Release Notes for IoT Field Network Director, Release 4.3

First Published: 2018-8-31
Last Updated: 2020-04-28

This release note contains the latest information about using the user interface for IoT Field Network Director (IoT FND), Release 4.3 to configure and manage IPv6 mesh endpoints, Cisco 1000 Series Connected Grid Routers (CGR 1000 or CGR), Cisco 800 Series Integrated Services Routers (C800), Cisco LoRaWAN IXM Gateway, Cisco 500 Series WPAN Industrial Routers (IR 500), Cisco 5921 (C5921) Embedded Service Routers, and Cisco 800 Series Industrial Integrated Services Routers (IR 807, IR 809 and IR 829), Cisco 1101 Industrial Integrated Services Router (IR1101), and Cisco Industrial Compute Gateway IC3000 Management.

The routers are easy to deploy and manage, with cutting-edge, scalable, multi-core separate data and control plane capabilities. and Cisco Industrial Compute Gateway IC3000 Management.

IoT Field Network Director (IoT FND) is a software platform that helps to enable a clear separation between communications network management and operational applications such as distribution management systems, outage management systems, and meter data management in utilities. Use the software to manage a multi-service network of routers or a combination of routers and endpoint devices deployed with end-to-end security for your specific use case.

IoT FND is highly secure, scalable, and modular. Its pluggable architecture can enable network connectivity to a multi-vendor ecosystem of legacy and next-generation IoT devices.

Listed below are documents that support this release:

- Cisco IoT FND 4.3.1 with Integrated Application Management with Postgres and Influx Database Deployment on OVA, VMware ESXi 5.5/6.0
- Cisco IoT Field Network Director Installation Guide-Oracle Deployment, Release 4.3.x
- IoT FND 4.3 Deployment on VMware ESXi 5.5 and 6.0
- Cisco IoT Field Network Director Post-Installation Guide-Release 4.3.x - High Availability and Tunnel Provisioning
- Cisco IoT Field Network Director User Guide, Release 4.3.x

You can find all of the docs above at the Support Documentation page for the IoT Field Network Director

Please refer to the Cisco IoT Field Network Director data sheet for an extensive list of the product capabilities and the required licenses to support specific platforms management by the FND application.

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

Be sure to refer to the following related CGR 1000 and NMS system documentation:

- Cisco IoT Device Manager, Release 5.4
- Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and Cisco Resilient Mesh Configuration Guide (Cisco IOS)

Organization

This guide includes the following sections:

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.
[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

Note: Do not use an underscore(_) in the FND hostname or OVA template names.

Note: For optimal performance, ensure that the network ping latency between the FND Application Server and Database Server is < 1ms.

Table 1 lists new platforms and features that are managed in IoT FND 4.3.

Table 1 New Features in IoT FND 4.3

Feature	Description	First IoT FND release support	Related Documentation
Cisco 1101 Industrial Integrated Services Router (IR1101) Management Support	The Cisco IR1101 Industrial Integrated Services Router is a next generation modular industrial router which has a base module with additional Pluggable Modules that can be added. The Pluggable Module provides the flexibility of adding different interfaces to the IR1101 platform, for example, a cellular module.	4.3.2-7	Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide
FND and Fog Director OVA software bundle for IC3000	You can manage IC3000 with an integrated FND and Fog Director OVA software bundle.	4.3.1-7	Cisco 3000 Series Industrial Compute Gateways
Device Contextual User Interface (UI) for Router Only, Gateway and AMI Deployments	For example, if you are configuring IR809/IR829 gateways or add a license for the IR800, only the related fields, device-specific details, groups or pages for those platforms appear on the user interface.	4.3.0-133	Cisco IoT Field Network User Guide, FND 4.3
View Device Health Permission	Use to limit the actions that a user can see or perform in FND. Items the user can select from a menu are in bold text and those menus the user cannot access are in faint, fine text. For example, in the CONFIG menu, a user with a Device Health permission can view details on Firmware Updates, Device File Management, Rules and Groups but cannot access the Device Configuration or Tunnel Provisioning pages.	4.3.0-133	Cisco IoT Field Network User Guide, FND 4.3

Table 1 New Features in IoT FND 4.3 (continued)

Feature	Description	First IoT FND release support	Related Documentation
Cisco Industrial Compute Gateway IC3000 Management, IOTFND-IC3000	IC3000 supports edge computing and communicates with IoT FND through the IOx application, Cisco Fog Director (FD). A subset of FD is provided. For FND management, you import IC3000 details using CSV files. You can perform the following IC3000 actions using the FD/FND APP Management page: DEVICES > FIELD DEVICES > APP. ■ Import APP ■ Install and uninstall image ■ Add or delete firmware CONFIG > FIRMWARE UPDATE IoT FND manages the following items for IC3000s: ■ Registration ■ Configuration ■ Refresh Metrics (On demand/Periodic) ■ Software Updates Users can initiate the following actions on the IC3000 through IoT FND: ■ Refresh Metrics ■ Reboot device DEVICES > FIELD DEVICES > APP	4.3.0-133	Cisco Fog Director Reference Guide, Release 1.7 Cisco 3000 Series Industrial Compute Gateways Cisco IoT Field Network Director, User Guide, Release FND 4.3.x
IR829M and IR829B Support	Two new IR800 Series Routers are supported on FND 4.3. Management features match those of the IR829G. DEVICES > FIELD DEVICES	4.3.0-133	Cisco IoT Field Network Director, User Guide, Release 4.3 Cisco IR829 Industrial Integrated Services Router Hardware Installation Guide
LoRWAN IXM Registration Support on CGR1240 and IR807	For the CGR1000, you can upload and enable LoRa Modem by employing LRR uploads (CGR) and for IR807 you can use existing template configurations for IR800. CONFIG > DEVICE CONFIGURATION CONFIG > DEVICE FILE MANAGEMENT	4.3.0-133	Cisco IoT Field Network Director, User Guide, Release FND 4.3.x

Table 1 New Features in IoT FND 4.3 (continued)

Feature	Description	First IoT FND release support	Related Documentation
CGR 1240 High Availability (HA) Reference Design to Maintain Connectivity to a Mesh Network	To ensure connectivity is maintained between CGR1240 and the mesh network, you can import a specified configuration via a CSV file into the CGR 1240. Please refer to the links noted in Related Documentation for details. HA involves deployment of two CGRs (each installed with a CGM-WPAN-OFDM module) with common switch management and FND management. DEVICES > FIELD DEVICES > WPAN HA	4.3.0-133	Cisco IoT Field Network Director Post-Installation Guide, Release 4.3.x-High Availability and Tunnel Provisioning
Zero Touch Deployment Enhancement	Changes entered into the ZTD Tunnel Provisioning script will now automatically update during bootstrap. No user-initiated reload required. Additionally, the status of the configuration update displays on the Device summary page. Statuses that display are: ■ Bootstrapping (displays when update is in process) ■ Bootstrapped (displays when process is complete) Supported for all router types: CGR1000, IR800 DEVICES > FIELD DEVICES	4.3.0-133	Cisco IoT Field Network Director Post-Installation Guide, Release 4.3.x-High Availability and Tunnel Provisioning
Northbound (NB) FSK Support	FSK10 support added for BACT and CAM devices to support CAM Star deployments where CAM is connected to BACT devices directly for densely populated topologies. See CAM Details page: Modulation Percent Usage Chart.	4.3.0-133	Cisco IoT Field Network Director, User Guide, Release FND 4.3.x
Controller BACT Support	FND now supports BACT controller devices along with existing BACT meters. BACT controllers operate on FSK 10kbps modulation. Note: Support for FSK 10kbps is introduced in this release.	4.3.0-133	Cisco IoT Field Network Director, User Guide, Release FND 4.3.x
CAM Details page	FSK 10kbps and FSK 15kbps modulation details are found on the Modulation Percentage Usage Chart of the CAM.	4.3.0-133	Cisco IoT Field Network Director, User Guide, Release FND 4.3.x
New Dashlet for IR500 Distribution of Modulation Across IR500.	New dashlet for IR500s: Distribution of Modulation Across IR500	4.3.0-133	Cisco IoT Field Network Director, User Guide, Release FND 4.3.x
New Endpoint Support	Two new mesh node network modules are introduced and managed as Endpoints: EV8KREF3 (Dual-Phy) and EV8KREF4 (RF only). Firmware images employ the same base names: EV8KREF3 and EV8KREF4 along with version numbers.	4.3.0-133	Cisco IoT Field Network Director, User Guide, Release FND 4.3.x

Table 1 New Features in IoT FND 4.3 (continued)

Feature	Description	First IoT FND release support	Related Documentation
Upgrade Router Firmware with Image Diff File for IR809 and IR829	Partial image file is sent to the router to reduce file size transferred across network. At Upload Image page: Select Type: IOS-IR800 Check box for option: “install patch for IOS and hypervisor from this bundle.”	4.3.0-133	Cisco IoT Field Network Director, User Guide, Release FND 4.3.x
Cisco Resilient Mesh Release 6.0 Support	**Note:** Cisco IOS Release 15.8(3) must be installed in the routers noted below for Mesh 6.0 feature support. Cisco Resilient Mesh Release 6.0 is supported on the following FND-managed platforms: ■ IR510 and IR530 routers ■ CGM-WPAN-FSK-NA and CGR WPAN-OFDM modules Specific Mesh 6.0 features include: ■ Cisco Ref 3&4 (Mesh6.0) ■ CoAP version 18 support (RFC 7252): An IETF Constrained Application Protocol (CoAP) as defined by the IETF CORE WG and will use port 61628. **Note:** FND 4.3 will continue to support the previous version of CoAP (Classic CoAP) and use port 61624. FND will automatically determine the CoAP protocol based on the port type required. No configuration required by the user. ■ For mesh firmware images, a Kernel Version displays at the CONFIG > FIRMWARE UPDATE > Images page. Version format displays for example: *<kernel version>(<build version>) such as 6.0 (6.0.19)* ■ New Firmware Display Format on the DEVICES > FIELD DEVICES > Device Info page for example: *Firmware Version: 6.0 (6.0.19)* ■ CGR and WPAN High Availability (HA)	4.3.0-133	Release Notes for Cisco Resilient Mesh Release 6.0 Release Notes for Cisco IOS Release 15.8(3)M Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and Cisco Resilient Mesh Configuration Guide (Cisco IOS) IR510 WPAN Gateway and IR530 WPAN Range Extender Hardware Installation Guide

Table 1 New Features in IoT FND 4.3 (continued)

Feature	Description	First IoT FND release support	Related Documentation
Cisco Resilient Mesh Release 6.0 Support (cont.)	■ Access Control List (ACL) configuration on IR510 to perform packet filtering for enhanced security by controlling which packets move through a network and limiting access of users and devices in the network.CONFIG > DEVICE CONFIGURATION > Edit Configuration Template page ■ Ability to monitor GPS info for IR510 by enabling GPS on the DEVICES > FIELD DEVICES page and pushing the configuration. You can view GPS details (location and time) for IR510 on its Device Info page under GPS Settings. ■ Adaptive Modulation Setting: New Adaptive option on the CONFIG > DEVICE CONFIGURATION > Edit Configuration Template page: Enable Interface ACL check box. ■ Field Devices Page Pop-up Chart shows Adaptive Modulation Change Over Time	4.3.0-133	Release Notes for Cisco Resilient Mesh Release 6.0 Release Notes for Cisco IOS Release 15.8(3)M Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and Cisco Resilient Mesh Configuration Guide (Cisco IOS) IR510 WPAN Gateway and IR530 WPAN Range Extender Hardware Installation Guide
Demo and Subscription Based Licenses for IC3000 and ESR5921	You can now view details on product licenses at the following pages in the IoT FND application for IC3000 and ESR5921. ADMIN > SYSTEM MANAGEMENT > LICENSE CENTER ■ To view a list of all licenses in use by a device against the total available for that device, select the License Summary tab at the License Center page. ■ To view a list of all active license files, select the License Files tab at the License Center page.	4.3.0-133	Cisco IoT Field Network Director, User Guide, Release FND 4.3.x
License Allocation per Domain	To view the license allocation (Assigned, Used, Available) for devices by domain, navigate to the page below: ADMIN > ACCESS MANAGEMENT > DOMAINS	4.3.0-133	Cisco IoT Field Network Director, User Guide, Release FND 4.3.x

Table 1 New Features in IoT FND 4.3 (continued)

Feature	Description	First IoT FND release support	Related Documentation
ESR 5921 Image and Device Type Support	ESR 5921 supports the following software images: ■ IOS-ESR5900-BASE (Cannot upgrade) ■ IOS-ESR5900-UNIVERSAL (Cannot downgrade to IOS-ESR5900-BASE or upgrade to IOS-SBR) ■ IOS-SBR (Supports universal-f image for Itron-based hardware containing the ESR5921. Image allows for upgrade and downgrade of software versions on the SBR.) Device Type for all is esr5900 Device Category for all is router CONFIG > FIRMWARE UPDATE	4.3.0-133	Cisco 5900 Series Embedded Services Routers
New OVA Software Bundle (Supported on new FND 4.3 installs only)	A new VMware OVA is now available for router only deployments with embedded FND and associated databases. This OVA cannot be used for AMI deployments (mesh). DEVICES > SERVERS > DB	4.3.0-133	Cisco IoT Field Network Director, User Guide, Release FND 4.3.x

IoT FND 4.3 Software Subscriptions

Table 2 Summary of IoT FND 4.3 Software Subscription Product IDs (PIDs)

Subscription PIDs	Description
IOTFND-SOFTWARE-K9	Top-level PID. Append this software entry with additional product entries noted below based on your network.
IOTFND-EP-1K	IoT FND device license for managing 1000 endpoints.
IOTFND-BEP-1K	IoT FND device license for managing 1000 battery endpoints.
IOTFND-CEP-1K	IoT FND device license for managing 1000 cellular endpoints.
IOTFND-CGR1000	IoT FND device license for managing CGR1000 routers.
IOTFND-ESR5921	IoT FND device license for managing ESR 5921 routers.
IOTFND-IR509	IoT FND device license for managing IR509 gateway routers.
IOTFND-IR800	IoT FND device license for managing IR800 gateway routers.
IOTFND-IC3000	IoT FND device license for managing IC3000 compute gateway routers.
IOTFND-C800	IoT FND device license for managing C800 routers.

IoT FND Perpetual Product IDs

Table 3 provides a summary of perpetual product licenses supported on IoT FND, Release 4.3..

Table 3 Summary of IoT FND Perpetual Product IDs

PID	License
IoT FND	Top-level perpetual product IDs (PIDs)
R-IOTFND-K9	IoT FND RPM distribution for bare metal deployment
R-IOTFND-V-K9	IoT FND OVA distribution for virtual machine deployment
L-IOTFND-EP-1K	IoT FND device license for managing 1000 endpoints
L-IOTFND-GIS-3YRS	License for GIS map
L-IOTFND-SBR	License for ESR 5921
L-IOTFND-CGR1K	IoT FND device license for managing CGR 1000 Series Connected Grid Routers
L-IOTFND-CEP-1K	IoT FND device license for managing 1000 cellular endpoints
L-IOTFND-IR509	IoT FND device license for managing IR509 routers
L-IOTFND-IR800	IoT FND device license for managing IR800 Industrial Integrated Services Routers
L-IOTFND-C800	IoT FND device license for managing Cisco 800 Series Integrated Services Routers
L-IOTFND-LORAWAN	IoT FND software license for LoRaWAN module
L-IOTFND-OPTIONKIT	IoT FND product license options for ordering additional device licenses outside of IoT FND

About Cisco IoT FND

The IoT Field Network Director (IoT FND) is a software platform that helps to enable a clear separation between communications network management and operational applications such as distribution management systems, outage management systems, and meter data management in utilities.The software features enterprise-class fault, configuration, accounting, performance, and security (FCAPS) functionality, as defined in the OSI Network Management reference model.

Through the browser-based interface, you can manage a multi-service network of routers or a combination of routers and endpoint devices such as:

- The IC3000 Industrial Compute Gateway (IC3000) is an edge computing platform which extends the cloud computing paradigm to the edge of the network. Instead of hosting applications in a remote data center, applications can now be hosted on the edge. The Cisco IC3000 Industrial Compute Gateway is fully supported by Cisco IoT Field Network Director for zero-touch deployment, lifecycle management, application management, monitoring, and troubleshooting securely at scale from a single pane of glass.
- The Cisco IR1101 Industrial Integrated Services Router is a next generation modular industrial router which has a base module with additional Pluggable Modules that can be added. The Pluggable Module provides the flexibility of adding different interfaces to the IR1101 platform.
- Cisco 800 Series Industrial Integrated Services Routers (IR800s) are ruggedized small-form factor cellular routers for mobile/vehicle applications. IR829 includes 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 IR800 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 devices:

  - 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) functions as mesh endpoints to provide 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, C800, IR800s, IR500s can coexist on a network, but cannot be in the same device group (see Creating Device Groups) or firmware management group. Refer to the following sections in the *IoT Field Network Director User Guide* for more information: “Creating Device Groups”, “Working with Mesh Endpoint Firmware Images” and “Configuring Firmware Group Settings”.

- 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.
- Cisco Interface Module for 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 800 Series Access Points are integrated access points on the Cisco 800 Series Integrated Services Routers (C800). 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 3900 Series Integrated Service Routers (ISRs) are referred to as *head-end routers* or HERs in this document.
- Cisco IPv6 RF mesh endpoints (smart meters and range extenders).

Cisco IoT FND Features and Capabilities

- **Configuration Management** – Cisco IoT FND facilitates configuration of large numbers of Cisco CGRs, Cisco C800s, Cisco ASRs, and 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 Management**– 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.
- **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 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.
- **Zero Touch Deployment** – Ease of deployment at scale with Zero-Touch Deployment (ZTD) of gateways and devices.
- **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 neighbors and establishes routes using ICMPv6 message exchanges. RPL manages routes based on the relative position of the endpoint 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.
- **Device Location Tracking** – For CGR 1000, C800, and IR800 devices, IoT FND displays real-time location and device location history.
- **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** – Cisco Resilient mesh Endpoints (RMEs) 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** – Allows 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 to manage the Cisco 1000 Series Connected Grid Routers (CGR1000), the Cisco 800 Series Industrial Integrated Routers (IR800), and the Cisco 500 Series WPAN Industrial Routers (IR500):

Command Line Interface

Use the command line interface (CLI) to configure, manage, and monitor the routers noted above.

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 router at a time. IoT-DM uses a local Ethernet or WiFi link to connect to the routers noted above.

System Requirements

Table 4 lists the hardware and software versions associated with this release.

Note: For a large scale system, refer to Table 5 and Table 7 for scale requirements.

Table 4 Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems

Component	Minimum Hardware Requirement	Software Release Requirements
Cisco IoT FND application server (or comparable system that meets the 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 7.5 and above, 64-bit with all packages installed (software development and web server) See Table 7 on page 17 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 (virtual cores) ■ RAM: 4 GB ■ Hard Drive Disk space: 50 GB	■ Red Hat Enterprise Linux 7.5 and above with all packages installed (software development and web server) ■ Internet connection **Note:** IoT FND software bundle includes required Java version.

Table 4 Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems (continued)

Component	Minimum Hardware Requirement	Software Release Requirements
Database server for IoT FND Scalable to 5,000/5,000,000 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: 32 GB ■ Disk space: 100 GB	■ Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production (with Patch 20830993) **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 Installation Guide, Release 4.3.* See Table 5 on page 17 for suggested Oracle Database server resource allocation profiles. ■ Red Hat Linux 7.5 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	When using FND 4.2 and higher, use Zingcharts for viewing charts. ■ Supported browsers: – Internet Explorer (IE): 11.0 – Mozilla Firefox: 63.x or later – Windows 7 works with IE 11.0
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 63.x or later ■ CNR license. Contact your Cisco partner for the necessary license.

Table 4 Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems (continued)

Component	Minimum Hardware Requirement	Software Release Requirements
IoT Device Manager (IoT-DM or Device Manager)	Laptop running Device Manager must have the following: ■ Microsoft Windows 7 Enterprise or Windows 10 ■ 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	■ IoT-DM 5.4
Cisco 1000 Series Connected Grid Router (CGR)	-	■ Cisco IOS Release 15.8(3)M0a ■ Cisco CG-OS Release CG4(5)
Cisco 5921 (C5921) Embedded Service Routers	-	■ Cisco IOS Release 15.8(3)M
Cisco ISR 800 Series Integrated Services Router (C800)	-	■ Cisco IOS Release 15.8(3)M0a
Cisco 800 Series Access Points (AP800)	-	■ AP802: ap802-k9w7-tar.153-3.JD.tar ■ AP803: ap1g3-k9w7-tar.153-3.JD.tar
Cisco 800 Series Industrial Integrated Services Router (IR800)	-	■ Cisco IOS Release 15.8(3)M0a
IR1101 Industrial Integrated Services Router	-	■ Cisco IOS-XE Release 16.10.1
Cisco IC3000 Industrial Compute Gateway	-	■ IC3000-K9-1.0.1.SPA **Note:** For IC3000 APP management, use Mozilla Firefox: 63.x or later
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)

Table 4 Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems (continued)

Component	Minimum Hardware Requirement	Software Release Requirements
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 and IR510, DA Gateway device: Firmware version 6.0.19 ■ Cisco IR529 and Cisco IR530, Range Extender: Firmware version 6.0.19
Cisco Resilient Mesh Module and supported endpoints	-	■ Firmware version 6.0.19 when communicating with CGR 1000s or Cisco ASRs and the minimum Cisco IOS software versions recommended for these routers in these release notes
Cisco RF Mesh endpoints	-	■ Firmware version 6.0.19 when communicating with IR500
Long Range Wide Area Network (LoRaWAN) Interface Module for Cisco 800 Series Industrial Integrated Services Routers (IR800)	-	■ Cisco IOS 15.8(3)M0a
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 7.5, 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 5 on page 17 lists example Oracle database server usage profiles for important resource parameters such as CPU, memory, and disk space

Table 5 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
6000/6,000,000	20	96	1000

Table 6 Tunnel Provisioning Server (TPS)

Nodes (Routers/Endpoints)	CPU (Virtual Cores)	Memory (RAM GB)	Hard Drive Disk Space (GB)
25/10,000	2	4	50
50/50,000	2	4	100
500/500,000	2	4	100
1,000/1,000,000	2	4	100
2,000/2,000,000	2	4	100
5,000/5,000,000	2	4	100
6000/6,000,000	2	4	100

Table 7 on page 17 lists example IoT FND Application server usage profiles for important resource parameters such as CPU, memory, and disk space.

Table 7 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	32	500
6000/6,000,000[1]	8	32	500

1. Clustered installations.

Note: RAID 10 is **mandatory** for deployments of 2 million endpoints and above. For 2 million endpoints, we recommend 16 Disks in RAID 10. For more than 2 million endpoints, we recommend 24 Disks in RAID 10. Disk Speed: 15000 RPM.

For Router Only Deployments

Information in Table 8 and Table 9 is relevant to Router Only deployments.

Table 8 Application Server Hardware Requirements Example Profile For Routers

Nodes (IR800)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
10,000	10	32	500

Table 9 Database Server Hardware Requirements Example Profile For Routers and LoRa Modules

Nodes (IR800/LoRa modules)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
10,000/30000	10	32	500

Installation Notes

The installation procedure for IoT FND comprises several tasks, as described in the Cisco IoT Field Network Director Installation Guide, Release 4.3.

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 Installation Guide.

Important Notes

Note: In the section, Caveats, page 18,any 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 (7.5 or later).

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:

APP Management Open Caveats

Table 10 Open Caveats in APP Management

Caveat Number	Description
CSCvm61319	Upgrade to ver 2 of the 90MB EFM app takes 6 min 38 sec whereas installation takes only 2 mins

FND Open Caveats

Table 11 Open Caveats in FND 4.3

Caveat Number	Description
CSCvt45004	Adding devices to groups via import file fails prior to creating groups

FND Resolved Caveats

Table 12 Resolved Caveats in Release 4.3

Caveat Number	Description
CSCvn08280	Unable to see firmware image add button
CSCvn36530	FND must check the IR1101's currently running version before proceeding with the firmware install

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:

- IoT Device Manager, 5.4
- Cisco ASR 1000 Series Aggregation Services Routers Configuration Guide

- Cisco 5921 Embedded Services Router
- 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
- Cisco Wireless Gateway for LoRaWAN
- IR1101 Industrial Integrated Services Router Hardware Installation Guide

No combinations are authorized or intended under this document.