Release Notes for IoT Field Network Director, Release 3.2.x

Last Updated: June 29, 2017

First Published: January 31, 2017

This release note contains the latest information about using Release 3.2 user interface for the IoT Field Network Director (IoT FND), IPv6 mesh endpoints, Cisco 1000 Series Connected Grid Routers (CGR 1000 or CGR), Cisco 800 Series Integrated Services Routers (C800s), Cisco 500 Series WPAN Industrial Routers (IR 500), and Cisco 800 Series Industrial Integrated Services Routers (IR809 and IR829).

Note: IoT FND was previously named Connected Grid Network Management System (CG-NMS) for releases 2.x and 1.x.

Organization

This guide includes the following sections:

Conventions	Conventions used in this document.
New Features	New features in Release 3.2.
IoT FND Licenses	Summary of supported licenses for Release 3.2.
About Cisco IoT FND	Description of the IoT FND application.
System Requirements	System requirements for Release 3.2.
Installation Notes	Procedures for downloading software.
Important Notes	Notes about Release 3.2.
Limitations and Restrictions	Known limitations in IoT FND.
Caveats	Open and resolved caveats in Release 3.2.
Related Documentation	Links to the documentation associated with this release.

Conventions

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x	y	z }	Required alternative keywords are grouped in braces and separated by vertical bars.

Conventions	Indication
[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

New Features

Table 1 lists new features that are in IoT FND 3.2.x.

Table 1   New Features in IoT FND 3.2

Feature	Description	Minimum Release Number Required	Related Documentation
TLV 61 support on Itron OpenWay RIVA G-W (CSCvc76617)	Modifications made to use TLV 61 to read RSSI values for Itron OpenWay RIVA G-W (Gas-Water) endpoints rather than TLV 25.	3.2.0-182	For more information, see *Cisco IoT Field Network Director User Guide, Release 3.2* at: http://www.cisco.com/go/fnd
Itron OpenWay (OW) RIVA CAM management	Itron OpenWay RIVA CAM module, installed within the CGR 1000 routers, provides connectivity to the Itron OpenWay RIVA electric and gas-water devices. Within the IoT FND user interface, Itron CAM module is identified as: ■ CAM module=OW Riva CAM	3.2.0-170	
Itron OpenWay RIVA Electric device and Itron OpenWay RIVA G-W (Gas-Water) device management	Itron OpenWay RIVA devices are identified in the IoT FND user interface as: ■ CAM module: OW Riva CAM ■ Electric devices: OW Riva CENTRON ■ Gas and water devices: OW Riva G-W		
Cisco LoRaWAN module Embedded Event Manger (EEM) Applet Template	Embedded Event Manager EEM applet for LoRaWAN configuration can be pushed to the router from IoT FND to monitor the protocol status (Up/Down). See Managing External Modules in Managing Devices chapter.		
Band 26 support on the Cisco IR829	Cisco 829 Industrial Integrated Services Routers (IR829) support the following new SKUs: ■ IR829GW-LTE-SC-K9: Provides support for LTE band 26 in North America ■ IR829GW-LTE-LA-(Q/D/Z/F/K/C/F/S)-K9: Provides expanded LTE band support for Asia Pacific and Latin America. ■ IR829GW-LTE-EA-K9: Multi-carrier band support for North America and Europe. Information on the module can be found on the following pages: Field Devices, Modem list for IR800 (IR809/IR829), Field Devices, Firmware Image Update Page, Events and Issues.		

New Features

Table 1   New Features in IoT FND 3.2 (continued)

Feature	Description	Minimum Release Number Required	Related Documentation
Dual-active 4G/LTE radio support on Cisco IoT router modules to provide support for multiple carriers	Cisco routers IR829, CGR1000 (CGR1240, CGR1120) and Cisco 819 4G LTE ISRs (C819) each support a new dual-active radio module SKU: ■ IR829GW-2LTE-K9 ■ CGM-LTE-LA for CGR 1000 routers ■ C819HG-LTE-MNA-K9 Supporting routers (noted above) must have Cisco IOS Release 15.6(3)M1 or greater installed to support the module. Two modem support displays four cellular interfaces (cellular 0/0, cellular 1/0, cellular 1/0, cellular 1/1) for the devices, where the first digit represents the modem and the second digit indicates the Packet Data Network (PDN). *See* Cellular Link Metrics on the Device Detail page within the User Guide.	3.2.0-170	For more information, see *Cisco IoT Field Network Director User Guide, Release 3.2* at: http://www.cisco.com/go/fnd
IXM-LORA: IPSec Configuration between Cisco IOS and LoRaWAN modem	For an example tunnel script: See Managing Tunnel Provision chapter		
IXM-LORA: Modem Reboot	On the **Devices > Field Devices** page, a new Reboot Modem button allows reboot of the modem. An additional parameter Last Reboot Time displays in the Device Info panel for the modem. See Managing Device chapter.		
Reboot Router	On the **Devices > Field Devices** page, a new Reboot button allows reboot of the selected router. See Managing Device chapter.		
IR500: Reboot option	On the **Device Detail** page for IR500, you can reboot the device by selecting the **Reboot** button. The Last Reboot time displays under Mesh Device Health. See Managing Device chapter.		
NB API Enhancements to support Gateway as a Service (GaaS)	Additions to the Group Management template and reprovisioning actions of the NB API provide support for GaaS. See North Bound API User Guide for the Cisco IoT Field Network Director, Release 3.2		
Issues Export	On the **Operations > Issues** page, you can export all or query for specific issues to export to a CSV file.		

Table 1   New Features in IoT FND 3.2 (continued)

Feature	Description	Minimum Release Number Required	Related Documentation
New Role Support for Domain Users	On the **Admin > Users** page, you can now assign two new roles to the user: Router Operator and Endpoint Operator.	3.2.0-170	For more information, see *Cisco IoT Field Network Director User Guide, Release 3.2* at: http://www.cisco.com/go/fnd
Log Debug Info for Specific Routers or Endpoints	On the **Admin > Logging** page, you can query as many as 10 Device EIDs at a time. See Monitoring System chapter.		
Zero Touch Deployment (ZTD) Reprovisioning	Allows IoT FND to support ZTD reprovisioning actions over IPSEC tunnels for routers behind the NAT boundary. Routers must be running Cisco IOS.		
Groups Management	On the **Config > Groups** page, you can define groups for general multicast purposes. You can add devices to the Group by either the UI or CSV file import.		
IOx Firmware Update	On the **Config > Firmware Update** page you can upload IOx firmware images for CGR 1000 series routers.		
Tool for encryption of passwords after keystore update	Admin Tool script prompts user for old and new keystore details as part of the automatic conversion process.		

IoT FND Licenses

Table 2 provides a summary of licenses supported on IoT FND, Release 3.2.x. Contact your Cisco partner to obtain the necessary licenses.

Table 2   Summary of IoT FND Licenses

PID	License
L-IOTFND-C800	IoT FND device license for managing the Cisco 800 Series Integrated Services Routers.
L-IOTFND-CGR1K	IoT FND device license for managing CGR 1000 Series Connected Grid Routers.
L-IOTFND-IR509	IoT FND device license for managing Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers.
L-IOTFND-IR800	IoT FND device license for managing the IR800 Industrial Integrated Services Routers.
L-IOTFND-EP-1K	IoT FND device license for managing 1000 endpoints.
L-IOTFND-K9	IoT FND software license for bare-metal deployment (RPMs).
L-IOTFND-V-K9	IoT FND software license for virtual deployments (VMs)
L-IOTFND-LORAWAN	IoT FND software license for LoRaWAN module.

About Cisco IoT FND

The IoT Field Network Director (IoT FND) is a software platform to manage a multi-service network and security infrastructure for IoT applications such as smart grid applications including advanced metering infrastructure (AMI). 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.

Through the browser-based interface, utility operators manage and monitor devices in a Cisco 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 identified by model (for example, CGR1000, CGR1120, or CGR1240) on the Field Devices page.

- Cisco 800 Series Industrial Integrated Services Routers (IR 800s) are ruggedized small-form factor cellular routers for mobile/vehicle applications. IR829 include WiFi providing connectivity in non-carpeted IT spaces, industrials, utilities, transportation, infrastructure, industrial M2M application, asset monitoring, Smart Grid, and utility applications. These devices are referred to as FARs 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 IR 800 models: IR809 and IR829.

- Cisco 800 Series Integrated Services Routers (C800s) 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). These devices are referred to as FARs 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:

  - C819HG-4G-V-K9

  - C819HG-4G-A-K9

  - C819HG-U-K9

  - C819HGW-S-A-K9

  - C819H-K9

  - C819G-B-K9

  - C819G-U-K9

  - C819G-4G-V-K9

  - C819G+7-K9

- Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR500) supply RF mesh connectivity to IPv4 and serial Internet of Things (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 mesh endpoint devices can coexist on a network, but cannot be in the same device group (see Creating Device Groups and Working with Mesh Endpoint Firmware Images) or firmware management group. Refer to the following sections in the *IoT Field Network Director User Guide* for more information: "Creating Device Groups" and "Working with Mesh Endpoint Firmware Images" and "Configuring Firmware Group Settings".

- Cisco Interface Module for LoRaWAN is an extension module for the industrial routers, Cisco IR809 and IR829, and serves as carrier-grade gateways 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 800 Series Access Points are integrated access points on the Cisco 800 Series Integrated Services Routers (C800s). These access points are referred to as FARs in this document; and identified by product ID (for example, AP800).

   Note: Both the C819 and IR829 have embedded APs and we support management of those two APs.

■ Cisco ASR 1000 Series Aggregation Services Routers (ASRs) and Cisco ISR 3900 Series Integrated Service Routers (ISRs), referred to as *head-end routers* or HERs in this document.

■ Cisco IPv6 RF mesh endpoints (smart meters and range extenders).

   Note: CGRs, C800s, IR800s, IR500s and other types of mesh endpoint devices can coexist on a network, but cannot be in the same device group or firmware management group.

   The software features enterprise-class fault, configuration, accounting, performance, and security (FCAPS) functionality, as defined in the OSI Network Management reference model.

Cisco IoT Features and Capabilities

■ **Configuration Management** – Cisco IoT FND facilitates configuration of large numbers of Cisco CGRs, Cisco C800s, Cisco ASRs, and MEs. 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 C800s, Cisco IR800 (which has a different group for firmware management) and ME 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.

■ **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 and C800s, and prevents unauthorized access to Cisco CGRs, to provide secure communication between devices. Cisco IoT FND can execute CLI commands to provision secure tunnels between Cisco CGRs, Cisco C800s, Cisco IR800s and Cisco ASRs. Use Cisco 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 ME 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 Flex VPN**– For Cisco C800 devices and Cisco IR800 devices, DMVPN and Flex VPN 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.

- **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 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.

- **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.

- **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, Cisco C800, Cisco IR800, range extender, 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** – Connected Grid Endpoints (CGEs) implement a power outage notification service to support timely and efficient reporting of power outages. In the event of a power outage, CGEs perform the necessary functions to conserve energy and notify neighboring nodes of the outage. FARs relay the power outage notification to IoT FND, which then issues push notifications to customers to relate information on the outage.

- **Mesh Upgrade Support** – Over-the-air software and firmware upgrades to field devices such as Cisco CGRs and CGEs (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.

Related Products

In addition to Cisco IoT FND, you can use the following tools with the Cisco 1000 Series Connected Grid Routers:

Command Line Interface

Use the command line interface (CLI) to configure, manage, and monitor Cisco 1000 Series Connected Grid Routers. Learn more at www.cisco.com/go/cgr1000-docs

Cisco IoT Device Manager

The Cisco IoT Device Manager (IoT-DM or Device Manager) is a Windows-based application for field management of a single Cisco CGR. IoT-DM uses a local Ethernet or WiFi link to connect to the CGR. Learn more at www.cisco.com/go/cgr1000-docs

System Requirements

Table 3 lists the hardware and software versions associated with this release.

Note: For a large scale system, refer to Table 4 and Table 5 for scale requirements.

Table 3   Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems

Component	Minimum Hardware Requirement	Minimum Software Release and Requirements
Cisco IoT FND application server (or comparable system that meets the minimum hardware and software requirements)	■ Processor: – Intel Xeon x5680 2.27 GHz (64-bit) – 4 CPUs ■ RAM: 16 GB ■ Disk space: 100 GB ■ Hardware Security Module (HSM) or Software Security Module (SSM)	■ Red Hat Enterprise Linux 6.4 and above, 64-bit with all packages installed (software development and web server) See Table 5 on page 13 for suggested application server resource allocation profiles. ■ Internet connection When you access IoT FND from a client browser, the browser connects to the Internet to download the necessary data files from the GIS maps provider. ■ A license to use SafeNet for mesh endpoint security **Note:** IoT FND software bundle includes required Java version.
Cisco IoT FND TPS proxy	■ Processor: – Intel Xeon x5680 2.27 GHz (64-bit) – 2 CPUs ■ RAM: 4 GB ■ Disk space: 25 GB	■ Red Hat Enterprise Linux 6.4 and above with all packages installed (software development and web server) ■ Internet connection **Note:** IoT FND software bundle includes required Java version.

Table 3   Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems (continued)

Component	Minimum Hardware Requirement	Minimum Software Release and Requirements
Database server for IoT FND Scalable to 25 routers/10,000 endpoints with minimum hardware requirement. See Resource Management Guidelines for additional scale sizes.	■ Processor: Intel Xeon x5680 3.33 GHz (64-bit) ■ 2 CPUs ■ RAM: 16 GB ■ Disk space: 100 GB	**Note:** IoT FND 3.1.x supports both of the Oracle releases listed below. ■ Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production (with Patch 20830993) ■ Oracle 11g Enterprise Edition (11.2.0.3 64-bit version only) **Note:** Before installing Oracle, install the Linux packages referenced in "Installing the Linux Packages Required for Installing Oracle" in the Installing Cisco IoT FND chapter of the Cisco *IoT Field Network Director User Guide, Release 3.2.x* See Table 4 on page 13 for suggested Oracle Database server resource allocation profiles. ■ Red Hat Linux 6.4 and above, 64-bit with all packages installed (software development and web server)
Cisco IoT FND Client	The client must meet the following minimum requirements to connect to the IoT FND application server and view IoT FND displays: ■ Windows 7 or Win2000 R2 Server ■ RAM: 8 GB ■ Processor: 2 GHz ■ Resolution: 1024 x 768	■ Adobe Flash Version 9.0.115 or later (required for viewing charts) ■ Supported browsers: – Internet Explorer (IE): 11.0 – Mozilla Firefox: 3.5 or later – Windows 7 works with IE 11.0

Table 3   Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems (continued)

Component	Minimum Hardware Requirement	Minimum Software Release and Requirements
Cisco Network Registrar (CNR) (used as a DHCP server)	Server must have the following minimum requirements: ■ Free disk space: 146 GB ■ RAM: 4 GB (small network), 8 GB (average network), 16 GB (large network) ■ Hard drives: – SATA drives with 7500 RPM drive > 500 leases/second *or* – SAS drives with 15K RPM drive > 1000 leases/second	The following software environment must exist before installing Cisco Network Registrar, software release 8.2 on the server: ■ Operating System: Windows Server 2008 ■ Development Kit (JDK) Java SE Runtime Environment (JRE) 8.0 (1.8.0_65-b17) or equivalent Java Development Kit (JDK). ■ User interfaces: Web browser and command-line interface (CLI) (Browser versions listed below): – Internet Explorer (IE) 11.0, Mozilla Firefox 3.0 or later ■ CNR license. Contact your Cisco partner for the necessary license.
IoT Device Manager (IoT-DM or Device Manager)	Laptop running Device Manager must have the following: ■ Microsoft Windows 7 Enterprise ■ 2 GHz or faster processor ■ 1 GB RAM minimum (for potential large log file processing) ■ WiFi or Ethernet interface ■ 4 GB disk storage space ■ Windows login enabled ■ Utility-signed Certificate Authority (CA) and Client Certificate for router authentication (obtained from your IT department) ■ Customer-specific IT security hardening to keep the Device Manager laptop secure	■ Version 5.0.0.16
Cisco 1000 Series Connected Grid Router (CGR)	–	■ Cisco IOS Release 15.6(3)M1b ■ Cisco CG-OS Release CG4(5)
Cisco ISR 800 Series Integrated Services Router (C800)	–	■ Cisco IOS Release 15.6(3)M1

Table 3   Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems (continued)

Component	Minimum Hardware Requirement	Minimum Software Release and Requirements
Cisco 800 Series Access Points (AP800)	–	■ AP802: ap802-k9w7-tar.153-3.JBB.tar ■ AP803: ap1g3-k9w7-tar.153-3.JBB2.tar
Cisco 800 Series Industrial Integrated Services Router (IR800)	–	■ Cisco IOS Release 15.6(3)M1b
Cisco 3900 Series Integrated Service Router (ISR)	–	■ Cisco IOS Release 15.4(3)M ■ Cisco IOS Release 15.4(2)T
Cisco ASR 1001 or 1002 Aggregation Services Router (ASR) serving as a head-end router	–	■ Cisco IOS XE Release 3.17.02.S for Flex tunnels (IOS) ■ Cisco IOS XE Release 3.11S for Point to Point tunnels (CG-OS)
Note: ASRs and ISRs with different releases can co-exist on the network.		
Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR500)	–	■ Cisco IR509, DA Gateway device: Firmware version 5.6.10 ■ Cisco IR529, Range Extender: Firmware version 5.6.10
Cisco Connected Grid CG-Mesh Module and supported endpoints	–	■ Firmware version 5.6.10 when communicating with CGR 1000s or Cisco ASRs and the minimum Cisco IOS software versions recommended for these routers in these release notes
Cisco Connected Grid RF Mesh endpoints	–	■ Firmware version 5.6.10 when communicating with IR500
Long Range Wide Area Network (LoRaWAN) Interface Module for Cisco 800 Series Industrial Integrated Services Routers (IR800)	–	■ Cisco IOS 15.6(3)M1b
Hardware Security Module (HSM)	Luna SA appliance, with client software installed on the IoT FND application servers	Luna SA appliance: ■ Release 6.10.2 firmware **Note:** Contact SafeNet to determine if you can run a higher version. ■ Release 5.4.7-1 software, plus security patches Luna SA client software: ■ Release 5.4.7-1 software
Software Security Module (SSM)	■ RAM: 8 GB ■ Processor: 2 GHz ■ 2 CPUs	■ Red Hat Enterprise Linux 6.4 or 7.1, 64-bit with all packages installed (software development and web server)

Note: If deploying a IoT FND server cluster, all nodes in the cluster should run on similar hardware. Additionally, all nodes must run the same version of IoT FND.

Resource Management Guidelines

Virtual machine (VM) configuration workload characterization is important. When using multiple VMs on the same physical host, allocate resources so that individual VMs do not impact the performance of other VMs. For example, to allocate 4 VMs on a 8-CPU host, do not allocate all 8 CPUs to ensure that one (or more) VM does not use all resources.

Table 4 on page 13 lists example Oracle database server usage profiles for important resource parameters such as CPU, memory, and disk space.

Table 4   Oracle DB Server Hardware Requirements Example Profiles

Nodes (Routers/Endpoints)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
25/10,000	2	16	100
50/50,000	4	16	200
500/500,000	8	32	500
1,000/1,000,000	12	48	1000
2,000/2,000,000	16	64	1000
5,000/5,000,000	20	96	1000

Table 5 on page 13 lists example IoT FND Application server usage profiles for important resource parameters such as CPU, memory, and disk space.

Table 5   Application Server Hardware Requirements Example Profile for Routers and Endpoints

Nodes (Routers/Endpoints)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
25/10,000	2	16	100
50/50,000	4	16	200
500/500,000	4	16	250
1,000/1,000,000	8	16	250
2,000/2,000,000[1]	8	16	500
5,000/5,000,000[1]	8	16	500

1. Clustered installations.

Note: We strongly recommend RAID 10 for deployments of 2 million endpoints and above.

For Router Only Deployments

Information in Table 6 and Table 7 is relevant to Router Only deployments.

Table 6   Application Server Hardware Requirements Example Profile For Routers and LoRa Modules

Nodes (IR800/LoRa modules)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
10,000/30,000	4	24	100

Table 7   Database Server Hardware Requirements Example Profile For Routers and LoRa Modules

Nodes (IR800/LoRa modules)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
10,000/30,000	6	32	500

Installation Notes

The installation procedure for IoT FND comprises several tasks, as described in the *Cisco IoT Field Network Director User Guide, Release 3.x.* Contact your Cisco partner to obtain a copy of this guide.

You can also find details on upgrading from Oracle 11g to Oracle 12c for existing installations; and, instructions for installing Oracle 12c in new installations within the User Guide.

Important Notes

In Limitations and Restrictions, page 14 and Caveats, page 17, caveats that reference CG-NMS are also relevant to IoT FND. In cases where the caveat was first posted to CG-NMS, we left the CG-NMS reference.

OpenSSH Version

Since IoT FND is supported on a variety of Red Hat Enterprise Linux (RHEL) 5 Update releases, the OpenSSH version that comes with a given release might be an older version with known security holes. Consequently, we recommend ensuring that OpenSSH on the RHEL IoT FND server is up to date. On initial installation, upgrade the OpenSSH package in the IoT FND server to the latest version (6.4 or later).

Limitations and Restrictions

Cisco recommends that you review this section before you begin working with IoT FND. These are known limitations that will not be fixed, and there is not always a workaround for these issues. Some features might not work as documented, and some features might be affected by recent changes to the software.

■   **CSCtx50284**

   Symptom: CG-NMS failed to shut down cleanly. The Cisco CG-NMS `server.log` file included exceptions.

   Conditions: Occurred when the Cisco CG-NMS server was shut down or restarted using the Red Hat service commands **service cgms stop** or **service cgms restart** and Cisco CG-NMS internal server components shut down in an incorrect sequence.

   Exceptions might have also appeared in the `server.log` file if any Cisco CG-NMS logging category is set to "Debug" level, as at this level, exceptions that represent normal internal activity might have been logged.

   If the Cisco CG-NMS server was not commanded to shut down using the service commands, then check the `cgms_watchdog.log` to see if watchdog restarted Cisco CG-NMS. If watchdog restarted Cisco CG-NMS, then there was a notation in `cgms_watchdog.log` providing the reason watchdog was triggered.

If the shutdown cannot be explained, then the exceptions might have indicated why the server shut down, and should be reviewed by the Cisco Technical Assistance Center (TAC).

Workaround: There is no workaround for this issue.

■ **CSCty78770**

Symptom: If two or more devices have the same GPS coordinate (which is likely if two Cisco CGRs are on the same pole), the icon in the map shows the devices as a cluster even at maximum zoom in.

Conditions: This issue occurs when two devices of the same type have the same GPS location.

Workaround: There is no workaround for this issue.

■ **CSCtz29999**

Symptom: On the Devices List page under "WiMAX Link Info", the Base Station Identifier (BSID) field is not populated.

Conditions: The issue only occurs for WiMAX links.

Workaround: There is no workaround for this issue.

■ **CSCub90976**

Symptom: When configuring high availability (HA) on the secondary database at initial setup, the entire output of the database content copy is unexpectedly seen in the log output. Logging is inconsistent with logs when a new database is set up.

Conditions: The issue occurs when configuring or setting up a secondary CG-NMS database.

Workaround: There is no workaround for this issue.

■ **CSCuc17916**

Symptom: When reprovisioning or creating workorders for the Cisco CGR, a Cisco CGR SSID entry greater than 31 characters in the CSV import file does not throw an error during import, but creates other issues.

Conditions: The issue occurs when an SSID entry with more than 31 characters is found.

Workaround: Limit the number of characters to less than or equal to 31.

■ **CSCui54154**

Symptom: On the **Device > Routers** or **Devices > Field Devices** page in List view with routers selected, on the Config tab the Config Error Details column may contain a hyperlink to the error description. If the Config tab is exported using the Export CSV option, the Config Error Details column is not included in the exported CSV file.

Conditions: This issue occurs when trying to export the Config tab with routers selected.

Workaround: There is no workaround for this issue.

■ **CSCui54221**

Symptom: On the **Device > Routers** or **Devices > Field Devices** page in List view with routers selected, on the Firmware tab the Firmware Error Details column may contain a hyperlink to the error description. If the Firmware tab is exported using the Export CSV option, Firmware Error Details column is not included in the exported CSV file.

Conditions: This issue occurs when trying to export the Firmware tab with routers selected.

Workaround: There is no workaround for this issue.

- **CSCuj70073**

  Symptom: Deleting a large number of elements from CG-NMS takes a long time.

  Conditions: This issue occurs when you delete a large number of elements from CG-NMS and devices with issues are included in the operation. CG-NMS must lock all devices. Devices with issue rows in the NMS database increase the time of the delete operation.

  Workaround: There is no workaround for this issue.

- **CSCul02893**

  Symptom: The Confirm dialog box does not display to start an SD Card Password push.

  Conditions: This issue occurs during an SD card password enable or disable operation.

  Workaround: There is no workaround for this issue.

- **CSCul05847**

  Symptom: On the **Config > Device Configuration > Push Configuration** page during a push SD card password operation, the start and end times displayed are the same.

  Conditions: This issue occurs during an SD card password enable or disable operation.

  Workaround: There is no workaround for this issue.

- **CSCuo96482**

  Symptom: A CGR module hot swap causes a CG-NMS metric retrieval failure, and an error displays in CG-NMS during **show interfaces** command processing.

  Conditions: This issue occurs during CGR reprovisioning where a module in the CGR was just swapped.

  Workaround: There is no workaround for this issue. Avoid removing modules during CGR provisioning.

- **CSCuo96336**

  Symptom: A success message displays on metrics refresh although WSMA was timed out. No WSMA error displays.

  Conditions: This issue occurs when you click Refresh Metrics and CG-NMS successfully refreshes, but WSMA was timed out.

  Workaround: There is no workaround for this issue.

- **CSCur38441**

  Symptom: On the **Field Devices** page, in Map view with the Overlay option and a group selected, clicking a cluster icon displays the device count either as zero or an incorrect number.

  Conditions: This issue occurs with the overlay feature enabled and set to All or Associated Endpoints/Routers, and the zoom level set so that a single marker denotes a group of devices.

  Workaround: To display an accurate device count, zoom in until the icons no longer appear clustered and display as individual icons on the map.

- **CSCur44911**

  Symptom: During the ZTD process, illegal state exceptions display in the server logs indicating tunnel interface change traps occurred.

  Conditions: This issue occurs when you add a new interface on the router that CG-NMS did not detect. Exceptions display in the server log when CG-NMS receives traps from that interface.

Workaround: There is no workaround for this issue. Exceptions are not logged after CG-NMS detects the interface either during periodic inventory polling or user-triggered refresh metrics.

- **CSCuv32208**

   Symptom: IoT FND GUI shows the database (DB) server in "down" state when checked under "Servers" section. All FND operations work correctly and no side effects are observed as a consequence of this apparent "down" state of the DB server. The database is marked "up" on the IoT FND application server restart but is soon marked "down" after 15 minutes of startup.

   Conditions: This is caused under certain circumstances when periodic jobs responsible for updating the DB server status are stuck in the ACQUIRED state and never recover. This prevents the IoT FND application from updating the status of the DB server.

   Workaround: The following workaround requires access to the DB server.

   1. Stop the IoT FND application server.

   2. Log in to the DB server as *cgms_dev_user*.

   3. Update the State column for the CgnmsDbJobTrigger row in the QRTZ_TRIGGER tables from ACQUIRED to WAITING.

   4. Commit the transaction.

   5. Start the IoT FND application server.

- **CSCuy49541**

   Symptom: When navigating to the Firmware page, the left pane and right pane do not show correct data.

   Conditions: Navigating to the images tab before the firmware tab has finished loading.

   Workaround: Wait for firmware tab to complete loading before navigating to the images tab.

- **CSCuz13240**

   Symptom: Software Security Monitor (SSM) server cannot generate more than one custom certificate. When attempting to generate a second certificate, the script generates the keypair and a CSR without logging any error but the signature verification fails.

   Conditions: SSM attempts to generate a second custom certificate. Red Hat Enterprise Linux 7.x was in use.

   Workaround: There is no workaround.

Caveats

This section presents open and resolved caveats in this release and information on using the Bug Search Tool to view details on those caveats. Section topics are:

Open Caveats

- **CSCvb12088**

Symptom: Maps Overlay ALL Zoom In errors with IndexOutofBounds Exception for C800 and IR800 routers.

Conditions: When Zoom In is clicked on the Maps for Overlay all view of C800 and IR800 routers, the operation should be successful and no errors should be displayed in the logs.

Workaround: Select Overlay "None" for routers and view the device details or Select All FAN Devices and view the devices on the Map.

- **CSCvb12216**

  Symptom: Devices with no GPS co-ordinates are displayed on the FND Maps with random coordinates at Overlay "All" view.

  Conditions: When no coordinates are present for the device, it should not be shown on the Maps (in any view).

  Workaround: There is no workaround.

- **CSCvb15297**

  Symptom: After a database HA failover, the secondary database is not displayed on the FND UI.

  Conditions: When the DB Failover happens, the secondary DB should be listed in the Servers page of FND UI.

  Workaround: There is no workaround.

- **CSCvc92006**

  Symptom: IoT FND does not log off all active sessions under the same user after changing that user's password in order to regenerate new <Session ID>.

  Conditions: Log the same user into IoT FND on 2 different browsers. Change password from one browser. Observe that session is only forced to disconnect on the browser making the password change but not on the other.

  Workaround: After changing password, go to Admin > Active Sessions > Logout Users for all open sessions for the same user.

- **CSCvc92628**

  Symptom: The Itron OpenWay RIVA CAM module (Device Type ACT, Mesh Function: METER) and the Itron OpenWay RIVA Electric device (OW Riva CENTRON) devices act in both RF and PLC can have different metrics accordingly. For RF, the metric should be dbM and for PLC the metric should be in db micro volts (dbuv).

  Conditions: Navigate to the Device Details page, and select the Mesh Routing Tree tab.

  Workaround: There is no workaround.

Resolved Caveats

- **CSCvb15255**

  Symptom: For a firmware upgrade progress chart, the histogram's Y-axis grid line numbers are exactly one greater than the counts shown through the tooltips hovering over the bar. This anomaly is more apparent when lower number of devices are being plotted.

  Conditions: A firmware update job has been triggered and the user can see the progress of the job through the histogram chart which uses a logarithmic scale.

  Workaround: This issue is resolved in IoT FND Release 3.2.0-170.

- **CSCvb16125**

  Symptom: Not able to update CGR images through FND. Old images stay on the device.

  Conditions: Will not delete file bootflash:/managed/images/cgr1000-uk9.5.2.1.CG4.3.SPA.bin because it is referenced in bootflash:/express-setup-config.

  Workaround: This issue is resolved in IoT FND Release 3.2.0-170.

- **CSCvb54169**

  Symptom: When testing 2000 routers on FND we may see event not coming in.

  Conditions: Occurs when stress testing FND.

  Workaround: This issue is resolved in IoT FND Release 3.2.0-170.

- **CSCvb67946**

  Symptom: When logging in as a non-root user, user is not able to see the LoRa modem details.

  Conditions: Log in as non-root user and go to the LoRa details page.

  Workaround: This issue is resolved in IoT FND Release 3.2.0-170.

- **CSCvb79366**

  Symptom: When the Metrics are pulled in from the meters the formula used is different from the formula used when we pull it from the CGR RPL.

  Conditions: FND Meshpath cost calculation formula used is incorrect when metrics are pulled from CGR.

  Workaround: This issue is resolved in IoT FND Release 3.2.0-170.

- **CSCvc41317**

  Symptom: Failed upgrade.

  ```
  MigrationException: Migration to version A.3.0.1.20160205.01 failed! Please restore backups and
  roll back dat abase and code!
  12-01-2016 16:38:09 BRST: ERROR: Migration failed. See log file for more information.
  ```

  Conditions: Upgrading from IoT FND Release 2.1 to Release 3.0. Oracle DB running on Windows Server.

  Workaround: This issue is resolved in IoT FND Release 3.2.0-170.

- **CSCvc87094**

  Symptom: When "Install Guest OS from this bundle" is NOT checked, the GOS image is always upgraded.

Conditions: During Firmware Upgrade of a router from IoT FND, GOS image is always upgraded.

Workaround: This issue is resolved in IoT FND Release 3.2.0-180.

■ **CSCvd18949**

Symptom: No BPD EventReport - Low Battery event is seen.

Conditions: IoT FND 3.2.0-174 and below does not support BPD EventReport - Low Battery event.

Workaround: This issue is resolved in IoT FND Release 3.2.0-180.

■ **CSCvd18966**

Symptom: FND displays Wrong BPD Reg reason from TLV43. FND displays "registered for unknown reason."

Conditions: When BPD sends the Reg reason DodagParentChange in TLV43 FND displays "registered for unknown reason".

Workaround: This issue is resolved in IoT FND Release 3.2.0-180.

■ **CSCvd41672**

Symptom: Itron OpenWay RIVA G-W (Gas-Water) endpoint mesh link traffic chart does not show correctly.

Conditions: With the latest BACT firmware, FND does not show any mesh link traffic.

Workaround: This issue is resolved in IoT FND Release 3.2.0-180.

■ **CSCvd69836**

Symptom: Nullpointer exception is observed when cgms-keystore-updater script is run.

Conditions: When there are null values in the DB for certain passwords and the cgms-keystore-updater script is run, the nullpointer exception is seen and the conversion is reverted.

Workaround: This issue is resolved in IoT FND Release 3.2.0-180.

■ **CSCvd76983**

Symptom: Mesh Key Refresh job raises exception if one of the router's key refresh fails and the automatic mesh key refresh job does not iterate through the entire list of routers to finish the job.

Conditions: If an exception is thrown during Mesh key refresh on any router, the key refresh processing on other routers stop and does not iterate the list.

Workaround: This issue is resolved in IoT FND Release 3.2.0-180.

■ **CSCvd86124**

Symptom: During Periodic polling, FND sends setup commands for IOx which is extra unneeded traffic.

Conditions: IOX is configured during periodic poll.

Workaround: This issue is resolved in IoT FND Release 3.2.0-180.

■ **CSCvd86883**

Symptom: During registration of a router, if the cgna global gzip is not enabled, the cgna payload size is bigger. This configuration needs to be part of the default Device config template.

Conditions: During registration of a router, if the cgna global gzip is not enabled, the cgna payload size is bigger. This configuration needs to be part of the default Device config template.

Workaround: This issue is resolved in IoT FND Release 3.2.0-180.

Accessing the Bug Search Tool

You can use the Bug Search Tool to find information about caveats for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

- Internet connection

- Web browser

- Cisco.com user ID and password

To access the Bug Search Tool, use the following URL: https://tools.cisco.com/bugsearch/search

To search using a specific bug ID, use the following URL: https://tools.cisco.com/bugsearch/bug/*<BUGID>*

Related Documentation

Find Cisco 1000 Series Connected Grid Routers and IoT Device Manager documentation at:

www.cisco.com/go/cgr1000-docs

For information on additional systems referenced in this release note, see the following documentation on Cisco.com:

- Cisco ASR 1000 Series Aggregation Services Routers Configuration Guide

- Cisco 3945 Series Integrated Services Router

- Cisco 800 Series Integrated Services Routers

- Cisco 800 Series Industrial Integrated Services Routers

- Cisco 800 Series Access Points

- Cisco 500 Series WPAN Industrial Routers

- Cisco LoRaWAN Interface Module Hardware Installation Guide