Release Notes for IoT Field Network Director, Release 4.5.x

First Published: 2019-07-20

Last Modified: 2023-04-19

Release Notes for IoT Field Network Director, Release 4.5.x

Last Updated: 2020-06-29

First Published: 2019-07-20

This release note contains the latest information about using the user interface for IoT Field Network Director (IoT FND), Release 4.5 to configure and manage IPv6 mesh endpoints, Cisco 1000 Series Connected Grid Routers (CGR1120 or CGR1240 or cgr1000), Cisco 800 Series Integrated Services Routers (C800), Cisco LoRaWAN IXM Gateway, Cisco 500 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 Industrial Compute Gateway IC3000 Management and Cisco 1100 Industrial Integrated Services Router (IR1101).

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.

Documentation

Listed below are the documents that support this release:

- Cisco IoT FND 4.3.1 and greater with Integrated Application Management with Postgres and Influx Database Deployment on an OVA, VMware ESXi 5.5/6.0/6.5
- Cisco IoT FND Deployment on an Open Virtual Appliance, VMware ESXi 5.5/6.0/6.5
- Cisco IoT Field Network Director Installation Guide-Oracle Deployment, Release 4.3.x, 4.4.x, and 4.5.x.
- Cisco IoT Field Network Director Post-Installation Guide - Release 4.3.x, 4.4.x and 4.5.x- High Availability and Tunnel Provisioning
- Cisco IoT Field Network Director User Guide, Release 4.5.x

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.x
- Cisco Industrial Operations Kit User Guide, Release 2.0
- 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	Conventions used in this document.
New Features	New features in Release 4.5.
IoT FND Perpetual Product IDs	Summary of supported licenses for Release 4.5.
About Cisco IoT FND	Description of the IoT FND application.
System Requirements	System requirements for Release 4.5.
Important Notes	Notes about Release 4.5.
Caveats	Open and resolved caveats in Release 4.5.
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.
[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.

Conventions	Indication
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 transalton 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 name.

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

New Features in IoT FND 4.5 lists new platforms and features that are managed in IoT FND 4.5.

Table 1: New Features in IoT FND 4.5

Feature	Description	First IoT FND release support	Related Documentation
Support for 4096 bits key size for RSA certificates		4.5.x, 4.4.1	---

Feature	Description	First IoT FND release support	Related Documentation
IoT Device Agent (IDA) Integration	Support for Cohda Wireless MK5 Road-side Units (RSUs) with fiber connections using TLV files and API.	4.5.x	Cohda MK5 RSU

Feature	Description	First IoT FND release support	Related Documentation
Guided Tours		4.5.x	Cisco IoT Field Network Director User Guide, Release 4.5 See “Monitoring System Activity” chapter.

Feature	Description	First IoT FND release support	Related Documentation
	Provides a step-by-step path on how to configure specific items within the FND User Interface. Directions appear in pop-up windows that navigate you through the configuration process. Once you are on the desired configuration pages (noted below), select Guided Tours from the User drop-down menu, upper-right hand corner, to display a window with the available tours. Guided Tours supported: • Add Devices (DEVICES > FIELD DEVICES) • Device Configuration • Device Configuration Group Management • Tunnel Group Management • Tunnel Provisioning • Provisioning Settings • Firmware Update **Note** The Guided Tour feature must be enabled by the first-time FND root user that logs into the FND system before you		

Feature	Description	First IoT FND release support	Related Documentation
	can use the feature.		
Plug and Play (PnP) Support for Cisco Kinetic Gateway Management Module (GMM)	FND now supports PnP based bootstrapping on Kinetic GMM to streamline provisioning and provide ongoing visibility and control of Cisco Gateways (such as IR809 and IR829).	4.5.x	Cisco Kinetic See Resources summary on the Cisco Kinetic page link above
AP800 Firmware Upgrade Support During Zero Touch Deployment	New device properties supported on IR829 and Cisco 800 Series Integrated Services Routers (C800) routers only. CONFIG > DEVICE CONFIGURATION	4.5.x	Cisco IoT Field Network User Guide, FND 4.5
Google Map Snap to Road Support for IR800s	Allows you to improve location tracking accuracy for IR800 by entering the Google Map API Key on the Map Settings page. ADMIN > SYSTEM MANAGEMENT > SERVER SETTING	4.5.x	Cisco IoT Field Network Director User Guide, Release 4.5
Domain Name Support (DNS) Support in the IC3000 Local Manager (LM) User Interface	You can configure and manage the following items for a DNS server in the IC3000 LM user interface: - Add and configure server NTP SETTINGS > NTP SERVER: Add/Edit Settings page	4.5.x	Cisco IC3000 Industrial Compute Gateway Deployment Guide

Feature	Description	First IoT FND release support	Related Documentation
Bandwidth Efficient Software Transfer (BEST)	When updating an existing installed software base for IR510 and IR530 devices, IoT FND uploads only the new software updates rather than the full image using bsdiff and bspatch files.	4.5.x	Cisco IoT Field Network Director User Guide, Release 4.5
Oracle Real Application Clusters (RAC)	Oracle RAC supports clustering of multiple Oracle databases to appear as one to support high availability in the network. IoT FND can validate up to 250,000 endpoints.	4.5.x	Real Application Clusters Administration and Deployment Guide

Feature	Description	First IoT FND release support	Related Documentation
Mesh 6.0 and 6.1 Feature Support		4.5.x	Cisco IoT Field Network Director User Guide, Release 4.5

Feature	Description	First IoT FND release support	Related Documentation
	Wi-SUN 1.0 is supported on the IR509, IR510, IR529 and IR530 and on the OFDM WPAN module installed within CGR 1000 platforms. Summary of new features: • A new search parameter, Mesh Protocol, allows you to filter based on Wi-SUN or Pre-Wi-SUN mode. • Registration and Configuration Push Validation Notifications (Success or Failure) sent for IR500 devices and other CG-mesh endpoints. • A new Block Mesh Device option under More Actions menu, allows you to block and blacklist mesh endpoints (CG-mesh, IR509, IR510, IR529 and IR530) that you suspect are not valid endpoints within the WPAN. • A new search parameter, Mesh Protocol, allows you to filter based on Wi-SUN or Pre-Wi-SUN mode. • DSCP Markings Rule: Allows configuration of low, medium, and high precedence with a combination of 4 classes to provide 8		

Feature	Description	First IoT FND release support	Related Documentation
	assignable options for DSCP Marking Profiles including default user controlled options. (Previously, only three markings were supported). This feature is applicable to IR510 only. • DEVICES > FIELD DEVICES > ENDPOINTS • CONFIG > DEVICE CONFIGURATION		
Dashboard Page Enhancements	On the Endpoint Inventory chart and Endpoint states Over Time Chart, there is a new state: Registering. DASHBOARD	4.5.x	Cisco IoT Field Network Director User Guide, Release 4.5

Feature	Description	First IoT FND release support	Related Documentation
Zero Touch Deployment Enhancements for the Router Template for Greater Error Handling	Error handling enhancements for the router template include: • Automatic import of a SUDI certificate upon FND startup • Error handling checks and validation of the following items: Bootstrap and Configuration templates, ZTD properties and Keystore • Generating a sample csv file from the template • Saving template version history • A Tour wizard which validates configurations and settings used for bootstrapping DEVICES > FIELD DEVICES	4.5.x	Cisco IoT Field Network Director User Guide, Release 4.5

Table 2: Summary of IoT FND 4.4 Subscription Licenses (formerly known as Classic Licenses) 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.

Subscription PIDs	Description
IOTFND-ESR5921	IoT FND device license for managing ESR 5921 routers.
IOTFND-IR509	IoT FND device license for managing IR500 gateways and extenders.
IOTFND-IR800	IoT FND device license for managing IR800 routers.
IOTFND-IC3000	IoT FND device license for managing IC3000 industrial compute gateway routers.
IOTFND-C800	IoT FND device license for managing C800 routers.

Note You can also find a list of the Cisco IoT Field Network Director product IDs on theCisco IoT Field Network Director Data Sheet.

Table 3: Licenses Validated Against IoT FND 4.5.x

Subscription PIDs	Description
IOTFND-LORAWAN	License for managing LoRaWAN
IOTFND-EP-100	License for managing 100 endpoints.

IoT FND Perpetual Product IDs

Summary of IoT FND Perpetual Product IDs provides a summary of perpetual product licenses supported on IoT FND, Release 4.5. Contact your Cisco partner to obtain the necessary licenses.

Table 4: IoT Field Network Director Perpetual Product IDs

PID	License
IOTFND-SOFTWARE-K9	Top-level PID
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
IOTFND-IR509	IoT FND device license for managing IR500 gateways and extenders.
IOTFND-IR800	IoT FND device license for managing IR800 router
IOTFND-C800	IoT FND device license for managing C800 router

Summary of IoT FND Perpetual Product IDs provides a summary of perpetual product licenses supported on IoT FND, Release 4.4. Contact your Cisco partner to obtain the necessary licenses.

Table 5: 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-GIS-3YRS	License for GIS map
L-IOTFND-EP-1K	IoT FND device license for managing 1000 endpoints
L-IOTFND-GIS-3YRS	License for GIS map
L-IOTFND-EP-1K	IoT FND device license for managing 1000 endpoints
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-SBR	License for ESR 5921
L-IOTFND-IR509	IoT FND device license for managing IR500 gateways and extenders
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 (available in IXM-LPWA-800-16-K9 and IXM-LPWA-900-16-K9)
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.

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

- Cisco IR1101 Industrial Integrated Services Routers with Cisco IOS XE Software combine Internet access, comprehensive security, and wireless services (LTE Advanced 3.0 wireless WAN and 802.11ac wireless LAN) in a single, high-performance device.

- 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.
- 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, C800, 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”, “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 gateway 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).

Note CGRs, C800, 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 FND Features and Capabilities

- **Configuration Management** – Cisco IoT FND facilitates configuration of large numbers of Cisco CGRs, Cisco C800s, Cisco IR800s, 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 on groups of similar 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 routers.
- **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. 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 firmware upgrades to field devices such as IR500s 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

Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems lists the hardware and software versions associated with this release.

Note For a large scale system, refer to Oracle DB Server Hardware Requirements Example Profiles and Application Server Hardware Requirements Example Profile for Routers and Endpoints for scale requirements.

Table 6: 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 8 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.

Component	Minimum Hardware Requirement	Software Release Requirements
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 7.5 and above with all packages installed (software development and web server) • Internet connection **Note** IoT FND software bundle includes required Java version.

Component	Minimum Hardware Requirement	Software Release 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	

Component	Minimum Hardware Requirement	Software Release Requirements
		Note IoT FND 4.5 supports both of the Oracle releases listed below. • Oracle Database 18c Enterprise Edition (formerly named 12.2c) • Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64-bit 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 “Table 1: Minimum Hardware and Software Requirements for Oracle Install” in the following guide: Cisco IoT Field Network Director Installation Guide-Oracle Deployment, Releases 4.3.x, 4.4.x and 4.5.x See Table 7 of these release notes 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

Component	Minimum Hardware Requirement	Software Release Requirements
		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 rather than Adobe Flash. (Browsers will no longer support Flash beginning January 2021). • Supported browsers: • Mozilla Firefox: 63 or later **Note** IE 11.0 is not supported in FND 4.4.x, 4.5.x and 4.5.1. Microsoft Edge browser will be used in FND 4.6 and onwards.
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): • Mozilla Firefox 63 or later • CNR license. Contact your Cisco partner for the necessary license.

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 5.5
Cisco 1000 Series Connected Grid Router (CGR)	–	• Cisco IOS Release 15.8(3)M2
Cisco 5921 (C5921) Embedded Service Routers		• Cisco IOS Release 15.8(3)M2
Cisco ISR 800 Series Integrated Services Router (C800)	–	• Cisco IOS Release 15.8(3)M2
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)M2
Cisco 3900 Series Integrated Service Router (ISR)	–	• Cisco IOS Release 15.4(3)M • Cisco IOS Release 15.4(2)T

Component	Minimum Hardware Requirement	Software Release Requirements
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 IR 509 and IR510, DA Gateway device: Firmware version 6.1.27 • Cisco IR529 and IR530 Range Extender: Firmware version 6.1.27
Cisco Resilient Mesh Module and supported endpoints	–	• Firmware version 6.1.27 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 6.1.27 when communicating with IR500
Long Range Wide Area Network (LoRaWAN) Interface Module for Cisco 800 Series Industrial Integrated Services Routers (IR800)	-	• LoRa/IXM-LPWA version is 2.0.32
Hardware Security Module (HSM)	Luna SA appliance, with client software installed on the IoT FND application servers	Luna SA appliance: • Release 7.3 firmware **Note** Contact SafeNet to determine if you can run a higher version. • Release 7.3 software, plus security patches Luna SA client software: • Release 7.3 software

Component	Minimum Hardware Requirement	Software Release Requirements
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 7 lists example Oracle database server usage profiles for important resource parameters such as CPU, memory, and disk space.

Table 7: 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 8 lists example IoT FND Application server usage profiles for important resource parameters such as CPU, memory, and disk space.

Table 8: 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 RAID 10 is mandatory for deployments of 2 million endpoints and above.

For Router Only Deployments

Information in Application Server Hardware Requirements Example Profile For Routers and LoRa Modules and Database Server Hardware Requirements Example Profile For Routers and LoRa Modules is relevant to Router Only deployments.

Table 9: 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 10: 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

Important Notes

Note In the section,Caveats,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).

Limitations and Restrictions

Cisco recommends that you review this section before you begin working with IoT FND. These are known limitations, 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.

Feature	IoT FND Release	Upgrade Impact
Firmware Upgrade during PnP	4.4 onwards	The PnP work flow supports device upgrade only if the target image version is higher than the running (current) image version. If the target image runs same or lower version, then the device upgrade is skipped during the PnP work flow.
External DHCP support for tunnel provisioning	Applicable for all IoT FND releases	External DHCP is not supported for tunnel provisioning in the Postgres-OVA deployment.

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
- Resolved Caveats
- Accessing the Bug Search Tool

Open Caveats

Table 11: Open Caveats

Caveat Number	Description
CSCvq39879	IR510 IOX image schedule reload and install failed from FND
CSCvr04686, CSCvr54494	Some drop downs are broken in IE11. (**Note** IE is not supported in FND 4.4.x and later. Please Use Mozilla Firefox: 63 or later.)
CSCvt45004	Adding devices to groups via import file fails prior to creating groups.

Resolved Caveats

Table 12: Resolved Caveats, FND 4.5.1

Caveat Number	Description
CSCvo36661	FND's Device file management does not work with Sparrow (IR1101)
CSCvp30353	Firmware Upgrade fails with timeout exceptions on a slow cellular link and does not retry
CSCvq72024	NullPointerException - uploading firmware image to callisto (IC3000)
CSCvq78699	IC3000: Native docker apps from docker hub/registry not being exported as a tar.gz file
CSCvq79628	Bootstrapping fails in Easy mode - archive config not processed
CSCvq84841	IC3000: prefix config for ipv6 throw out error when pushing down the configuration
CSCvq86468	IC3000 (callisto) devices are not connecting back when upgrading from 4.4.0-79 to 4.5.1-6
CSCvq86541	Tunnel provisioning failing - ORA-01795: list > 1000 Fixed (4.5.1-8)
CSCvq99128	Firmware upload on IR800 with Diff upload option selected (4.5.1-9)

Table 13: Resolved Caveats, FND 4.5.0

Caveat Number	Description
CSCvn41785	Google maps API configuration is not documented
CSCvo03741	Monitor Only User: Permission denied for Isr3900 and Isr4000 device details page
CSCvo64275	Provide public accessible manual for setting up RSA and ECC CA and integrate it with IoT FND
CSCvp29143	Documentation regarding Google maps requirement points to non-working mailer
CSCvp44017	Not possible to deploy IOx app twice on same device
CSCvp44027	Not possible to change port mapping for IOx application
CSCvp67453	Kinetic GMM Firmware upgrade feature did not installed the correct version of IOx
CSCvq02832	traceroute command missing from FND Docker

Caveat Number	Description
CSCvq11552	First config push after registration doesn't correctly set tbit
CSCvq13643	Meet issue after FND upgrade the image to IR8x9

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 Industrial Operations Kit 2.0
- IoT Device Manager, 5.4
- Cisco ASR 1000 Series Aggregation Services Routers Configuration Guide
- Cisco 5921 Embedded Services Router
- Cisco 3000 Series Industrial Compute Gateways (IC3000)
- 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

No combinations are authorized or intended under this document.