



# Release Notes for IoT Field Network Director, Release 4.2

**First Published:** 2018-3-30

**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 4.2 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).

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 two primary documents that support this release:

- [Cisco IoT Field Network Director User Guide, Release 4.2.x](#)
- [Cisco IoT Field Network Director Installation Guide, Release 4.2.x](#)

Please refer to the [Cisco IoT Field Network Director](#) data sheet for an extensive list of the product capabilities.

**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 5.3](#)
- [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:

<a href="#">Conventions</a>	Conventions used in this document.
<a href="#">New Features</a>	New features in Release 4.2.
<a href="#">IoT FND Perpetual Product IDs</a>	Summary of supported licenses for Release 4.2.
<a href="#">About Cisco IoT FND</a>	Description of the IoT FND application.
<a href="#">System Requirements</a>	System requirements for Release 4.2.
<a href="#">Installation Notes</a>	Procedures for downloading software.
<a href="#">Important Notes</a>	Notes about Release 4.2.
<a href="#">Caveats</a>	Open and resolved caveats in Release 4.2.
<a href="#">Related Documentation</a>	Links to the documentation associated with this release.

## Conventions

This document uses the following conventions.

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

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

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

**Warning:** IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

## New Features

## New Features

Table 1 lists new platforms and features that are managed in IoT FND 4.2.

**Table 1 New Features in IoT FND 4.2**

Feature	Description	First IoT FND release support	Related Documentation
User-defined Tunnel Groups for LoRaWAN	You can define LoRaWAN tunnel groups by Name and by Device Category (GATEWAY). The user-defined tunnel group displays under the defined Device type in the Browse Devices pane.  CONFIG > TUNNEL PROVISIONING	4.2	<a href="#">“Managing the Cisco Wireless Gateway for LoRaWAN”</a>  <a href="#">Cisco Wireless Gateway for LoRaWAN</a>
LoRaWAN Gateway Health LED Status	Monitors the cumulative health of Memory, Storage and CPU of a LoRaWAN (IXM-LPWA-900 or IXM-LPWA-800) system. LED states are OFF, RED, GREEN. The LED Status displays under Gateway Health on the LoRaWAN Device Details page.  DEVICES > FIELD DEVICES	4.2	<a href="#">“Managing the Cisco Wireless Gateway for LoRaWAN”</a>  <a href="#">Cisco Wireless Gateway for LoRaWAN</a>
Gateway States Over Time and Gateway Inventory dashlets	Displays the following states for Gateways: Down, Unheard, Unmanaged and Up.  Device count and Date and Time are the X and Y parameters, respectively.  DEVICES > DASHBOARD	4.2	<a href="#">Using the Dashboard</a>
ACTD Firmware Image for CAM endpoint	The ACTD firmware image includes the IOx application software for installation within the GOS image. You initiate the upload by clicking the ACTD Start button on the Guest OS tab on the CGR1000 router Device Details page.  DEVICES > FIELD DEVICES	4.2	<a href="#">Uploading a Firmware Image to a Router Group</a>
User-Defined Chart Display Options	For some user-defined charts, you can select how the data displays. Options are Bar or Pie chart.  DEVICES > DASHBOARD	4.2	<a href="#">Using the Dashboard</a>
Zoom Option for Line Graph dashlet	For Line Graphs, you can right-click and select Zoom In, Zoom Out or View All options.  <b>Zoom in</b> or <b>Zoom Out</b> allows you to modify the number of days that display on the graph.  <b>View All</b> shows the default display.  DEVICES > DASHBOARD	4.2	<a href="#">Using the Dashboard</a>
Firmware Upgrade REST API	Allows you to initiate and monitor the FND Firmware Update process using an external user interface or tool that can call this API.	4.2	---

## IoT FND 4.2 Software Subscriptions

**Table 2 Summary of IoT FND 4.2 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 4.2. 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
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.

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 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

## About Cisco IoT FND

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 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.

---

## About Cisco IoT FND

- **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 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)	<ul style="list-style-type: none"> <li>■ Processor:               <ul style="list-style-type: none"> <li>– Intel Xeon x5680 2.27 GHz (64-bit)</li> <li>– 4 CPUs</li> </ul> </li> <li>■ RAM: 16 GB</li> <li>■ Disk space: 100 GB</li> <li>■ <a href="#">Hardware Security Module (HSM)</a> or <a href="#">Software Security Module (SSM)</a></li> </ul>	<ul style="list-style-type: none"> <li>■ Red Hat Enterprise Linux 6.4 and above, 64-bit with all packages installed (software development and web server)</li> </ul> <p>See <a href="#">Table 6 on page 12</a> for suggested application server resource allocation profiles.</p> <ul style="list-style-type: none"> <li>■ Internet connection</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>■ A license to use SafeNet for mesh endpoint security</li> </ul> <p><b>Note:</b> IoT FND software bundle includes required Java version.</p>
Cisco IoT FND TPS proxy	<ul style="list-style-type: none"> <li>■ Processor:               <ul style="list-style-type: none"> <li>– Intel Xeon x5680 2.27 GHz (64-bit)</li> <li>– 2 CPUs</li> </ul> </li> <li>■ RAM: 4 GB</li> <li>■ Disk space: 25 GB</li> </ul>	<ul style="list-style-type: none"> <li>■ Red Hat Enterprise Linux 6.4 and above with all packages installed (software development and web server)</li> </ul> <ul style="list-style-type: none"> <li>■ Internet connection</li> </ul> <p><b>Note:</b> IoT FND software bundle includes required Java version.</p>



## System Requirements

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

Component	Minimum Hardware Requirement	Software Release Requirements
<p>Database server for IoT FND</p> <p>Scalable to 25 routers/10,000 endpoints with minimum hardware requirement. See <a href="#">Resource Management Guidelines</a> for additional scale sizes.</p>	<ul style="list-style-type: none"> <li>■ Processor: Intel Xeon x5680 3.33 GHz (64-bit)</li> <li>■ 2 CPUs</li> <li>■ RAM: 16 GB</li> <li>■ Disk space: 100 GB</li> </ul>	<p><b>Note:</b> IoT FND 4.2.0 supports both of the Oracle releases listed below.</p> <ul style="list-style-type: none"> <li>■ Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production (with Patch 20830993)</li> <li>■ Oracle 11g Enterprise Edition (11.2.0.3 64-bit version only)</li> </ul> <p><b>Note:</b> 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 <i>Cisco IoT Field Network Director Installation Guide, Release 4.2.0</i>.</p> <p>See <a href="#">Table 5 on page 12</a> for suggested Oracle Database server resource allocation profiles.</p> <ul style="list-style-type: none"> <li>■ Red Hat Linux 6.4 and above, 64-bit with all packages installed (software development and web server)</li> </ul>
Cisco IoT FND Client	<p>The client must meet the following minimum requirements to connect to the IoT FND application server and view IoT FND displays:</p> <ul style="list-style-type: none"> <li>■ Windows 7 or Win2000 R2 Server</li> <li>■ RAM: 8 GB</li> <li>■ Processor: 2 GHz</li> <li>■ Resolution: 1024 x 768</li> </ul>	<p>When using FND 4.2 and higher, use Zingcharts for viewing charts.</p> <ul style="list-style-type: none"> <li>■ Supported browsers: <ul style="list-style-type: none"> <li>– Internet Explorer (IE): 11.0</li> <li>– Mozilla Firefox: 3.5 or later</li> <li>– Windows 7 works with IE 11.0</li> </ul> </li> </ul>

## System Requirements

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

Component	Minimum Hardware Requirement	Software Release Requirements
Cisco Network Registrar (CNR) (used as a DHCP server)	Server must have the following minimum requirements: <ul style="list-style-type: none"> <li>■ Free disk space: 146 GB</li> <li>■ RAM: 4 GB (small network), 8 GB (average network), 16 GB (large network)</li> <li>■ Hard drives:               <ul style="list-style-type: none"> <li>– SATA drives with 7500 RPM drive &gt; 500 leases/second <i>or</i></li> <li>– SAS drives with 15K RPM drive &gt; 1000 leases/second</li> </ul> </li> </ul>	The following software environment must exist before installing Cisco Network Registrar, software release 8.2 on the server: <ul style="list-style-type: none"> <li>■ Operating System: Windows Server 2008</li> <li>■ Development Kit (JDK) Java SE Runtime Environment (JRE) 8.0 (1.8.0_65-b17) or equivalent Java Development Kit (JDK).</li> <li>■ User interfaces: Web browser and command-line interface (CLI) (Browser versions listed below):               <ul style="list-style-type: none"> <li>– Internet Explorer (IE) 11.0, Mozilla Firefox 3.5 or later</li> </ul> </li> <li>■ CNR license. Contact your Cisco partner for the necessary license.</li> </ul>
IoT Device Manager (IoT-DM or Device Manager)	Laptop running Device Manager must have the following: <ul style="list-style-type: none"> <li>■ Microsoft Windows 7 Enterprise or Windows 10</li> <li>■ 2 GHz or faster processor</li> <li>■ 1 GB RAM minimum (for potential large log file processing)</li> <li>■ WiFi or Ethernet interface</li> <li>■ 4 GB disk storage space</li> <li>■ Windows login enabled</li> <li>■ Utility-signed Certificate Authority (CA) and Client Certificate for router authentication (obtained from your IT department)</li> <li>■ Customer-specific IT security hardening to keep the Device Manager laptop secure</li> </ul>	<ul style="list-style-type: none"> <li>■ IoT-DM 5.3</li> </ul>
Cisco 1000 Series Connected Grid Router (CGR)	-	<ul style="list-style-type: none"> <li>■ Cisco IOS Release 15.7(3)M2</li> <li>■ Cisco CG-OS Release CG4(5)</li> </ul>
Cisco 5921 (C5921) Embedded Service Routers	-	<ul style="list-style-type: none"> <li>■ Cisco IOS Release 15.7(3)M2</li> </ul>
Cisco ISR 800 Series Integrated Services Router (C800)	-	<ul style="list-style-type: none"> <li>■ Cisco IOS Release 15.7(3)M2</li> </ul>

## System Requirements

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

Component	Minimum Hardware Requirement	Software Release Requirements
Cisco 800 Series Access Points (AP800)	-	<ul style="list-style-type: none"> <li>■ AP802: ap802-k9w7-tar.153-3.JD.tar</li> <li>■ AP803: ap1g3-k9w7-tar.153-3.JD.tar</li> </ul>
Cisco 800 Series Industrial Integrated Services Router (IR800)	-	<ul style="list-style-type: none"> <li>■ Cisco IOS Release 15.7(3)M2</li> </ul>
Cisco 3900 Series Integrated Service Router (ISR)	-	<ul style="list-style-type: none"> <li>■ Cisco IOS Release 15.4(3)M</li> <li>■ Cisco IOS Release 15.4(2)T</li> </ul>
Cisco ASR 1001 or 1002 Aggregation Services Router (ASR) serving as a head-end router	-	<ul style="list-style-type: none"> <li>■ Cisco IOS XE Release 3.17.02.S for Flex tunnels (IOS)</li> <li>■ Cisco IOS XE Release 3.11S for Point to Point tunnels (CG-OS)</li> </ul>
<b>Note:</b> ASRs and ISRs with different releases can co-exist on the network.		
Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR500)	-	<ul style="list-style-type: none"> <li>■ Cisco IR509, DA Gateway device: Firmware version 5.7.27</li> <li>■ Cisco IR529, Range Extender: Firmware version 5.7.27</li> </ul>
Cisco Resilient Mesh Module and supported endpoints	-	<ul style="list-style-type: none"> <li>■ 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</li> </ul>
Cisco RF Mesh endpoints	-	<ul style="list-style-type: none"> <li>■ Firmware version 5.7.27 when communicating with IR500</li> </ul>
Long Range Wide Area Network (LoRaWAN) Interface Module for Cisco 800 Series Industrial Integrated Services Routers (IR800)	-	<ul style="list-style-type: none"> <li>■ Cisco IOS 15.7(3)M2</li> </ul>
Hardware Security Module (HSM)	Luna SA appliance, with client software installed on the IoT FND application servers	<p>Luna SA appliance:</p> <ul style="list-style-type: none"> <li>■ Release 6.10.2 firmware</li> </ul> <p><b>Note:</b> Contact <a href="#">SafeNet</a> to determine if you can run a higher version.</p> <ul style="list-style-type: none"> <li>■ Release 5.4.7-1 software, plus security patches</li> </ul> <p>Luna SA client software:</p> <ul style="list-style-type: none"> <li>■ Release 5.4.7-1 software</li> </ul>
Software Security Module (SSM)	<ul style="list-style-type: none"> <li>■ RAM: 8 GB</li> <li>■ Processor: 2 GHz</li> <li>■ 2 CPUs</li> </ul>	<ul style="list-style-type: none"> <li>■ Red Hat Enterprise Linux 6.4 or 7.1, 64-bit with all packages installed (software development and web server)</li> </ul>

## System Requirements

**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 12](#) 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

[Table 6 on page 12](#) 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 <sup>1</sup>	8	16	500
5,000/5,000,000 <sup>1</sup>	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 [Table 7](#) and [Table 8](#) is relevant to Router Only deployments.

**Table 7 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 8 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 4.2.0*. 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 13](#), 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 (6.4 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:

- [Open Caveats, page 13](#)
- [Resolved Caveats, page 14](#)
- [Accessing the Bug Search Tool, page 14](#)

## Open Caveats

- CSCvt45004

**Symptom:** Before you can add groups, at least one device must be added to FND. Once a device is added, then groups can be created, and the device added to the groups. Do not try to add device to groups via import file prior to creating groups.

**Workaround:** Once a device is added, then groups can be created, and the device added to the groups.

## Resolved Caveats

- CSCvi05881

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

Conditions: FND 4.0 with static tunnel configuration.

Workaround: Add "attempt-tunnel-cleanup=TRUE" in cgms.properties and restart FND.

- 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: None.

## 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](http://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, 5.3](#)
- [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](#)

## Related Documentation

- [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.

© 2018 Cisco Systems, Inc. All rights reserved.

Related Documentation