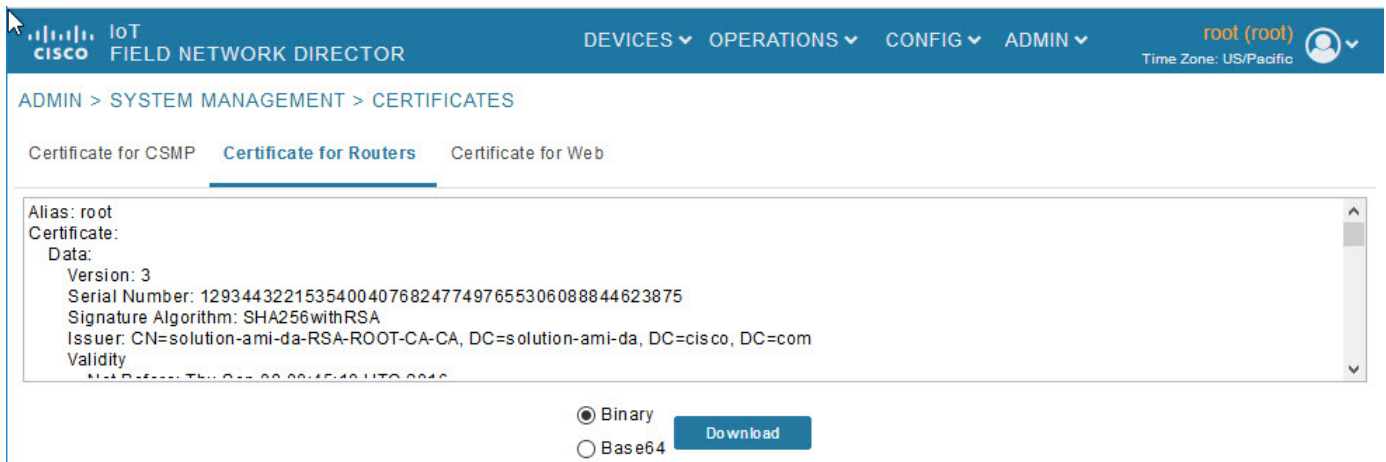
Tip: To remove the filter, from the User Name drop-down menu, uncheck the **Filters** check box or click **Clear Filter** (left of the screen).

Managing Certificates

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

To display the CSMP, IoT-DM and Web certificates:

1. Choose **ADMIN > System Management > Certificates**.
2. To view a certificate, click its corresponding heading (such as Certificate for Routers).



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 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:

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

- For each of the retention categories, specify the number of days to retain data.

Table 3 lists the allowable maximum values for each field.

Table 3 Data Retention Fields Allowable Maximum Values

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

- To save the maximum values, click the disk icon.
- To revert to default settings, click **Reset**.

Managing Licenses

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

- [Viewing License Summary](#)
- [Viewing License Files](#)
- [Adding License Files](#)
- [Deleting License Files](#)

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

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

Viewing License Summary

To view IoT FND license summary:

- Choose **ADMIN > System Management > License Center**.
- Click **License Summary**.

ADMIN > SYSTEM MANAGEMENT > LICENSE CENTER

License Summary License Files

PackageName ▲	CGR1K Count Used / Total	C800 Count Used / Total	IR800 Count Used / Total	LORAWAN Count Used / Total	IR500 Count Used / Total	Days Until Expiry
⊕ DEVICE_LICENSE	10 / 1000000	3 / 1000000	10 / 1000000	1 / 1000001	3 / 1000000	Permanent
⊕ SOFTWARE_LICENSE	NA	NA	NA	NA	NA	Permanent

For every license, IoT FND displays the information described in [Table 4](#).

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

Table 4 Device License Summary Information

Field	Description
Package Name	Name of license package.
CGR1K Count Used/Total	Lists the number of CGR1000 devices currently active in the network and the maximum number of CGR1000s supported by the license.
C800 Count Used/Total	Lists the number of C800 devices currently active in the network and the maximum number of C800 devices supported by the license.
IR800 Count Used/Total	Lists the number of IR800 (IR809 and IR829) devices currently active in the network and the maximum number of IR800 devices supported by the license.
LORAWAN Count Used/Total	Lists the number of Cisco interface modules for LoRaWAN devices currently active in the network and the maximum number of Cisco interface modules for LoRaWAN devices that are supported by the license.
IR500 Count Used/Total	Lists the number of IR509 devices currently active in the network and the maximum number of IR509 devices supported by the license.
Days Until Expiry	Number of days remaining until the license expires.

Viewing License Files

To view IoT FND license files:

1. Choose **ADMIN > System Management > License Center**.
2. Click **License Files** to display details on all active licenses.

ADMIN > SYSTEM MANAGEMENT > LICENSE CENTER

License Summary **License Files**

Add Delete					
<input type="checkbox"/>	ID	PAK	Added At ▲	License Filename	
<input type="checkbox"/>	2016051915...	N/A	2016-08-11 10:06	CGNMSFEAT201605191543320070.lic	
<input type="checkbox"/>	2016062819...	N/A	2016-08-11 10:06	CGNMSFEAT201606281927430090.lic	

For every file, IoT FND displays the fields described in [Table 5](#).

Table 5 License File Fields

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

Adding License Files

To add a license file:

1. Choose **ADMIN > System Management > License Center**.
2. Click **License Files**.
3. Click **Add** to open a search window.
4. Click **Browse** to locate the desired license file and then click **Open**.
5. Click **Upload**. To cancel the upload, click **Reset**.
6. Click **Reset** to cancel the selected file and search for another file.

Deleting License Files

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

To delete a single license or multiple license files:

1. Choose **ADMIN > System Management > License Center**.
2. Click **License Files**.
3. Select the box next to each license file that you want to delete.
4. Click **Delete**. To confirm deletion, click **Yes**. To cancel the action, click **No**.

Managing Logs

- [Configuring Log Settings](#)
- [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:

1. Choose **ADMIN > System Management > Logging**.
2. Select **Log Level Settings**.
3. Check the check boxes of all logging categories to configure.

4. From the **Change Log Level to** 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.

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

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

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

Downloading Logs

To download logs:

1. Choose **ADMIN > System Management > Logging**.
2. Click the **Download Logs** tab.
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.
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 (Figure 3). See Figure 1 for an example of tunnels as used in the IoT FND architecture. See “Tunnel Provisioning Configuration Process for information on provisioning tunnels in the “Managing Tunnel Provisioning” chapter in the IoT FND 4.2 Installation Guide.

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.

Figure 3 Provisioning Settings Page

ADMIN > SYSTEM MANAGEMENT > PROVISIONING SETTINGS

Provisioning Process

IoT-FND URL:
 Field Area Router uses this URL to register with IoT-FND after the tunnel is configured

DHCPv6 Proxy Client

Server Address:
 IPv6 address to send (or multicast) DHCPv6 messages to (can be multiple addresses, separated by commas)

Server Port:
 Port to send (or multicast) DHCPv6 messages to


Client Listen Address:
 IPv6 address to bind to, for sending and receiving DHCPv6 messages (can be multiple addresses, separated by commas)

DHCPv4 Proxy Client

Server Address:
 IPv4 address to send (or broadcast) DHCPv4 messages to (can be multiple addresses, separated by commas)

Server Port:
 Port to send (or broadcast) DHCPv4 messages to

Client Listen Address:
 IPv4 address to bind to, for sending and receiving DHCPv4 messages (can be multiple addresses, separated by commas)



This section provides the following topics for configuring tunnel settings:

- [Configuring the IoT FND Server URL](#)
- [Configuring DHCP Option 43 on Cisco IOS DHCP Server](#)
- [Configuring DHCPv6 Proxy Client](#)
- [Configuring DHCPv4 Proxy Client](#)

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:

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

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 DHCPv6 Proxy Client

To configure DHCPv6 Proxy Client settings:

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

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.

3. Click **Save**.

Configuring DHCPv4 Proxy Client

To configure DHCPv4 Proxy Client settings:

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

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.

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.

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.

3. Click **Save**.

Configuring Server Settings

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

- [Configuring Download Logs Settings](#)
- [Configuring Web Sessions](#)
- [Configuring Device Down Timeouts](#)
- [Configuring Billing Period Settings](#)
- [Configuring RPL Tree Polling](#)
- [Configuring the Issue Status Bar](#)

Configuring Download Logs 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 Logs settings:

1. Choose **ADMIN > System Management > Server Settings**.
2. Click the **Download Logs** tab.
3. Configure these settings:

Table 6 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	

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:

1. Choose **ADMIN > System Management > Server Settings**.
2. Click the **Web Session** tab.
3. Enter the number of timeout seconds. Valid values are 0–86400 (24 hours).

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

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

Configuring Device Down Timeouts

The Device Down Timeouts page lets you specify the number of timeout seconds after which the status of Head-end routers (ASR) and Routers (CGR1000, IR800, C800, ESR) and Endpoints changes to *Down* in IoT FND. The device down poll interval is five minutes. The system uses the device down timeouts values and the last heard time to decide whether to change the device status to Down. For example, if the router device down timeout value is set to two hours (7200 seconds), all routers with a last heard time older than 2 hours are marked as status Down.

You can also configure the device timeout setting for router Config groups and Endpoint Config Groups.

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:

1. Choose **ADMIN > System Management > Server Settings**.
2. Click the **Device Down Timeouts** tab.

ADMIN > SYSTEM MANAGEMENT > SERVER SETTINGS

Download Logs Web Session **Device Down Timeouts** Billing Period Settings RPL Tree Settings Issue Settings

Mark Head-End Routers Down After (secs):	1800
Mark Routers Down After (secs):	1800
Mark ACT Endpoints Down After (secs):	57600
Mark BACT Endpoints Down After (secs):	172800
Mark CAM Endpoints Down After (secs):	57600
Mark Cellular Endpoints Down After (secs):	57600
Mark IR500 Endpoints Down After (secs):	57600
Mark Meter Endpoints Down After (secs):	57600
Mark Gateway Down After (secs):	1800

- For each device type listed, enter the number of seconds after which the device status changes to Down in IoT FND.

The parameter value must be greater than the corresponding polling intervals. For example, the default polling interval for endpoints is 8 hours (28800 seconds), so the value in the **Mark {ACT | BACT | CAM | Cellular | IR500> Meter} Endpoints Down After (secs)** field must be greater than 28800.

- To save the configuration, click the **disk** icon.

Device Down Timeout Settings for Router Config Groups and Endpoint Config Groups

To configure device down timeout settings for Router Config groups or Endpoint Config Groups:

- Choose **CONFIG > Device Configuration**.
- Select the Device you want to configure **{ROUTER | ENDPOINT}** in the left pane.
- Click the **Group Properties** tab.
- In the **Mark Routers Down After (secs)** field, enter the number of seconds after which the status of the devices (router or endpoints) in the group changes to Down in IoT FND.

This value must be greater than the corresponding polling interval.

For example, the default polling interval for routers is 30 minutes (1800 seconds), so the value in the Mark Routers Down After (secs) field must be 1801 or greater.

The default polling interval for ENDPOINTS is 960 minutes (57600 seconds), so the value in the Mark Routers Down After (secs) field must be greater than 57600 seconds.

- To save the configuration, click the **disk** icon.

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:

1. Choose **ADMIN > System Management > Server Settings**.
2. Click the **Billing Period Settings** tab.
3. Enter the starting days for the cellular and Ethernet billing periods.
4. From the drop-down menu, choose the time zone for the billing period.
5. To save the configuration, click the **disk** icon.

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, 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.

Caution: CG-NMS 1.1(5) release does not support router RPL tree updates. Do not enable RPL tree updates from Routers.

To configure RPL tree polling settings:

1. Choose **ADMIN > System Management > Server Settings**.
2. Choose the **RPL Tree Settings** tab.
3. Choose the **Enable RPL tree update from** radio button for Mesh Nodes to receive the RPL tree update from those devices.
4. 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:

1. Choose **ADMIN > System Management > Server Settings > Issue Settings**.
2. To display the Issue status bar in the browser frame, check the **Enable/Disable Issue Status Bar** check box.
3. In the Issue **Status Bar Refresh Interval** (seconds) field, enter a refresh value in seconds.
 - Valid values are 30 secs (default) to 300 secs (5 minutes).
4. In the **Certificate Expiry Threshold** (days) field for all supported routers or an IoT FND application server, enter a value in days.
 - 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.

To configure Syslog forwarding:

1. Choose **ADMIN > System Management > Syslog Settings**.
2. In the **Syslog Server IP Address** field, enter the IP address of the Syslog server.
3. In the **Syslog Server Port Number** field, enter the port number (default is 514) over which to receive device events.
 - To enable message forwarding to the Syslog server, click **Enable Syslog Sending Events**.
 - To disable message forwarding to the Syslog server, click **Disable Syslog Sending Events**.

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

Managing Devices

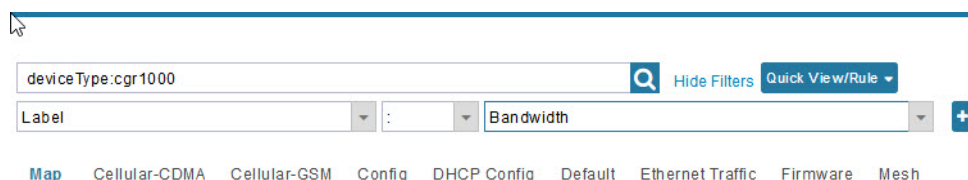
This section describes how to manage devices in IoT FND, and includes the following topics:

- [Overview](#)
- [Managing Routers](#)
- [Managing Endpoints](#)
- [Managing the Cisco Industrial Compute \(IC3000\) Gateway](#)
- [Managing the Cisco Wireless Gateway for LoRaWAN](#)
- [Managing Cisco IR510 WPAN Industrial Routers](#)
- [Managing Head-End Routers](#)
- [Managing External Modules](#)
- [Managing Servers](#)
- [Tracking Assets](#)
- [Common Device Operations](#)
- [Configuring Rules](#)
- [Configuring Devices](#)
- [Monitoring a Guest OS](#)
- [Managing Files](#)
- [Managing Work Orders](#)
- [Demo and Bandwidth Operation Modes](#)
- [Device Properties](#)

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:

Figure 1 **Devices menu options**



- To work with Field Devices such as Routers (CGR1000, C800, IR800, SBR (C5921)) and Endpoints (meters and IR500 gateways), and IoT Gateways (such as the LoRaWAN gateway and IC3000), use the **DEVICES > Field Devices** page.
 - **Note:** In some textual displays of the IoT FND, routers may display as “FAR” rather than the router model (cgr1000, etc).
- To work with Head-end Routers (ASR1000, ISR3900, ISR4000) use the **DEVICES > Head-End Routers** page.
- To work with 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 of this book for details on firmware updates for Routers and Gateways mentioned in this chapter.

Managing Routers

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

- [Working with Router Views](#)
- [Managing Embedded Access Points on Cisco C819 and Cisco IR829 ISRs](#)
- [Using Router Filters](#)
- [Refreshing the Router Mesh Key](#)
- [Managing Embedded Access Points on Cisco C819 and Cisco IR829 ISRs](#)
- [Displaying Router Configuration Groups](#)
- [Displaying Router Firmware Groups](#)
- [Displaying Router Tunnel Groups](#)

Working with Router Views

Unless you select the **Default to map view** option in user preferences (see [Figure 2 Setting User Preferences for User Interface Display](#)) the Field Devices page defaults to the List view, which contains basic device properties. Select a router or group of routers in the **Browse Devices** pane (left pane) to display tabs in the main pane.

The router or routers you select determine which tabs display.

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

- Map
- Cellular-CDMA
- Cellular-GSM
- Config
- DHCP Config
- Default
- Ethernet Traffic

Managing Routers

- Firmware
- Group
- LoRaWAN
- Mesh
- Mesh Config
- Physical
- PLC Mesh
- RF Mesh
- Tunnel
- WiMAX

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

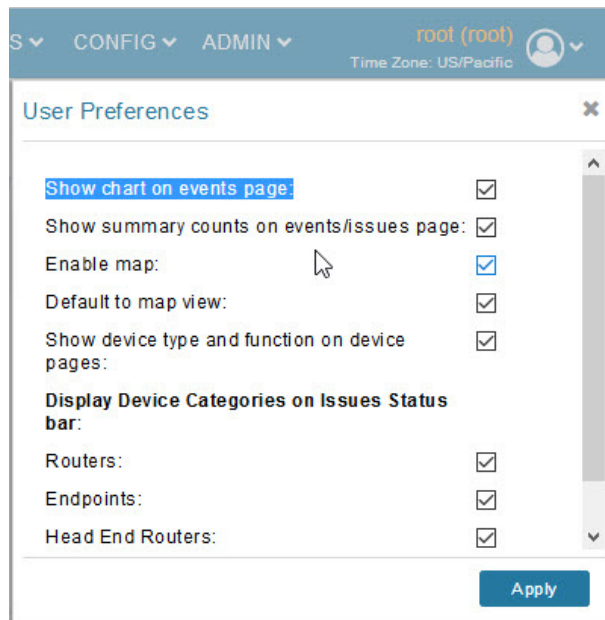
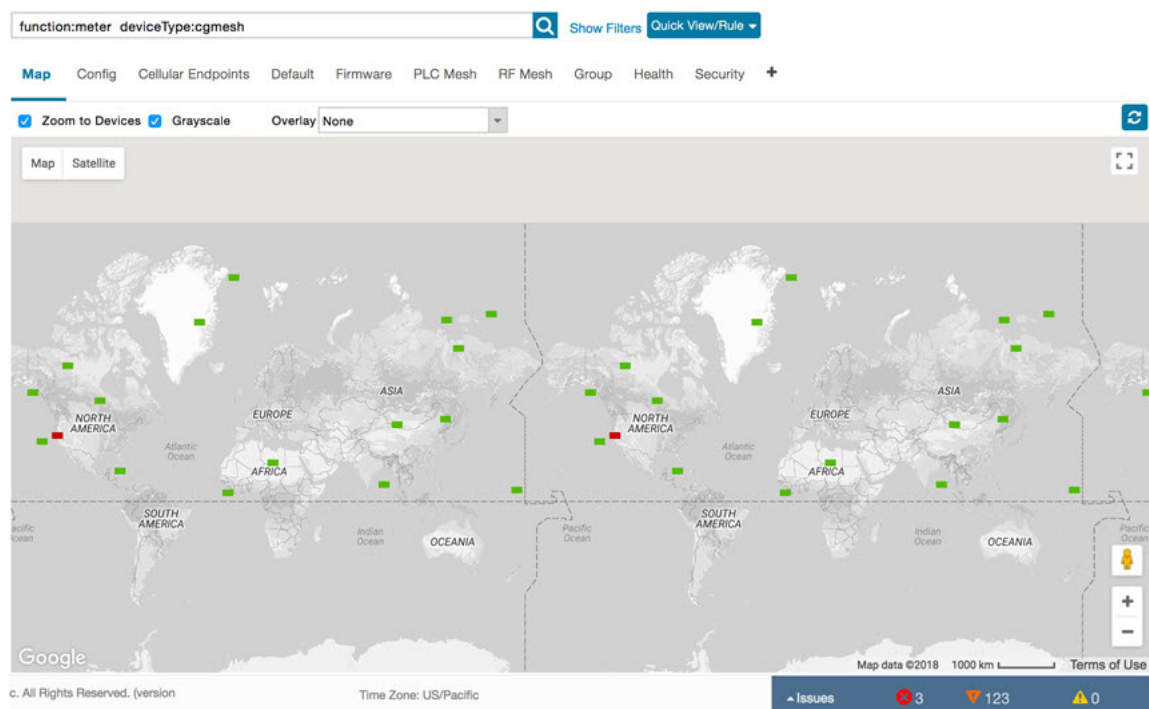
For information on how to customize router views, see [Customizing Device Views](#).

For information about the device properties that display in each view, see [Device Properties](#).

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

Viewing Routers in Map View

To view routers in Map view, check the **Enable map** check box in *<user>* > **Preferences** (see [Figure 2](#)), and then click the **Map** tab (see [Figure 3](#)) in the main pane.

Figure 2 Setting User Preferences for User Interface Display**Figure 3** Map View

Note: You can view any RPL tree by clicking the device in Map view, and closing the information popup window.

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

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

Migrating Router Operating Systems

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

Refreshing the Router Mesh Key

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

Caution: Refreshing the router mesh key can result in mesh endpoints being unable to communicate with the router for a period of time until the mesh endpoints re-register with the router, which happens automatically.

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

1. Check the check boxes of the routers to refresh.
2. Choose **More Actions > Refresh Router Mesh Key** from the drop-down menu.
3. Click **Yes** to continue.

Managing Embedded Access Points on Cisco C819 and Cisco IR829 ISRs

IoT Field Network Director allows you to manage the following embedded access point (AP) attributes on C819 and IR829 ISRs:

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

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

Note: Not all C800 Series and IR800 routers have embedded APs. A C800 ISR features matrix is [here](#). The IR800 ISR features matrix is [here](#).

Using Router Filters

To refine the list of displayed routers, use the built-in router filters under ROUTERS in the Browse Devices pane or saved custom searches in the Quick View pane (left pane). For example, to display all operational 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

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

deviceType:sbr

Config DHCP Config Default Ethernet Traffic Tunnel +

Ping Traceroute Label Bulk Import More Actions Export CSV Location Tracking

Displaying 1 - 2

<input type="checkbox"/>	Name	Status	Last Heard	Config Group	Config Last Status Date	Config Push Status	SD Card Pass Lock
<input type="checkbox"/>	CISCO5921-K9+94W9433K9WG	?	never	default-sbr	2017-12-04 12:07	ERROR	
<input type="checkbox"/>	CISCO5921-K9+9IA8497ANDY	✖	11 days ago	default-sbr	2017-12-04 12:09	SUCCESS	

Displaying Router Tunnel Groups

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

deviceType:ir800

Map Cellular-CDMA Cellular-GSM Config DHCP Config Default Ethernet Traffic Firmware Tunnel LoRaWAN +

Ping Traceroute Label Bulk Import More Actions Export CSV Location Tracking

Displaying 1 - 9

<input type="checkbox"/>	Name	Status	Last Heard	Tunnel Source Interface 1	OSPF Area 1	OSPFv3 Area 1	IPsec Tunnel Dest Addr 1	GRE Tunnel Dest Addr 1	Tunnel Source Interface 2
<input type="checkbox"/>	IR809G-LTE-NA-K9+JM2033X003	✓	1 minute ago	GigabitEther...			2.2.56.190		
<input type="checkbox"/>	IR809G-LTE-VZ-K9+FCW2105001Q	✓	1 minute ago	GigabitEther...			2.2.56.190		

Managing Endpoints

To manage endpoints, view the **DEVICES > Field Devices** page. By default, the page displays the endpoints in List view. This section includes the following topics:

- [Viewing Endpoints in Default View](#)
- [Viewing Mesh Endpoints in Map View](#)
- [Blocking Mesh Devices](#)
- [Displaying Mesh Endpoint Configuration Groups](#)
- [Displaying Mesh Endpoint Firmware Groups](#)

Viewing Endpoints in Default View

When you open the **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).

- Map
- Config
- Cellular Endpoints
- Default
- Firmware
- PLC Mesh
- RF Mesh
- Group
- Health
- Security
- + (Allows you to define a new View (tab))

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

For information on how to customize endpoint views, see [Customizing Device Views](#).

For information about the device properties displayed in each view, see [Device Properties](#).

For information about the common actions in these views (for example, adding labels and changing device properties) that also apply to other devices, see [Common Device Operations](#).

Viewing Mesh Endpoints in Map View

To view mesh endpoints in Map view, select Enable map in <user> > **Preferences**, and click the **Map** tab.

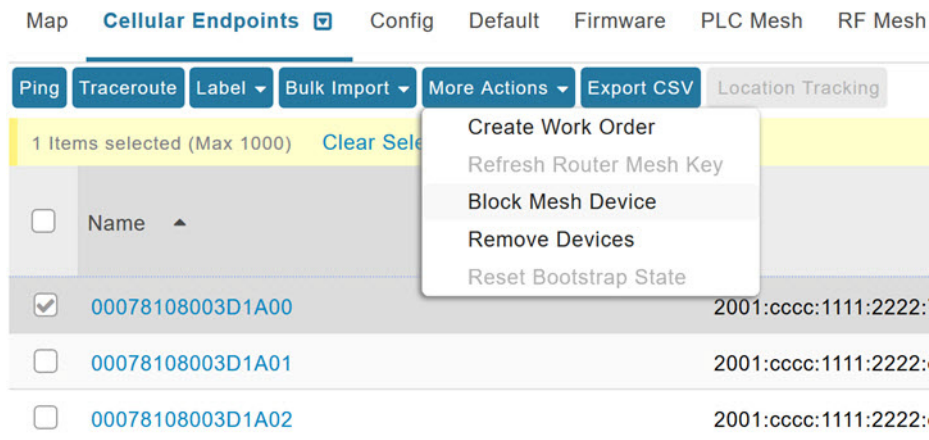
Blocking Mesh Devices

If you suspect unauthorized access attempts to a mesh device, block it from accessing IoT FND.

Caution: If you block 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 > METER-MESH**):

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



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

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

Displaying Mesh Endpoint Configuration Groups

You can 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.

Managing the Cisco Industrial Compute (IC3000) Gateway

Prerequisite

IMPORTANT: Before you can manage the IC3000 Gateway using IoT FND 4.3.1, you must first Deploy Pre-built IOx Applications via the App tab within FND 4.3.1.

For details, refer to the Phase 2 section (summarized below) within the [Cisco IC3000 Industrial Compute Gateway Deployment Guide](#).

■ Phase 2: Deploy Pre-Built IOx Applications via FND

The Phase 2 section within the Cisco IC3000 Industrial Compute Gateway Deployment Guide addresses the following actions, specific to IC3000:

Step 1: Installing FND (This action will most likely already be complete)

Step 2: Adding Devices List to FND

Step 3: Device Registration and DHCP Server Settings

Step 4: Understanding the Device Configuration Template

Step 5: Uploading the Firmware to FND

Step 6: Upgrading Firmware with FND

Step 7: Deploying the IOx Applications via the APP Tab

Overview

IC3000 supports edge computing and communicates with IoT FND through the IOx application, [Cisco Fog Director \(FD\)](#) which accessible via IoT FND.

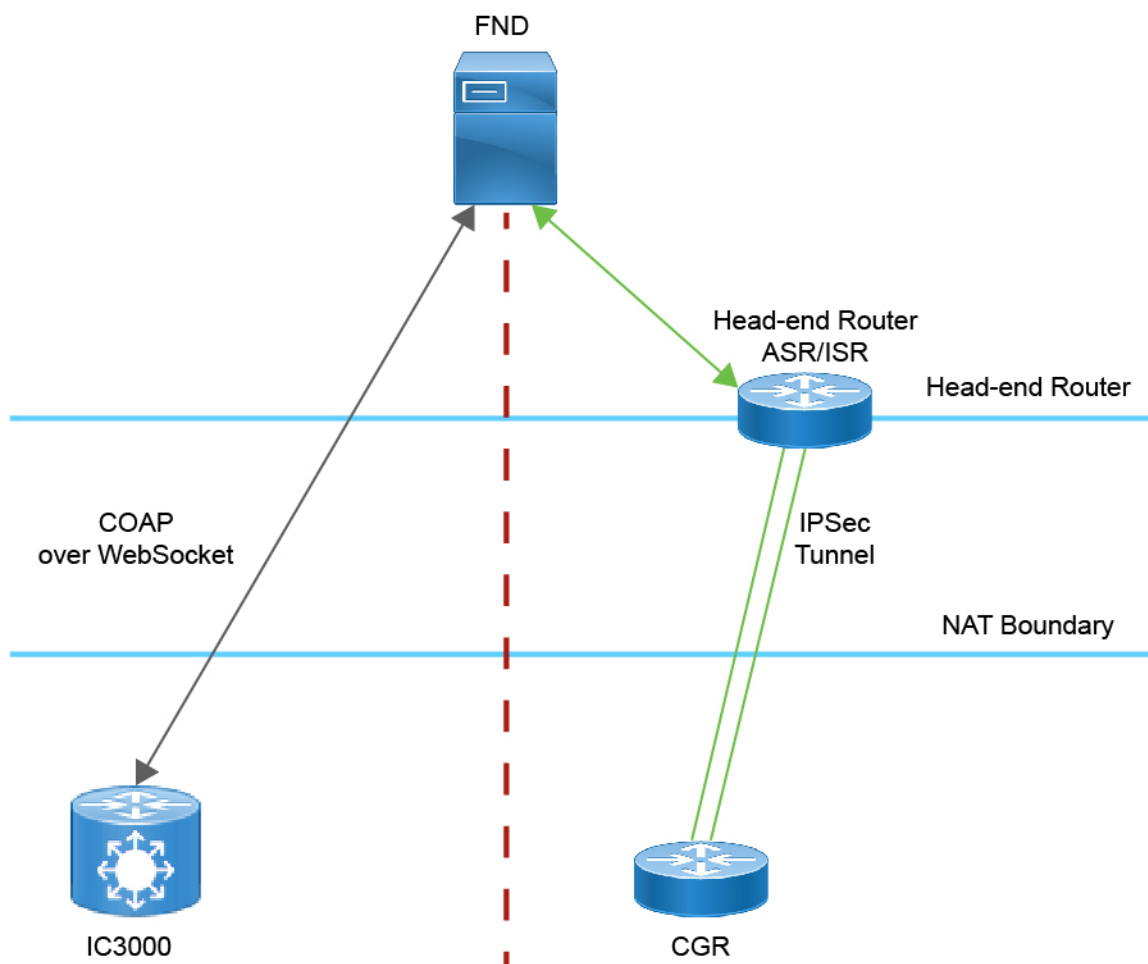
When the IC3000 starts up, it registers with IoT FND. FND then pushes the configuration to the device. Information pushed includes: metric periodic profile interface settings, user management settings and the heartbeat time interval of the device.

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 (see [Figure 4](#)). 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.

Figure 4 IC3000 Communicates with FND using CoAP over WebSocket



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

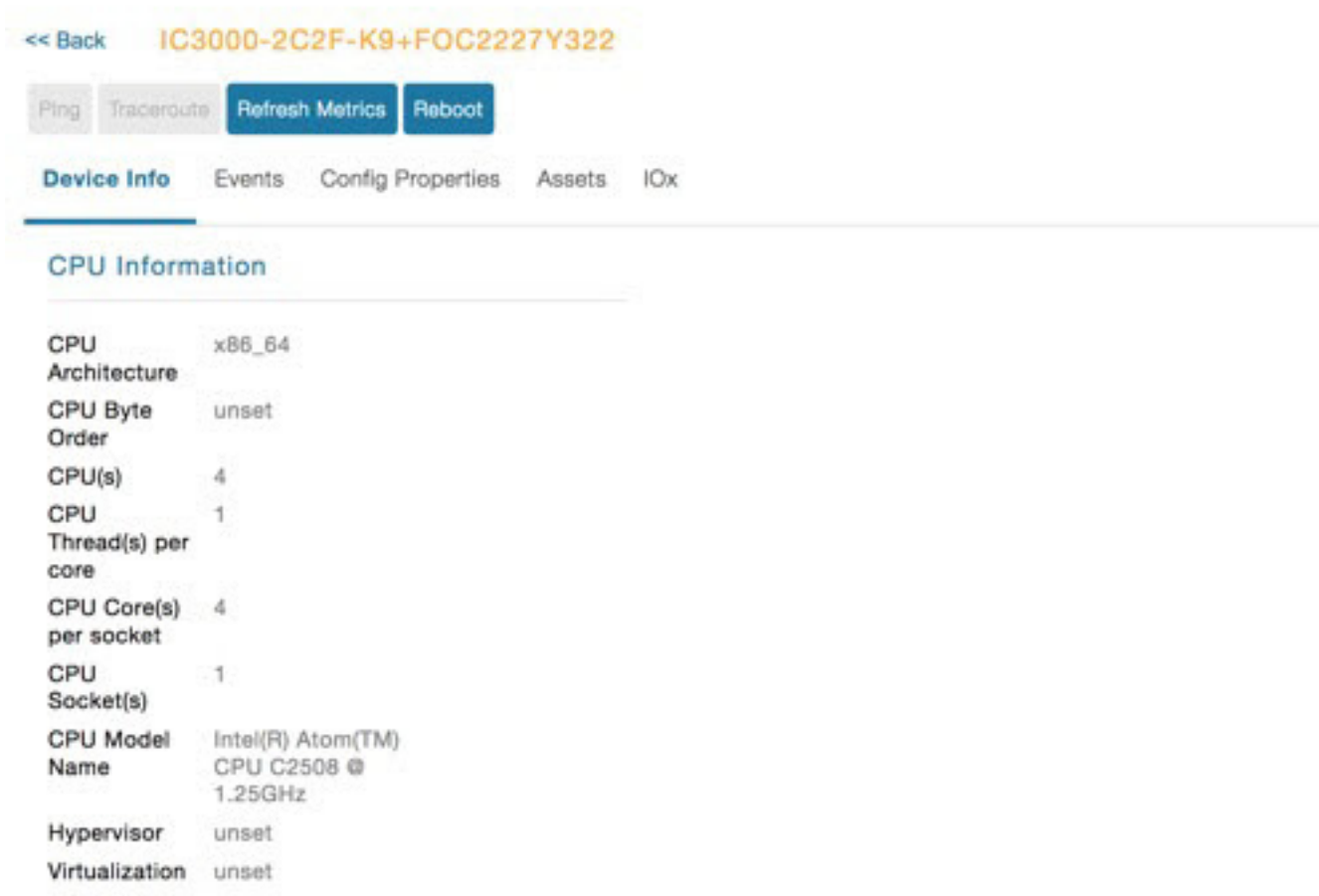
- Refresh Metrics
- Reboot

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 (Figure 5). At the Device Info page, you can Refresh Metrics and Reboot the IC3000.

Figure 5 Device Info Page for an IC3000 Device



You can view the following information on the Application Management Servers Fog Director.

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](#)
- 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)

Figure 6 IoT Gateway Device Info Page, 1 of 2

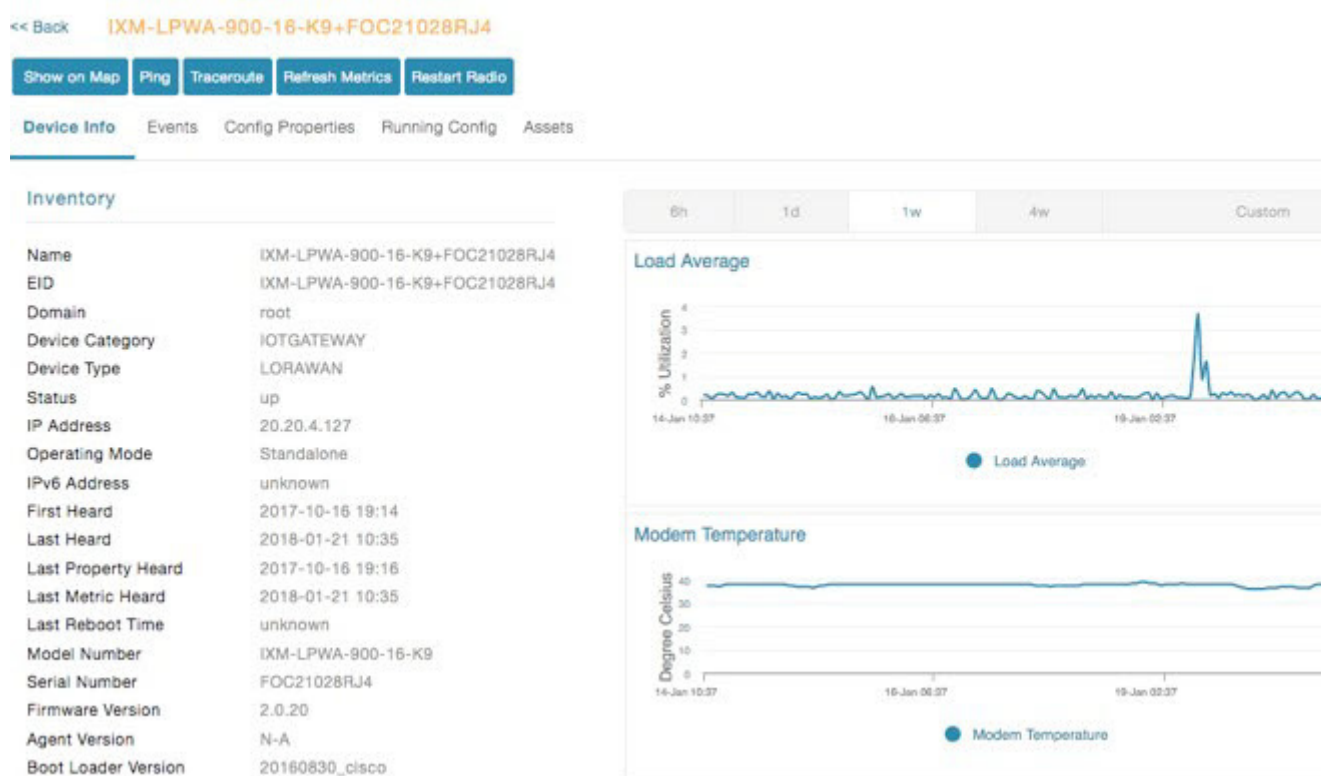


Figure 7 IoT Gateway Device Info Page, 2 of 2

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 = 0x2676f90f MSB = 0x00f14212
Tx Power Calibration	<NA,NA,NA,54,35,106,99,91,82,74,66,56,47,38,29,20-NA,NA,NA,51,32,106,97,89,80,72,64,55,46,37,28,19>
Antenna 1 RSSI Offset(dBm)	-205.00
Antenna 2 RSSI Offset(dBm)	-205.00

Managing Cisco IR510 WPAN Industrial Routers

Cisco IR510 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.

Adaptive Modulation

Adaptive Modulation allows IR510 to dynamically adapt to changes in channel conditions to maximize throughput.

Based on the channel conditions, the node may run on OFDM or FSK mode. FND retrieves info on both modes at the same time and then selects which modulation the IR510 runs on.

To edit the configuration template for the IR510, you enter:

0- Adaptive Modulation

1-FSK

2-OFDM

1. Choose CONFIG > Device Configuration.> Edit Configuration Template

- a. To add a new Adaptive PHY Mode setting for the IR510, select an option from Available Columns panel and click the left-arrow to move the value into the Active Columns panel.
- b. To remove an Adaptive PHY Mode setting for the IR510, select an option from Active Columns panel and click the right-arrow to move the value into the Available Columns panel.

2. Select Default-ir510

Based on the channel conditions, the node may run on OFDM mode or FSK mode, this info should be retrieved by FND, at the same time, FND can select which modulation the node run on.

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 1Pre-defined Profiles for IR510” task on page -75](#) 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 and select the **Profile** type from the drop-down menu.
4. Click **Add** button. A new Profile entry appears in the left pane under the Profile Type sub-heading.

Table 1 Pre-defined Profiles for IR510

Profile Name	Description	Properties Configurable in CSV File
<p>Access Control List (ACL) Profile</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > ACL PROFILE > Config Profiles tab</p> <p>Interface configuration</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > Default-ir500 > Edit Configuration Template</p>	<p>Perform packet filtering to control which packets move through the network for increased security.</p> <p>You can define up to 20 ACL Profiles. Each defined ACL has one associated Access Control Entry (ACE) for a maximum of 20 ACEs.</p> <p>The check process goes through ACL from 1 to 20.</p> <p>There is an implicit deny for all ACL at the end of 20 ACL unless configured differently.</p> <p>To configure the interface for the Default-IR500, with Groups tab selected:</p> <p>In right-pane, choose Edit Configuration Template tab and select the Enable Interface ACL check box.</p>	---
<p>Forward Mapping Rule (FMR) Profile</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > FMR PROFILE > Config Profiles tab</p>	<p>Processes IPv4 traffic between MAP nodes that are in two different MAP domains.</p> <p>Each FMR rule has IPv4 Prefix, IPv4 Prefix Length and EA Bits Length.</p> <p>You can define up to 10 FMR Profiles.</p> <p>FMR settings are pushed to the device as a part of MAP-T Settings during configuration push.</p>	<p>Forward Mapping Rule IPv6 Prefix: fmrlIPv6Prefix0 to fmrlIPv6Prefix9</p> <p>Forward Mapping Rule IPv6 Prefix Length: fmrlIPv6PrefixLen0 to fmrlIPv6PrefixLen9</p>
<p>DSCP profile</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > DSCP PROFILE > Config Profiles tab</p>	<p>Sets the DSCP marking for the Ethernet QoS configuration.</p> <p>DSCP marking has three priority levels (low, normal, and medium).</p> <p>You can specify a maximum of 10 IPv4 addresses and associated DSCP markings.</p>	---
<p>MAP-T Profile</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > DSCP PROFILE > Config Profiles tab</p>	<p>Configures endUser properties.</p>	<p>endUserIPv6Prefix</p> <p>bmrlIPv6PrefixLen</p>

Table 1 Pre-defined Profiles for IR510

Profile Name	Description	Properties Configurable in CSV File
Serial Port Profile (DCE and DTE) CONFIG > DEVICE CONFIGURATION > ENDPOINT > SERIAL PROFILE > Config Profiles tab	<p>You can use different serial port profiles for DCE and DTE serial port settings).</p> <p>You can configure the following settings on the serial interface:</p> <ul style="list-style-type: none">Port affinityMedia TypeData BitsParityFlow ControlDSCP MarkingBaud rateStop Bit <p>Note: You can also configure Raw Socket Sessions settings at the this page.</p>	---

Table 1 Pre-defined Profiles for IR510

Profile Name	Description	Properties Configurable in CSV File
<p>DHCP Client Profile</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > DHCP CLIENT PROFILE > Config Profiles tab</p>	<p>The DHCPv4 server allocates an address to each client according to a static binding between a client-id and an IPv4 address.</p> <p>FND configures this static binding supports up to 10 client mappings.</p> <p>The DHCP Client ID binding profile configuration associates a client ID to an IPv4 Host address.</p> <p>The Client-id of each Client is expected to be unique within a single IR510.</p> <p>Any string can be used as client-id (for example, client-id="iox") can be mapped to a binding address in the pool.</p>	---
<p>DHCP Server Profile</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > DHCP SERVER PROFILE > Config Profiles tab</p>	<p>Information that the DHCPV4 Server returns as part of DHCP Options in the response, can be configured in the DHCP server profile configuration includes:</p> <ol style="list-style-type: none"> 1. Lease Time 2. DNS server list 	---
<p>NAT44 Profile</p> <p>CONFIG > DEVICE CONFIGURATION > ENDPOINT > NAT 44 PROFILE > Config Profiles tab</p>	<p>You can use one of the following methods to configure the NAT44 properties for the IR500 device:</p> <ul style="list-style-type: none"> - CSV import method - NAT44 profile instance within FND user interface <p>You configure three fields for NAT44: Internal Address, Internal Port and External Port</p> <p>You can configure up to fifteen NAT 44 Static Map entries</p> <p>Note: Before you push the configuration, be sure to:</p> <ol style="list-style-type: none"> 1. Enable Ethernet on the configuration group to which the device belongs (select check box) 2. Save Configuration Group 	---

Figure 8 Configuration Template for a Profile

CONFIG > DEVICE CONFIGURATION

Assign Devices to Group Change Device Properties

Groups Config Profiles

Configuration Profiles +

- ENDPOINT
 - FMR PROFILE
 - Default-FMR-Profile
 - Prasam-FMR-Profile
 - ConfigTemplateRegress-FMR
 - DSCP PROFILE
 - Default-DSCP-Profile
 - ConfigTemplateRegress-DSCP
 - ConfigTemplateRegress-DSCP-1** [edit] [copy] [delete]
 - MAP-T PROFILE
 - Default-MAPT-Profile
 - ConfigTemplateRegress-MAPT

ConfigTemplateRegress-DSCP-1

DSCP Marking Rules

+ - Max 10 entries

<input type="checkbox"/>	Source IPv4 Address	DSCP Marking
<input type="checkbox"/>	10.21.32.42	Medium
<input type="checkbox"/>	10.21.32.43	Low
<input type="checkbox"/>	10.21.32.44	Normal

[save]

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 (Figure 9).
- 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.

Figure 9 Configuration Template for a Group

default-ir500

Sync Membership

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

Current Configuration revision #87 - Last Saved on 2017-12-06 00:54

Active Columns
OFDM-800Kbps

←

→

Available Columns
OFDM-50kbps
OFDM-200kbps
OFDM-1200kbps

Note: This settings is applicable for **IR510** devices only.

FMR Profile:	ConfigTemplate_FMR	▼	📄
DSCP Profile:	ConfigTemplate_DSCP	▼	📄
Map-T Domain Profile:	Default-MAPT-Profile	▼	📄
DHCP Client Profile:	sce_DHCPClient	▼	📄
NAT44 Profile:	sce_2	▼	📄
DHCP Server Profile:	sce_DHCPServerProfile	▼	📄
Serial Port Profile (DCE):	sce_1_Dce	▼	📄
Serial Port Profile (DTE):	sce_2_dte	▼	📄

📄

Managing Head-End Routers

To manage Head-end routers (HERs), open the Head-End Routers page by choosing Devices > Head-End Routers (Figure 10). Unless Enable Map is selected in user preferences, by default, the page displays the HERs in List view. When you open the Head-End Routers page in List view, IoT FND displays the Default list view. This view displays basic HER device properties. In addition, IoT FND provides these tabs to display additional HER property views:

- Tunnel 1
- Tunnel 2

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

Figure 10 Head-End Routers Page

For information on how to customize HER views, see [Customizing Device Views](#).

For information about the device properties displayed in each view, see [Device Properties](#).

For information about the common actions in these views (for example, adding labels and changing device properties) that also apply to other devices, see [Common Device Operations](#).

Managing External Modules

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

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.

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 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>
```

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 and Select Type ACTD-CGR and select the appropriate Image from the drop-down menu such *app-actd-ver-x.y.z.tar*.

D) Click **Upload Image**.

E) Click **Yes** to confirm upload.

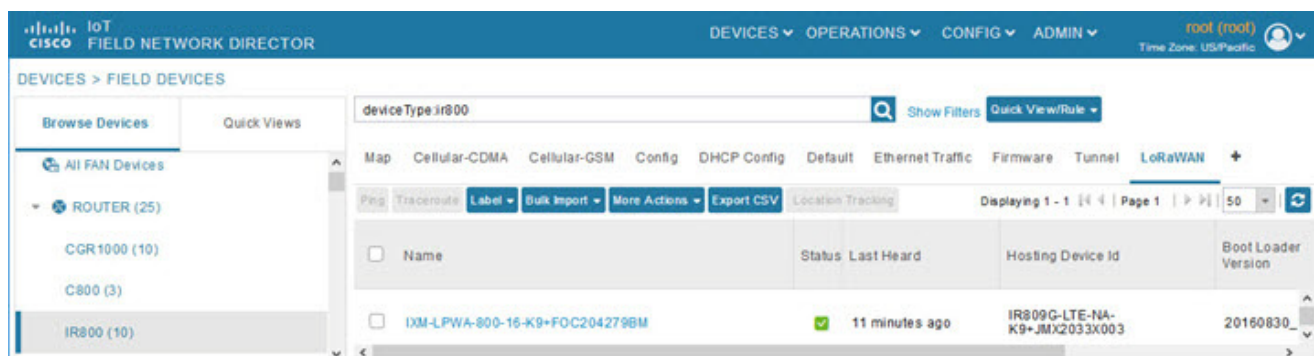
LoRaWAN Gateway Module

- 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.

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



- To reboot the modem on the LoRaWAN module:
 - Click on the relevant IXM-LORA link under the **Name** column to display the information seen below:

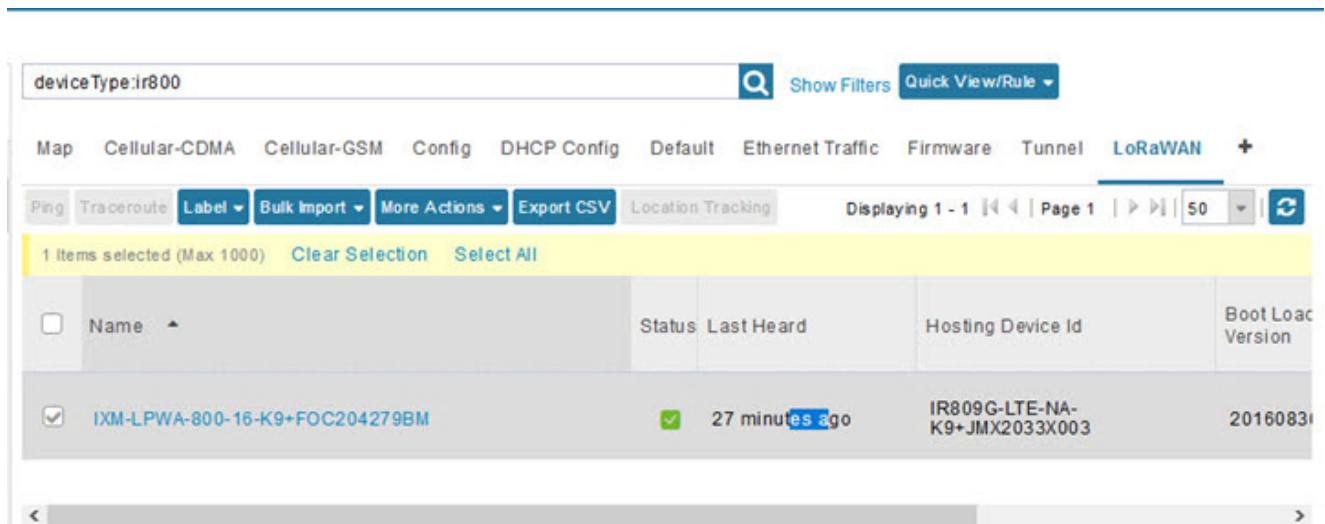


- Click **Reboot Modem**. When the reboot completes, the date and time display in the **Last Reboot Time** field in the Device Info pane for the LoRaWAN module. You can only process one modem reboot at a time.

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

- To remove a LoRaWAN module from the IR800 router inventory:
 - 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 menu, select **Remove Devices**.
- 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. Click **Add**. The new tunnel appears under the GATEWAY heading in the left-pane.

Managing Servers

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

To add additional views, see [Customizing Device Views](#).

For more information about the device properties displayed in each view, see [Device Properties](#).

For information about the common actions in this view, see [Common Device Operations](#).

Managing NMS 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 displays details on CPU Usage and Memory Usages

Tracking Assets

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

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

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

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

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

Example of Asset content in CSV file:

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

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

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

Guidelines for Adding or Associating an Asset with a Device:

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

Common Device Operations

This section describes how to use IoT FND to manage and view information about devices, and includes the following topics:

- [Selecting Devices](#)
- [Customizing Device Views](#)
- [Viewing Devices in Map View](#)
- [Configuring Map Settings](#)

- [Changing the Sorting Order of Devices](#)
- [Exporting Device Information](#)
- [Pinging Devices](#)
- [Tracing Routes to Devices](#)
- [Managing Device Labels](#)
- [Removing Devices](#)
- [Displaying Detailed Device Information](#)
- [Using Filters to Control the Display of Devices](#)
- [Performing Bulk Import Actions](#)

Selecting Devices

In List view, IoT FND lets you select devices on a single page and across pages. When you select devices, a yellow bar displays that maintains a count of selected devices and has the **Clear Selection** and **Select All** commands. The maximum number of devices you can select is 1000. Perform the following to select devices:

- To select 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](#) for available properties)
- Change the order of columns

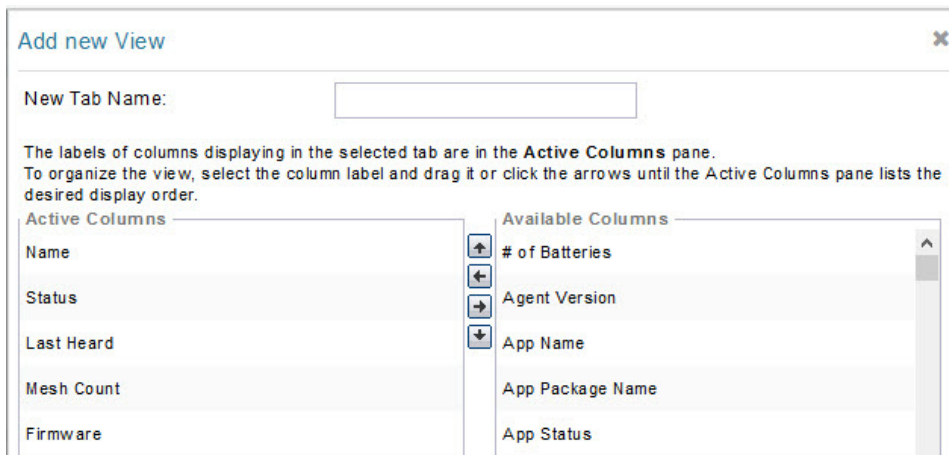
Adding Device Views

To add a custom device view tab to a device page in list view:

1. Click the + tab.



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



3. Add properties to the Active Columns list by selecting them from the Available Columns list, and then clicking the left arrow button, or dragging them into the Active Columns list.

- To change column order, use the up and down arrow buttons or drag them to the desired position.
- To remove properties from the Active Columns list, select those properties and click the right arrow button, or drag them out of the list.

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

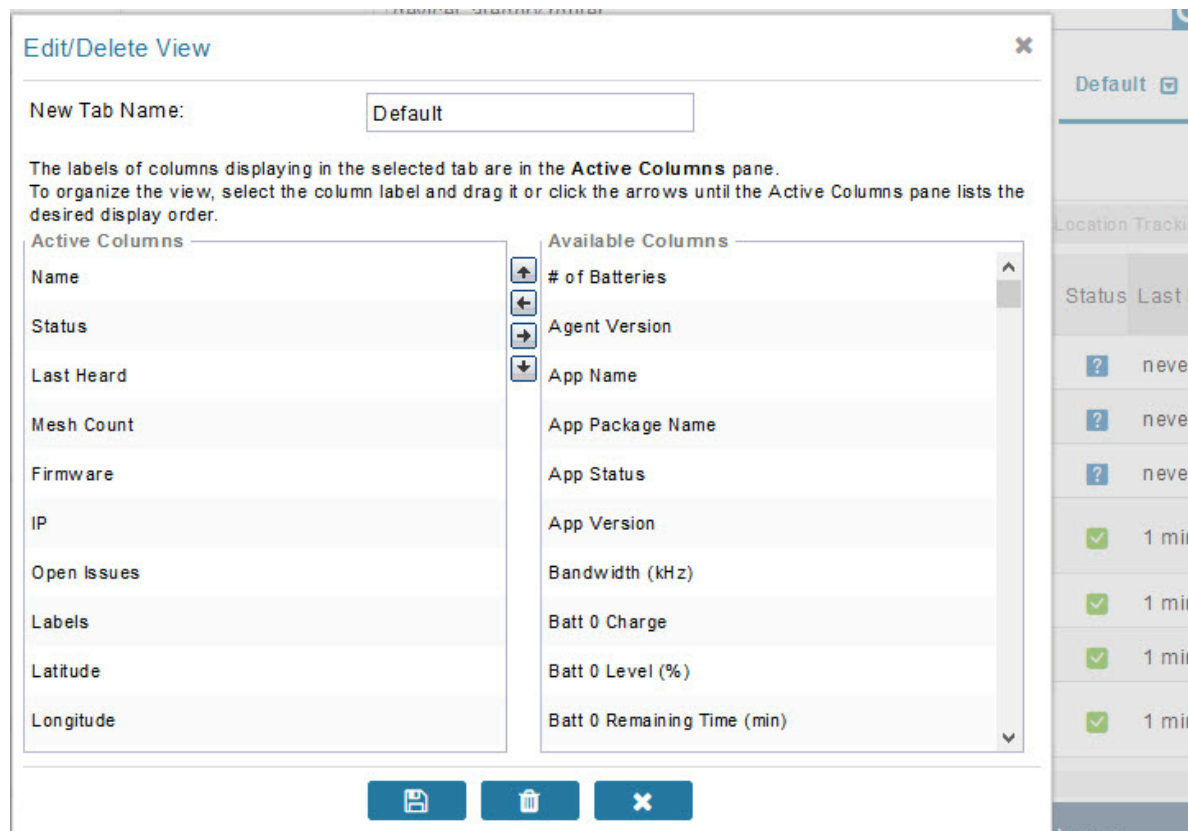
4. Click **Save View**.

Editing Device Views

To edit a device view:

1. Select a device type under the Browse Devices pane, and click the **Default** drop-down arrow to open the Edit/Delete View.
2. In the Edit/Delete View dialog box:
 - a. To remove properties from the Active Columns list, select those properties and click the right-arrow button or drag them out of the Active Columns list.
 - b. To add properties to the Active Columns list, select those properties from the Available Columns list and click the left-arrow button, or drag them into position in the Active Columns list.
 - c. To change the sort order of the active columns, use the up- and down-arrow buttons, or drag them to the desired position.

To close the View without making any changes, select **X** icon.



3. Click disk image to **Save View**.

Deleting a Device View

To remove a View entirely:

1. Select a device type under the Browse Devices pane, and click the **Default** drop-down arrow to open the Edit/Delete View.
2. In the Edit/Delete View dialog box, select the desired label in the Active Columns pane.
3. To delete the view, click the trash icon.

Viewing Devices in Map View

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

To view devices in Map view:

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

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

User Preferences

Show chart on events page: ☒

Show summary counts on events/issues page: ☒

Enable map: ☒

Default to map view: ☒

Show device type and function on device pages: ☒

Display Device Categories on Issues Status bar: ☒

Routers: ☒

Endpoints: ☒

Head End Routers: ☒

Apply

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

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.

deviceType:cgr1000

Show Filters Quick View/Rule

Map Cellular-CDMA Cellular-GSM Config DHCP Config Default Ethernet Traffic Firmware Mesh Mesh Config Physical Tunnel

☒ Zoom to Devices ☐ Grayscale Overlay None

Map Satellite

CGR1240/K9+JAF1723AHHP
 Cisco Connected Grid Router 1000-Series
 2001:420:7bf:8e8:2168:a3ae:aa06:89e0

Details Ping Traceroute Create Work Order

Status	down	Last Heard	2017-03-16 22:52
Model	CGR1240/K9	Serial Number	JAF1723AHHP
Number	default-cgr1000	Firmware Group	test2
Config Group	default-cgr1000	Hostname	NXT-ANDERSON2
Tunnel Group	15.6(2.10.31)GB		
Firmware Version			

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](#).
- 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.

5. Close the Device popup window to view the RPL tree associated with the device. See [Configuring RPL Tree Polling](#).

The RPL tree connection displays as blue or orange lines; where blue indicates that the link is down, and orange indicates that the link is up.

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:

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

2. Click the **Map** tab.

- To automatically zoom to devices, check the **Zoom to Devices** check box.
- To display the map in grayscale, check the **Grayscale** check box.

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).

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:

1. Select the devices to export by checking their corresponding check boxes.
2. Click **Export CSV**.
3. Click **Yes** in the confirmation dialog box.

IoT FND creates a CSV file, export.csv, containing the information that displays in the List view pane. By default, IoT FND saves this file to your default download directory. When a file with the same name exists, IoT FND adds a number to the default filename (for example, export-1.csv and export-2.csv).

The export.csv file consists of one header line defining the exported fields followed by one or more lines, each representing a device. Here is an example of an export of selected devices from the Field Devices page:

```
name,lastHeard,meshEndpointCount,uptime,runningFirmwareVersion,openIssues,labels,lat,lng
CGR1240/K9+JSJLABTES32,2012-09-19 00:58:22.0,,,,Door Open|Port Down,,50.4,-130.5
sgbuA1_cgr0,,,,,,42.19716359,-87.93733641
sgbuA1_cgr1,,,,,,44.3558597,-114.8060403
```

Pinging Devices

When troubleshooting device issues, ping registered devices to rule out network connectivity issues. If you can ping a device, it is accessible over the network.

To ping selected devices, in List view:

1. Check the check boxes of the devices to ping.
Note: If the status of a device is Unheard, a ping gets no response.
2. Click **Ping** 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.

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:

1. Check the check boxes of the devices to trace.

Note: You can only trace routes to devices registered with IoT FND. If the status of a device is Unheard, you cannot trace the route to it.

2. Click **Traceroute**.

A window displays with the route-tracing results.

The screenshot shows a web-based network management interface. At the top, there are tabs for 'Map', 'Cellular-CDMA', 'Cellular-GSM', 'Config', 'DHCP Config', 'Default' (selected), 'Ethernet Traffic', 'Firmware', 'Mesh', 'Mesh Config', and 'Physical'. Below these tabs is a toolbar with buttons for 'Ping', 'Traceroute' (highlighted), 'Label', 'Bulk Import', 'More Actions', and 'Export CSV'. A status bar indicates '2 items selected (Max 1000)' with 'Clear Selection' and 'Select All' links. The main content area has a table with columns: 'Started At', 'Device', 'Status', and 'Result'. The table contains two rows of data. The first row shows a successful traceroute to 2.2.56.228. The second row shows a successful traceroute to 2.2.55.196. Below the table is a pagination control showing 'Page 1 of 1' and a '10' items per page dropdown. A blue 'X' button is at the bottom right of the window.

Started At	Device	Status	Result
2017-06-14 09:20	2.2.56.228	Completed successfully	traceroute to 2.2.56.228 (2.2.56.228), 30 hops max, 60 byte packets 1 2.2.56.228 (2.2.56.228) 1.726 ms * *
2017-06-14 09:20	2.2.55.196	Completed successfully	traceroute to 2.2.55.196 (2.2.55.196), 30 hops max, 60 byte packets 1 ARennes-659-1-96-196.w2-2.abo.wanadoo.fr (2.2.55.196) 3.691 ms 4.245 ms 4.936 ms

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.

3. Click **X** to close the window.

Managing Device Labels

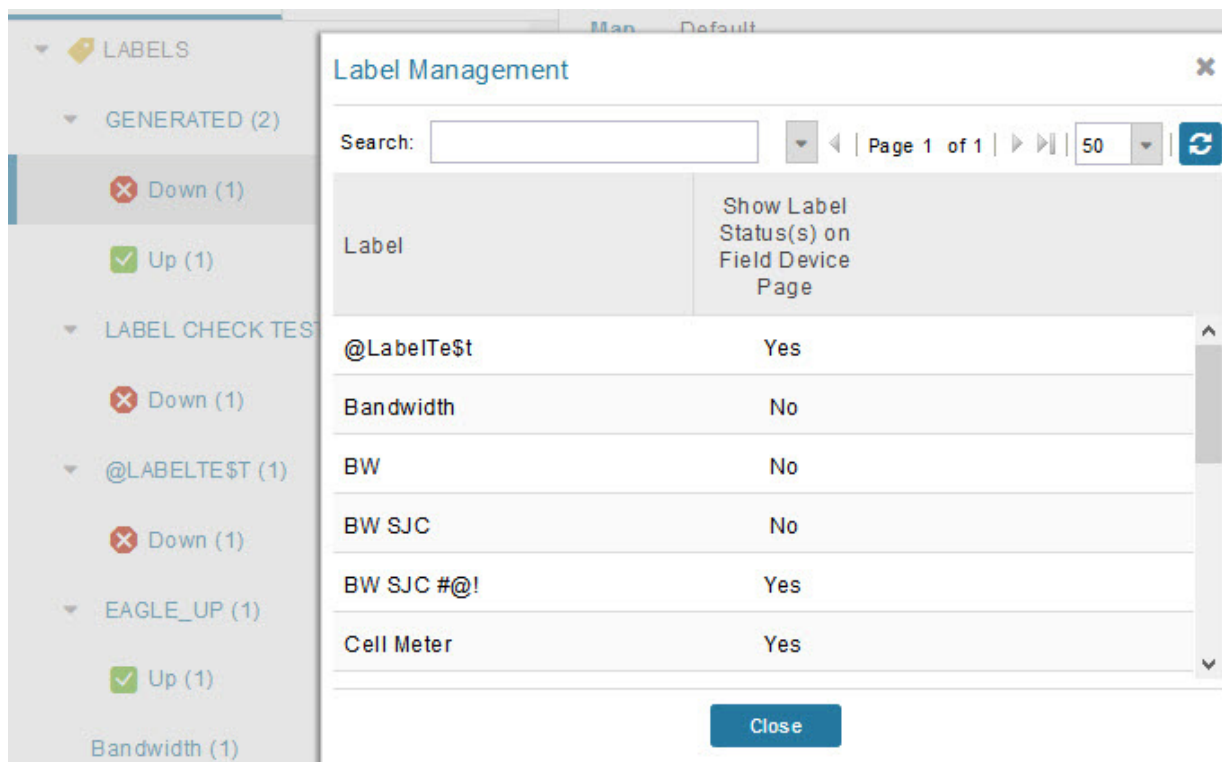
You use labels to create logical groups of devices to facilitate locating devices and device management.

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:

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.

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

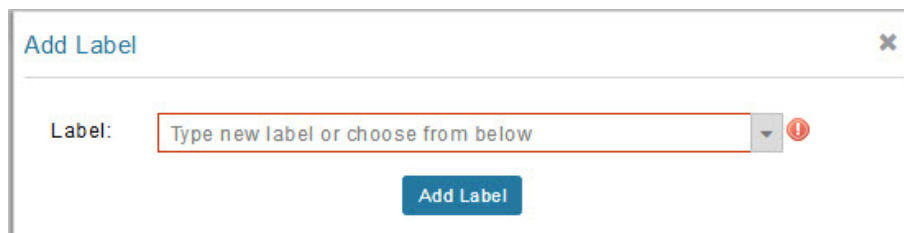
3. Click **Close**.

Adding Labels

To add labels to selected devices, in List view:

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

Choose **Label > Add Label**.



The 'Add Label' dialog box features a title bar with a close button (X). Below the title bar is a label 'Label:' followed by a text input field containing the placeholder text 'Type new label or choose from below'. To the right of the input field is a small red warning icon. Below the input field is a blue button labeled 'Add Label'.

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

Tip: You can add multiple labels to one device.

4. Click **OK**.

To add labels in bulk, see [Adding Labels in Bulk](#).

Removing Labels

To remove labels from selected devices, in List view:

1. Check the check boxes of the devices from which to remove the label.
2. Choose **Label > Remove Label**.
3. Click **OK**.

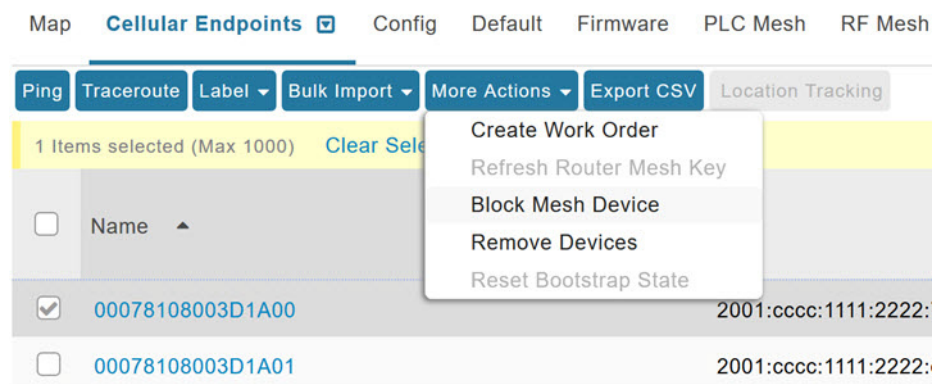
To remove labels in bulk, see [Removing Labels in Bulk](#).

Removing Devices

Caution: When you remove 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:

1. Check the check boxes of the devices to remove



The screenshot shows the 'Cellular Endpoints' tab selected in a navigation bar. Below the navigation bar are several buttons: 'Ping', 'Traceroute', 'Label', 'Bulk Import', 'More Actions', 'Export CSV', and 'Location Tracking'. A yellow banner indicates '1 Items selected (Max 1000)' with a 'Clear Selection' link. Below this is a table with columns for checkboxes, 'Name', and IP addresses. The first row is selected, and a context menu is open over the 'More Actions' button, showing options: 'Create Work Order', 'Refresh Router Mesh Key', 'Block Mesh Device', 'Remove Devices', and 'Reset Bootstrap State'.

	Name	IP Address
<input checked="" type="checkbox"/>	00078108003D1A00	2001:cccc:1111:2222:
<input type="checkbox"/>	00078108003D1A01	2001:cccc:1111:2222:

2. Choose **More Actions > Remove Devices**.
3. Click **Yes**.

Displaying Detailed Device Information

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

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

Detailed Device Information Displayed

- [Server Information](#)
- [Head-end Router, Router, and Endpoint Information](#)

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.

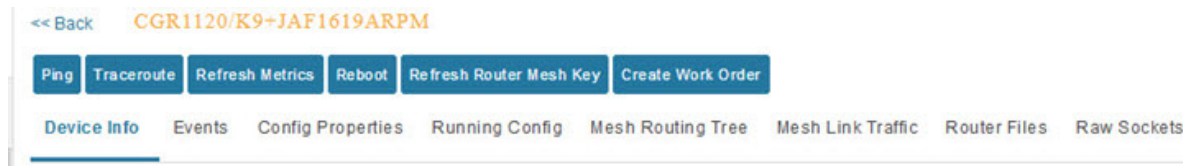
Table 2 NMS Server Pane Areas

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

Head-end Router, Router, and Endpoint Information

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

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



Information Category	Description
Device Info (all)	Displays detailed device information (see Device Properties). For routers and endpoints, IoT FND also displays charts (see Viewing Device Charts).
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). You can configure these properties by importing a CSV file specifying the properties to configure and their new values, as described in Changing Device Configuration Properties .
Running Config (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 29 on page 153).
Embedded AP (IR829 only)	Lists inventory (configuration) details and metrics for the attached access point.
AP Running Config (C800 and IR8829 only)	Lists the running configuration file for the attached access point.

Actions You Can Perform from the Detailed Device Information Page



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

Action	Description
Show on Map (C800, endpoints)	Displays a popup window with a map location of the device. This is the equivalent of entering eid:Device_EID in the search field in Map View.
Ping	Sends a ping to the device to determine its network connectivity. See Pinging Devices .
Traceroute	Traces the route to the device. See Tracing Routes to Devices .

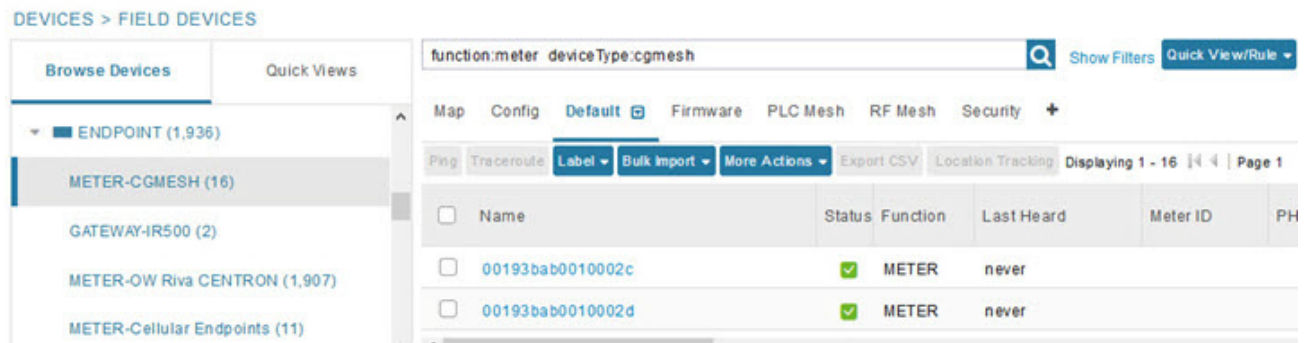
Action	Description
Refresh Metrics	Instructs the device to send metrics to IoT FND.
(Head-end routers and routers only)	Note: IoT FND assigns historical values for metrics for each device. To access historical metric values, use the GetMetricHistory North Bound API call.
Reboot	Enables a reboot of the modem on LoRaWAN.
Sync Config Membership	Synchronizes the configuration membership for this device. See Synchronizing Endpoint Membership .
(Mesh endpoints only)	
Sync Firmware Membership	Click Sync Firmware Membership to synchronize the firmware membership for this device, and then click Yes to complete the process.
(Mesh endpoints only)	
Block Mesh Device	Blocks the mesh endpoint device.
(Mesh endpoints only)	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	Creates a work order. See Creating Work Orders .
(Routers and DA Gateway only)	

Using Filters to Control the Display of Devices

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

Browse Devices Filters

Built-in device filters display in the Browse Devices pane. These filters control the display of devices in List and Map views. For every filter entry, IoT FND provides a device count in parenthesis. IoT FND automatically updates the device count without having to reload the page. In the example in [Figure 11](#), the top-level Endpoints label is selected, which inserts the following built-in filter in the Search Devices field: `deviceType:cgmesh firmwareGroup:default-cgmesh`.

Figure 11 Built-in Filter to Search for Mesh Endpoints

Creating and Editing Quick View Filters

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

Creating a Quick View Filter

To create a Quick View filter:

1. On any device page, click **Show Filters** and add filters to the Search field.
For more information about adding filters, see [Adding a Filter](#).
2. From the **Quick View/Rule** drop-down menu, choose **Create Quick View**.
3. In the Create Quick View dialog box that opens, enter a Name for the view.
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:

1. Click the Quick View tab and select the filter to edit.
2. From the **Quick View/Rule** drop-down menu, choose **Edit Quick View**.
3. In the **Update Quick View** dialog box, make the necessary modifications, and then click **Save**.
4. To delete the Quick View, click the **Delete** button.

Adding a Filter

To add a filter to the Search field:

1. If the Add Filter fields are not present under the Search field, click **Show Filters**.
2. From the **Label** drop-down menu, choose a filter.

The drop-down menu defines filters for all device information categories. For more information about these categories, see [Working with Router Views](#).

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

For more information about operators, see [Table 3](#). If you choose a numeric metric from the Label menu (for example, **Transmit Speed**), you can specify a range of values in the filter you are adding. For date/time filters, “between” is the operator. Use the calendar buttons to specify the date range for the filter.

4. In the **Value** field, enter a value to match or a range of values in the case of numeric metrics or select an available value from the drop-down menu.
5. Click the Add (+) button to add the filter to the existing filter syntax in the Search field.
6. (Optional) Repeat the process to continue adding filters.

Filter Operators

[Table 3](#) describes the operators you can use to create filters.

Table 3 Filter Operators

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

Search Syntax

IoT FND supports this simple query language syntax:

Search := filter [filter ...]

Filter := fieldname operator value

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

Note the following when creating filters to search fields:

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

[Table 4](#) describes filter examples.

Table 4 Filter Examples

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

Table 4 Filter Examples

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

Performing Bulk Import Actions

In IoT FND, you can perform these bulk import device actions:

- [Adding Routers, Head-End Routers, IC3000 Gateway, Endpoint and Extenders and IR500 in Bulk](#)
- [Adding HERs to IoT FND](#)
- [Changing Device Properties in Bulk](#)
- [Adding Labels in Bulk](#)
- [Removing Labels in Bulk](#)

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:

1. On any Device page (such as **DEVICES > FIELD DEVICES**), choose **Add Devices**.
2. In the Add Devices window, click **Browse** to locate the CSV file containing the device information to import, and then click **Add**.

For more information about adding gateways, see [Adding an IC3000 Gateway](#)

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

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

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

3. Click **Add**.
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,IOUserName,IOUserPassword
IC3000+FOC2219Y47Z,ic3000,10,10,system,

r6Bx/jSWuFi2vs9U1Zh21NSILakPJNwS1CY/jQBYRcxSH8qLpgUtOn7nqywr/vOkVPYbNPAFXj4Pbag6m1spjZLR6oc1
PkT9eF6108frFXy+eI2FFaUZ1SCKTdjSqfur5EwEu1E5u54ckMi1e07X8INZuNdFNFU7ZgElt3es8yrpR3i/EgD0dSb5dqw
0u31OeVrEtPY0xBHraYgPv+dBh3XtW4i2Kv/sveiTBPx2FiNRvuLWl17Qm+D7b11Fh4ZJCivapy7EYZirwHHAVJlQh6bWYr
GAccNPkY+KqIZDCyX/Ck5psmgzyAHKmJ8Dq7K0nBsnq2+b2VKReEhsj9+Fw==
```


Adding HERs to IoT FND

Configuring HERs Before Adding them to IoT FND

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

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

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

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

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

Adding HERs

To add HERs, create a CSV file like the following example that consists of a header line followed by one or more lines, each representing an HER:

```
eid,deviceType,lat,lng,ip,netconfUsername,netconfPassword
ASR1001+JAE15460070,asr1000,40.0,-132.0,172.27.166.57,admin,cisco
ASR1001+JAE15460071,asr1000,40.0,-132.0,172.27.166.58,admin,cisco
```

[Table 5](#) describes the fields to include in the CSV file.

Note: For device configuration field descriptions, see [Device Properties](#).

Table 5 HER Import Fields

Field	Description
eid	The element identifier (EID) of the device, which consists of the product ID (PID), a plus sign, and the serial number (SN) of the HER (for example, <i>HER_PID+HER_SN</i>).
deviceType	The device type must be asr1000 or isr3900.
lat	(Optional) The location (latitude and longitude) of the HER.
lng	
ip	The IP address of the HER. The address must be reachable from the IoT FND server.
netconfAddress	
netconfUsername	The SSH username and password that IoT FND uses to connect to the HER.
netconfPassword	

When you add an HER, IoT FND displays its status as Unheard. IoT FND changes the status to Up after it polls the HER. IoT FND polls HERs in the background every 15 minutes to collect device metrics, so it should take no more than 15 minutes for the status of HERs to change to Up after you add them to IoT FND. However, you can trigger the polling of HERs by clicking **Refresh Metrics** ([Refresh Metrics](#)).

Adding 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](#), page 139.

Table 6 describes the router properties defined in the <R> record used in this example:

Table 6 Router Import Fields

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

Mapping Routers to HERs

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

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

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

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

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

For example:

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

Adding Router-to-HER Mappings to a CSV File

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

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

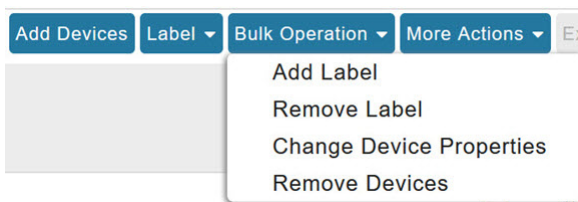
Removing Devices in Bulk

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

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

To remove devices in bulk:

1. Choose **Devices** > *Device Type*.
2. Choose **Bulk Operation** > **Remove Devices**.



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

 A screenshot of the 'Upload File' section of a web interface. It includes a label 'Upload File' and a close button 'x'. Below is a section for 'CSV/XML File:' with a text input field containing 'Devices to be removed ...' and a 'Browse' button. At the bottom of this section is a 'Remove' button. Below the 'Remove' button is a 'Status' label.

This is an example of the CSV format expected. In this case, the CSV file specifies three CGRs and one HER:

```
eid
cgr1000-CA-107
cgr1000-CA-108
cgr1000-CA-109
asr1000-CA-118
```

4. Click **Remove**.

The Status section of the Remove Devices window displays the status of the operation. The History section describes additional information about the operation. If there was any failure, click the corresponding link in the Failure# column to get more information about the error.

5. Click **Close** when done.

Changing Device Properties in Bulk

IoT FND lets you configure device properties in bulk using a CSV file. For example, this CSV file changes the latitude and longitude for the specified HER:

```
eid,lat,lng,ip,  
ASR1001+JAE15460070,42.0,-120.0
```

To configure device properties in bulk:

1. On any device page, choose **Bulk Operation > Change Device Properties**.
2. Click **Browse** to locate the CSV containing the list of devices and corresponding properties to configure, and then click **Open**.
3. Click **Change**.
4. Click **Close** when done.

Adding Labels in Bulk

You can group devices logically by assigning them labels. Labels are independent of device type, and devices of any type can belong to any label. A device can also have multiple labels. Unlike configuration groups and firmware groups, there are no policies or metadata associated with labels.

IoT FND lets you add labels in bulk using a CSV file. In the CSV file, specify the list of devices to be labeled.

To add device labels:

1. On any device page, choose **Bulk Operation > Add Label**.
2. Click **Browse** to locate the CSV file that contains the list of devices to label, and then click *Open*.

This is an example of the expected CSV format:

```
eid  
cgr1000-CA-107  
cgr1000-CA-108  
cgr1000-CA-109  
asr1000-CA-118
```

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

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

5. Click **Close** when done.

Removing Labels in Bulk

IoT FND lets you delete labels in bulk using a CSV file.

To delete device labels:

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

Configuring Rules

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

For example, whenever the status of a 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:

1. Choose **CONFIG > Rules**.

IoT FND displays the list of rules stored in its database. [Table 7](#) describes the fields displayed in the list.

Table 7 Rule Fields

Field	Description
Name	The name of the rule.
Active?	Whether the rule is active. Rules are not applied until you activate them.
Rule definition	<p>The syntax of the rule.</p> <p>For example, IoT FND executes this rule when a device battery 0 level drops below 50%:</p> <pre>battery0Level<50</pre>

Table 7 Rule Fields

Field	Description
Rule Actions	<p>The actions performed by the rule. For example:</p> <p>Log Event With: CA-Registered , Add Label: CA-Registered</p> <p>In this example, the actions:</p> <ul style="list-style-type: none">■ Set the eventMessage property of the Rule Event generated by this rule to CA-Registered.■ Add the label CA-Registered to the matching device.
Updated By	The username of user who last updated the rule.
Updated At	The date and time when the rule was last updated.

2. To edit a rule, click its name.

For information on how to edit rules, see [Creating a Rule](#).

Creating a Rule

To add a rule:

1. Choose **CONFIG > Rules**.
2. Click **Add**.
3. Enter a name for the rule.

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

4. To activate the rule, check the **Active** check box.
5. In the Construct Rule panel, enter the syntax of the rule.

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

Create Rule

Name:

☐ Active

Construct Rule

Actions

☐ Log event with:

Severity:

User-defined Event Name:

☐ Add Label:

☐ Remove Label:

☐ Show label status on Field Device page

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 (see [Searching By Event Name, page 197](#)).

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,
eventType=1045, eid=CGR1240/K9+JAF1603BBFF]
```

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

- **Add Label**—Enter the name of a new label or choose one from the **Add Label** drop-down menu.
- **Show label status on Field Devices page**—Shows the status of the device that triggered this rule in the LABELS section of the Browse Devices pane.
- **Remove Label**—Choose the label to remove from the **Remove Label** drop-down menu.

7. Click the **disk** icon to save changes.

Activating Rules

IoT FND only applies rules that you activate.

To activate a rule:

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

Deactivating Rules

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

To deactivate rules:

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

Deleting Rules

To delete rules:

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

Configuring Devices

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

- [Configuring Device Group Settings](#)
- [Editing the ROUTER Configuration Template](#)
- [Editing the ENDPOINT Configuration Template](#)
- [Pushing Configurations to Routers](#)
- [Pushing Configurations to Endpoints](#)

Configuring Device Group Settings

IoT FND uses groups to manage devices in bulk. When you add routers to IoT Field Network Director, IoT FND automatically adds them to the appropriate default ROUTER configuration groups, for example, **default-cgr1000** or **default-c800**. When you add MEs (meters and range extenders), IoT FND adds them to the default ENDPOINT configuration group, **default-cgmesh**. When you add IR500s, CG-NMS adds them to the default ENDPOINT configuration group, **default-ir500**.

- [Creating Device Groups](#)
- [Changing Device Configuration Properties](#)
- [Moving Devices to Another Group](#)
- [Listing Devices in a Configuration Group](#)
- [Configuring Periodic Inventory Notification and Mark-Down Time](#)
- [Renaming a Device Configuration Group](#)
- [Deleting Device Groups](#)

Creating Device Groups

By default, IoT FND defines the following device groups listed on the **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. <ul style="list-style-type: none"> ■ Individual RIVA electric devices listed under the Group heading display as <i>OW Riva CENTRON</i>.
Default-bact	By default, all Itron OpenWay RIVA G-W (Gas-Water) devices (ENDPOINT) are members of this group. <ul style="list-style-type: none"> ■ Individual RIVA water meters listed under the Group heading display as <i>OW Riva G-W</i>. ■ Individual RIVA gas meters listed under the Group heading display as <i>OW Riva G-W</i>.
Default-cam	By default, all Itron OpenWay RIVA CAM modules (ENDPOINT) are members of this group. <ul style="list-style-type: none"> ■ Individual RIVA CAM modules listed under the CAM heading display as <i>OW Riva CAM</i>.
Default-c800	By default, all C800s and ISRs (ROUTER) are members of this group.
Default-ir800	By default, all IR807s, IR809s, and IR829s (ROUTER) are members of this group.
Default-cgmesh	By default, all cgmesh endpoints (ENDPOINT) are members of this group.
Default-cgr1000	By default, all CGRs (ROUTER) are members of this group.
Default-sbr	By default, all ESRs (ROUTER) are members of this group. This product is also identified as C5921.
Default-ir500	By default, all IR500s (ENDPOINT) are members of this group.
Default-lorawan	By default all LoRaWAN Gateways (IOT GATEWAY) are members of this group.
default-c800	By default, all ISR 800s are members of this group.
default-ir500	By default, all IR500s are members of this group.

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

Note: You cannot delete the default groups, but you can change their names, although we do not recommend it. Also, the default ROUTER and ENDPOINT groups use the same icon, while custom groups use a different icon. See [Table 5](#) for icon definitions.

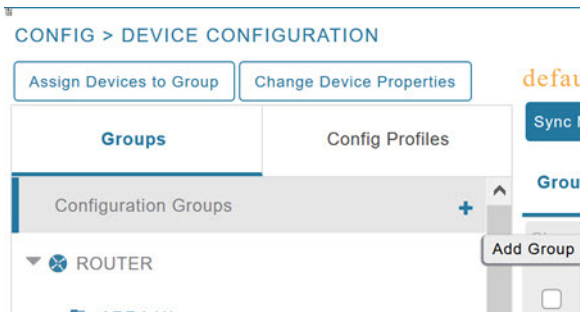
- [Creating ROUTER Groups](#)
- [Creating Endpoint Groups](#)

Creating ROUTER Groups

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

To create a ROUTER configuration group:

1. Choose **CONFIG > Device Configuration**.
2. Select the default Configuration Group: Default-cgr1000, Default-ir800 or **default-c800.**, Default-c800 or Default-sbr.
3. With the Groups tab selected (top, left pane of page), click the + icon (under the heading) to open the **Add Group** entry panel.



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.

5. Click **Add**.

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

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

Creating Endpoint Groups

To create an Endpoint configuration group:

1. Choose **CONFIG > Device Configuration**.
2. Select the default group (Default-act, Default-bact, Default-cam, Default-cgmesh, Default-ir500)
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.
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.

5. Click **Add**.

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

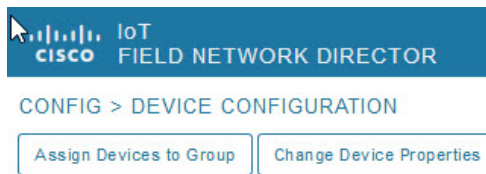
- To change the name of a group, see [Renaming a Device Configuration Group](#).
- To remove a group, see [Deleting Device Groups](#).

Changing Device Configuration Properties

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

To change device configuration properties:

1. Choose **CONFIG > Device Configuration**.
2. Click **Change Device Properties**.



3. Click **Browse** and select the Device Properties CSV or XML file to upload.
 4. Click **Change**.
 5. Click **Close** when done.
- For a list of configurable device properties in IoT FND, see [Device Properties](#).

Moving Devices to Another Group

There are two ways to move devices from one configuration group to another:

- [Moving Devices to Another Configuration Group Manually](#)
- [Moving Devices to Another Configuration Group in Bulk](#)

Moving Devices to Another Configuration Group Manually

To move devices to another configuration group:

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

2. Select a group from the list of configuration groups (left pane).
3. Select the check box of the devices to move.
4. Click **Change Configuration Group**.



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

Moving Devices to Another Configuration Group in Bulk

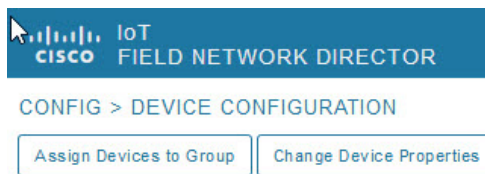
To move a large number of devices from one group to another, you can import a CSV file containing the list of the devices to move.

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:

1. Choose **CONFIG > Device Configuration**.
2. Click **Assign Devices to Group**.



3. Click **Browse** to locate the CSV or XML file containing the list of devices to move, and then click **Open**.
4. From the Group drop-down menu, choose the target group for the devices.
5. Click **Assign to Group**.
6. Click **OK**.

Listing Devices in a Configuration Group

To list the devices in a configuration group:

1. Choose **CONFIG > Device Configuration**.
2. Select a group from the list of configuration groups (left pane).
3. To get more information about a device in the list, click its EID (for example: CGR1240/K9+JAF1723AHGD).

Configuring Periodic Inventory Notification and Mark-Down Time

You can change the periodic inventory notification interval for a configuration group of routers without affecting the logic that IoT FND uses to mark those routers as **Down**. However, for this to happen, you must enable the periodic configuration notification frequency for the router group so that it is less than the mark-down timer.

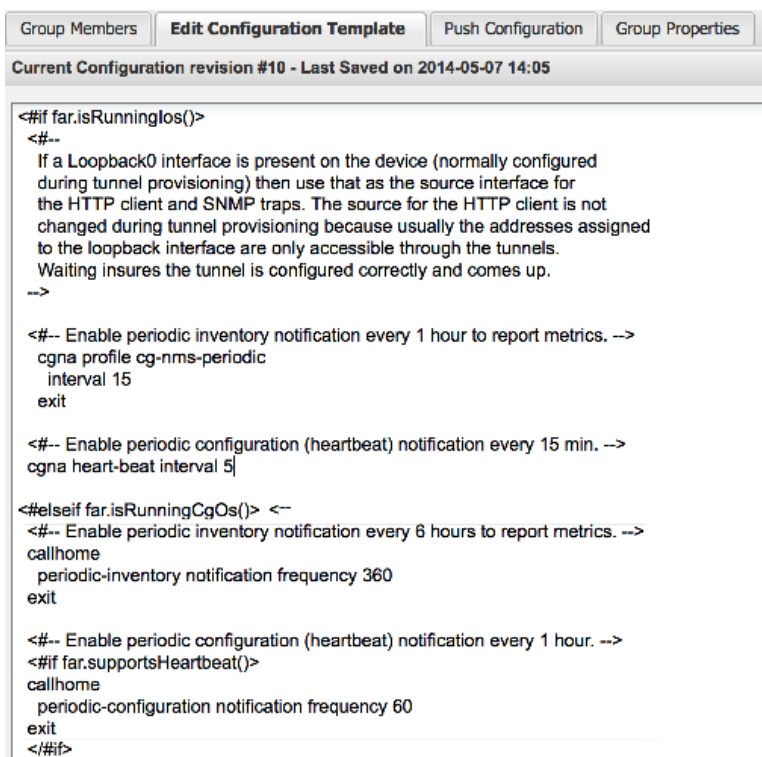
You can configure the mark-down timer by clicking the Group Properties tab for the group and modifying the value of the Mark Routers Down After field.

- [Configuring Periodic Inventory Notification](#)
- [Configuring the Mark-Down Timer](#)

Configuring Periodic Inventory Notification

To configure the periodic inventory notification interval for a ROUTER configuration group:

1. Click **CONFIG > Device Configuration**.
2. Select a ROUTER configuration group.
3. Click **Edit Configuration Template**.



4. This step is OS-specific:

- For Cisco IOS CGRs, change the value of the **cgna heart-beat interval** parameter. The time is in minutes.
For example, to enable periodic inventory notification to report metrics every 20 minutes for a Cisco IOS CGR, add these lines to the template:


```

<!-- Enable periodic configuration (heartbeat) notification every 20 min. -->
cgna heart-beat interval 20
exit

```
- For CG-OS CGRs, change the value of the **periodic-inventory notification frequency** parameter to the new value. The time unit is minutes.

5. Click disk icon to save changes.

Configuring the Mark-Down Timer

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

1. Click **CONFIG > Device Configuration**.
2. Select a ROUTER configuration group.
3. Click **Group Properties**.

CGOS-IOS

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

Mark Routers Down After (secs):	<input type="text" value="1800"/>
Number of Periodic Notifications between RPL Tree Polls:	<input type="text" value="2"/>
Maximum Time between RPL Tree Polls (minutes):	<input type="text" value="480"/>

- In the **Mark Routers Down After** field, enter the number of seconds after which IoT FND marks the routers as down if they do not send periodic configuration notifications (heartbeats) to IoT FND during that time.

Note: We recommend a 1:3 ratio of heartbeat interval to mark-down timer.

- Click the disk icon to save changes.
- Ensure that the periodic-configuration notification frequency in the configuration template is less than the value you entered the **Mark Routers Down After** field:
 - Click **Edit Configuration Template**.
 - Ensure that the value of the periodic-configuration notification frequency parameter is less than the **Mark Routers Down After** value.

Use a notification value that is at most one-third of the mark-down value. For example, if you choose a mark-down value of 3600 seconds (60 minutes), set the periodic-configuration notification frequency parameter to 20 minutes:

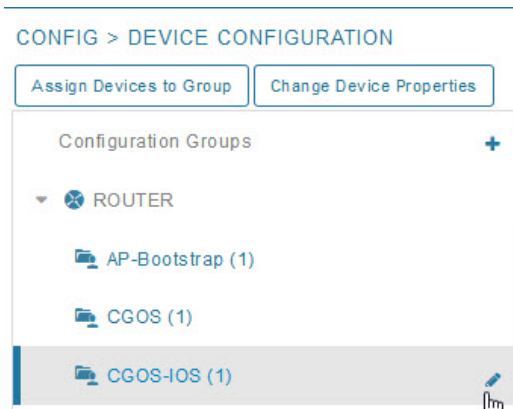
```
<!-- Enable periodic configuration (heartbeat) notification every 20 minutes. -->
<#if far.supportsHeartbeat()>
callhome
    periodic-configuration notification frequency 20
exit
</#if>
```

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

Renaming a Device Configuration Group

To rename a device configuration group:

- Choose **CONFIG > Device Configuration**.
- Select a group from the list of configuration groups (left pane).
- Hover over the name of the group in the list. A pencil icon appears.
- Click on the pencil icon to open the **Edit Group** panel.



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:

1. Choose **CONFIG > Device Configuration**.
2. Select a group from the list of configuration groups (left pane).
3. Ensure that the group is empty.
4. Click **Delete Group (-)**.

The Delete icon displays as a red minus sign when you hover over the name of the group in the list.

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

Synchronizing Endpoint Membership

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:

1. Choose **CONFIG > Device Configuration**.
2. Select an ENDPOINT group (left pane).
3. In the Group Members pane, click on the name of an endpoint.
4. Click **Sync Config Membership** button on the page that appears.
5. When prompted, click **Yes** to confirm synchronization.

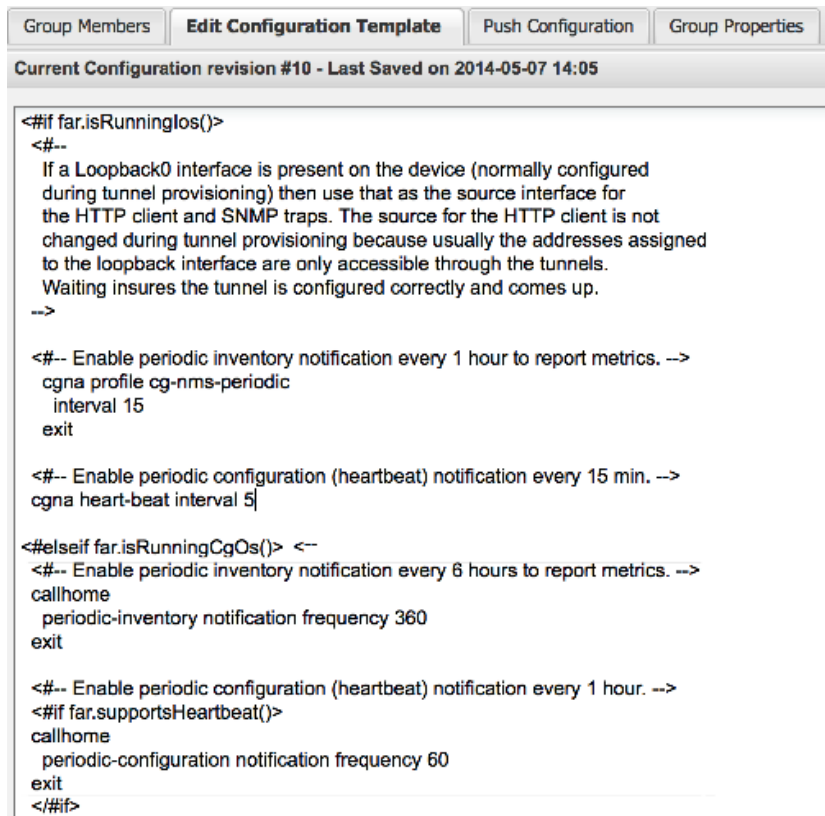
6. Click **OK**.

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:

1. Choose **CONFIG > Device Configuration**.
2. Under CONFIGURATION GROUPS (left pane), select the group with the template to edit.
3. Click **Edit Configuration Template**.



```
<#if far.isRunningIos()>
<!--
If a Loopback0 interface is present on the device (normally configured
during tunnel provisioning) then use that as the source interface for
the HTTP client and SNMP traps. The source for the HTTP client is not
changed during tunnel provisioning because usually the addresses assigned
to the loopback interface are only accessible through the tunnels.
Waiting insures the tunnel is configured correctly and comes up.
-->

<!-- Enable periodic inventory notification every 1 hour to report metrics. -->
cgna profile cg-nms-periodic
interval 15
exit

<!-- Enable periodic configuration (heartbeat) notification every 15 min. -->
cgna heart-beat interval 5

<#elseif far.isRunningCgOs() <--
<!-- Enable periodic inventory notification every 6 hours to report metrics. -->
callhome
periodic-inventory notification frequency 360
exit

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

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.

5. Click **Save Changes**.

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

Editing the AP Configuration Template

IoT FND lets you configure APs in bulk using a configuration template. When the AP registers with IoT FND, it pushes the configuration defined in the default template to devices and commits the changes to the startup configuration. IoT FND then retrieves the running configuration from the AP before changing the device status to **Up**.

To edit a AP group configuration template:

1. Choose **CONFIG > Device Configuration**.
2. Under CONFIGURATION GROUPS (left pane), select the C800 device group with embedded AP devices with the template to edit.
3. Click **Edit AP Configuration Template**.

<< Back **CGR1240/K9+JAF1623BNLD**

Ping Traceroute Refresh Metrics Reboot Refresh Router Mesh Key Create Work Order

Device Info Events Config Properties Running Config Mesh Routing Tree Mesh Link Traffic Router Files Raw Sockets **Guest OS**

Restart GOS

Name:	CGR1000_JAF1623BNLD-GOS-1
Status:	up
IP Address:	192.168.168.2
OS Version:	1.6.1.1
OS Family:	Linux
External IP Address:	unset
IOx Access Port:	8443

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.

5. Click **Save Changes.**

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

Enabling Dual PHY Support on IoT FND

You can configure CGR master and slave interfaces. For more information about configuring a dual-PHY WPAN interface, refer to [Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide \(Cisco IOS\)](#).

Configuring IoT FND for Dual-PHY

For Dual-PHY CGRs, you must configure all Dual-PHY WPAN modules—master and slaves—by setting the Dual-PHY WPAN Properties (see [Table 22](#)). The parameters to set in the appropriate device addition file are **masterWpanInterface** and **slaveWpanInterface**. For slave Dual-PHY WPAN devices, you must also set the **slave-mode** parameter.

EXAMPLE

The following instructs IoT FND which WPAN devices to allocate as the master interface and slave interface during the configuration push:

```
deviceType,eid,ip,meshPrefixConfig,meshPrefixLengthConfig,meshPanidConfig,meshAddressConfig,
dhcpV4LoopbackLink,dhcpV4TunnelLink,dhcpV6LoopbackLink,dhcpV6TunnelLink,tunnelSrcInterface1,
tunnelHerEid,adminUsername,adminPassword,certIssuerCommonName,ipsecTunnelDestAddr1,
masterWpanInterface,slaveWpanInterface,lat,lng
cgr1000,CGR1240/K9+JAF1741BFQS,2.2.56.253,2319:EXTRA:BEEF:CAFE::,64,1233,
2319:EXTRA:BEEF:CAFE::,20.211.0.1,20.211.0.1,2001:420:7bf:7e8::1,
2001:420:7bf:7e8::1,GigabitEthernet2/1,cg-isr900,cg-nms-administrator,
0ERIF+cKsLwyT0YTFd0k+NpVAAPxcIvFfoXlsogAXVkSOAczUFT8TG0U58ccJuhds52KXL4dtu5iljZsQNH+
pEQ1aIQvIGuIas9wp9MKUARYpNErXRIHEnpeH044Rfa4uSgsWXEyrVNxHyuvSefB5j6H0uA7tIQwEHDxOiq
/d0yxvfd4IYos7NzPXlJNiR+Cp6bwx7dG+d9Jo+JuNxLXpi8Fo5n88usjMoXPNbyrqvgn7SS4f+VYgXxliyDNP0k
+70EE8uSTVeUJXe7UXkndz5CaU17yk94UxOxamv2i1KEQxTFgw/UvrkCwPQoDMijPstDBXpFv8dqtA0xDGKuaRg
==,cenbursaca-cenbu-sub-ca,2.2.55.198,Wpan3/1,Wpan5/1,41.413324,-120.920315
```

The following is a typical template for configuring the master/slave interface on CGR WPAN modules:

```
interface ${device.masterWpanInterface}
  no shut
  ipv6 address ${device.meshAddressConfig}/${device.meshPrefixLengthConfig}
  ieee154 panid ${device.meshPanidConfig}
  outage-server ${device.relayDest}
exit

interface ${device.slaveWpanInterface}
  no ip address
ip broadcast-address 0.0.0.0
no ip route-cache
ieee154 beacon-async min-interval 10 max-interval 10 suppression-coefficient 0
ieee154 ssid cisco_muruga_dual
ieee154 txpower 21
slave-mode 3
rpl dag-lifetime 240
rpl dio-min 21
rpl version-incr-time 240
authentication host-mode multi-auth
authentication port-control auto
ipv6 dhcp relay destination global 2001:420:7BF:5F::705
dot1x pae authenticator
  ieee154 panid ${device.meshPanidConfig}
exit
```

```
end
```

Mesh Security Keys for Dual-PHY Devices

Note: Do not configure mesh security keys on slave WPAN devices.

With master/slave mode configured correctly in IoT FND, IoT FND automatically detects the master WPAN and sets its the mesh security keys. When configuring an existing CGR and adding another WPAN interface, remove all mesh security keys from both interfaces, and then configure master/slave mode through IoT FND. If CGRs are connected, all meters go through re-authentication.

You can remove mesh keys using the command:

```
mesh-security expire mesh-key interface wpan <slot>/<slot 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 wlan 4/1 rpl stable
```

```
----- WPAN RPL ROUTE SLOT TABLE [4] -----
```

Configuring Devices

```

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

```

Configuring Devices

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
nodes										// CY PLC
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 -->
```

Tip: Because GPS traps only generate Informational logs, we recommend that you create a rule-based event with high severity (such as CRITICAL) to inform the administrator of router movement. An example of this type of rule definition is: configGroup:name eventName:deviceLocChanged (see [Creating a Rule](#)).

Configuring SNMP v3 Informational Events

For Cisco IOS routers you configure SNMP v3 Informational Events to replace the default SNMP v3 traps. In CG-OS by default, SNMP v3 traps are configured for any IoT FND event-related changes that generate a trap on the router. IoT FND maps these traps to the corresponding event. For Cisco IOS routers, converting these SNMP v3 traps to SNMP v3 Informational Events sends an acknowledgment to the router for every event received from the router. The router then verifies that the trap was received by IoT FND. To enable SNMP v3 Informational Events, uncomment the following lines in the default configuration file and push the new configuration file to all router(s) in the group:

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



```
<!-- snmp-server user ${far.adminUsername} cgnms remote ${nms.host} v3 auth sha ${far.adminPassword}
priv aes 256 ${far.adminPassword} -->
<!-- snmp-server host ${nms.host} informs version 3 priv ${far.adminUsername} -->
```

Editing the ENDPOINT Configuration Template

To edit an ENDPOINT configuration template:

1. Choose **CONFIG > Device Configuration**.
2. Under CONFIGURATION GROUPS (left pane), select the **ENDPOINT group** with the template to edit.
3. Click **Edit Configuration Template**.
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

5. Click **Save Changes**.

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

Pushing Configurations to Routers

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

To push the configuration to routers:

1. Choose **CONFIG > Device Configuration**.
2. Select the group or subset of a group to push the configuration to in the CONFIGURATION GROUPS pane.
3. Click the **Push Configuration** tab to display that window.
4. In the **Select Operation** drop-down menu, choose **Push Router Configuration**.

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

5. In the Select Operation drop-down menu, choose **Push Endpoint Configuration**. Click **Start**.
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.

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

Enabling CGR SD Card Password Protection

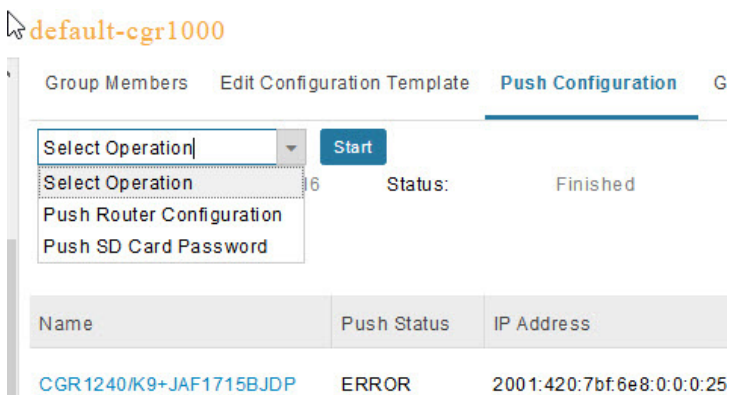
Password protection for the SD card in the CGR helps prevent unauthorized access and prevents transference of the CGR SD card to another system with a different password.

Note: This does not apply to C800s or IR800s.

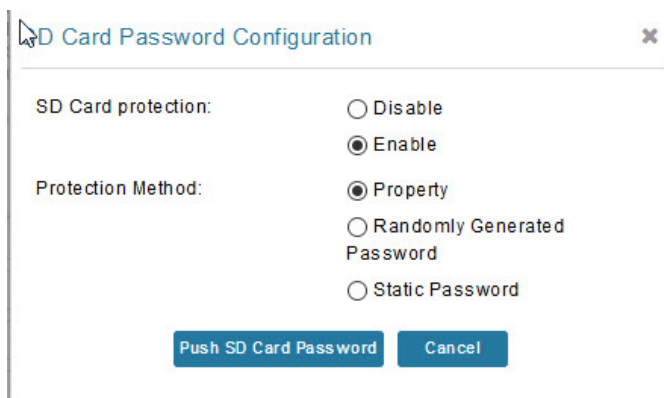
The Device Info pane displays CGR SD card password protection status in the Inventory section. The Config Properties tab displays the SD card password in the Router Credentials section.

To enable CGR SD card password protection:

1. Choose **CONFIG > Device Configuration**.
2. Select the CGR group or CGRs to push the configuration to in the Configuration Groups pane.
3. Select the **Push Configuration** tab.



4. In the **Select Operation** drop-down menu, choose **Push SD Card Password**.
5. Click **Start**. Click **Yes** to confirm action or **No** to stop action.
6. Select **SD Card protection > Enable**.



7. Select the desired protection method:
 - Property: This password is set using a CSV or XML file, or using the Notification Of Shipment file.
 - Randomly Generated Password: Enter the password length.
 - Static Password: Enter a password.
8. Click **Push SD Card Password**.

Pushing Configurations to Endpoints

To push configuration to mesh endpoints:

1. Choose **CONFIG > Device Configuration**.
2. Select the group or subset of a group to push the configuration to in the **ENDPOINT** list.
3. Click the **Push Configuration** tab.

Note: The Push Configuration tab supports a subnet view for cgmesh Endpoints that summarizes:

Pan ID	Identifies the Personal Area Network Identifier for a group of endpoints (nodes).
Subnet Prefix	Identifies the IPv6 subnet prefix for the endpoint.
Nodes in Group (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.

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

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

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” section on page -159](#)). The GOS, Hypervisor, and Cisco IOS all upgrade when you perform a Cisco IOS image bundle installation or update.

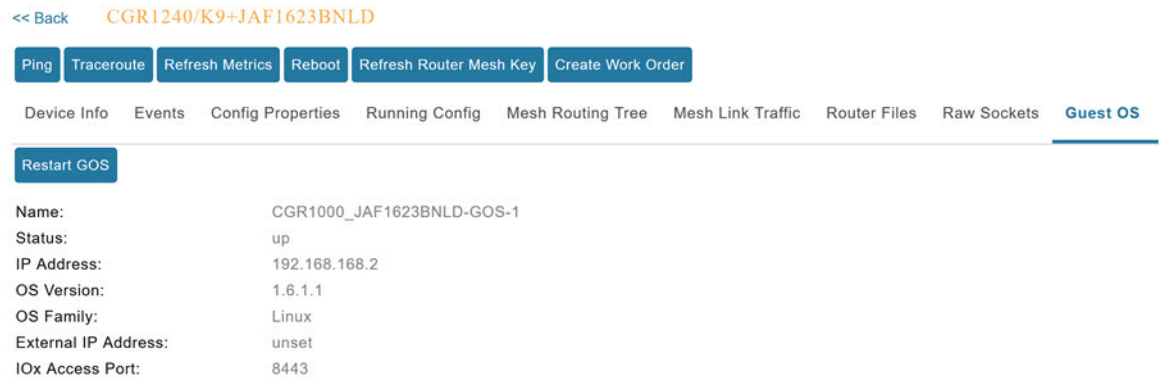
After any Cisco IOS install or upgrade, when IoT FND discovers a GOS, it checks if the initial communications setup is complete before it performs the required setup. The CGR must have a DHCP pool and Gigabit Ethernet 0/1 interface configured to provide an IP address and act as the gateway for the Guest 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 will populate a new **Guest OS** tab on the Device Info page for that particular router. From that page, we could also trigger a Guest-OS restart. Once the Guest-OS is restarted a pop-up with the status of the operation would be seen on the UI and messages would be 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 12 DEVICES > Field Devices Information Page Showing Guest OS tab and Restart GOS Button



This section includes the following topics:

- [Pushing GOS Configurations](#)

Pushing GOS Configurations

You can push the GOS configuration to the CGR using the IoT FND config template. This is the only way to configure the DHCP pool.

Managing Files

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

- [File Types and Attributes](#)
- [Adding a File to IoT FND](#)
- [Transferring Files](#)
- [Viewing Files](#)
- [Monitoring Files](#)
- [Monitoring Actions](#)
- [Deleting Files](#)

Note: File management is role-dependent and may not be available to all users. See [Managing Roles and Permissions](#).

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](#)). This feature works with all router OS versions currently supported by IoT FND.

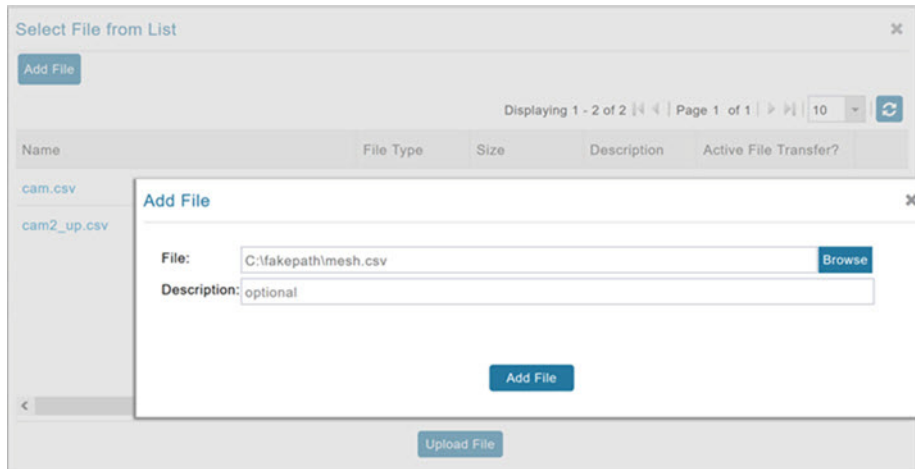
You can also transfer other file types to the router for better file management capability. You must first import the files to IoT FND to upload files to the router. IoT FND processes the file and stores it in the IoT FND database with the following attributes:

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

Adding a File to IoT FND

To add a file to IoT FND:

1. On the **CONFIG > Device File Management** page, click **Import Files** (far-left pane) or **Upload** (Actions tab) to open a Select File from List dialog box.
2. Click on the file you want to add (import) to FND.



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

Note: The maximum import file size is 200 MB.

4. (Optional) Type a description for the file.
5. Click **Add File**.

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

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

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 100KB).

To delete a file from IoT FND:

1. On the **CONFIG > Device File Management** page, select a file from the List dialog box (far-left panel).
2. At the Actions tab, click **Delete** button.
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:

1. On the **CONFIG > Device File Management** page, select the group to transfer the file to from the **Browse Devices** left pane.
2. Click **Import Files** or **Upload** on the **Actions** tab. The **Select File from List** dialog box displays.

3. Select the file to transfer to the routers in the selected group.
4. Click **Upload File**.

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

5. Check the check boxes of the routers to which you want to transfer the file.
6. Click **Upload**.

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

You can choose to transfer files to all 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 transferred from IoT FND reside on the router in flash:/managed/files/ for Cisco IOS CGRs, and bootflash:/managed/files/ for CG-OS CGRs.

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

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

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

1. Select **CONFIG > Device File Management**.
2. Click the EID link (such as CGR1240/K9+JAF1626BLDK) listed under the Name column to display the Device Info pane.
3. Click the **Router Files** tab.
4. Click the file name link to view the content in a new window.

Note: IoT FND only displays files saved as plain text that are under 100 KB. 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:

1. On the **CONFIG > Device File Management** page, within the **Browse Devices** pane, select the file that you want to delete.
2. On the **Actions** tab, click **Delete**.
3. In the **Delete file from List** dialog, select a file to delete.

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

4. Click **Delete File**.

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

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.

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 file deletion 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

Managing Work Orders

CGR1000, IR800, and IR500 routers support work orders. The IoT FND Work Order feature works with IoT-DM Release 3.0 or later.

For integration instructions, see [“Accessing Work Authorizations”](#) in the *Cisco Connected Grid Device Manager Installation and User Guide, Release 3.1*, or [“Managing Work Orders”](#) in the *Cisco Connected Grid Device Manager Installation and User Guide (Cisco IOS), Release 4.0 and 4.1* or *Cisco IoT Device Manager Installation and User Guide (Cisco IOS), Release 5.0*.

Note: For more details on actions supported by platform and minimum software releases required and configuration details, refer to following documents, respectively:

- [Release Notes for Cisco IoT Device Manager 5.4](#)
- [Cisco IoT Device Manager Installation and User Guide, Release 5.x](#)

Note: If you are using CGDM Release 3.1 and later, you must enable SSLv3 for IoT-DM-IoT FND connection authentication as follows:

1. Stop IoT FND:

```
service cgms stop
```

2. For IoT-DM Release 3.x and later, in the following files, replace **protocol="TLSv1"** attribute:

- /opt/cgms/standalone/configuration/standalone.xml
- /opt/cgms/standalone/configuration/standalone-cluster.xml

For CGDM 3.x

- Replace the attribute with: **protocol="TLSv1,SSLv3"**

For CGDM 4.x and IoT-DM 5.x

- Replace the attribute with: **protocol="TLSv1.x,SSLv3"**

3. Start IoT FND:

```
service cgms start
```

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

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

Before creating work orders, you must create user accounts in IoT FND for the field technicians who use IoT-DM to download work orders from IoT FND.

To create a Device Manager user account:

1. If not defined, create a Device Manager User role:
 - a. Choose **ADMIN > Access Management > Roles**.
 - b. Click **Add**.
 - c. (CG-OS only) In the Role Name field, enter a name for the role.
 - d. Check the check box for **Device Manager User**, and click the disk icon to save the changes.
2. Create the user account:
 - a. Choose **ADMIN > Access Management > Users**, and then click **+** to add a user.
 - b. Enter the user name, new password, confirm password and time zone information.
 - c. Select **Time Zone**.
 - d. Click **Assign Domain**. In the panel that appears, check the check boxes for **Monitor Only** and the Device Manager User role you created in Step 1.
 - e. Click **Assign**.

Creating Work Orders

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

CGR1000, IR800, and IR500 support work orders.

Before you can create a work order:

- Your user account must have the Work Order Management permissions enabled. See [Managing Roles and Permissions](#).
- To provide a signed work order to IoT-DM on request, you must import IoT-DM certificates to cgms_keystore using the alias cgms.
- Create the user account for the field technician.

To create a work order for an IR500:

1. In the **Browse Devices** panel under ENDPOINT, select GATEWAY-IR500.
2. In the **Inventory** view (right-pane):
 - a. Select the check box of the faulty GATEWAY-IR500.
 - b. From the drop-down menu options, select **More Actions > Create Work Order**.

The Operations > Work Orders page appears. IoT Field Network Director adds the names of the selected field device to the Field Device Names/EIDs field as a comma-separated list.

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

Viewing Work Orders

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

Table 8 lists the fields that display on the Work Orders page.

Table 8 Work Orders Page Fields

Field	Description
Work Order Number	Unique identifier of the work order.
Work Order Name	Name of the work order.
Role	(CG-OS only) Role of the user assigned to the work order: tech, admin, or viewer.
Device Type	EID of the system associated with the work order.
FAR Name/EID	Product name such as CGR1240 followed by EID.
Technician User Name	User name of the assigned technician.
Time Zone	The time zone where the router is located— <i>not</i> the user's time zone. This value is deployment dependent, and can match the user's time zone.
Start Date	Project start date allotted to the field technician.
End Date	Project start date allotted to the field technician.
Last Update	Time of last work order status update.
Status	Work order status. Valid status values are: New, Assigned, InService, Completed, Incomplete, or Expired.

Creating Work Orders

DETAILED STEPS

To create a work order for an existing Router (CGR1000) or Endpoint (GATEWAY-IR500) in the network:

1. At the **DEVICES > FIELD DEVICES** page, select the **ROUTER** or **ENDPOINT** heading within the Browse Devices panel.
2. Locate the device on the Inventory page (right panel) and select the box next to the Name of that device.
3. Select **More Actions > Create Work Order**.
4. At the **OPERATIONS > WORK ORDERS** page that appears, click **Add Work Order**.
5. In the **Work Order Name** field, enter the name of the work order.
6. In the **Field Device Names/EIDs** field, enter a comma-separated list of router names or EIDs.

For every router in the list, IoT FND creates a separate work order.

7. **Device Type** (Router or Endpoint) and **CGR OS** version (CG-OS or IOS) auto-populate.
8. Enter the IoT-DM system name in the **Device Username** field.

Select the **Technician User Name** for the IoT-DM from the drop-down menu. This menu only lists users with IoT-DM User permissions enabled.

9. From the **Status** drop-down menu, choose the status of the work order (**New**, **Assigned**, **In Service**, **Completed**, or **InComplete**). The **New** option auto-populates.

Note: For a IoT-DM user to retrieve a work order, the work order must be in the **Assigned** state in IoT FND for that user. If the work order is in any other state, IoT-DM cannot retrieve the signed work order.

Note: After the work order has been successfully requested by the IoT-DM user, the state of work order changes to **In Service**.

10. In the **Start Date** and **End Date** fields, specify the starting and ending dates for which the work order is valid.

If the work order is not valid, the technician cannot access the router.

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

12. To save your entries, click the disk icon. (To cancel your entries, click **x**.)

13. Click **OK**.

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

Downloading Work Orders

To download the work orders created by IoT FND, a field technician uses Cisco IoT-DM, which is a Windows-based application used to manage a single Cisco CGR 1000 router. The technician can download all work orders in the *Assigned* state.

Field technicians use IoT-DM to update work order status, which is sent to IoT FND.

Note: Certificates are not included in the work order and are preinstalled on the IoT-DM field laptop prior to downloading work orders from IoT FND.

For more information about IoT-DM, see the [Cisco IoT Device Manager User Guide](#) for Release 5.2.

Editing Work Orders

To edit work order details:

1. Choose **OPERATIONS > Work Orders**.
2. Click the box next to the work order you want to edit. Click **Edit Work Order**.

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

3. After editing the work order, click **Save**.

Deleting Work Orders

To delete work orders:

1. Choose **OPERATIONS > Work Orders**.
2. Check the check box of the work order(s) to delete.
3. Click **Delete Work Order**.
4. Click **Yes** to confirm or to cancel action click **No**.

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 9 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	

Demo Mode Configuration

FND Configuration Changes

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

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

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

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
```

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:

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
```

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
```

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
```

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 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:

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

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.

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:

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

The screenshot shows the Cisco Field Network Director (FND) web interface. The top navigation bar includes the Cisco logo, 'IoT FIELD NETWORK DIRECTOR', and tabs for 'DEVICES', 'OPERATIONS', 'CONFIG', and 'ADMIN'. The user is logged in as 'root (root)' with a time zone of 'US/Pacific'.

The main content area is titled 'ADMIN > SYSTEM MANAGEMENT > PROVISIONING SETTINGS'. It contains three main sections:

- Provisioning Process:**
 - IoT-FND URL:** A text input field containing 'https://nms.iot.cisco.com:9121'. Below it, a note states: 'Field Area Router uses this URL to register with IoT-FND after the tunnel is configured'.
- DHCPv6 Proxy Client:**
 - Server Address:** A text input field containing '2001:420:7bf:5f::703'. Below it, a note states: 'IPv6 address to send (or multicast) DHCPv6 messages to (can be multiple addresses, separated by commas)'.
 - Server Port:** A text input field containing '547'. Below it, a note states: 'Port to send (or multicast) DHCPv6 messages to'.
 - Client Listen Address:** A text input field containing '2001:420:7bf:5f::5525'. Below it, a note states: 'IPv6 address to bind to, for sending and receiving DHCPv6 messages (can be multiple addresses, separated by commas)'.
- DHCPv4 Proxy Client:**
 - Server Address:** A text input field containing '2.2.55.60'. Below it, a note states: 'IPv4 address to send (or broadcast) DHCPv4 messages to (can be multiple addresses, separated by commas)'.
 - Server Port:** A text input field containing '67'. Below it, a note states: 'Port to send (or broadcast) DHCPv4 messages to'.
 - Client Listen Address:** A text input field containing '2.2.55.25'. Below it, a note states: 'IPv4 address to bind to, for sending and receiving DHCPv4 messages (can be multiple addresses, separated by commas)'.

At the bottom of the form, there is a blue button with a save icon.

Device Properties

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

- [Types of Device Properties](#)
- [Device Properties by Category](#)

Types of Device Properties

IoT FND stores two types of device properties in its database:

- **Actual device properties**—These are the properties defined by the device, such as IP Address, Transmit Speed, and SSID.
- **IoT FND device properties**—These are properties defined by IoT FND for devices, such as Latitude and Longitude properties, which IoT FND uses to display device locations on its GIS map.

Note: The Key column provides the version of the property name in the IoT FND database that you can use in filters. For example, to search for the device with an IP address of 10.33.0.30, enter **ip:10.33.0.30** in the Search Devices field.

Device Properties by Category

This section presents IoT FND device properties by category:

- [Cellular Link Settings](#)
- [Cellular Link Metrics for CGRs](#)
- [DA Gateway Properties](#)
- [Dual PHY WPAN Properties](#)
- [Embedded Access Point \(AP\) Credentials](#)
- [Embedded AP Properties](#)
- [Ethernet Link Metrics](#)
- [Guest OS Properties](#)
- [Head-End Routers > Netconf Config](#)
- [Head-End Routers > Tunnel 1 Config](#)
- [Head-End Routers > Tunnel 2 Config](#)
- [Inventory](#)
- [Mesh Link Config](#)
- [Device Health](#)
- [Mesh Link Keys](#)
- [Link Settings](#)
- [Link Metrics](#)
- [NAT44 Metrics](#)
- [PLC Mesh Info](#)
- [Raw Sockets Metrics and Sessions](#)

Device Properties

- Router Battery
- Router Config
- Router Credentials
- Router DHCP Proxy Config
- Router Health
- Router Tunnel Config
- Router Tunnel 1 Config
- Router Tunnel 2 Config
- SCADA Metrics
- User-defined Properties
- WiFi Interface Config
- WiMAX Config
- WiMAX Link Metrics
- WiMAX Link Settings

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

Cellular Link Settings

Table 10 lists the fields in the Cellular Link area of the Device Detail page for all Cellular interfaces.

Note: Beginning with IoT FND 3.2, Cisco routers IR829, CGR1240, CGR1120, and Cisco 819 4G LTE ISRs (C819) support a new dual-active radio module that 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 Metrics		
Cellular Link Settings	Interface 0 and Interface 1	Interface 2 and Interface 3

Additionally, the 4G LTE dual-active radio module does not support or display all fields summarized in Table 10.

Table 10 Cellular Link Settings Fields

Field	Key	Configurable?	Description
Cellular Network Type	N/A	Yes	Defines the type of cellular network for example, GSM or CDMA.
Module Status	cellularStatus	No	Displays whether the cellular interface module is active in the network. There is also an unknown state for the module.
Network Name	–	Yes	Defines the service provider name, for example, AT&T or Verizon.
APN	cellularAPN	No	Displays the Access Point Name (APN) of the AP to which the cellular interface connects.
Cell ID	cellularID	No	Displays the cell ID for the cellular interface. This value must exist to activate the interface.
Cellular SID	cellularSID	No	Displays the System Identification Number for the CDMA cellular area.
Cellular NID	cellularNID	No	Displays the Network Identification Number for the CDMA cellular area.
Cellular Roaming Status	cellularRoamingStatus	No	Indicates whether the modem is in the Home network or Roaming.
Cellular Modem Serial Number	N/A	No	Displays the serial number of the connected modem.
Cellular Modem Firmware Version	cellularModemFirmwareVersion	No	Displays the version of the modem firmware on the module installed within the CGR.
Connection Type	connectionType	No	Displays the connection type as: <ul style="list-style-type: none"> ■ Packet switched ■ Circuit switched ■ LTE
Location Area Code	locationAreaCode	No	Displays the Location Area Code (LAC) given by the base station.
Routing Area Code	routingAreaCode	No	Displays the routing area code given by the base station.
APN	cellularAPN	No	Displays the Access Point Name (APN) of the AP to which the cellular interface connects.
Cellular Modem Firmware Version	cellularModemFirmwareVersion	No	Displays the version of the modem firmware on the Cellular module installed within the CGR.

Table 10 Cellular Link Settings Fields (continued)

Field	Key	Configurable?	Description
Connection Type	connectionType	No	Displays the connection type as: <ul style="list-style-type: none"> ■ Packet switched ■ Circuit switched
IMSI	cellularIMSI	No	The International Mobile Subscriber Identity (IMSI) identifies an individual network user as a 10-digit decimal value within a GSM and CDMA network. Possible values are: <ul style="list-style-type: none"> ■ 10-digit decimal value ■ Unknown
IMEI	cellularIMEI	No	Displays the International Mobile Equipment Identity (IMEI) for the cellular interface within a GSM network only. The IMEI value is a unique number for the cellular interface.

Cellular Link Metrics for CGRs

[Table 11](#) describes the fields in the Cellular Link Metrics area of the Device Info view.

Table 11 Cellular Link Metrics Area Fields

Field	Key	Description
Transmit Speed	cellularTxSpeed	Displays the current speed (bits/sec) of data transmitted by the cellular interface over the cellular uplink for a defined period (such as an hour).
Receive Speed	cellularRxSpeed	Displays the average speed (bits/sec) of data received by the cellular uplink network interface for a defined period (such as an hour).
RSSI	cellularRssi	Indicates the radio frequency (RF) signal strength of the cellular uplink. Valid values are 0 to -100. The LED states on the cellular interface and corresponding RSSI values are: <ul style="list-style-type: none"> ■ Off: RSSI < = -110 ■ Solid amber: -100 < RSSI <= -90 ■ Fast green blink: -90 < RSSI <= -75 ■ Slow green blink: -75 < RSSI <= -60 ■ Solid green: RSSI > -60
Bandwidth Usage (Current Billing Cycle)	CellBwPerCycle (bytes)	Displays current bandwidth usage (in bytes) of a particular route for the current billing cycle.

Table 11 Cellular Link Metrics Area Fields (continued)

Field	Key	Description
Cell Module Temperature	cellModuleTemp	Internal temperature of 3G module.
Cell ECIO	cellularEcio	Signal strength of CDMA at the individual sector level.
Cell Connect Time	cellConnectTime	Length of time that the current call lasted. This field only applies only to CDMA.

DA Gateway Properties

[DA Gateway Metrics Area Fields](#) describe the fields in the DA Gateway area of the Device Info view.

Table 12 DA Gateway Metrics Area Fields

Field	Key	Description
SSID	-	The mesh SSID.
PANID	-	The subnet PAN ID.
Transmit Power	-	The mesh transmit power.
Security Mode	-	Mesh Security mode: <ul style="list-style-type: none"> ■ 0 indicates no security mode set ■ 1 indicates 802.1x with 802.11i key management
Meter Certificate	meterCert	The subject name of the meter certificate.
Mesh Tone Map Forward Modulation	toneMapForwardModulation	Mesh tone map forward modulation: <ul style="list-style-type: none"> ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Tone Map Reverse Modulation	-	Mesh tone map reverse modulation: <ul style="list-style-type: none"> ■ 0 = Robo ■ 1 = DBPSK ■ 2 = DQPSK ■ 3 = D8PSK
Mesh Device Type	-	The primary function of the mesh device (for example, meter, range extender, or DA gateway).
Manufacturer of the Mesh Devices	-	Manufacturer of the mesh device as reported by the device.
Basic Mapping Rule End User IPv6 Prefix	-	End-user IPv6 address for basic rule mapping for the device.
Basic Mapping Rule End User IPv6 Prefix Length	-	Specified prefix length for the end-user IPv6 address.
Map-T IPv6 Address	-	IPv6 address for MAP-T settings.

Table 12 DA Gateway Metrics Area Fields (continued)

Field	Key	Description
Map-T IPv4 Address	-	IPv4 address for MAP-T settings.
Map-T PSID	-	MAP-T PSID.
Active Link Type	-	Link type of the physical link over which device communicates with other devices including IoT FND.

Dual PHY WPAN Properties

Table 13 describes the fields in the Dual PHY area of the Device Info view.

Table 13 Dual PHY Metrics Area Fields

Field	Key	Description
SSID	ssid	The mesh SSID.
PANID	panid	The subnet PAN ID.
Transmit Power	txpower	The mesh transmit power.
Security Mode	-	Mesh Security mode: <ul style="list-style-type: none"> 0 = No security mode set 1 = 802.1x with 802.11i key management
Meter Certificate	meterCert	The subject name of the meter certificate.
Mesh Tone Map Forward Modulation	toneMapForwardModulation	Mesh tone map forward modulation: <ul style="list-style-type: none"> 0 = Robo 1 = DBPSK 2 = DQPSK 3 = D8PSK
Mesh Tone Map Reverse Modulation	-	Mesh tone map reverse modulation: <ul style="list-style-type: none"> 0 = Robo 1 = DBPSK 2 = DQPSK 3 = D8PSK
Mesh Device Type	-	The primary function of the mesh device (for example, meter, range extender, or DA gateway).
Manufacturer of the Mesh Devices	-	Manufacturer of the mesh device as reported by the device.
Basic Mapping Rule End User IPv6 Prefix	-	End-user IPv6 address for basic rule mapping for the device.
Basic Mapping Rule End User IPv6 Prefix Length	-	Specified prefix length for the end-user IPv6 address.
Map-T IPv6 Address	-	IPv6 address for Map-T settings.

Table 13 Dual PHY Metrics Area Fields (continued)

Field	Key	Description
Map-T IPv4 Address	-	IPv4 address for Map-T settings.
Map-T PSID	-	MAP-T PSID.
Active Link Type	-	Link type of the physical link over which device communicates with other devices including IoT FND.

Embedded Access Point (AP) Credentials

[Table 14](#) describes the fields in the Embedded Access Point Credentials area of the Device Info view.

Table 14 Embedded Access Point Credentials Fields

Field	Key	Configurable?	Description
AP Admin Username	-	Yes	The user name used for access point authentication.
AP Admin Password	-	Yes	The password used for access point authentication.

Embedded AP Properties

[Table 15](#) describes the fields on the Embedded AP tab of the C800 or IR800 Device Info view.

Table 15 Embedded AP Properties

Field	Key	Description
Inventory	-	Summary of name, EID, domain, status, IP address, hostname, domain name, first heard, last heard, last property heard, last metric heard, model number, serial number, firmware version, and uptime details.
Wi-Fi Clients	-	Provides client MAC address, SSID, IPv4 address, IPv6 address, device type, state, name, and parent.
Dot11Radio 0 Traffic	-	Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps), and Rx speed (bps).
Dot11Radio 1 Traffic	-	Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps,) and Rx speed (bps).
Tunnel3	-	Provides admin status (up/down), operational status (up/down), Tx speed (bps), Tx drops (bps), and Rx speed (bps).
BVI1	-	Provides admin status (up/down), operational status (up/down), IP address, physical address, Tx speed (bps), Tx drops (bps) and Rx speed (bps).
GigabitEthernet0	-	Provides admin status (up/down), operational status (up/down), physical address, Tx speed (bps), Tx drops (bps), and Rx speed (bps).

Ethernet Link Metrics

Table 16 describes the fields in the Ethernet link traffic area of the Device Info view.

Table 16 Ethernet Link Metrics Area Fields

Field	Key	Description
Transmit Speed	ethernetTxSpeed	Indicates the average speed (bits/sec) of traffic transmitted on the Ethernet interface for a defined period of time.
Receive Speed	ethernetRxSpeed	Indicates the average speed (bits/sec) of traffic received on the Ethernet interface for a defined period of time.
Transmit Packet Drops	ethernetTxDrops	Indicates the number of packets dropped (drops/sec) when the transmit queue is full.

Guest OS Properties

Table 17 describes the fields in the Guest OS Properties area of the Config Properties page.

Table 17 Guest OS Properties Fields

Field	Key	Description
GOS Password	-	Password to access the GOS.
DHCPv4 Link for Guest OS Gateway	-	The DHCPv4 gateway address.
Guest OS IPv4 Subnet mask	-	The IPv4 subnet mask address.
Guest OS Gateway IPv6 Address	-	The IPv6 gateway address.
Guest OS IPv6 Subnet Prefix Length	-	The IPv6 subnet prefix length.

Head-End Routers > Netconf Config

Table 18 describes the fields in the Netconf Client area of the **Head-End Routers > Config Properties** page.

Table 18 Head-End Routers > Netconf Config Client Fields

Field	Key	Configurable?	Description
Netconf Username	netconfUsername	Yes	Identifies the username to enter when establishing a Netconf SSH session on the HER.
Netconf Password	netconfPassword	Yes	Identifies the password to enter when establishing a Netconf SSH session on the HER.

Head-End Routers > Tunnel 1 Config

Table 19 describes the fields in the Tunnel 1 Config area of the **Head-End Routers > Config Properties** page.

Table 19 Head-End Routers > Tunnel 1 Config Fields

Field	Key	Configurable?	Description
IPsec Tunnel Source 1	ipsecTunnelSrc1	Yes	Identifies the source interface or IP address of IPsec tunnel 1.

Table 19 Head-End Routers > Tunnel 1 Config Fields (continued)

Field	Key	Configurable?	Description
IPsec Tunnel Dest Addr 1	ipsecTunnelDestAddr1	Yes	Identifies the destination interface or IP address of IPsec tunnel 1.
GRE Tunnel Source 1	greTunnelSrc1	Yes	Identifies the source interface or IP address of GRE tunnel 1.
GRE Tunnel Dest Addr 1	greTunnelDestAddr1	Yes	Identifies the destination interface or IP address of GRE tunnel 1.

Head-End Routers > Tunnel 2 Config

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

Table 20 Head-End Routers > Tunnel 2 Config Device Fields

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

Inventory

[Table 21](#) describes the fields in the Inventory area of the Device Info page.

EXAMPLE PATH to Device Info page which summarizes the Inventory details: DEVICES> Field Devices > ROUTERS > CGR1000 > EID Name

Table 21 Inventory Fields

Field	Key	Configurable?	Description
Config Group	configGroup	Yes	The name of the configuration group to which the device belongs.
Device Category	deviceCategory	No	This field lists the type of device.
Device Type	deviceType	No	This field determines all other fields, as well as how the device communicates, and how it displays in IoT FND.
Domain Name	domainName	Yes	The domain name configured for this device.
EID	eid	No	The primary element ID of the device, which is used as the primary unique key for device queries.
Firmware Group	firmwareGroup	Yes	The name of the firmware group to which the device belongs.
Firmware Version	runningFirmwareVersion	No	The firmware version running on the device.
Hardware Version	vid	No	The hardware version of the device.
Hypervisor Version	hypervisor	No	(Cisco IOS CGRs running Guest OS only) The version of the Hypervisor.

Table 21 Inventory Fields (continued)

Field	Key	Configurable?	Description
Hostname	hostname	No	The hostname of the device
IP Address	ip	Yes	The IP address of the device. Use this address for the IoT FND connection through a tunnel.
Labels	label	Yes	Custom label assigned to the device. A device can have multiple labels. Labels are assigned through the UI or API, but not through a XML or CSV file.
Last Heard	lastHeard	No	The last date and time the device contacted IoT FND.
Last Metric Heard	N/A	No	The time of last polling (periodic notification).
Last Property Heard	N/A	No	The time of last property update for the router.
Last RPL Tree Update	N/A	No	The time of last RPL tree poll update (periodic notification).
Location	N/A	No	The latitude and longitude of the device.
Manufacturer	-	No	The manufacturer of the endpoint device.
Function	cgmesh	No	Function of the mesh device. Valid values are Range Extender and Meter.
Meter Certificate	meterCert	No	The global or unique certificate reported by the meter.
Meter ID	meterId	No	ME meter ID.
Model Number	pid	No	The product ID of the device.
Name	name	Yes	The unique name assigned to the device.
SD Card Password Lock	-	Yes	(CGRs only) The state of the SD card password lock (on/off).
Serial Number	sn	No	The serial number of the device.
Status	status	No	The device status.
Tunnel Group	tunnelGroup	Yes	The name of the tunnel group to which the device belongs.

Mesh Link Config

Table 22 describes the fields in the Mesh Link Config area of the **Routers > Config Properties** page.

Table 22 Mesh Link Config Fields

Field	Key	Configurable?	Description
Mesh Prefix Config	meshPrefixConfig	Yes	The subnet prefix address.
Mesh Prefix Length Config	meshPrefixLengthConfig	Yes	The subnet prefix address length.
Mesh PAN ID Config	meshPanidConfig	Yes	The subnet PAN ID.
Mesh Address Config	meshAddressConfig	Yes	The IP address of the mesh link.
Master WPAN Interface	masterWpanInterface	Yes	(Dual-PHY CGRs only) The interface on which the device is master.
Slave WPAN Interface	slaveWpanInterface	Yes	(Dual-PHY CGRs only) The interface on which the device is slave.

Device Health

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

Table 23 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. <i>Unknown</i> appears when the system is not connected to the network.

Mesh Link Keys

Table 24 describes the fields in the Mesh Link Keys area of the Device Info view.

Table 24 Mesh Link Keys Fields

Field	Key	Configurable?	Description
Key Refresh Time	meshKeyRefresh	No	The last date the mesh link keys were uploaded.
Key Expiration Time	meshKeyExpire	Yes	The date the mesh link keys expire.

Link Settings

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

Table 25 Link Settings Fields

Field	Key	Description
Firmware Version	meshFirmwareVersion	The Cisco Resilient Mesh Endpoint (RME) firmware version.
Mesh Interface Active	meshActive	The status of the RME.
Mesh SSID	meshSsid	The RME network ID.
PANID	meshPanid	The subnet PAN ID.
Transmit RF Power	meshTxPower	The RME transmission power (dBm).
Security Mode	meshSecMode	The RME security mode.
Transmit PLC TX Level	tx_level dBuV	The PLC level for Itron OpenWay RIVA CAM module and Itron OpenWay RIVA Electric devices (dBuV) <i>where u = micro</i>

Table 25 Link Settings Fields (continued)

Field	Key	Description
RPL DIO Min	meshRplDioMin	An unsigned integer used to configure the lmin of the DODAG Information Object (DIO) Trickle timer.
RPL DIO Double	meshRplDioDbI	An unsigned integer used to configure the lmax 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.

Link Metrics

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

Table 26 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	The meter ID.
PANID	meshPanid	The endpoint PANID.
Mesh Endpoints	meshEndpointCount	Number of RMEs.
Mesh Link Transmit Speed	meshTxSpeed	The current speed of data transmission over the uplink network interface (bits/sec) averaged over a short element-specific time period (for example, an hour).
Mesh Link Receive Speed	meshRxSpeed	The rate of data received by the uplink network interface (bits/sec) averaged over a short element-specific time period (for example, an hour).
Mesh Link Transmit Packet Drops	-	The number of data packets dropped in the uplink.
Route RPL Hops	meshHops	The number of hops that the element is from the root of its RPL routing tree.
Route RPL Link Cost	linkCost	The RPL cost value for the link between the element and its uplink neighbor.
Route RPL Path Cost	pathCost	The RPL path cost value between the element and the root of the routing tree.
Transmit PLC Level	tx_level dBuV	Supported on the PLC and the Itron OpenWay RIVA Electric devices and the Itron OpenWay RIVA G-W (Gas-Water) devices only (u within dBuV = micro)

NAT44 Metrics

Table 27 describes the fields in the NAT44 area of the Device Info page.

Table 27 NAT44 Metrics Fields

Field	Key	Description
NAT44 Internal Address	nat44InternalAddress0	The internal address of the NAT 44 configured device.
NAT 44 Internal Port	nat44InternalPort0	The internal port number of the NAT 44 configured device.
NAT 44 External Port	nat44ExternalPort0	The external port number of the NAT 44 configured device.

PLC Mesh Info

Table 28 describes the fields in the PLC Mesh Info area of the Device Info view.

Table 28 PLC Mesh Info Fields

Field	Key	Description
Mesh Tone Map Forward Modulation	toneMapForwardModulation	Mesh tone map forward modulation: <ul style="list-style-type: none"> 0 = Robo 1 = DBPSK 2 = DQPSK 3 = D8PSK
Mesh Tone Map Forward Map	toneMapForward	Indicates the number of usable subcarriers in the channel, shown as a binary octet (for example, 0011 1111). Ones indicate viable channels. The more ones on the map, the higher the channel capacity.
Mesh Tone Map Reverse Modulation	toneMapRevModulation	Mesh tone map reverse modulation: <ul style="list-style-type: none"> 0 = Robo 1 = DBPSK 2 = DQPSK 3 = D8PSK
Mesh Tone Map Reverse Map	toneMapReverse	Indicates the number of usable subcarriers in the channel, shown as a binary octet (for example, 0011 1111). Ones indicate viable channels. The more ones in the map, the higher the channel capacity. The reverse map information and RSSI combine to determine viable channels.
Mesh Absolute Phase of Power	-	Mesh absolute phase of power is the relative position of current and voltage waveforms for a PLC node.
LMAC Version	-	Version of LMAC firmware in use by the PLC module DSP processor, which provides lower media access functionality for PLC communications compliant with the IEEE P1901.2 PHY standard.

Raw Sockets Metrics and Sessions

Table 29 describes the fields in the TCP Raw Sockets area of the **Field Devices > Config Properties** page.

Table 29 Raw Sockets Metrics and Sessions View

Field	Key	Description
Metrics		
Tx Speed (bps)	rawSocketTxSpeedS[portNo]	The transmit speed of packetized streams of serial data in bits per second.
Rx Speed (bps)	rawSocketRxSpeedS[portNo]	The receive speed of packetized streams of serial data in bits per second.
Tx Speed (fps)	rawSocketTxFramesS[portNo]	The transmit speed of packetized streams of serial data in frames per second.
Rx Speed (fps)	rawSocketRxFramesS[portNo]	The receive speed of packetized streams of serial data in frames per second.
Sessions		
Interface Name	-	The name of the serial interface configured for Raw Socket encapsulation.
TTY	-	The asynchronous serial line on the router associated with the serial interface.
VRF Name	-	Virtual Routing and Forwarding instance name.
Socket	-	The number identifying one of 32 connections.
Socket Mode	-	Client or server. The mode in which the asynchronous line interface is set up.
Local IP Address	-	The IP address that either the server listens for connections on (in Server Socket Mode), or to which the client binds to initiate connections to the server (in Client Socket Mode).
Local Port	-	The port that either the server listens to for connections (in Server Socket Mode), or to which the client binds to initiate connections to the server (in Client Socket Mode).
Dest. IP Address	-	The destination IP address of the remote TCP Raw Socket server.
Dest. Port	-	Destination port number to use for the connection to the remote server.
Up Time	-	The length of time that the connection has been up.
Idle Time	-	The length of time that no packets were sent.
Time Out	-	The currently configured session idle timeout, in minutes.

Router Battery

Table 30 describes the fields in the Router Battery (Battery Backup Unit (BBU) area of the Device Info page.

Table 30 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.

Table 30 Router Battery Device View (continued)

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

Router Config

[Table 31](#) describes the fields in the Router Config area of the **Field Devices > Config Properties** page.

Table 31 Router Config Device View

Field	Key	Configurable?	Description
Use GPS Location	useGPSLocationConfig	Yes	The internal GPS module provides the router location (longitude and latitude).

Router Credentials

[Table 32](#) describes the fields in the Router Credentials area of the **Field Devices > Config Properties** page.

Table 32 Router Credentials Fields

Field	Key	Configurable?	Description
Administrator Username	-	Yes	The user name used for root authentication.
Administrator Password	-	Yes	The password used for root authentication.
Master key	-	Yes	The master key used for device authentication.
SD Card Password	-	No	SD card password protection status.
Token Encryption Key	-	Yes	The token encryption key.
CGR Username	-	Yes	The username set for the CGR.
CGR Password	-	Yes	The password set on the CGR for the associated username.

Router DHCP Info

[Table 33](#) describes the fields in the DHCP Info area of the Device Info page.

Table 33 Router DHCP Fields

Field	Key	Description
DHCP Unique ID (DUID)	-	A DHCP DUID in hex string format (for example, 0xHHHH).

Router DHCP Proxy Config

[Table 34](#) describes the fields in the DHCP Proxy Config area of the **Field Devices > Config Properties** page.

Table 34 DHCP Proxy Config Fields

Field	Key	Configurable?	Description
DHCPv4 Link for Loopback Interfaces	dhcpV4LoopbackLink	Yes	Refers to the IPv4 link address to use within DHCP DISCOVER messages when requesting a lease for loopback interfaces.
DHCPv4 Link for Tunnel Interfaces	dhcpV4TunnelLink	Yes	Refers to the IPv4 link address to use within DHCP DISCOVER messages when requesting a lease for tunnel interfaces.
DHCPv6 Link for Loopback Interfaces	dhcpV6LoopbackLink	Yes	The IPv6 link address to use in DHCPv6 Relay-forward messages when requesting a lease for loopback interfaces.
DHCPv6 Link for Tunnel Interfaces	dhcpV6TunnelLink	Yes	The IPv6 link address to use in DHCPv6 Relay-forward messages when requesting a lease for tunnel interfaces.

Router Health

[Table 35](#) describes the Router Health fields in the Device Info view.

Table 35 Router Health Device View

Field	Key	Configurable?	Description
Uptime	uptime	No	Indicates the length of time (in seconds) that the router has been up and operating since its last reset.
Door Status	doorStatus	No	Options for this field are: <ul style="list-style-type: none"> ■ “Open” when the door of the router is open ■ “Closed” after the door is closed
Chassis Temperature	chassisTemp	No	Displays the operating temperature of the router. You can configure alerts to indicate when the operating temperature falls outside of the customer-defined temperature range.

Router Tunnel Config

[Table 36](#) describes the fields in the Router Tunnel Config area of the **Field Devices > Config Properties** page.

Table 36 Router Tunnel Config Device View

Field	Key	Configurable?	Description
Tunnel Config	tunnelHerEid	Yes	Displays the EID number of the HER that the router connects with through secure tunnels.
Common Name of Certificate Issuer		No	Displays the name of the certificate issuer.
NMBA NHS IPv4 Address		Yes	Displays the Non-Broadcast Multiple Access (NBMA) IPv4 address.
NMBA NHS IPv6 Address		Yes	Displays the NBMA IPv6 address.
Use FlexVPN Tunnels		Yes	Displays the FlexVPN tunnel setting.

Router Tunnel 1 Config

[Table 37](#) describes the fields in the Router Tunnel 1 Config area of the **Field Devices > Config Properties** page.

Table 37 Router Tunnel 1 Config Device View

Field	Key	Configurable?	Description
Tunnel Source Interface 1	tunnelSrcInterface1	Yes	Defines the interface over which the first tunnel is built to provide WAN redundancy.
OSPF Area 1	ospfArea1	Yes	Defines the OSPFv2 Area 1 in which the router (running IPv4) is a member.
OSPFv3 Area 1	ospfv3Area1	Yes	Defines OSPFv3 Area 1 in which the router (running IPv6) is a member.
OSPF Area 2	ospfArea1	Yes	Defines the OSPFv2 Area 2 in which the router (running IPv4) is a member.
OSPFv3 Area 2	ospfv3Area1	Yes	Defines OSPFv3 Area 2 in which the router (running IPv6) is a member.
IPsec Dest Addr 1	ipsecTunnelDestAddr1	Yes	Defines the destination IP address for IPsec tunnel 1.
GRE Dest Addr 1	greTunnelDestAddr1	Yes	Defines the destination IP address for GRE tunnel 1.

Router Tunnel 2 Config

[Table 38](#) describes the fields in the Router Tunnel 2 Config area of the **Field Devices > Config Properties** page.

Table 38 Router Tunnel 2 Config Device View

Field	Key	Configurable?	Description
Tunnel Source Interface 2	tunne2SrcInterface1	Yes	Defines the interface over which the second tunnel is built to provide WAN redundancy.
OSPF Area 2	ospfArea2	Yes	Defines the OSPFv2 Area 2 in which the router (running IPv4) is a member.
OSPFv3 Area 2	ospfv3Area2	Yes	Defines OSPFv3 Area 2 in which the router (running IPv6) is a member.
IPsec Dest Addr 2	ipsecTunnelDestAddr2	Yes	Defines the destination IP address for IPsec tunnel 2.
GRE Dest Addr 2	greTunnelDestAddr2	Yes	Defines the destination IP address for GRE tunnel 2.

SCADA Metrics

Table 39 describes the fields on the SCADA tab of the Device Info page.

Table 39 SCADA Metrics View

Field	Key	Configurable?	Description
Channel Name	channel_name	No	Identifies the channel on which the serial port of the router communicates to the RTU.
Protocol Type	protocol	No	Identifies the Protocol Translation type.
Messages Sent	-	No	The number of messages sent by the router.
Messages Received	-	No	The number of messages received by the router.
Timeouts	-	No	Displays the timeout value for connection establishment.
Aborts	-	No	Displays the number of aborted connection attempts.
Rejections	-	No	Displays the number of connection attempts rejected by IoT FND.
Protocol Errors	-	No	Displays the number of protocol errors generated by the router.
Link Errors	-	No	Displays the number of link errors generated by the router.
Address Errors	-	No	Displays the number of address errors generated by the router.
Local IP	-	No	Displays the local IP address of the router.
Local Port	-	No	Displays the local port of the router.
Remote IP	-	No	Displays the remote IP address of the router.
Data Socket	-	No	Displays the Raw Socket server configured for the router.

User-defined Properties

The User-defined Properties area of the Routers > Config Properties page displays any customer defined properties.

WiFi Interface Config

Table 40 describes the fields in the WiFi Interface Config area of the **Field Devices > Config Properties** page.

Table 40 WiFi Interface Config Fields

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

WiMAX Config

Table 41 describes 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 41 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 42 describes the fields in the WiMAX Link Health area of the Device Info page.

Table 42 WiMAX Link Health Fields

Field	Key	Description
Transmit Speed	wimaxTxSpeed	The current speed of data transmission over the WiMAX uplink network interface, measured in bits per second, averaged over a short element-specific time period (for example, an hour).
Receive Speed	wimaxRxSpeed	The rate of data that has been received by the WiMAX uplink network interface, measured in bits per second, averaged over a short element-specific time period (for example, an hour).
RSSI	wimaxRssi	The measured RSSI value of the WiMAX RF uplink (dBm).
CINR	wimaxCinr	The measured CINR value of the WiMAX RF uplink (dB).

WiMAX Link Settings

Table 43 describes the fields in the WiMAX Link Settings area of the Device Info page.

Table 43 WiMAX Link Settings Fields

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



Managing Firmware Upgrades

This section describes managing firmware upgrade settings in IoT FND, and includes the following sections:

- [Router Firmware Updates](#)
- [Image Diff Files for IR809 and IR829](#)
- [Gateway Firmware Updates](#)
- [Configuring Firmware Group Settings](#)
- [Working with Router Firmware Images](#)
- [Performing CG-OS to Cisco IOS Migrations](#)
- [Working with Resilient Mesh Endpoint Firmware Images](#)

Use IoT FND to upgrade the firmware running on routers (CGR1000s, C800s, IR800s), AP800s and Cisco Resilient Mesh Endpoints (RMEs) such as meters and range extenders. IoT FND stores the firmware binaries in its database for later transfer to routers in a firmware group through an IoT FND and IoT-DM file transfer, and to RMEs using IoT FND.

Cisco provides the firmware bundles as a zip file. For Cisco IOS, software bundles include hypervisor, system image and IOx images (for example, Guest-OS, Host-OS).

For Cisco CG-OS, IoT FND automatically unzips the kickstart and system images included in the bundle. 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:

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](#)

Because of their large size, firmware-image uploads to routers take approximately 30 minutes, depending on interface speeds.

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* cгна 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](#)). 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](#)).

See the [Cisco 1000 Series Connected Grid Routers Configuration Guides](#) documentation page 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, page 167](#).

Changing Action Expiration Timer

You can use the `cgms_preferences.sh` script to set or retrieve the action expiration timer value in the IoT FND database:

```
/opt/cgms
/bin/cgms_preferences setCgrActionExpirationTimeout 50
```

Valid options are:

- `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).
- `setCgrActionExpirationTimeout <value>`
- `get<pkg>actionExpirationTimeoutMins`
- `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/cgms_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

```

Resilient Mesh Endpoint Firmware Update

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.

Mesh Firmware Migration (CG-OS CG4 platforms only)

Note: Mesh Firmware Migration to Cisco Resilient Mesh is not supported for CGRs running CG-OS version CG4(4).

IoT FND allows you to update earlier versions of CGR firmware to allow Cisco Resilient Mesh networking using the following IoT FND North Bound APIs:

- findEidByIpAddress
- startReprovisionByEidList
- startReprovisionByEidListAbridged
- startReprovisionByGroup
- startReprovisionByGroupAbridged

See the [North Bound API User Guide for the Cisco IoT Field Network Director, Releases 3.x and 4.x](#) for usage information.

Image Diff Files for IR809 and IR829

To reduce 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.

At the Images tab on that page, expand the Gateway icon and click on IC3000 to see a list of available IC3000 images.

Configuring Firmware Group Settings

This section describes how to add, delete, and configure firmware groups, and includes the following topics:

- [Adding Firmware Groups](#)
- [Assigning Devices to a Firmware Group](#)
- [Renaming a Firmware Group](#)
- [Deleting Firmware Groups](#)

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.

Note: When creating firmware groups note the guidelines:

- CGRs, IR800s, and C800s can coexist on a network; however, for firmware management, they cannot belong to the same firmware group.
- IR500s and other RMEs devices can coexist on a network; however, for firmware management, they cannot belong to the same group.

The Groups tab on the **CONFIG > Firmware Update** page displays various device metrics.

IoT FND displays this information about the image on the routers in the selected firmware group:

Field	Description
Selected Firmware Image	The name of the current image zip archive or the image being uploaded to group members.
Current Action	The name of the firmware action being performed.

Field	Description
Current Status	<p>The status of the image uploading. Possible statuses are:</p> <ul style="list-style-type: none">■ Image Loading, Upload Paused, Upload Stopped, Upload Finished, Upload Stopping, Upload Pausing■ Scheduling Reload, Reload Paused, Reload Stopped, Reload Scheduling Finished, Reload Stopping, Reload Pausing■ Setting Backup, Backup Paused, Backup Stopped, Backup Finished, Backup Stopping, Backup Pausing
Written/Devices	<p>Specifies how many devices received or installed the image out of the total number of devices in the group.</p> <p>For example, 1/3 means that one device received the firmware image out of 3 devices in the group.</p>
Error/Devices	<p>Specifies how many devices failed to receive or install the image out of the total number of devices in the group. For example, 2/3 means that two out of the three devices in the group failed to install the image.</p> <p>Tip: Click the Error/Devices link (1 in Figure 1) to view the devices that are in the errored state.</p>

For every router in the group, IoT FND displays this information:

Field	Description
Status	Device status of the (for example, Up, Down, or Unheard).
Name	EID of the device.
IP Address	IP address of the device.
Firmware Version	Version of the firmware image installed on the device.
Activity	Device activity.
Update Progress	Firmware image updating progress. A progress of 100% indicates that the image uploading is complete.
Last Firmware Status Heard	The last time the firmware status was heard.
Error Message	Error message if image upload failed.
Error Details	Displays error details for the selected device.

Tip: At the Firmware Update page, click the Error/Devices link (not shown) in [Figure 1](#) to apply a filter. Click the **Clear Filter** to revert to an unfiltered view of the selected device group.

Figure 1 Firmware Update Page – Viewing Errored Devices

IOS

Firmware Upgrade Migration To IOS

Selected Firmware Image: cgr1000-universalk9-bundle.SSA.156-3.0.64.GB (IOS-CGR)
 Current Action: Install Image
 Current Status: Finished
 Written/Devices: 0/1
 Error/Devices: 0/1

Displaying 1 - 1 | Page 1 | 200

IP Address	Firmware Version	Activity	Update Progress	Last Firmware Status Heard	Error Message	Error Details
172.27.88.248	5.2(1)CG4(3)	Unknown	0%	2017-01-22 16:35		

Adding Firmware Groups

To add a firmware group:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.

CONFIG > FIRMWARE UPDATE

default-cgmesh

Firmware Management | **Devices** | **Logs** | **Transmission Settings**

Groups | **Images**

Firmware Groups

- ROUTER
 - 001Q (1)
 - C800-test (2)
 - CGOS4-5 (1)

Add Group

Name:
 Device Category:

3. In the **Groups** pane, select one of the following: **Default-cgr1000**, **Default-c800**, **Default-ir500**, **Default-ir800**, **Default-cgmesh** or **Default-sbr**.
4. Click **+** next to Firmware Groups heading in the Groups pane to Add Group.
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.
6. Click **Add**.

The new group label appears under the corresponding device type in the Firmware Groups pane.

To assign devices to the new group, see [Assigning Devices to a Firmware Group](#).

Assigning Devices to a Firmware Group

This section describes moving devices, and includes the following topics:

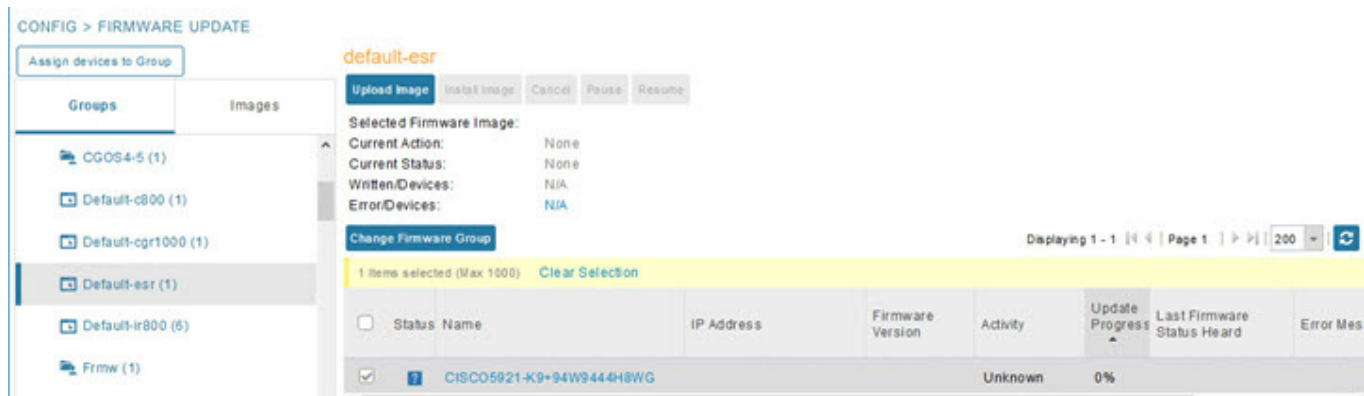
- [Moving Devices to Another Group Manually](#)
- [Moving Devices to Another Group In Bulk](#)

Moving Devices to Another Group Manually

To manually move devices to a group:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.
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.



4. Check the check boxes of the devices that you want to move.
5. Click **Change Firmware Group**. to open a pop up window.
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.
7. Click **Change Firmware Group**.
8. Click **Close**.

Moving Devices to Another Group In Bulk

To move devices from one group to another in bulk:

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

EID only for mesh endpoints:

```
eid
00078108003c1e07
00078108003C210b
```

EID only for IR800s

```
eid
ir800
```

EID only for ISR 800s:

```
eid
C819HGW-S-A-K9+FTX174685V0
C819HGW-S-A-K9+FTX174686V0
C819HGW-S-A-K9+FTX174687V0
```

EID only for IR500s:

```
eid
da1
da2
da3
```

EID only for IC3000

```
eid
IC3000+FOC2219Y47Z
```

Note: Each file can only list one device type.

2. Choose **CONFIG > Firmware Update**.
3. Click the **Groups** tab.
4. Click **Assign devices to Firmware Group** button (found above Groups tab).
5. In the window that appears, click **Browse** and locate the device list CSV or XML file.
6. From the **Group** drop-down menu, choose the destination group.
7. Click **Assign to Group**.

IoT FND moves the devices listed in the file from their current group to the destination group.

8. Click **Close**.

Renaming a Firmware Group

To rename a firmware group:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.
3. In the Firmware Groups pane, select the firmware group to rename.
4. Move the cursor over the group and click the **Edit Group Name** pencil icon.



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:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.
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.
4. Check the box next to the firmware group that you want to delete.
5. Click **Clear Selection** that appears above the entry (yellow bar).
6. To confirm deletion, click **Yes**.
7. Click **OK**.

Working with Router Firmware Images

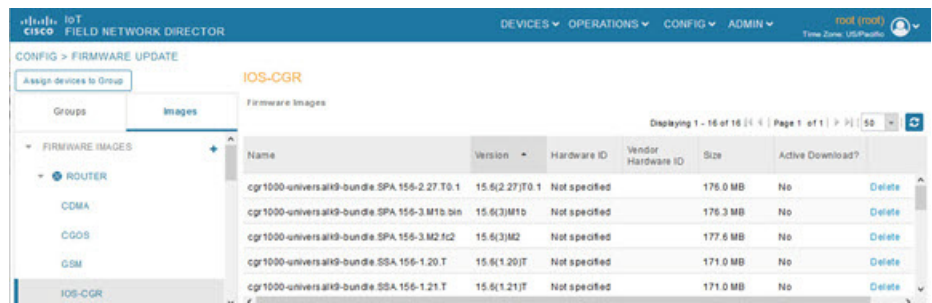
This section describes how to add router firmware images to IoT FND and how to upload and install the images on routers, and includes the following topics:

- [Viewing Firmware Image Files in IoT FND](#)
- [Adding a Firmware Image to IoT FND](#)
- [Uploading a Firmware Image to a Router Group](#)
- [Canceling Router Firmware Image Upload](#)
- [Pausing and Resuming Router Firmware Image Uploads](#)
- [Installing a Firmware Image](#)
- [Stopping Firmware Image Installation](#)
- [Pausing and Resuming Router Firmware Image Installation](#)

Viewing Firmware Image Files in IoT FND

You can display firmware image information from the **Images** pane in the **CONFIG > Firmware Update** page. Select ROUTER or ENDPOINT to display all firmware images for those devices in the IoT FND database. Select the firmware image type to refine the display (see [Figure 2](#)).

Figure 2 CONFIG > Firmware Update Images Pane



For every image in the list, IoT FND provides this information:

Field	Description
Name	The filename of the firmware image bundle.
Version	The version of the firmware bundle. Click the arrowhead icon to switch between ascending and descending listing of the firmware version.
Hardware ID	The hardware family to which you can download this image.
Size	The size of the firmware bundle.
Active Download?	The active firmware using the firmware image.

Adding a Firmware Image to IoT FND

Before you can upload and install a firmware image on a device, add the image file (as a zip archive) to IoT FND. IoT FND stores the image in its database.

Note: Do not unzip the image file. IoT FND unzips the file.

To add a firmware image to IoT FND:

- 1. Choose **CONFIG > Firmware Update**.
- 2. Click the **Images** tab (Figure 2).
- 3. In the Images pane, select **ROUTER**, **ENDPOINT** or **GATEWAY**, and the type of device group.
- 4. Click the + icon to select an image found to the right of the Firmware Images heading.
- 5. Click **Browse** to locate the firmware image. Select the image, then click **Add File**.
- 6. Click **Upload**.

The image appears in the Firmware Images panel (Figure 2).

- To delete an image, click **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](#).

Uploading a Firmware Image to a Router Group

When you upload a firmware image to router firmware group members, IoT FND pushes the image to the group members in the background and tracks the upload progress to ensure that the devices receive the image.

On routers, firmware image upload and installation requires 200 MB of free disk space. IoT FND stores image files in the `.../managed/images` directory on the router.

Note: If there is not enough disk space on the router for the firmware image, the IoT FND initiates disk cleanup process on the router and removes the following files, sequentially, until there is enough disk space to upload the new image:

- Unused files in the `.../managed/images` directory that are not currently running or referenced in the `before-tunnel-config`, `before-registration-config`, `express-setup-config`, and `factory-config` files for IOS CGRs; `golden-config`, `ps-start-config`, `express-setup-config`, or `factory-config` for CG-OS CGRs
- Unused `.gbin` and `.bin` files from the bootflash directory in CG-OS CGRs

If there is still not enough space, you must manually delete unused files on the router.

To upload a firmware image to router group members:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.
3. In the Groups pane, select the router firmware group that you want to update.

Note: CGR groups can include devices running Cisco IOS and CG-OS. Therefore, Cisco IOS software images only upload to devices running Cisco IOS (C5921s, IR800s, ISR800s, CGR1000s); only CGRs accept CG-OS images.

IoT FND displays the firmware image type applicable to the router:

Image	Type	Applicable Device
ACTD-CGR	cgr1000	Cisco IOS CGRs running Guest OS
CDMA	all	Cisco IOS CGRs, IR800s, and ISR800s
CGOS	cgr1000	Cisco IOS CGRs running Guest OS
ENDPOINT	IR500	Cisco IR500
GSM	all	Cisco IOS CGRs, IR800s, and ISR800s
IOS-CGR	cgr1000	Cisco IOS CGRs (CGR 1240 and CGR 1120)
IOS-ESR	c5921	Cisco 5921 ESR (C5921)
IOS-IOx	cgr1000	Cisco IOS CGRs (CGR 1240 and CGR 1120) universal image
IOS-C800	c800	Cisco 800 Series ISR connected devices.
IOS-AP800	ap800	Cisco 800 Series Access Points.
IOS-IR800	ir800	Cisco 800 Series ISRs.
IOS-IR807	ir800	Image (Cisco IOS only) loads to IR807 within the IR800 firmware group.
IOS-WPAN-IXM	ir800	LoRaWAN IXM module when operating as an interface for Cisco IR809.
IOS-WPAN-RF	cgr1000	Cisco IOS-CGR
IOS-WPAN-PLC	cgr1000	Cisco IOS-CGR
IOT-FND-IC3000	ic3000	Cisco IC3000 Gateway
IOx-CGR	cgr1000-ioxvm	Cisco IOS-CGR
IOx-IR800	ir800	Cisco 800 Series ISRs.
LMAC	lmac	Local MAC connected devices.
LORAWAN	lorawan	Cisco IR829-GW

4. Click **Upload Image** to open the entry panel.

5. From the **Select Type:** drop-down menu, choose the firmware type for your device.
6. From the **Select an Image:** drop-down menu, choose the firmware bundle to upload.

For some software bundles, you also have the option to select one or more of the following options (as noted in parenthesis next to the options listed below):

- Install Guest OS from this bundle (IOS-CGR, IOS-IR800)
- Clean LoRaWAN application data on the install (LORAWAN)
- Install WPAN firmware from this bundle (IOS-CGR)

7. Click **Upload Image**.
8. Click **OK**.

IoT FND starts the upload process. After the image uploads, install the image as described in [Installing a Firmware Image](#).

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:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.
3. In the Groups pane, select the firmware group.
4. Click **Cancel**.
5. Click **Yes**.

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:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.
3. In the Groups pane, select the firmware group.
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.

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.

Installing a Firmware Image

To install an image on devices in a router firmware group:

1. Choose **CONFIG > Firmware Update**.

2. Click the **Groups** tab.

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.

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.

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.

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](#)
- [Pausing and Resuming Router Firmware Image Installation](#)

Note: The firmware installation operation can time out on some routers. If routers are not heard from for more than an hour, IoT FND logs error messages.

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:

1. Choose **CONFIG > Firmware Update**.

2. Click **Groups**.

3. In the Groups pane, select the firmware group.

4. In the Firmware Upgrade window, click **Cancel** button.

5. Click **Yes** to confirm action.

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:

1. Choose **CONFIG > Firmware Update**.
2. In the Groups pane, select the firmware group.
3. In the Firmware Upgrade window, click **Pause** button.
4. Click **Yes** to confirm action.

You can resume the installation process by clicking **Resume**.

Performing CG-OS to Cisco IOS Migrations

You can upgrade CGRs from CG-OS to IOS in bulk or by device. The migration package is in the IoT Field Network Director installation package, and is available in the **Select IOS Image** menu.

Note: The **Migration to IOS** button is disabled if all CGRs in the group are IOS.

BEFORE YOU BEGIN

For CG-OS CGRs that you are migrating, modify the device configuration properties CSV or XML file to include the following IOS properties (see [Changing Device Configuration Properties, page 110](#)):

EXAMPLE BOOTSTRAP PROPERTIES

This example preserves tunnels during migration:

```
enable
!
configure terminal
!
!
!
interface GigabitEthernet2/2
    no switchport
    ip address 66.66.0.75 255.255.0.0
    duplex auto
    speed auto
    no shut
!
crypto key generate rsa label LDevID modulus 2048
!
hostname IOS-IOT1
!
enable password cisco
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
!
aaa session-id common
```

```

clock timezone PDT -8 0
!
!
no ip domain lookup
ip domain name ios.com
ip host nms.sgbu.cisco.com 55.55.0.5
ip host ps.sgbu.cisco.com 55.55.0.8
ip cef
ipv6 unicast-routing
ipv6 cef
!
!
!
crypto pki profile enrollment NMS
enrollment url http://55.55.0.17/certsrv/mscep/mscep.dll
!
crypto pki trustpoint LDevID
    enrollment mode ra
    enrollment profile NMS
    serial-number none
    ip-address none
    password
    fingerprint 1D33B1A88574F11E50F5B758EF217D1D51A7C83F
    subject-name CN=mig.ios.com/serialNumber=PID:CGR1240/K9 SN:JAF1712BCAP
    revocation-check none
    rsakeypair LDevID 2048
!
!
!
license accept end user agreement
license boot module cgr1000 technology-package securityk9
license boot module cgr1000 technology-package datak9
!
!
!
username admin password 0 cisco
username cg-nms-administrator privilege 15 secret Sgbu123!
!
!
do mkdir flash:archive
#await Create directory filename
#send_CR
!
!
archive
    path flash:archive/
    maximum 8
!
!
!
no ip http server
ip http authentication local
ip http secure-server
ip http secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha dhe-aes-256-cbc-sha
ip http secure-client-auth
ip http secure-port 8443
ip http secure-trustpoint LDevID
ip http max-connections 2
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 GigabitEthernet2/2

```

```

ip http client secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha
dhe-aes-256-cbc-sha
!
ip route 0.0.0.0 0.0.0.0 66.66.0.8
!
!
privilege exec level 2 dir /recursive
privilege exec level 2 dir
privilege exec level 2 show memory statistics
privilege exec level 2 show memory
privilege exec level 2 show inventory
privilege exec level 2 show platform hypervisor
privilege exec level 2 show platform led summary
privilege exec level 2 show platform led
privilege exec level 2 show processes cpu
privilege exec level 2 show processes
privilege exec level 2 show environment temperature
privilege exec level 2 show environment
privilege exec level 2 show module
privilege exec level 2 show version
privilege exec level 2 show logging
privilege exec level 2 show platform
privilege exec level 2 show
!
!
wsma agent exec
    profile exec
!
wsma agent config
    profile config
!
!
wsma profile listener exec
    transport https path /wsma/exec
!
wsma profile listener config
    transport https path /wsma/config
!
cgna 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 ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
    add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
    add-command show version | format flash:/managed/odm/cg-nms.odm
    interval 10
    url https://ps.sgbu.cisco.com:9120/cgna/ios/tunnel
    active
!
!
cgna exec-profile CGNA-default-exec-profile
    add-command event manager run no_config_replace.tcl flash:/before-tunnel-config cg-nms-tunnel 1 0
    interval 1
    exec-count 1
!
event manager environment ZTD_SCEP_CGNA_Profile cg-nms-tunnel
event manager environment ZTD_SCEP_LDevID_trustpoint_name LDevID
event manager directory user policy "flash:/managed/scripts"
event manager policy tm_ztd_scep.tcl type system authorization bypass
event manager policy no_config_replace.tcl type system authorization bypass
event manager environment ZTD_SCEP_Enabled TRUE
!
!
do write memory
!
do reload in 005

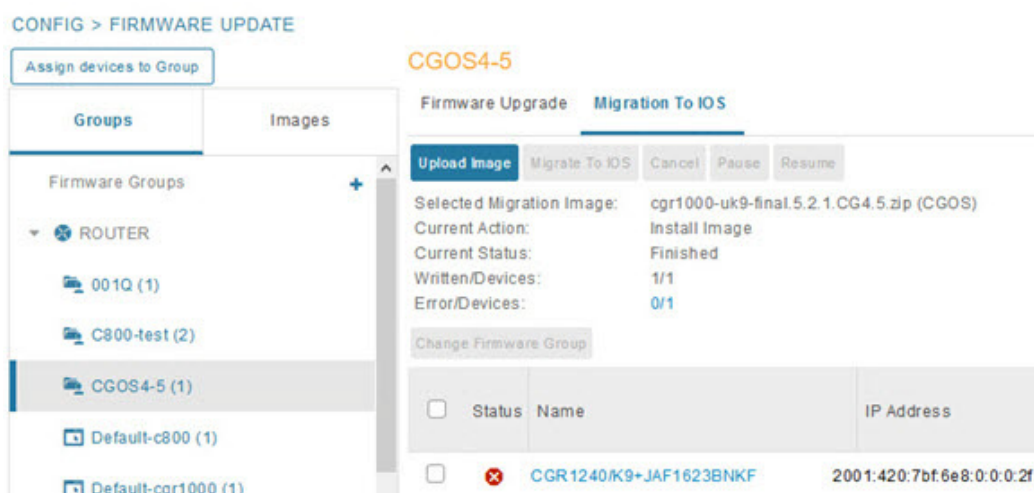
```

```
#await Proceed with reload?
#send_CR
!
crypto pki authenticate LDevID
!
end
```

Note: You can only migrate from CG4(3) to the minimum IOS image for that device. Refer to [Table 1 on page 176](#) for minimum IOS image requirements.

To add CGR IOS images to IoT Field Network Director and upload and install the migration image on CGRs:

1. Select **CONFIG > Firmware Update**, and click the **Migration to IOS** tab.



2. In the Groups pane, select a CGR (or a group of CGRs) running CGOS4(5) software.
3. Select the Cisco IOS software image to upload to the CGR(s), and click **Upload Image** (right-pane).
4. Click **OK** to begin the upload.

Upload progress appears in the device list.

5. Upload the following properties files (see Installing Cisco IoT FND in the appropriate Cisco IoT FND 4.3 installation guide):
 - [Cisco IoT Field Network Director Installation Guide-Oracle Deployment, Release 4.3.x](#)
 - [Cisco IoT Field Network Director Post-Installation Guide - Release 4.3.x \(Tunnel Provisioning and High Availability\)](#)

:

- config
- bootstrap
- tunnel provisioning
- runtime configuration

6. Click the **Migrate To IOS** button.
7. Click **Yes** to confirm and begin the migration process.

The Update Progress displays as a percentage during the software image upload. If an upload fails, error messages and error details also appear for the software image. You can cancel, pause, or resume the migration process.

Tip: If any routers fail to upgrade, restart migration on the group. IoT Field Network Director skips routers that were successfully upgraded.

Interface Names After Migration

IoT Field Network Director preserves metrics for the various interfaces and associated properties during migration. [Table 1](#) maps CG-OS interfaces to the corresponding IOS interfaces to preserve metrics.

Table 1 CG-OS-to-IOS Interface Migration Map

CG-OS Interface	Corresponding IOS Interface
Wifi2/1	Dot11Radio2/1
Ethernet2/1	GigabitEthernet2/1
Ethernet2/2	GigabitEthernet2/2
Ethernet2/3	FastEthernet2/3
Ethernet2/4	FastEthernet2/4
Ethernet2/5	FastEthernet2/5
Ethernet2/6	FastEthernet2/6
Wpan4/1	Wpan4/1
Serial1/1	Async1/1
Serial1/2	Async1/2
Cellular3/1	Cellular3/1
N/A	GigabitEthernet0/1

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, and includes the following topics:

- [Uploading a Firmware Image to a Resilient Mesh Endpoint Group](#)
- [Viewing Mesh Device Firmware Image Upload Logs](#)
- [Viewing Mesh Endpoint Firmware Update Information](#)

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.

Uploading a Firmware Image to a Resilient Mesh Endpoint Group

To upload a firmware image to mesh endpoint group members:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab (left pane).
3. Select the firmware group to update.

4. In the right panel, select **Firmware Management** and the click **Upload Image** button and an entry panel appears.

- a. From the **Select Type** drop-down menu, choose the firmware type for your device.

IoT FND can upload these image types to ENDPOINT devices.

Image Type	Description
RF	RFLAN connected devices.
PLC	Power line communication devices.
BBU	Devices with battery back up.
LMAC	Local MAC connected devices.
PLC-RF	PLC-Radio Frequency devices.
IOx-IR500	IR500 devices.

- b. From the **Select an Image** drop-down menu, choose the firmware bundle to upload.

- c. Click **Upload Image**.

- d. Check the appropriate box based on the Selected Type and Image:

- Install Guest OS from this bundle
- Clean LoRaWAN application data on install?
- install WAPN firmware from this bundle:

- 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 (percent complete). You can filter the display by Subnet, PanId or Group.

default-cgmesh

Firmware Management

Devices

Logs

Transmission Settings

Upload Image

Current Status:

Reload Scheduling Finished

Image:

Reloaded/Devices:

0/17



Error/Devices:

0/17


Not Synced/Devices: 16/17

Sync Membership

ALL(2) | BL(1) | RF(1)

Image	Uploaded	Running	Backup	Boot Loader	LMAC	BBU	Status	Scheduled Reload	Actions
cg-mesh-bloader-REL-2.0.3-EV8KREF1-1.0-1.0	0	0	0	1	0	0			
cg-mesh-node-5.7.11-EV8KREF1-1.0-1.0	0	1	0	0	0	0			 

Clear Filter

Displaying 1 - 1 of 1 | Page 1 of 1 | 50 | 

- 1
- Sync membership button
- Click button to sync the group members in the same firmware group.

For every image in the list, IoT FND displays the following information:

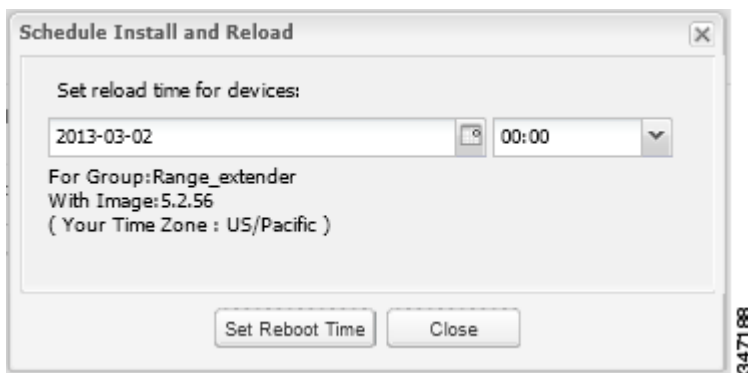
Column	Description
Image	Image name.
Uploaded	Specifies the number of devices that uploaded the image. Click the number to display a list of these devices.
Running	Specifies the number of devices running this image. Click the number to display a list of these devices.
Backup	Specifies the number of devices 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.

Column	Description
Scheduled Reload	Specifies the scheduled reload time.
Actions	Provides two actions: <ul style="list-style-type: none"> ■ Schedule Install and Reload icon—Schedule the installation date and time of the loaded image and the rebooting of the endpoint. ■ Set as Backup icon—Set the image as the backup image.

Setting the Installation Schedule

To set the installation schedule:

1. Click the **Schedule Install and Reload** button under the **Actions** heading.
2. Specify the date and time for the installation of the image and the rebooting of the device.



3. Click **Set Reboot Time**.
 - To set the selected image as the firmware image backup, click the **Set as Backup** button.
4. Click **Yes**.
 - To sync the group members in the same firmware group, click **Sync Membership (1)**.
 - To view member devices, click the **Devices** tab.
 - To view log files for the group, click the **Logs** tab.

Viewing Mesh Device Firmware Image Upload Logs

To view the firmware image upload logs for mesh devices:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab (left-pane).
3. Under the Firmware Groups heading of the Groups pane, select the *Default-cgmesh* firmware group.
4. Click the **Logs** tab (right-pane).

Viewing Mesh Endpoint Firmware Update Information

You can view the endpoint firmware update process down to the subnet level for greater visibility. To view details of firmware updates for mesh endpoint devices (by Subnet, Pan Id or Group) in a table or histogram, during the upgrade process or after the firmware upgrade completes, follow these steps:

Note: For Subnet and Pan Ids, you must enter the value in the text box provided:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.
3. Under the Groups heading, select a mesh devices group (such as Default-cgmesh or Default-ir500).
4. Click the **Firmware Management** tab (right-pane).

Firmware Management Devices Logs Transmission Settings												
<input type="text"/> Show Filter												
Change Firmware Group Displaying 1 - 16 Page 1 50												
<input type="checkbox"/>	Status	Name	IP Address	Firmwa Version	Backup Version	Upload Version	Boot Loader Version	LMAC Version	BBU Version	Member Synced?	Activity	Upd. Prog
<input type="checkbox"/>	✓	00193bab0010002c	200c:0:0:0:0:0:5							No	Unknown	0
<input type="checkbox"/>	✓	00193bab0010002d	200c:0:0:0:0:0:6							No	Unknown	0
<input type="checkbox"/>	✓	00193bab0010002e	200c:0:0:0:0:0:7							No	Unknown	0

Field	Description
(Top, Left Panel)	
Upload Image radio button	<p>Select the software image type and image type from the drop-down menus and click Upload Image radio button to begin the firmware upload.</p> <p>Note: By default, all subnets listed at the bottom of the screen will receive the image upload.</p> <p>To exclude a subnet from the firmware upload, check the box (such as 1 or 2) next to that subnet. For more details, see PAN ID definition below.</p>
Current Status	<p>Status of the firmware upload (for example, Image Loading or Upload Finished).</p> <ul style="list-style-type: none"> ■ Image Loading, Upload Paused, Upload Stopped, Upload Finished, Upload Stopping, Upload Pausing ■ Scheduling Reload, Reload Paused, Reload Stopped, Reload Scheduling Finished, Reload Stopping, Reload Pausing ■ Setting Backup, Backup Paused, Backup Stopped, Backup Finished, Backup Stopping, Backup Pausing
Image	Firmware image name.
Uploaded/Devices	Number of completed, successful firmware updates against the total devices that will receive the updates.
Error/Devices	Number of devices the operation failed (error) against the total devices in the group.
Not Synced/Devices	Number of firmware group membership non-synchronized devices against the total number of devices in the group.
(Right Panel) Histogram	
% Completed	Visual status of upload percentage completed.
Filter by	Filter and display results by: Subnet, Pan ID, Group
(Bottom Panel)	
All or RF	<p>All displays information about all images in the Running, uploaded and backup slot as well as the BBU and PLC information for all device images (RF mesh, IR500 WPAN Range Extender and WPAN Range Extender with BBU and PLC) in the group; and the schedule reload and status information.</p> <p>RF displays information regarding RF mesh images in the Running, uploaded and backup slots as well as the schedule reload and status information.</p>
Image	<p>Displays image file name and provides the completion percentage of the firmware upload (0 to 100) with respect to the following states:</p> <ul style="list-style-type: none"> ■ Uploaded, Running, Backup, Bootloader, LMAC, BBU, Status, Sched Reload
Clear filter	Click radio button to clear selected firmware image update results.

Field	Description
PAN ID	<p>Identifies the Personal Area Network Identifier for a group of endpoints (nodes).</p> <p>To exclude a group of nodes from a new firmware upload, you must select the Pan ID check box next to that group of nodes before selecting the Upload Image radio button in the Firmware Management pane.</p> <p>Note: The check boxes next to the PAN IDs are not visible during a firmware upload.</p> <p>Note: You can sort PAN IDs in an ascending or descending manner or filter by PAN ID to define which PAN ID displays in the window by selecting the downward arrow to the right of the column. Select Clear Filter to leave that view.</p> <p>Note: To see a listing of all nodes within a subnet, select the Device tab.</p>
Subnet Prefix	<p>Identifies the IPv6 subnet prefix for the endpoint. To view all of the nodes within a given subnet, select the Devices tab.</p> <p>Note: You can filter by Subnet by entering a portion of the subnet (for example, 200b:0:0) by selecting the downward arrow to the right of the column. Select Clear Filter to leave that view.</p>
Nodes in Group	<p>Number of nodes within the group. In the screen shot above, there are a total of 25 nodes within the group, which are split across two different subnets (8 nodes in 200b:0:0:0:0:0:0 and 17 nodes in 200c:0:0:0:0:0:0).</p>
Total in Subnet	<p>Number of nodes with the subnet. In the screen shot above, there are 19 nodes in the subnet.</p>
Upload status	<p>Number of nodes out of the total nodes that have been successfully upgraded with the new firmware.</p>
Last message sent	<p>Display of latest message relevant to the current firmware update process within the given PAN.</p>

Viewing Mesh Device Firmware Information

To view the firmware information for mesh devices:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.
3. In the Groups pane under the Firmware Groups heading, select a Mesh devices group.
4. Click the **Devices** tab.

CONFIG > FIRMWARE UPDATE

Assign devices to Group

default-cgmesh

Firmware Management

Devices

Logs

Transmission Settings

Groups

Images

Test-File-Upload (1)

Test-FW (1)

Test2 (1)

ZTD-IR800 (1)

ENDPOINT

Checking (0)

Default-cgmesh (17)

Change Firmware Group

	Status	Name	IP Address	Firm... Vers...	Bac... Vers...	Uplo... Vers...	Boot Loa... Vers...	LMAC Vers...	BBU Vers...	Member Sync...	Activity
<input type="checkbox"/>	✖	00173B00010088BB	2009:aaaa:1111:bbbb...	5.7.11			2.0.3			Yes	Partially Uploaded
<input type="checkbox"/>	✔	00193bab0010002c	200c:0:0:0:0:0:5							No	Partially Uploaded

For every device in the group, IoT FND displays the following Device Info:

Field	Description
Status	Status of the device (for example, Up, Down, or Unheard).
Name	EID of the device.
IP Address	IP address of the device.
Firmware Version	Version of the firmware image running on the device.
Backup Version	Version of the firmware image used as a backup.
Uploaded Version	Version of the firmware image loaded on the device.
Boot Loader Version	Version of bootloader loaded on the device.
LMAC Version	Version of Local MAC connected device.
BBU Version	Displays BBU version if present on device.
Member Synced?	Whether the device is in sync with the rest of the group.
Activity	Firmware image upload activity.
Update Progress	Firmware image upload progress. An update progress of 100% indicates that the upload is complete.
Last Firmware Status Heard	Last time the firmware status was heard.
Scheduled Reload Time	The time set for upload image reloads.
Error Message	Error message if image upload failed.



Monitoring System Activity

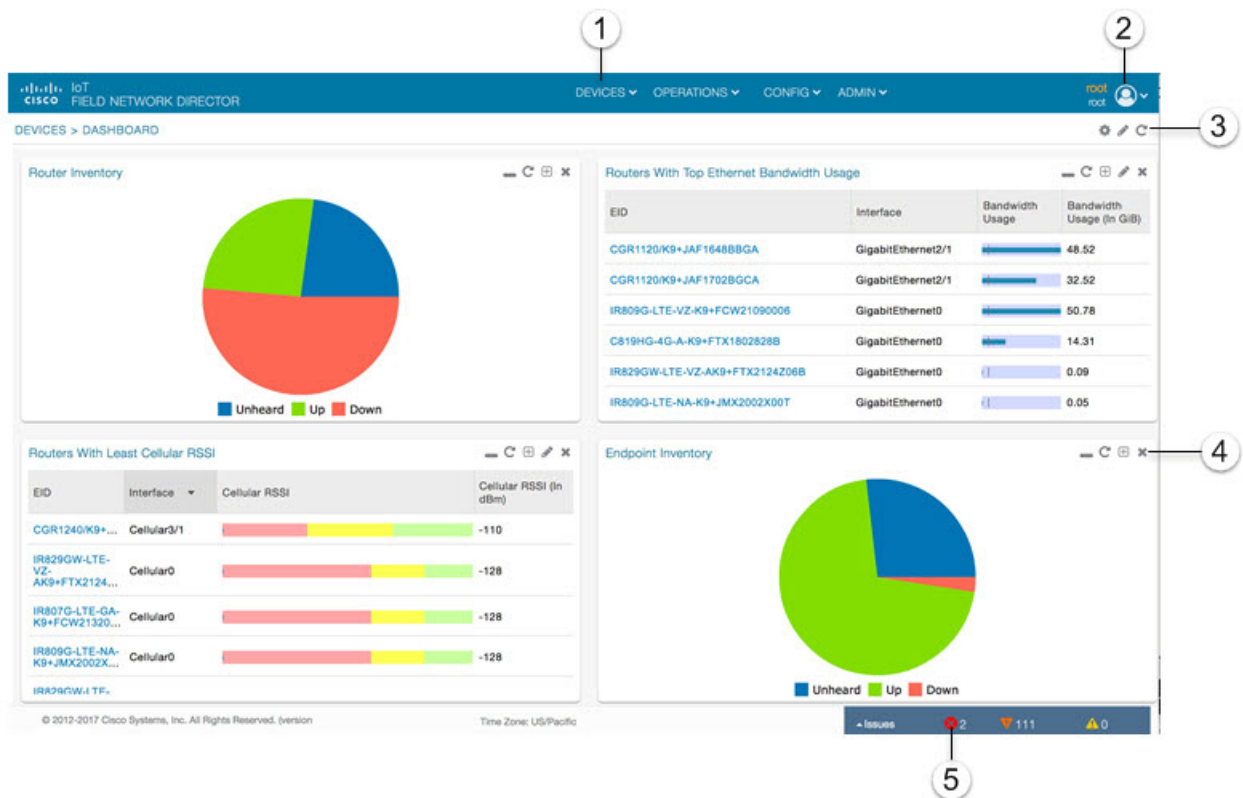
This section describes how to monitor IoT FND system activity, including the following topics:

- [Using the Dashboard](#)
- [Monitoring Events](#)
- [Monitoring Issues](#)
- [Viewing Device Charts](#)

Using the Dashboard

The IoT FND Dashboard (Figure 1) displays *dashlets* to provide a visual overview of important network metrics for a device. Click **Device > Dashboard** to view.

Figure 1 IoT FND Dashboard



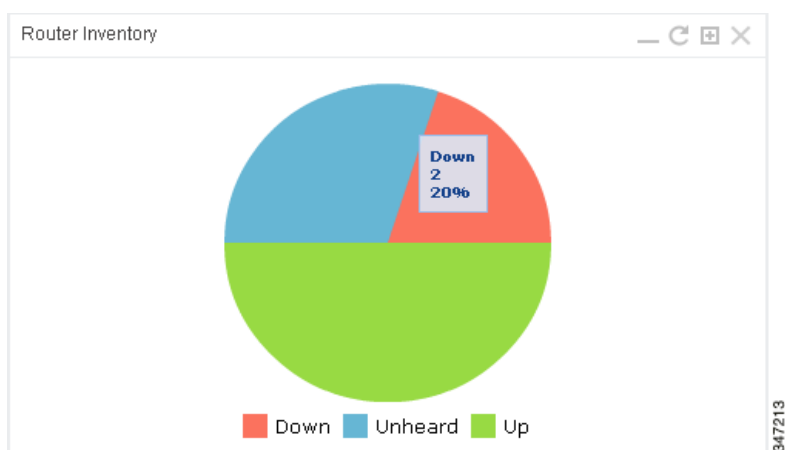
1	<p>Menu and Submenu tabs.</p> <p>Roll over the Menus to display Sub-menus, which display as tabs below the main menus.</p>	5	<p>Dashlet action buttons (left to right):</p> <ul style="list-style-type: none"> ■ Minimize (close) dashlet window. ■ Refresh dashlet. ■ Export data. ■ Filter (not available on all pages) ■ Close dashlet.
2	<p><user name> menu</p> <ul style="list-style-type: none"> ■ Preferences: Sets display settings of the user interface. ■ Switch Domain. ■ Change Password. ■ Time Zone. ■ Log Out. 	6	<p>Issues Status bar.</p> <p>Summary of issues by devices (routers, head-end routers, servers, endpoints) and their severity (critical, major, minor).</p> <p>Viewing Device Severity Status on the Issues Status Bar</p>
3	<ul style="list-style-type: none"> ■ Dashboard Settings-Allow you to set the refresh rate for the page and Add Dashlets to the Dashboard. ■ Filter-Allows you to define custom filters. You can also define time periods for the filter. ■ Refresh page. 	7	<p>Line Graphs: Zoom In, Zoom Out, View All Options.</p> <p>Right click on a line graph dashlet and select Zoom in or Zoom Out to modify the number of days that display on the graph.</p> <p>Right click on View All to show the default display.</p>
4	<p>User-Defined Charts.</p> <p>For some user-defined charts, you can select how the data displays. Options are Bar or Pie.</p>		

This section describes the following Dashboard features:

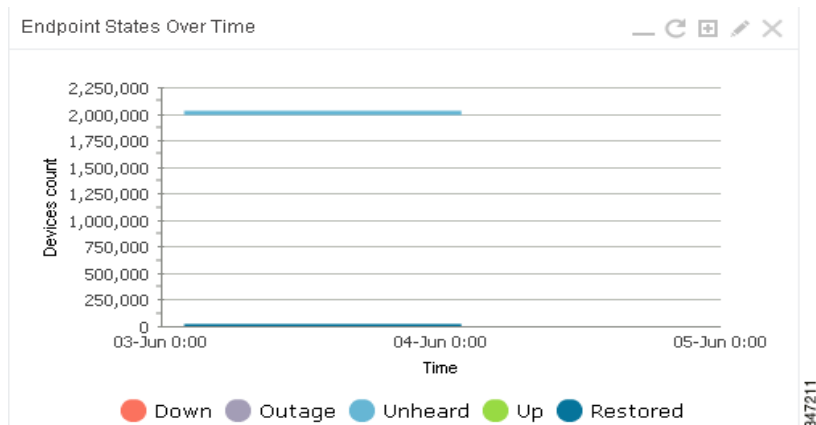
- [Types of Dashlets](#)
- [Repositioning Dashlets](#)
- [Setting the Dashlet Refresh Interval](#)
- [Adding Dashlets](#)
- [Removing Dashlets](#)
- [Exporting Dashlet Data](#)

Types of Dashlets

The Dashboard displays three types of dashlets for a selected device:

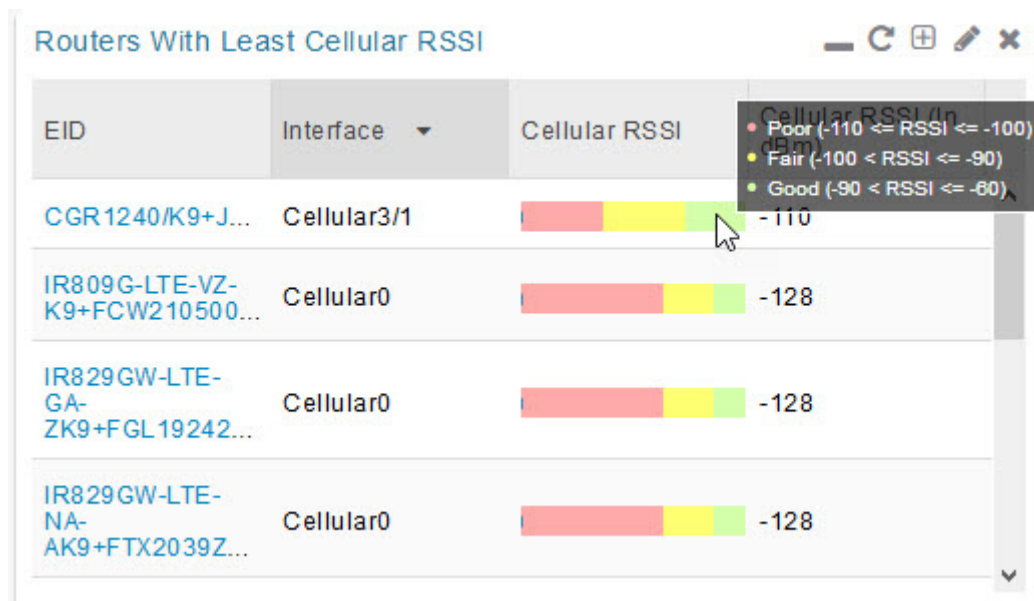


- Pie-chart dashlets display a ratio of device properties as a pie chart.



- Line-graph dashlets display graphs that show device counts 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.



- Bar charts show percentages of a whole

Customize Dashboard Dashlets

At the upper-right corner of the **Devices > Dashboard** page, you can:

- Click the Dashboard Settings (cog) button to Add Dashlets and Set Refresh Interval for all active dashlets.
- Click the pencil icon to Add or Remove a Filter for a device.
- Click Refresh icon to refresh the dashlet.

At individual dashlets you can:

- Click the dash (-) icon to minimize the dashlet.
- Click the Refresh icon to refresh the dashlet.
- Click the (+) icon to export data (.csv format) from the dashlet.
- 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
- Click (X) to close the dashlet.

Pre-defined Dashlets

The IoT FND Dashboard dashlets are described in the table below.

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).
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.
Endpoint Config Group 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: Up, Down, and Outage.
Endpoint States Over Time	This line graph shows a count of endpoints and their states for the configured time interval. States shown: 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).
Hop Count Distribution	This pie chart shows the hop count distribution for mesh devices.
RF and PLC Media Utilization Over Time	This pie chart summarizes active PLC and RF mesh devices on CGR 1000 and IR800 routers over a user-defined period of time (6h, 1d, 1w or custom).
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	

Dashlet

Routers With Top Cellular Bandwidth Usage

Description

This bandwidth chart displays the following information for the top n routers: EID, Interface, Bandwidth Usage and Bandwidth in 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**.

This bandwidth chart displays the following information for the top n routers: EID, Interface, Bandwidth Usage and Bandwidth in Usage (in Gigabits) for a router per the defined filter. The filter defines possible time periods (6h, 1d, 1w, 4w, Custom, Last Billing Period) to display. To define the filter, click the pencil icon.

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**.

This dashlet displays a chart of routers with the lowest RSSI values at the last poll, which indicates the quality of the signal strength and identifies each cellular interface. Use this chart to gauge the cellular channel conditions for routers.

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, C800, 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.

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, C800, 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.

Routers With Top Ethernet Bandwidth Usage

Routers With Least Cellular RSSI

Service Providers with Maximum Down Routers for Cellular 1

Service Providers with Maximum Down Routers for Cellular 2

Repositioning Dashlets

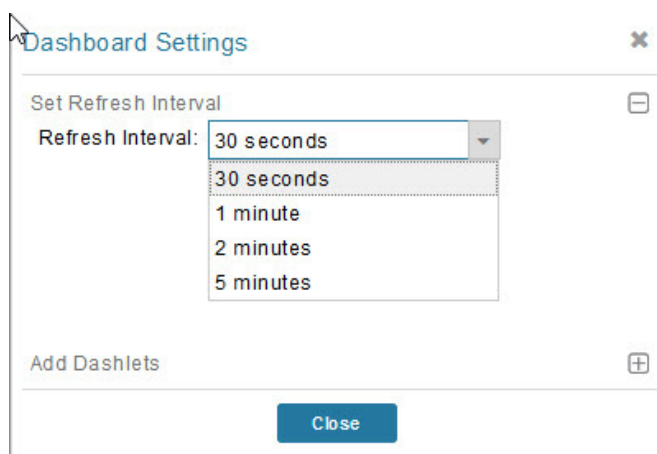
You can configure the Dashboard to display charts in your preferred arrangement.

- Click and drag the title bar of a chart to the desired position.
- Click (x) within a chart to remove the chart from the page.
- Collapse a dashlet to display only its title bar (such as Endpoint Inventory) by clicking the Minimize button (-).
- To refresh a dashlet, click its **Refresh** button.

Setting the Dashlet Refresh Interval

To set the refresh interval for dashlets:

1. Choose **DEVICES > Dashboard**.
2. Click the Dashboard **Settings** button (cog icon).
3. Click **Set Refresh Interval**.



4. From the drop-down menu, choose a refresh interval.
5. **Close** the Dashboard Settings dialog box when finished.

Adding Dashlets

To add dashlets to the Dashboard:

1. Choose **DEVICES > Dashboard**.
2. Click the **Settings** button (cog icon) in the upper-right hand corner of the page.
3. Click **Add Dashlets (+)**.

Note: No dashlets display in this dialog box if all are displaying on the Dashboard.

4. To add a listed dashlet to the Dashboard, select the name of dashlet.
5. Close the Dashboard Settings dialog box by clicking (x) in upper-right corner of panel when finished.

Removing Dashlets

To remove dashlets from the Dashboard:

1. Choose **DEVICES > Dashboard**.
2. Close the dashlet by clicking **(X)** in the upper-right corner of the panel.

Using Pie Charts to Get More Information

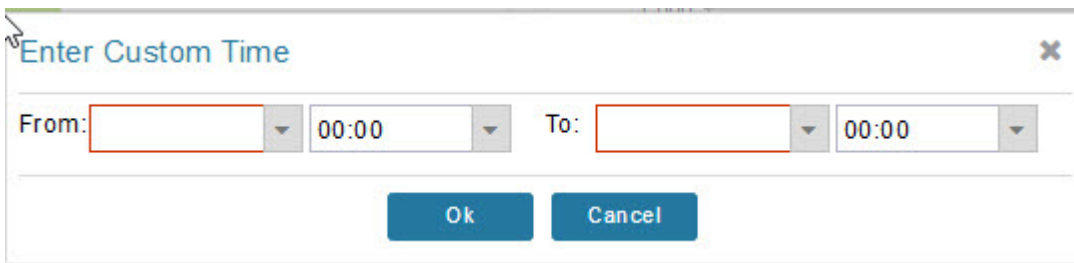
Roll over any segment of a pie chart to display a callout with information on that segment.

Click the Router Inventory and Mesh Endpoint Inventory pie charts to display the devices in List View.

Setting Dashlet Time Properties

To specify the time interval for data collection for line-graph dashlets, click the interval icon (a pencil icon), in the title bar to display the **6h**, **1d**, **1w**, **4w**, or **Custom** buttons on the dashlet. The **6h** button sets the data-collection time interval to the last six hours. The **1d** button sets the time interval to the last 24 hours.

1. Click **Custom**.
2. In the window that appears, select the time frame using the **From and To** fields. Click **OK**.



Enter Custom Time

From: 00:00 To: 00:00

Ok Cancel

Collapsing Dashlets

Click the minimize icon (-) at the upper-right of the dashlet window to hide the window.

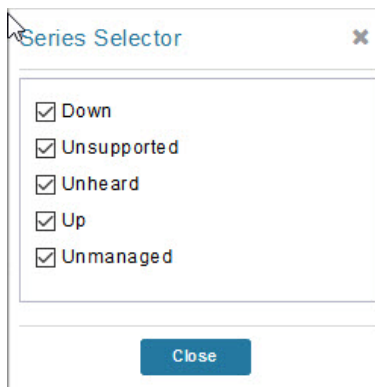
Using the Series Selector

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:

1. Click **Series Selector**.
2. In the **Series Selector** dialog box, check the check boxes for the data series to show in the graph.



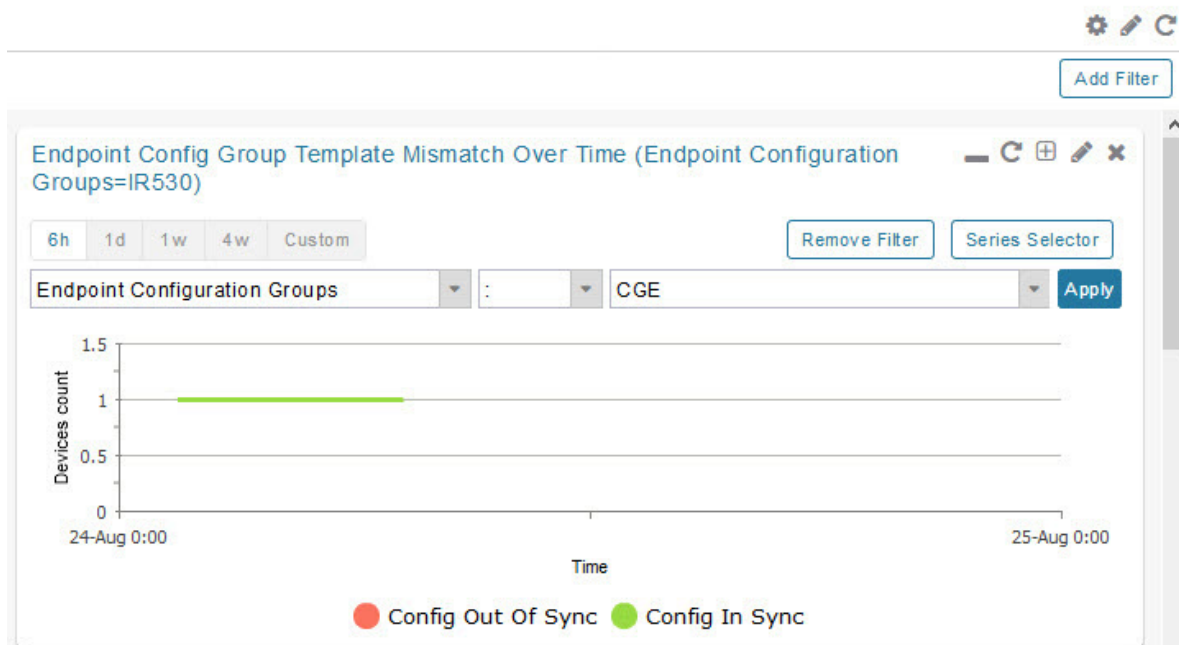
3. Click **Close**.

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:

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)).
2. Click a time frame.



3. From the first drop-down menu, choose a group type.
4. From the third drop-down menu, choose a group.
5. 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:

1. On the desired dashlet, click the export button (+).

A browser download session begins.

2. Navigate to your default download directory to view the export file.

The filename begins with the word “export-” and includes the dashlet name (for example, export-Node_State_Over_Time_chart-1392746225010.csv).

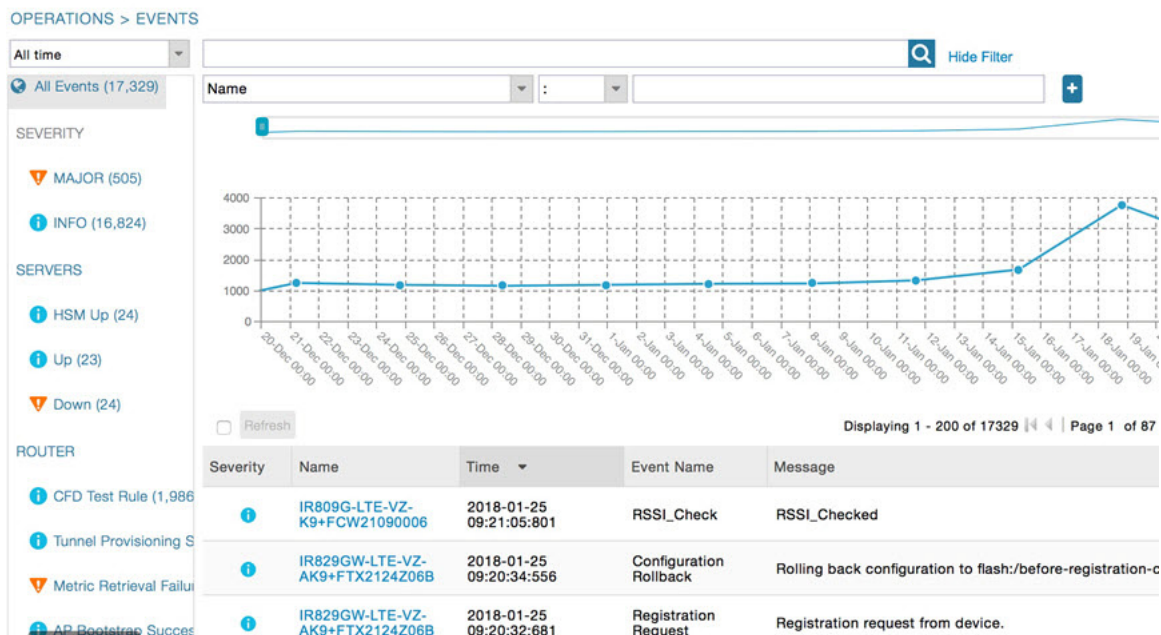
Monitoring Events

This section provides an overview of events and how to search and sort events, including the following topics:

- [Viewing Events](#)
- [Filtering by Severity Level](#)
- [Advanced Event Search](#)
- [Sorting Events](#)
- [Searching By Event Name](#)
- [Searching by Labels](#)

Viewing Events

As shown in [Figure 2](#), the Events page (**OPERATIONS > Events**) lists all events for those devices that IoT FND tracks. All events are stored in the IoT FND database server.

Figure 2 Operation > Events Page

By default, the **Operations > Events** page displays the Events chart, which is a visual view of events in a time line. 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), clearing the check boxes for showing chart and summary counts on the Events page, and clicking **Apply**.

- To limit the amount of event data displayed on this page, use the Filter drop-down menu (at the top of the left pane). 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.
- To enable automatic refresh of event data to refresh every 14 seconds, check the check box 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
- CG 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.

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.

Filtering by Severity Level

To filter by severity level, click the pencil icon:

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

3. Click a severity level to display all events of that severity level in the Events pane (right-pane).

Advanced Event Search

To use the filter to search for events:

1. Choose **OPERATIONS > Events**.
2. Under All Events (left pane), select an event category to narrow down your search.
3. Click the **Show Filter** link at the top of the main pane.
4. Use the filter drop-down menus and fields to specify your search criteria.
5. Click the plus button (+) to add the search strings to the Search field.

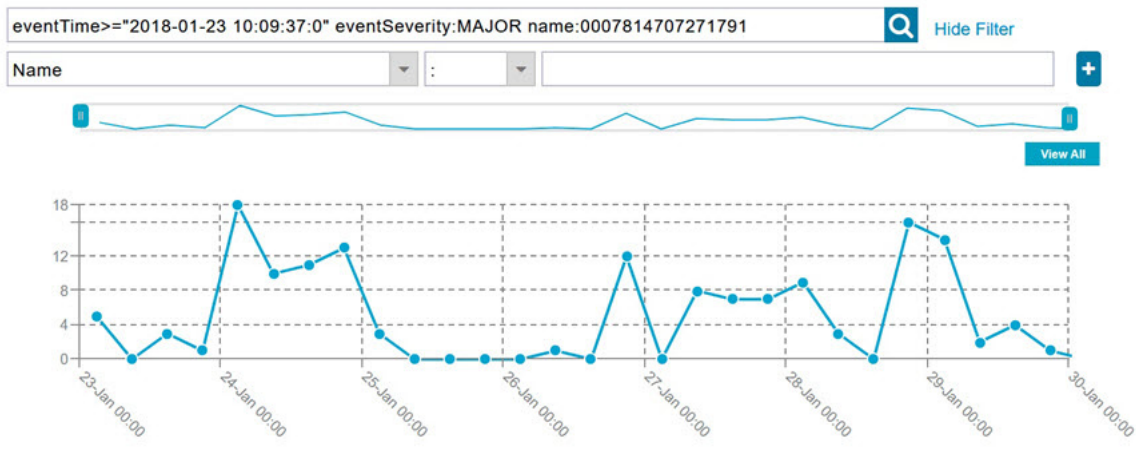
Repeat the process of adding search strings to the Search field as needed.

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, as shown in [Figure 2](#):
name: router eid string.
Search Events by Name Filter



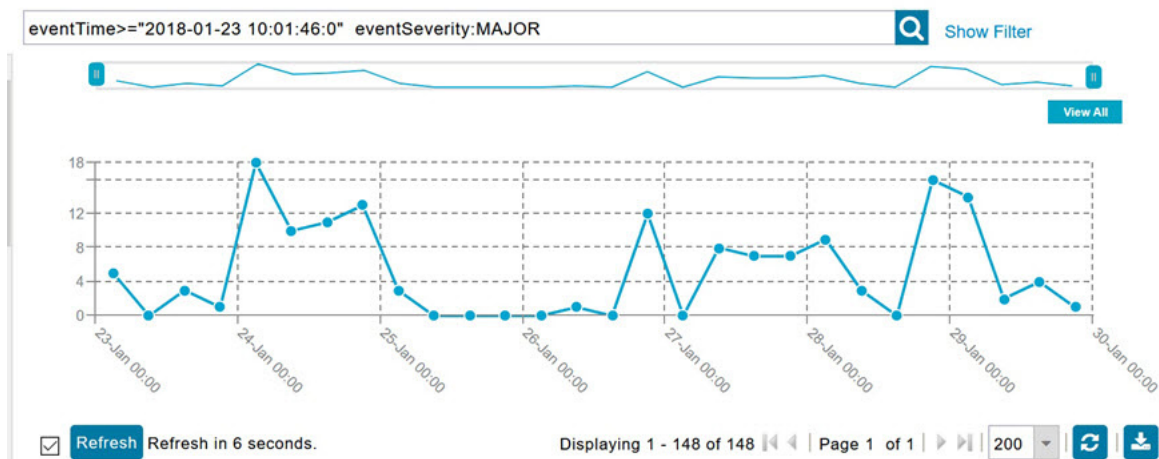
Note: Note the use of the asterisk (*) wild card with this filter.

- To filter by event time period, enter the following string in the Search Events field, as shown in graph below:

eventTimeoperator"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):

1. Choose **OPERATIONS > Events**.

2. In the left pane, click the device type.
3. Click the **Show Filter** link at the top of the right pane to display the search fields.
4. Choose **Event Name** from the left drop-down menu.
5. Choose the event name from the options in the right drop-down menu.
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.
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.

1. Choose **OPERATIONS > Events**.
2. Click **All Events** in the left pane.
3. Click the **Show Filter** link at the top of the right pane.
4. Choose **Label** from the left drop-down menu.
5. Choose the event name from the options in the right drop-down menu or create your own.
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.
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:

1. Choose **OPERATIONS > Events**.
2. Click the desired severity level or device type in the left pane.
3. Click the **Export** button (+).
A browser download session begins.
4. Navigate to your default download directory to access the CSV file.

Events Reported

[Table 1](#) lists the events reported by IoT FND 3.1.x (and later). Details include the event severity (Critical, Major, Minor, Information) and the devices that report those events.

Table 1 Events Reported

Event	Devices	Severity
CRITICAL EVENTS		
Certificate Expired	AP800, CGR1000, C800, FND, IR800	Critical
DB FRA Space Critically Low	Database	Critical
DB Table Space Critically Low	Database	Critical
Invalid CSMP Signature	CGMESH, IR500	Critical
Outage	Cellular, CGMESH, IR500	Critical
RPL Tree Size Critical	CGR1000	Critical
SD Card Removal Alarm	CGR1000	Critical
MAJOR EVENTS		
AAA Failure	C800, CGR1000, IR800	Major
ACT2L Failure	C800, CGR1000, IR800	Major
Archive Log Mode Disabled	Database	Major
Battery Failure	CGR1000	Major
Battery Low	CGR1000, IR500	Major
BBU Configuration Failed	IR500	Major
BBU Firmware Download Failed	IR500	Major
BBU Firmware Mismatch Found	CGR1000	Major
BBU Firmware Upgrade Failed	IR500	Major
BBU Lock Out	IR500	Major
BBU Power Off	IR500	Major
Block Mesh Device Operation Failed	CGR1000	Major
Certificate Expiration	AP800, C800, CGR1000, FND, IR800	Major
DB FRA Space Very Low	Database	Major
Default Route Lost	CGMESH, IR500	Major
Device Unknown	FND	Major
Door Open	C800, CGR1000, IR800, LORA	Major
Dot1X Authentication Failure	CGR1000	Major
Dot1X Authentication Flood	C800, CGR1000, IR800	Major
Down	AP800, ASR, C800, Cellular, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900, LORA	Major
Element Configuration Failed	C800, CGR1000, IR800	Major
High CPU Usage	LORA	Major
High Flash Usage	LORA	Major
High Temperature	LORA	Major
HSM Down	FND	Major
Interface Down	ASR, ISR3900	Major
Linecard Failure	C800, CGR1000, IR800	Major
Line Power Failure	C800, CGR1000, IR800	Major

Table 1 Events Reported

Event	Devices	Severity
Link Down	IR500	Major
Low Flash Space	C800, CGR1000, IR800	Major
Low Memory/Memory Low	C800, CGR1000, FND, IR800, LORA (Memory Low)	Major
Low Temperature	LORA	Major
Mesh Connectivity Lost/ Node Connectivity Lost	CGMESH, IR500	Major
Mesh Link Key Timeout/ Node Link Key Timeout	CGMESH, IR500	Major
Metric Retrieval Failure	ASR, C800, CGR1000, IR800, ISR3900	Major
Modem Temperature Cold Alarm	C800, CGR1000, IR800	Major
Modem Temperature Warm Alarm	C800, CGR1000, IR800	Major
Node Connectivity Lost	CGMESH, IR500	Major
Node Link Key Timeout	CGMESH, IR500	Major
Packet Forwarder Usage High	LORA	Major
Port Down	AP800, C800, CGR1000, IR800	Major
Port Failure	AP800, C800, CGR1000, IR800	Major
Refresh Router Mesh Key Failure	CGR1000	Major
RPL Tree Size Warning	CGR1000	Major
Software Crash	C800, CGR1000, IR800	Major
SSM Down	FND	Major
System Software Inconsistent	C800, CGR1000, IR800	Major
Temperature Major Alarm	C800, CGR1000, IR800	Major
Time Mismatch	CGMESH, IR500	Major
Tunnel Down	C800, CGR1000, IR800	Major
Tunnel Provisioning Failure	C800, CGR1000, IR800	Major
Unknown WPAN Change	CGMESH, IR500	Major
MINOR EVENTS		
DB FRA Space Low	Database	Minor
Dot1X Re-authentication	CGMESH, IR500	Minor
Temperature Minor Alarm	C800, CGR1000, IR800	Minor
Temperature Low Minor Alarm	C800, CGR1000, IR800	Minor
RPL Tree Reset	CGR1000	Minor
INFORMATION EVENTS		
Archive Log Mode Enabled	Database	Information
Battery Normal	CGR1000	Information
Battery Power	CGR1000	Information
BBU Firmware Download Passed	CGR1000	Information
Certificate Expiration Recovery	AP800, C800, CGR1000, FND, IR800	Information
Cold Boot	AP800, C800, CGMESH, CGR1000, IR500, IR800	Information

Table 1 Events Reported

Event	Devices	Severity
Configuration is Pushed	FND	Information
Configuration Rollback	AP800, C800, CGR1000, IR800	Information
DB FRA Space Normal	Database	Information
DB Table Space Normal	Database	Information
Device Added	Cellular, C800, CGMESH, CGR1000, IR500, IR800	Information
Device Location Changed	C800, CGR1000, IR800	Information
Device Removed	Cellular, C800, CGMESH, CGR1000, IR500, IR800	Information
Door Close	C800, CGR1000, IR800, LORA	Information
Dot11 Deauthenticate Send	C800, CGR1000, IR800	Information
Dot11 Disassociate Send	C800, CGR1000, IR800	Information
Dot11 Authentication Failed	C800, CGR1000, IR800	Information
Hardware Insertion	C800, CGR1000, IR800	Information
Hardware Removal	C800, CGR1000, IR800	Information
High CPU Usage Recovery	LORA	Information
High Flash Usage Recovery	LORA	Information
High Temperature Recovery	LORA	Information
HSM Up	FND	Information
Interface Up	ASR, ISR3900	Information
Line Power	C800, CGR1000, IR800	Information
Line Power Restored	C800, CGR1000, IR800	Information
Link Up	IR500	Information
Low Flash Space OK	C800, CGR1000, IR800	Information
Low Memory OK/Low Memory Recovery	C800, CGR1000, IR800, LORA (Low Memory Recovery)	Information
Manual Close	ASR, Cellular, C800, CGMESH, CGR1000, IR500, IR800, ISR3900	Information
Major RPL Tree Size Warning OK	CGR1000	Information
Manual NMS Address Change	CGMESH, IR500	Information
Manual Re-Registration	CGMESH, IR500	Information
Mesh Certificate Change/ Node Certificate Change	CGMESH, IR500	Information
Mesh Module Firmware Upgrade has been successful	CGR1000	Information
Migrated To Better PAN	CGMESH, IR500	Information
Modem Status Changed	LORA	Information
Modem Temperature Cold Alarm Recovery	C800, CGR1000, IR800	Information
Modem Temperature Warm Alarm Recovery	C800, CGR1000, IR800	Information
NMS Address Change	CGMESH, IR500	Information

Table 1 Events Reported

Event	Devices	Severity
NMS Returned Error	CGMESH, IR500	Information
Node Certificate Change	CGMESH, IR500	Information
Packet Forwarded High Usage Recovery	LORA	Information
Packet Forwarder Status	LORA	Information
Packet Forwarded High Usage Recovery	LORA	Information
Port Up	AP800, C800, CGR1000, IR800	Information
Power Source OK	C800, CGR1000, IR800	Information
Power Source Warning	C800, CGR1000, IR800	Information
Registered	ASR, ISR3900	Information
Registration Failure	AP800, Cellular, C800, CGR1000, IR800, LORA	Information
Registration Request	AP800, C800, CGR1000, IR800, LORA	Information
Registration Success	AP800, Cellular, C800, CGR1000, IR800, LORA	Information
Rejoined With New IP Address	CGMESH, IR500	Information
Restoration	Cellular, CGMESH, IR500	Information
Restoration Registration	CGMESH, IR500	Information
RPL Tree Size Critical OK	CGR1000	Information
Rule Event	ASR, C800, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900	Information
SSM Up	FND	Information
Temperature Low Recovery	LORA	Information
Temperature Low Minor Alarm Recovery	C800, CGR1000, IR800	Information
Temperature Major Recovery	C800, CGR1000, IR800	Information
Temperature Low Major Alarm Recovery	C800, CGR1000, IR800	Information
Temperature Minor Recovery	C800, CGR1000, IR800	Information
Time Mismatch Resolved	CGMESH, IR500	Information
Tunnel Provisioning Request	C800, CGR1000, IR800	Information
Tunnel Provisioning Success	C800, CGR1000, IR800	Information
Tunnel Up	C800, CGR1000, IR800	Information
Unknown Event	AP800, ASR, C800, Cellular, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900, LORA	Information
Unknown Registration Reason	CGMESH, IR500	Information
Unsupported	AP800, C800, CGR1000, IR800, LORA	Information
Up	AP800, ASR, C800, Cellular, CGMESH, CGR1000, Database, FND, IR500, IR800, ISR3900, LORA,	Information
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, including the following topics:

- [Viewing Issues](#)
- [Viewing Device Severity Status on the Issues Status Bar](#)
- [Adding Notes to Issues](#)
- [Searching Issues Using Predefined Filters](#)
- [Search Issues Using Custom Filters](#)
- [Closing an Issue](#)

Viewing Issues

IoT FND offers different ways to monitor issues:

- The **OPERATIONS > Issues** page ([Figure 3](#)) provides a snapshot of the health of the network by highlighting only major and critical events that are active within the network.
- The Issues Status bar ([Figure 4](#)) displays in the footer of the browser window and shows a count of all issues by severity for selected devices.

Figure 3 OPERATIONS > Issues Page

Events	Notes	Severity	Name	Last Update Time	Occur Time	Issue	Is
<input type="checkbox"/>	Events	Notes	IR807G-LTE-GA-K9+FCW21320020	2018-01-24 11:53:15 PST	2018-01-24 11:53:15 PST	Down	OI
<input type="checkbox"/>	Events	Notes	IR807G-LTE-GA-K9+FCW21320020	2018-01-19 04:17:53 PST	2018-01-10 22:53:57 PST	Port Down	OI
<input type="checkbox"/>	Events	Notes	CISCO5921-K9+9IA8497ANDY	2018-01-11 05:52:58 PST	2018-01-11 05:52:58 PST	Down	OI
<input type="checkbox"/>	Events	Notes	IR809G-LTE-NA-K9+JMX2002X00T	2017-12-22 13:03:44 PST	2017-12-20 12:51:41 PST	Port Down	OI
<input type="checkbox"/>	Events	Notes	CISCO5921-K9+9IA8497ANDY	2017-12-21 16:34:19 PST	2017-12-21 16:34:19 PST	Port Down	OI
<input type="checkbox"/>	Events	Notes	CGR1120/K9+JAF1648BBGA	2017-12-18 13:15:46 PST	2017-12-18 13:15:46 PST	Port Down	OI

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.

Note: The amount of 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.

Viewing Device Severity Status on the Issues Status Bar

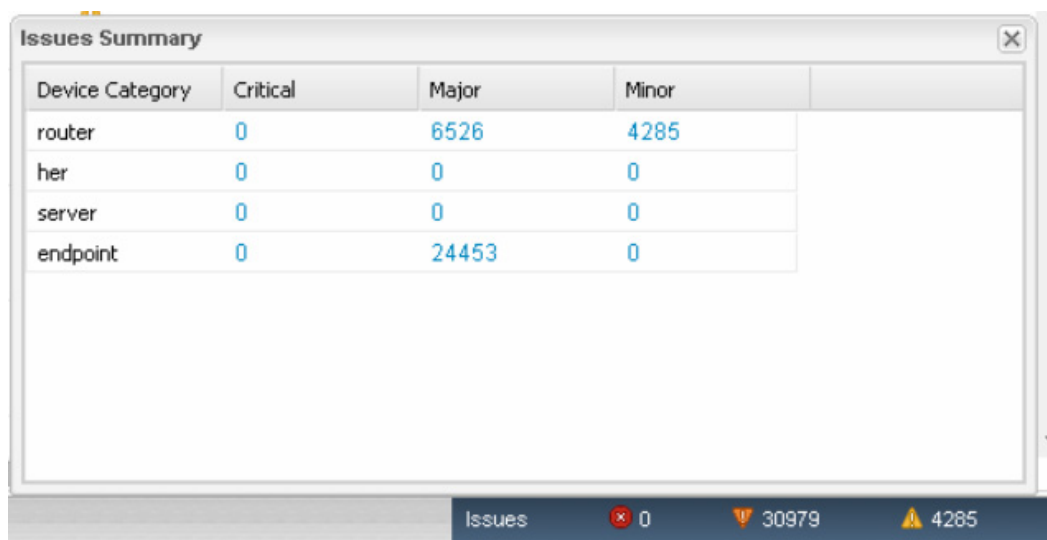
A tally of issues listed by severity for the selected devices displays in the Issues status bar in the bottom-right of the browser window frame (Figure 4). You can set the device types for issues that display in the Issues status bar in User Preferences.

Figure 4 Issues Status Bar



Click the Issues status bar to view the Issues Summary pane (Figure 5), 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.

Figure 5 Issues Summary Pane

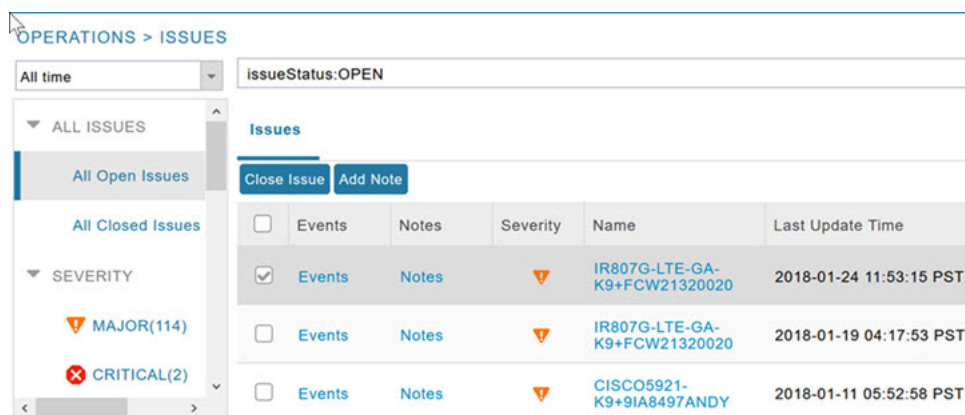


Adding Notes to Issues

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:

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.

2. Click **Add Note**.

The Add Note dialog displays.

3. Insert your cursor in the **Note** field and type your note.

4. Click **Add** when finished.

To edit an existing note in an issue:

1. Click the **Notes** link inline with the issue.

The Notes for Issues Name pane displays.

2. Click the pencil icon () at the right of the note that you want to edit.

3. Edit the note, and click **Done** when finished.

To delete a note from an issue:

1. Click the **Notes** link inline with the issue.

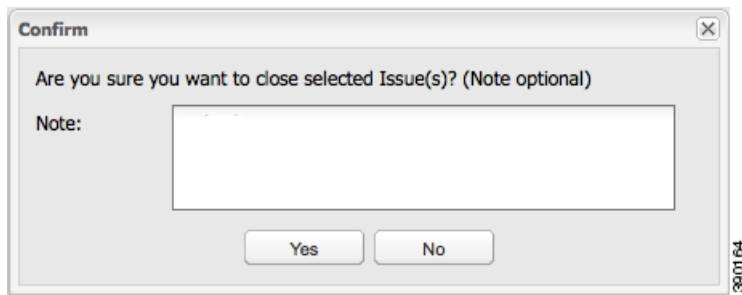
The Notes for Issues Name pane displays.

2. Click the red (X) icon at the right of the note.

3. Click **Yes** to confirm the deletion.

To add a note when closing an issue:

1. At the **Operations > Issues** page, check the box next to the issue you are closing.
2. Click **Close Issue** button that appears above the event listings.
3. In the Confirm dialog box, insert your cursor in the Note field and type the note text.



4. 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:

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](#)):

- 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 **Search Issues**.
- To list all closed issues, in the left pane, click **All Closed Issues**.

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:

1. Choose **OPERATIONS > Issues**.
2. Click **Show Filter**.
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
```

4. Click **Search Issues**.

The issues, if any, display in the Search Issues section (right pane).

OPERATIONS > ISSUES

All time [Hide Filter](#)

Issue Severity

Issues

Close Issue Add Note

Displaying 1 - 2 of 2

<input type="checkbox"/>	Events	Notes	Severity	Name	Last Update Time	Occur Time	Issue	Issue Status
<input type="checkbox"/>	Events	Notes	MAJOR	IR807G-LTE-GA-K9+FCW21320020	2018-01-24 11:53:15 PST	2018-01-24 11:53:15 PST	Down	OPEN
<input type="checkbox"/>	Events	Notes	MAJOR	IR807G-LTE-GA-K9+FCW21320020	2018-01-19 04:17:53 PST	2018-01-10 22:53:57 PST	Port Down	OPEN

5. Click the **Events** link to display events associated with an issue.

The Events for Issue Name pane displays all events for that device.

issueSeverity:MAJOR issueStatus:OPEN [Show Filter](#)

Events for Issue Name: Port Down EID: IR807G-LTE-GA-K9+FCW21320020 on: 2018-01-19 04:17:53 PST

Last Update Time: 2018-01-19 04:17:53 PST Occur Time: 2018-01-10 22:53:57 PST
 Name: Port Down EID: IR807G-LTE-GA-K9+FCW21320020 Status: OPEN Severity: MAJOR
 Message: Interface is down. Check event list for more details.

Time	Event Name	EID	Severity	Message
2018-01-10 22:53:57:188	Port Down	IR807G-LTE-GA-K9+FCW21320020	MAJOR	Tunnel123 interface is down.

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:

1. Choose **OPERATIONS > Issues**.
2. Locate the issue by following the steps in either the [Searching Issues Using Predefined Filters](#) or [Search Issues Using Custom Filters](#) section.
3. In the Search Issues section (right pane), check the check boxes of the issues to close.
4. Click **Close Issue**.

Note: You can also add a note to the issue at this time.
5. Click **Yes**.

Viewing Device Charts

- [Router Charts](#)
- [Mesh Endpoint Charts](#)

Router Charts

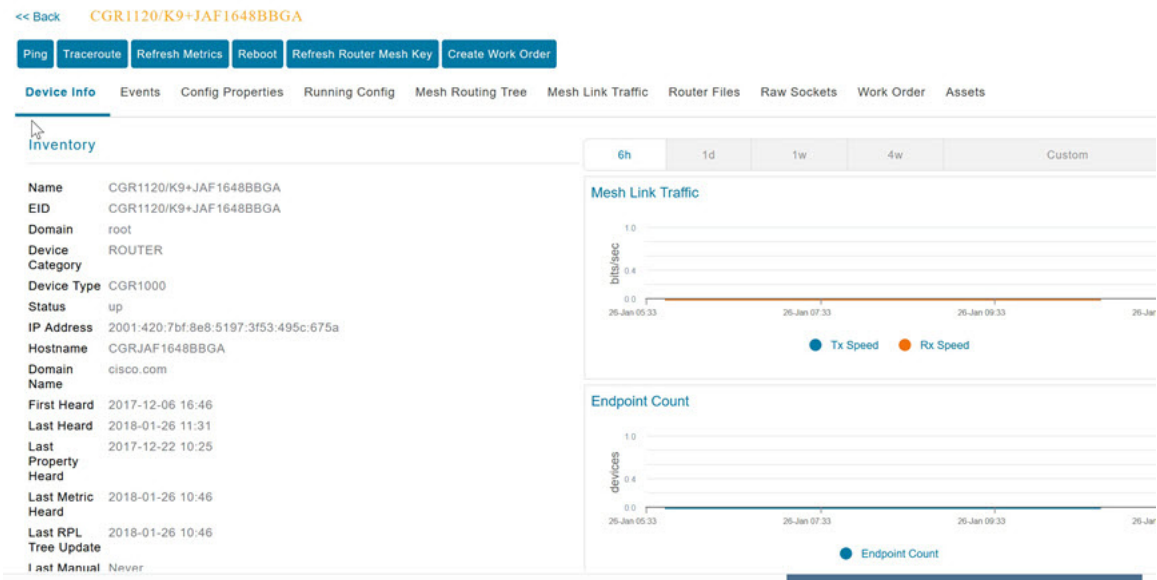
IoT FND provides these charts in the Device Info pane on the Device Details page for any router:

Table 2 **Device Detail Charts**

Chart	Description
Link Traffic	Shows the aggregated WPAN rate for a router over time.
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.
WPAN Traffic	(Master only) Shows Dual PHY WPAN traffic trends.
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.

[Figure 6](#) shows the Router Device Info page.

Figure 6 Router Device Page



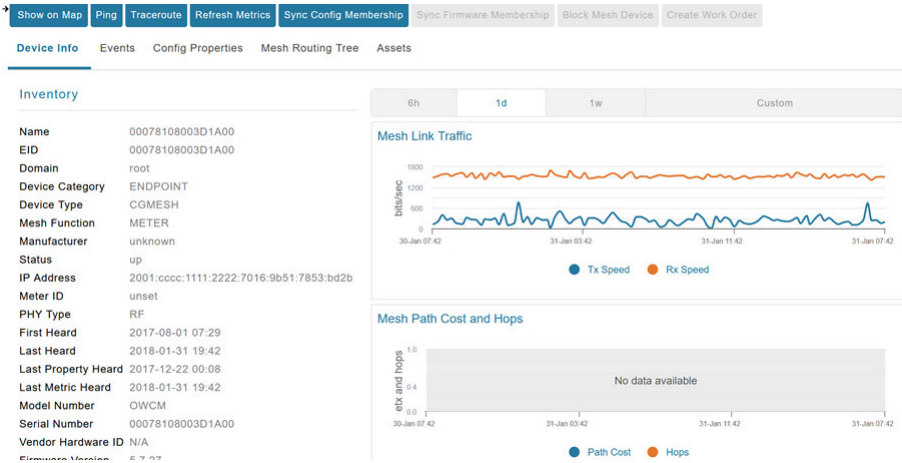
Mesh Endpoint Charts

IoT FND provides the charts listed in Table 3 in the Device Info pane on the Device Details page for any mesh endpoint.

Table 3 Device Detail Charts

Chart	Description
Link Traffic	Shows the aggregated WPAN rate for a router over time.
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 7 Mesh Endpoint Device Info Page (partial view)





Troubleshooting IoT FND

This section describes how to troubleshoot common IoT FND issues.

- [Tunnel Provisioning DHCP Configuration Issues](#)
- [Mesh Endpoint Registration Issues](#)
- [Recovering an Expired Database Password](#)
- [Unlocking the IoT FND Database Password](#)
- [IoT FND Service Will Not Start](#)
- [Exception in the server.log File on the IoT FND Server](#)
- [Resetting the root Password](#)
- [Second IoT FND Server Not Forming a Cluster](#)
- [IoT FND Service Restarts Automatically](#)
- [FAR Management Issues](#)
- [Mesh Endpoint Management Issues](#)

Note: Always reference the release notes for your IoT FND version.

Tunnel Provisioning DHCP Configuration Issues

If there is a problem allocating an address, IoT FND logs a Tunnel Provisioning Failure event. The log entry includes details of the error.

To monitor the address allocation process:

- Check the IoT FND server.log file to determine if IoT FND is sending a DHCP request during tunnel provisioning.
- Check your DHCP server log file to determine if the DHCP request from IoT FND reached the DHCP server.

If requests are not reaching the server:

- Ensure that the DHCP server address is correct on the **Provisioning Settings** page in IoT FND (**Admin > System Management > Provisioning Settings**).
- Check for network problems between IoT FND and the DHCP server.

If the DHCP server is receiving the request but not responding:

- View the DHCP server log file, and ensure that the DHCP server is configured to support requests from the link address included in the DHCP requests. The link address is defined in the tunnel provisioning template.
- Ensure that the DHCP server has not exhausted its address pool.

If the DHCP server is responding, but IoT FND is not processing the response:

- Ensure that the lease time is infinite. Otherwise, IoT FND will not process the response.
- View the DHCP server logs and IoT FND server logs for other errors.

Mesh Endpoint Registration Issues

To determine why MEs register with IoT FND, IoT FND collects the registration reason code from the MEs and logs events and the code with other relevant information as printed key value pairs to help diagnose registration issues.

Here is an example of a logged event:

```
?Event logged: Event(id=0, eventTime=1335304407477, eventSeverity=0, eventSource=cgmesh,
eventMessage=Mesh node registered due to cold boot: [lastReg: 0, lastRegReason: 1],
NetElement.id=10043, EventType.name=null, lat=1000.0, lng=1000.0, geoHash=null)
```

Table 1 lists reason codes for ME registration and corresponding event:

Table 1 Mesh Endpoint Registration Reason Codes

Registration Reason Code	Code	Event Type Name	Severity	Message	Description
REASON_UNKNOWN	0	unknownRegReason	INFO	Mesh node registered for unknown reason.	
REASON_COLDSTART	1	coldBoot	INFO	Mesh node registered due to cold boot.	The message includes the new IP address of the ME.
REASON_ADMIN	2	manualReRegistration	INFO	Mesh node registered due to manual registration.	The endpoint received an NMSRedirectRequest without a URL field.
REASON_IP_CHANGE	3	rejoinedWithNewIP	INFO	Mesh node registered with new IP address.	The message includes the new IP address of the ME.
REASON_NMS_CHANGE	4	nmsAddrChange	INFO	Mesh node registered due to NMS address change.	The IoT FND IP address changed OUTSIDE of an NMSRedirect (a new DHCPv6 option value was received).
REASON_NMS_REDIRECT	5	manualNMSAddrChange	INFO	Mesh node registered due to manual NMS address change.	Endpoint received an NMSRedirect request.
REASON_NMS_ERROR	6	nmsError	INFO	Mesh node registered due to NMS error.	Endpoint received an error from IoT FND.

In addition to generating events when MEs register with IoT FND, IoT FND also generates events after receiving a WPAN change TLV `WPANStatus`.

```
Event logged: Event(id=0, eventTime=1335304407974, eventSeverity=0, eventSource=cgmesh,
eventMessage=WPAN change due to migration to better PAN: [lastChanged: 0, astChangedReason: 4],
NetElement.id=10044, EventType.name=null, lat=1000.0, lng=1000.0, geoHash=null)
```

Table 2 lists reasons for ME WPAN changes and the corresponding event.

Table 2 Reasons for Mesh Endpoint WPAN Changes

Registration Reason Code	Code	Event Name	Severity Type	Description
IEEE154_PAN_LEAVE_UNKNOWN	-1	unknownWPANChange	MAJOR	WPAN change for unknown reason.
IEEE154_PAN_LEAVE_INIT	0	meshInit	N/A	No event is generated for this code.
IEEE154_PAN_LEAVE_SYNC_TIMEOUT	1	meshConnectivityLost	MAJOR	WPAN change due to mesh connectivity loss.
IEEE154_PAN_LEAVE_GTK_TIMEOUT	2	meshLinkKeyTimeout	MAJOR	WPAN change due to mesh link key timeout.
IEEE154_PAN_LEAVE_NO_DEF_ROUTE	3	defaultRouteLost	MAJOR	WPAN change for no default route.
IEEE154_PAN_LEAVE_OPTIMIZE	4	migratedToBetterPAN	MAJOR	WPAN change due to migration to better PAN.

For these events, the message includes the time elapsed since the ME left the network to when it rejoined. IoT FND displays the amount of time the ME was offline since the event was logged (for example, 4 hours 23 minutes ago).

Recovering an Expired Database Password

To recover from an expired password, run these commands:

```
su - oracle

sqlplus sys/cgmsDbAccount@cgms as sysdba
alter user cgms_dev identified by test;
alter user cgms_dev identified by password;
exit;
```

Unlocking the IoT FND Database Password

If you enter an incorrect IoT FND Database password multiple times, Oracle locks your user account. Unlock your password using the Oracle software, as shown in this example:

```
# su - oracle
# sqlplus sys/<database_password>@cgms as sysdba
alter user cgms_dev account unlock;
exit;
```

IoT FND Service Will Not Start

If the IoT FND service does not start:

1. Validate connectivity to the database:
 - a. Log in as root on the IoT FND server.
 - b. Enter the following at the command prompt:

```
service cgms status
```

- c. Verify the database server IP address and that IoT FND can connect to the database.
 - If the IP address is incorrect or if IoT FND cannot access the database, run **setupCgms.sh** and enter the correct values.
 - d. Run the **service cgms status** command and verify connectivity.
 - e. Start IoT FND.
2. Verify that the JRE version installed on the server is correct (see the System Requirements chapter).
 3. Verify that database migration was performed successfully.

Exception in the server.log File on the IoT FND Server

If there is an exception in the server.log file indicating that IoT FND could not open the cgms_keystore file, then the cgms_keystore password stored in the cgms.properties file on the IoT FND server is incorrect.

The password for the cgms_keystore file is encrypted and stored in the /opt/cgms/server/cgms/conf/cgms.properties file.

To encrypt or decrypt the password, use the /opt/cgms/bin/**encryption_util.sh** script.

Verify or update the password in the cgms.properties file, and if an update is required, restart IoT FND after modifying the password.

Resetting the root Password

If you forget the password of the IoT FND root user account, reset the password by running the /opt/cgms/bin/**password_admin.sh** script.

Second IoT FND Server Not Forming a Cluster

Typically, discovery of nodes in a IoT FND cluster is automatic. As long as the IoT FND servers are on the same subnet, they form a cluster.

If you install a IoT FND server and it does not join the cluster:

1. Verify that your servers are on the same subnet, can ping each other, and share the same cluster name.
2. Check the status of all members by running the /opt/cgms/bin/print_cluster_view.sh script.
3. Modify the cluster name, as follows:
 - a. Change the value of the HA_PARTITION_NAME parameter on all IoT FND cluster nodes, and then restart them.
 - b. Change the value of the UDP_MULTICAST_ADDR parameter (unique multicast address) to match on all nodes in the cluster.
 - c. Change the value of the CLUSTER_BIND_ADDR parameter to the interface to which you want the NMS to bind.
4. Verify that all the cluster nodes are configured to use NTP (see Configuring NTP Service)
5. Check the /etc/hosts file and verify that the IP address is correctly mapped to the hostname of the local server.

IoT FND Service Restarts Automatically

When the IoT FND services are started, the watchdog script is invoked. The watchdog script checks the health of the IoT FND services. If the watchdog script detects an anomaly, it logs the conditions in the `/opt/cgms/server/cgms/log/cgms_watchdog.log` file

The watchdog script tries three times to determine if the anomaly condition improved. If not, it restarts the IoT FND services automatically, unless the database has become unreachable. If the database is not reachable, the watchdog stops the IoT FND services. Check the log files, including `server.log`, to determine what is causing the restarts.

Manually disable the watchdog process by running the `/opt/cgms/bin/deinstall_cgms_watchdog.sh` script on the IoT FND server as root.

FAR Management Issues

This section presents common issues with FAR management and possible resolutions.

Certificate Exception

If this exception appears in the `server.log` file stored on the IoT FND server when a FAR attempts to register with IoT FND, the `cgms_keystore` file does not contain the CA server certificates or the CA certificates that were imported into the `cgms_keystore` file are incorrect:

```
SSLException: Received fatal alert: unknown_ca
```

For information about how to import certificates into the `cgms_keystore` file, see “Generating and Installing Certificates in the Cisco IoT FND Installation Guide, 4.0.x and greater.

FAR Keeps Reloading and Does Not Switch to the Up State

When a FAR is continuously reloading every time it contacts IoT FND, it could be because the configuration pushed to the FAR by IoT FND is not being applied successfully.

Check the `server.log` file on the IoT FND server for clues on the cause of the configuration push failure. Sometimes, typos in the in the Field Area Router Tunnel Addition template cause this failure (IoT FND does not provide template validation).

Note: When a FAR registers with IoT FND, IoT FND queries the FAR with `show` commands. IoT FND then configures the FAR based on the configuration commands in the Field Area Router Tunnel Addition template.

Other reasons for continuous reloads may be:

- A bad WAN link that drops packets and does not allow the registration to complete.
- Firewall issues. Ensure that the firewall allows traffic in both directions and that traffic to and from the correct ports is allowed to pass.

Incorrect FAR State in IoT FND

In IoT FND, a FAR might appear in a Down state even though you can ping and trace the route to it without a problem.

IoT FND manages the FAR via the IoT-DM service running on the FAR. So even though the FAR is pingable and reachable, it is important to verify that the jetty server and call home features are enabled on the FAR:

```
'show run callhome' should have 'enable' in the config and 'sh jvm status'
```

Mesh Endpoint Management Issues

This section presents common issues with ME management and possible resolutions.

Mesh Endpoints Not Registering with IoT FND

Verify that the MEs have joined the FAR and are pingable from IoT FND over IPv6. If they are pingable, verify the following:

- The clock is in sync.
- The DHCP server used by the MEs is programmed with the correct IoT FND IP address.
- The MEs are running an image compatible with the current version of IoT FND.
- If HSM is used, HSM must be online and responding correctly.

Licensing Issues

This section presents common issues with license management and possible resolutions.

Device Import Failure

The importing of devices into IoT FND is dependent on the number of allotted IoT FND server licenses.

Verify that your IoT FND server has the adequate license count available for the number and type of devices being imported into the IoT FND database.

Only unique device EIDs are allowed in IoT FND. Check that no one else imported this device EID in to IoT FND or is currently trying to import the same device EID. Verify that no other user is simultaneously importing the same device into IoT FND.

License File Upload Failure

An expired license file will cause an error. Check the license file validity and expiration date.