Release Notes for IoT Field Network Director, Release 4.1.2

First Published: 2018-11-21
Last Updated: 2021-06-15

These release notes contains the latest information about using the user interface for the IoT Field Network Director (IoT FND) 4.1.x 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 Embedded Service Routers, and Cisco 800 Series Industrial Integrated Services Routers (IR 807, IR 809 and IR 829).

Note: IoT FND 4.1.1 was a bug fix only release (see Caveats Resolved in IoT FND 4.1.1.) It supports all of the features first introduced in IoT FND 4.1.0 as summarized In the New Features section below.

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

Documentation

Listed below are the two primary documents that support this release:

- Cisco IoT Field Network Director User Guide, Release 4.1.x
- Cisco IoT Field Network Director Installation Guide, Release 4.1.x

Please refer to the Cisco IoT Field Network Director data sheet for an extensive list of the product capabilities.

Be sure to refer to the following related 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 4.1.x.
IoT FND Perpetual Product IDs	Summary of supported licenses for Release 4.1.x.
About Cisco IoT FND	Description of the IoT FND application.
System Requirements	System requirements for Release 4.1.x.

Conventions	Conventions used in this document.
New Features	New features in Release 4.1.x.
Installation Notes	Procedures for downloading software.
Important Notes	Notes about Release 4.1.x.
Caveats	Open and resolved caveats in Release 4.1.x.
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.
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 platforms and features that are managed by IoT FND 4.1.x releases.

Table 1 New Features Introduced in IoT FND 4.1.0 and Supported in 4.1.2

Feature	Description	First FND release support	IoT FND 4.1 and Related Documentation
Support for Red Hat Enterprise Linux (RHEL) 7.5	Provides RHEL 7.5 support within IoT FND Release 4.1 software.	4.1.2-17	---
Day 0 Bootstrapping for Routers	Allows Cisco IR807, IR809, and IR829 routers operating with software that supports Plug and Play (PnP) to be deployed in the field without any bootstrap configuration. Minimum Cisco IOS software releases required: ■ IR807: ir800l-universalk9-mz.SPA.157-3.M0a.bin ■ IR 809: ir800-universalk9-bundle.SPA.157-3.M1.fc2 ■ IR 829: ir800-universalk9-bundle.SPA.157-3.M1.fc2	4.1.0	Managing External Modules: LoRaWAN Gateway Cisco IR807 Industrial Integrated Services Router Software Configuration Guide: Plug and Play Cisco IR800 Integrated Services Router Software Configuration Guide (IR809, IR829)
New Operating Modes for IoT FND	You can configure FND to operate in two additional modes: - Demo mode: Allows you to quickly bring up routers and set up a small network to support demonstrations without having to configure SSL certificates. - Bandwidth optimization mode: Allows transmission of periodic metrics across HTTP versus HTTPS to optimize bandwidth.	4.1.0	See the “Demo and Bandwidth Operation Modes” section within the Managing Devices chapter in the Cisco IoT Field Network Director User Guide, Release 4.1.x
Cisco 4000 Series Integrated Services Routers (ISR 4000) Support	The 4000 Series runs Cisco Intelligent WAN (IWAN) and provides a comprehensive set of traffic control and security features that support branch deployments. DEVICES > Head-end Routers	4.1.0	Cisco 4000 Series Integrated Services Routers Managing Head-End Routers Device Properties

Table 1 New Features Introduced in IoT FND 4.1.0 (continued)and Supported in 4.1.2

Feature	Description	First FND release support	IoT FND 4.1 and Related Documentation
Cisco Industrial Integrated Services Router, IR807 Support	IR807 is a highly compact, low-power industrial router for install within industrial applications (distribution automation for utilities, transportation, manufacturing) and remote asset management across the extended enterprise.	4.1.0	Cisco IR807 Industrial Integrated Services Router Software Configuration Guide Managing Devices: Managing Routers Managing Firmware Upgrades: Uploading a Firmware Image to a Router Group Monitoring System Activity: Search Issues Using Custom Filters
ESR 5921 Embedded Services Router Firmware Upgrade	You can now upgrade ESR 5921 firmware using IoT FND. Device Type: SBR Device Category: router CONFIG > FIRMWARE UPDATE	4.1.0	Managing Firmware Upgrades: Uploading a Firmware Image to a Router Group Cisco 5921 Embedded Services Router
Health tab for Endpoints	You can display Health parameters on the Health tab, when you select any ENDPOINT device group (except Root OW Riva CAM) in the Browse Devices pane when viewing the Devices > Field Devices page. Heath Tab parameters include: Hops, Path Cost, RSSI(dBm), Mesh Parents, Mesh Descendants, Intra Pan Migrations/day (per day), Inter Pan Migrations/day, and Missed Periodic Reads/day. DEVICES > FIELD DEVICES	4.1.0	Managing Endpoints: Viewing Endpoints in Default View
Standalone mode for LoRaWAN IXM Gateway	When configured for standalone mode, you can view FPGA information on the Device Details page and active tunnel information on the Operations page. DEVICES > FIELD DEVICES OPERATIONS > TUNNEL STATUS	4.1.0	Cisco Wireless Gateway for LoRaWAN Managing the Cisco Wireless Gateway for LoRaWAN
Sub Profiles for IR510 WPAN Industrial Router Gateway Configuration	You can associate one or more profiles (MapT, Nat44, and/or Serial) to IR510 using the Configuration Template. CONFIG > DEVICE CONFIGURATION	4.1.0	Managing Cisco IR510 WPAN Industrial Router
Read-Only Monitoring Mode Option	Allows the administrator to limit what some users can view on specific user interface pages of FND.	4.1.0	Managing User Access:System-Defined Roles

Table 1 New Features Introduced in IoT FND 4.1.0 (continued)and Supported in 4.1.2

Feature	Description	First FND release support	IoT FND 4.1 and Related Documentation
Work Order and Asset Enhancements	You can access Work Order and Assets pages from the CGR1000 and IR800 Device Detail pages. At the C800 Device Detail page, you can access Assets only. You can add notes to a Work Order by selecting the (+) icon on the Work Order page. You can add and delete Work Orders from the Operations > Work Orders page. DEVICES > FIELD DEVICES OPERATIONS > WORK ORDERS	4.1.0	Managing Devices: Overview Cisco IoT Device Manager Installation and User Guide, Release 5.2

IoT FND 4.1.x Software Subscriptions

Table 2 Summary of IoT FND 4.1.x 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 router.
IOTFND-IR509	IoT FND device license for managing IR509 gateway router.
IOTFND-IR800	IoT FND device license for managing IR800 gateway router.
IOTFND-C800	IoT FND device license for managing C800 router.

IoT FND Perpetual Product IDs

Table 3 provides a summary of perpetual product licenses supported on IoT FND, Release 4.1.x. Contact your Cisco partner to obtain the necessary licenses.

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

Table 3 Summary of IoT FND Perpetual Product IDs

PID	License
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 Cisco® IoT Field Network Director (FND), the operating system for a multi-service Field Area Network (FAN), is a software platform that manages multi-service networks of Cisco industrial, connected grid routers, and endpoints.

Features that distinguish the IoT FND are as follows:

- Ease of deployment at scale with Zero-Touch Deployment (ZTD) of gateways and devices
- Secure and scalable end-to-end enrollment and management of these gateways and devices
- Optimized for operation in constrained bandwidth network
- Ease of use with an intuitive web interface and GIS map visualization and monitoring
- Rich set of northbound APIs for third-party integration

IoT FND is essential to the success of Internet-of-Things (IoT) solution deployments: Advanced Metering Infrastructure (AMI), transportation, Distribution Automation (DA), fleet management, asset tracking, and LoRaWAN infrastructures. It is a proven system on which many of our customers rely every day for their operation to deliver critical infrastructure services to millions of their customers.

Cisco IoT Field Network Director is built on a layered system architecture to enable clear separation between network management functionality and applications in fleet management, asset tracking, and utility, such as a Distribution Management System (DMS), Outage Management System (OMS), and Meter Data Management (MDM). This clear separation between network management and applications helps customers to deploy IoT projects incrementally, for example, in utilities with AMI to be extended into DA by using a shared multi-service network infrastructure and a common network management system across various utility operations. Further, a northbound API from the IoT Field Network Director allows various applications to pull appropriate, service-specific network communications data from a shared, multi-server communication network infrastructure.

Through the IoT FND browser-based interface, you can manage and monitor 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 (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) 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 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 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 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 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 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** – 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 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.
- **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.
- **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 6 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 6 on page 15 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 7.5 and above with all packages installed (software development and web server) ■ Internet connection **Note:** IoT FND software bundle includes required Java version.
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 4.1.0 supports both of the Oracle releases listed below. ■ 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 4.1.0.* See Table 5 on page 14 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)

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

Component	Minimum Hardware Requirement	Software Release Requirements
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
Cisco Network Registrar (CNR) (used as a DHCP server) **Note:** CNR is only required for utility deployments.	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.

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) **Note:** Manages utility deployments only.	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 5.2
Cisco 1000 Series Connected Grid Router (CGR)	-	■ Cisco IOS Release 15.8(3)M0a ■ Cisco CG-OS Release CG4(5)
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
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 5.7.27 ■ Cisco IR529, Range Extender: Firmware version 5.7.27

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

Component	Minimum Hardware Requirement	Software Release Requirements
Cisco Connected Grid CG-Mesh Module and supported endpoints	-	■ Firmware version 5.7.27 when communicating with CGR 1000s or Cisco ASRs and the minimum Cisco IOS software versions recommended for these routers in these release notes
Cisco Connected Grid RF Mesh endpoints	-	■ Firmware version 5.7.27 when communicating with IR500
Long Range Wide Area Network (LoRaWAN) Interface Module for Cisco 800 Series Industrial Integrated Services Routers (IR800)	-	■ 15.8(3)M0a
Hardware Security Module (HSM)	See the Hardware Security Module (HSM) Minimum Hardware and Software Requirements, page 13 section below.	
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.

Hardware Security Module (HSM) Minimum Hardware and Software Requirements

The following are the minimum hardware requirements for Cisco IoT FND and Supporting systems:

Luna SA appliance, with client software installed on the IoT FND application servers.

Note: When upgrading from FND 4.1.2 to 4.3, follow these steps:
(**IMPORTANT**: Upgrades from FND 4.4.0 and greater require Lunaclient 7.3. Refer to the relevant FND release note for those upgrades).

a) Enter the following backup commands:

```
cp /opt/cgms/jre/lib/ext/LunaProvider.jar /opt/cgms/jre/lib/ext/LunaProvider.jar_bkup09242020

cp /opt/cgms/jre/lib/ext/libLunaAPI.so /opt/cgms/jre/lib/ext/libLunaAPI.so_bkup09242020

cp /opt/cgms-tools/jre/lib/ext/LunaProvider.jar
/opt/cgms-tools/jre/lib/ext/LunaProvider.jar_bkup09242020

cp /opt/cgms-tools/jre/lib/ext/libLunaAPI.so /opt/cgms-tools/jre/lib/ext/libLunaAPI.so_bkup09242020
```

b) Copy these files from SafeNet to replace in cgms directory:

```
cp /usr/safenet/lunaclient/jsp/lib/LunaProvider.jar /opt/cgms/jre/lib/ext/
To overwrite Type yes

cp /usr/safenet/lunaclient/jsp/lib/libLunaAPI.so /opt/cgms/jre/lib/ext/
To overwrite Type yes
```

c) Copy these files from SafeNet to replace in the cgms-tools package to facilitate csmp requests later:

```
cp /usr/safenet/lunaclient/jsp/lib/LunaProvider.jar /opt/cgms-tools/jre/lib/ext/
To overwrite Type yes

cp /usr/safenet/lunaclient/jsp/lib/libLunaAPI.so /opt/cgms-tools/jre/lib/ext/
To overwrite Type yes
```

d) Verify NTLS connection on CMD:

```
netstat -n |grep 1792
tcp 0 0 10.142.229.16:45994 10.142.104.177:1792 ESTABLISHED
```

e) Verify CSMP certificate in FND user interface by logging into FND and then go to:

Admin> Certificates> Certificate for CSMP

The following are the minimum software requirements for Cisco IoT FND and Supporting systems:

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

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 14 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
6,000/6,000,000	24	96	1000

Table 6 on page 15 lists example IoT FND Application server usage profiles for important resource parameters such as CPU, memory, and disk space.

Table 6 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
6,000/6,000,000[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 32 Disks in RAID 10. Disk Speed: 15000 RPM.

Table 7 Tunnel Provisioning Server (TPS)

Nodes Routers/Endpoints	CPU (Virtual Cores)	Memory (RAM GB)	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
6,000/6,000,000	2	4	100

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 and LoRa Modules

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

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)
10,000/30,000	6	32	500

Installation Notes

The installation procedure for IoT FND comprises several tasks, as described in the *Cisco IoT Field Network Director Installation Guide, Release 4.1.0*. 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 Installation Guide.

Important Notes

Note: In the section, Caveats, page 17,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).

Enhancements in Release 4.1.2

- CSMP processing rate is greater than 35 ms. (CSCvh97478)
- Ability to customize line width for showing RPL links on map (CSCvk08437)
- Make the number of threads for processing metrics configurable. (CSCvk61896)
- Make ASR Polling interval configurable. (CSCvk69484)

  The ASR polling interval is now user configurable. This enhancement applies to all HER types.
- Not locking DB rows for issues/events. This impacts only when there is more than one app server (CSCvk69509)
- Implement heartbeat for ASR (CSCvm36042)

  FND is enhanced to implement heartbeat mechanism with ASR (HER).
- Provide a confirmation prompt to alert user about delay in listing large number of events.

When a user selects a time duration that will result in more than 50 million events, a confirmation prompt will be displayed to alert user of delay in listing the events. User can choose to proceed or cancel the selection.

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, page 17
- Resolved Caveats, page 17
- Accessing the Bug Search Tool, page 20

Open Caveats

There are no known open caveats.

Resolved Caveats

Caveats Resolved in IoT FND 4.1.2

- CSCvj65725

  Symptom: FND failed to add audit logs into database due to audit log message ID value being larger than maximum integer value.

  Conditions: Every time FND restart, the audit log message ID will move to a new starting number. If FND is restarted frequently, the audit log message ID could become larger than the maximum value allowed in the database table definition.

  Workaround: This issue is resolved in IoT FND Release 4.1.2.

- CSCvj82286

  Symptom: In FND maps, devices that function as extenders do not show up on the maps.

  Conditions: This issue occurs with devices that are listed as extenders.

  Workaround: This issue is resolved in IoT FND Release 4.1.2.

- CSCvk08435

  Symptom: Mesh links on maps are taking long to load when clicked on router.

  Conditions: This issue occurs when viewing RPL links in maps for a router.

  Workaround: This issue is resolved in IoT FND Release 4.1.2.

- CSCvk29259

  Symptom: Observing the OutofMemory exception and XARecoveryModule exceptions in FND server.logs file.

  Conditions: None.

  Workaround: This issue is resolved in IoT FND Release 4.1.2.

- CSCvk32730

  Symptom: Application server shows 90% CPU usage.

  Workaround: This issue is resolved in IoT FND Release 4.1.2.

- CSCvk74663

  Symptom: The periodic router metrics processing in a scale system is slowed due to inefficient processing of cellular bandwidth usage The cellular bandwidth usage is being calculated for all the routers whenever any router receives router metrics.

  Overall performance of the system is impacted because of the above inefficient processing.

  Conditions: Need a scale system to see the issue.

  Workaround: This issue is resolved in IoT FND Release 4.1.2.

- CSCvm23982

  Symptom: Mesh metrics for endpoints are not updated or showing unknown.

  Conditions: This happens after endpoint device has IP address changed. The sub-net prefix for the endpoint gets updated to the new full address instead of just the 64 bit prefix. This incorrect sub-net prefix causes the RPL data processing to skip this endpoint without updating its mesh metrics.

  Workaround: This issue is resolved in IoT FND Release 4.1.2.

- CSCvm50004

  Symptom: CSMP Message drops may occur during heavy load of registration messages being received by FND. Oracle's alert log (alert_cgms.log) would show deadlock detected messages (with corresponding named trace file showing the details of the deadlock detected).

  Conditions: The symptoms are observed in 6 million cgmesh meters scale system.

  Workaround: This issue is resolved in IoT FND Release 4.1.2.

- CSCvn05758

  Symptom: Serialization errors in server.log file and core dump files seen on FND application server.

  Conditions: Occurs in FND clustered setup only. The issue occurs when users are logged into FND GUI on serverA in a cluster and FND serverB is shut down and brought back up. When serverB comes back up, serverA tries to sync the session info with serverB and it runs into the serialization errors.

  Workaround: This issue is resolved in IoT FND Release 4.1.2.

- CSCvn32501

  Symptom: FND fails to start in cluster deployment. “Caused by: org.infinispan.CacheException"

  Conditions: FND operating in Clustered environment and seen only while starting second application server.

  Workaround: This issue is resolved in IoT FND Release 4.1.2.

Caveats Resolved in IoT FND 4.1.1

- CSCvh48565

Symptom: Firmware upload to a gateway with the retry property set fails with an error message indicating 'Insufficient flash space' on the device when there is enough space available on the device.

Conditions: Issue will not be triggered by default when the cgms property router-firmware-upload-retries is not set. Connection timeout of the router is the cause.

Workaround: This issue is resolved in IoT FND Release 4.1.1.

- CSCvh81539

  Symptom: When a router is added to FND after a FND restart and then registered with FND, traps are not received for that device.

  Conditions: New Router registration with FND after the cgms service restart.

  Workaround: This issue is resolved in IoT FND Release 4.1.1.

- CSCvi05881

  Symptom: CGR tunnel staying in HER config even after removing CGR from FND.

  Conditions: FND 4.0 with static tunnel configuration.

  Workaround: This issue is resolved in IoT FND Release 4.1.1.

- CSCvi16319

  Symptom: IXM registration should wait until the FPGA upgrade is complete.

  Conditions: FND did not check for FPGA Status if FPGA upgrade is triggered after firmware update. FND would reload the device with the appropriate checkpoint file even if FPGA upgrade is in progress.

  Workaround: This issue is resolved in IoT FND Release 4.1.1.

- CSCvi16453

  Symptom: When loading CSV file with Label column, approximately half the uploads were failing. Same issue was seen during removing of devices using the CSV file.

  Conditions: Add/Remove devices using CSV file with Label column.

  Workaround: Remove Label column and add/remove. This issue is resolved in IoT FND Release 4.1.1.

- CSCvi16488

  Symptom: Config group properties are incorrect for BACTs with user defined config group.

  Conditions: The config group properties are incorrect for the devices added with the csv.

  Workaround: This issue is resolved in IoT FND Release 4.1.1.

- CSCvi23957

  Symptom: Select Devices > Field Devices page On the Browse Devices tree. ENDPOINTS > UP is selected.

  The map comes up. The Default view is selected. Number of devices per page is changed to 200. Time to load is long. F12 > Network shows long wait on object. Long time to load can be duplicated by selecting another view/page and then re-selecting the ENDPOINT > UP > Default view.

  Conditions: Takes about 16 – 25 seconds to load 200 devices.

  Workaround: This issue is resolved in IoT FND Release 4.1.1.

- CSCvi34363

  Symptom: Firmware upgrade fails for multiple CG-Mesh endpoints.

  Conditions: Firmware upgrade of Mesh endpoints on User-defined groups with logical error, randomly.

  Workaround: This issue is resolved in IoT FND Release 4.1.1.

- CSCvi54380

  Symptom: When AP registrations are sent continuously to FND from a single router, DB connections leak.

  Conditions: AP register profile execution is not successful due to route problems/bootstrap issues.

  Workaround: This issue is resolved in IoT FND Release 4.1.1.

- CSCvi69057

  Symptom: Dashlet 'Service providers with maximum down Routers' charts do not load if the 'Down Routers Over Time column' is not present.

  Conditions: The 'Down Routers Over Time' column should be disabled.

  Workaround: This issue is resolved in IoT FND Release 4.1.1.

- CSCvi96638

  Symptom: When performing Router Firmware image installation in the non-root domain, it is failing with an exception.Firmware image transfer works fine but when clicking on Install, it fails with an exception.

  Conditions: Firmware upgrade of router in non-root domain.

  Workaround: This issue is resolved in IoT FND Release 4.1.1.

The following caveat was resolved in IoT FND 4.1.0:

- CSCvg83964

  Symptom: ASR does not receive configuration when using dual tunnel templates.

  Conditions: When using an IOS CGR and dual tunnel policies, the ASR does not receive any configuration even though a netconf session is opened with the ASR.

  Workaround: This issue is resolved in IoT FND Release 4.1.0.

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
- Cisco Wireless Gateway for LoRaWANI

No combinations are authorized or intended under this document.