Release Notes for IoT Field Network Director, Release 4.4.x

First Published: 2018-12-26

Last Modified: 2023-04-19

Release Notes for IoT Field Network Director, Release 4.4.x

Last Updated: 2020-04-28

First Published: 2018-12-26

This release note contains the latest information about using the user interface for IoT Field Network Director (IoT FND), Release 4.4 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 (IR500), Cisco 5921 (C5921) Embedded Service Routers, and Cisco 800 Series Industrial Integrated Services Routers (IR807, IR809 and IR829), Cisco IR1101 Industrial Integrated Service Routers, Cisco Industrial Compute Gateway IC3000 Management and Cisco 1100 Integrated Services Router.

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 4.4 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 and 4.4.x
- Cisco IoT Field Network Director Post-Installation Guide - Release 4.3.x and 4.4.x - High Availability and Tunnel Provisioning
- Cisco IoT Field Network Director User Guide, Release 4.4.x
- Cisco IoT Field Network Director Post-Installation Guide, Release 4.4.x

Please refer to thehttps://www.cisco.com/c/en/us/products/cloud-systems-management/iot-field-network-director/index.htmlCisco 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 1.x and 2.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:

Table 1:

Conventions	**Conventions used in this document.**
New Features	**New features in Release 4.4.x**
IoT FND Perpetual Product IDs	Summary of supported licenses for Release 4.4.x
About Cisco IoT FND	Description of the IoT FND application.
System Requirements	System requirements for Release 4.4.x
Installation Notes	Procedures for downloading software.
Important Notes	Notes about Release 4.4.x
Caveats	Open and resolved caveats in Release 4.4.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.

Conventions	Indication
{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 transaltion 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 4.4.x lists new platforms and features that are managed in IoT FND 4.4.x

Table 2: New Features in IoT FND 4.4.x

Feature	Description	First IoT FND release support	Related Documentation
Support for Oracle 12c Release 2 and Oracle 18c Database Software	Support for Oracle 12c Release 2 (12.2.0.1.0) for a Database Appliance install into a rack. Support for Oracle 18C (18.3.0.0.0.0) in FND OVA installs.	4.4.4	Cisco IoT Field Network Director Installation Guide-Oracle Deployment Releases 4.3.x, 4.4.x and 4.5.x Cisco IoT FND Deployment on an Open Virtual Appliance, VMware ESXi 5.5/6.0
Custom PKI can use RSA key with size up to 4096 bits.		4.4.1	---

Feature	Description	First IoT FND release support	Related Documentation
Cisco 1101 Industrial Integrated Services Router (IR1101) Firmware image Upgrade during Bootstrapping		4.4.0	Cisco IoT Field Network Director User Guide, Release 4.4.x

Feature	Description	First IoT FND release support	Related Documentation
	You can use bootstrapping to enter a different image than that installed during the manufacturing process for IR1101. PnP must be supported on the device. PnP Device Information service retrieves current firmware version on the device and the Image Install service performs the image upgrade. CGNA ‘image-retrieve' command transfers image from FND to router. You can enter the relevant commands by selecting Default-ir1100 (version 16.10 or later) in the left pane of the FND UI and the Router Bootstrap Configuration tab in the FND UI right pane. Note: On the Tunnel Provisioning Page, “Router Bootstrap Configuration’ replaces the term ‘Router Factory Provisioning’ CONFIG > TUNNEL PROVISIONING > ROUTER BOOTSTRAP CONFIGURATION **Note** The PnP work flow supports device upgrade only if the target image version is higher than the running (current)		

Feature	Description	First IoT FND release support	Related Documentation
	image version. If the target image runs the same or lower version, then the device upgrade is skipped during the PnP work flow.		

Feature	Description	First IoT FND release support	Related Documentation

App Management Support for IR829 and User Interface changes	Cisco IOx is now the operating system (OS) for IR829 rather than Guest OS (GOS).
	Screen changes:
	• On the Routers Device page, a Cisco IOx tab replaces the Guest OS tab.
	• An App tab appears on the IR829 Device Details page after discovery of the IOx Node on the router.
	• New device type: deviceType:ir800 module:iox
	• New Management Operations term:
	  • Restart IOx replaces 'Restart GOS'
	• Renaming of Configuration Properties as follows:
	  • dhcpV4IOxLink replaces dhcpV4GosLink
	  • GOSpassword field is removed
	DEVICES > FIELD DEVICES
		4.4.0	Cisco IoT Field Network Director User Guide, Release 4.4.x

Feature	Description	First IoT FND release support	Related Documentation
GPS Failure Detection	Helps identify faulty or failing devices or GPS antennas before they fail. On the CGR 1000 Device Info page, a new property, Last GPS Heard, identifies an unsuccessful delivery of a GPS signal and displays one of the following messages: • IOS: 'No GPS Signal Available' or 'weak signal, reading may not be accurate' • CG-OS: 'Unable to communicate with GPS' When there are no issues with the GPS signal, the Last GPS Heard field shows the date and time that the signal was last heard. Additionally, as a proactive action, you can use Last GPS Heard as a Quick View/Rule search field option found on the Inventory tab to review the date entry. An older date entry than expected for the Last GPS Heard field, might be predictive of a failing device. DEVICES > FIELD DEVICES	4.4.0	Cisco IoT Field Network Director User Guide, Release 4.4.x
CGR 1000 GPS Outage and Restore Event	Field Event Name: Heartbeat Retrieval Failure The new event displays on the Device Detail page. DEVICES > FIELD DEVICES	4.4.0	Cisco IoT Field Network User Guide, FND 4.4.x

Feature	Description	First IoT FND release support	Related Documentation
Utility to translate Oracle event and metrics data to Influx data	Before you run the utility, ensure the following requirements are met: • FND software version is 4.1.2 or greater. • Influx node must be already setup (setupInfluxDB.sh in cgms-influx-43.x86_64.rpm) • FND App server should not be running when data translation is executed After you run the translation utility, you should run: • setupCgms.sh to configure FND using the Influx node • db-migrate.sh (run this utility in the background to ensure the process remains running even if the terminal connection is lost)	4.4.0	Cisco IoT Field Network Director Installation Guide-Oracle Deployment, Release 4.3.x and 4.4.x
Application (App) Management User Interface Changes	You can import multiple versions for each defined App. All versions of a specific App will be listed beneath the App in the User Interface. Although you can delete versions of a given App, you cannot delete the App, itself. This differs from FND 4.3. DEVICES > FIELD DEVICES > APP	4.4.0	Cisco IoT Field Network Director User Guide, Release FND 4.4.x

Feature	Description	First IoT FND release support	Related Documentation
Security Enhancements for Security Readiness Compliance	This release introduces two new security enhancements: • You can generate self-signed certificates for each install or upgrade instance for Web and NBAPI access by checking the 'Allow self-signed certificate' box on the Certificate Settings tab. • FND validates the server certificate of the NB event receiver. **Note** FND continues to support a customer's own PKI certificates. ADMIN > SYSTEM MANAGEMENT > CERTIFICATES	4.4.0	---

Feature	Description	First IoT FND release support	Related Documentation
Safenet Upgrades in FND to support Gemalto Hardware Security Module (HSM)	To support higher performance on the newly supported Gemalto HSM platform, FND now supports: • Lunaclient Library 7.3 • Lunaclient Tool 7.3 (backwards compatible with HSMs running 6.x) **Note** FND 4.4 is bundled with the new HSM 7.3 libraries and requires the Luna client software to be on the same version. If a different version of client is detected, the new libraries may not be backward compatible with it. To resolve this issue, copy over the following two files to the FND directory and restart the FND services. cp /usr/safenet/lunaclient/jsp/lib/LunaProvider.jar /opt/cgms/jre/lib/ext/ cp /usr/safenet/lunaclient/jsp/lib/libLunaAPI.so /opt/cgms/jre/lib/ext/	4.4.0	---

IOT FND 4-4-x Software Licenses

Table 3: Summary of IoT FND 4.4.x Managed Service License Agreement (MSLA) Product and Entitlement Tags

Product Tag	Entitlement Tag	Description
IoT-FND	BATTERY_ENDPOINT	IoT FND device license for managing battery endpoints
IoT-FND	CGR1K	IoT FND device license for managing CGR1000 routers.
IoT-FND	ENDPOINT	IoT FND device license for managing endpoints

Table 4: Summary of IoT FND 4.4.x 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.
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 (subscription and MSLA) on theCisco IoT Field Network Director Data Sheet.

IoT FND Perpetual Product IDs

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

Table 5: 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.x Contact your Cisco partner to obtain the necessary licenses.

Table 6: Summary of IoT FND Perpetual Product IDs

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 Integrated Services Router Rugged, or IR1101, is Cisco's smallest industrial router. Designed in a highly modular form factor makes it an ideal solution for remote asset management across multiple industrial vertical markets such as utilities, oil and gas, and transportation.
- Cisco 5900 Series Embedded Services Routers (ESRs) provide highly secure data, voice, and video communications to stationary and mobile network nodes across wired and wireless links. They solve critical size, weight, and power challenges, and can operate reliably in harsh environments. These routers are powered by Cisco IOS Software and feature Cisco Mobile Ready Net capabilities.
- 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 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 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 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. For example, the hop count information received from the RPL tree can determine the use of unicast or multicast for the firmware download process. IoT FND maintains a periodically updated snapshot of the RPL tree.
- **Dynamic Multipoint VPN and Flex VPN** – For Cisco C800 devices and Cisco IR800 devices, DMVPN and Flex VPN do not require IoT FND to apply device-specific tunnel configuration to the HER during tunnel provisioning. HER tunnel provisioning is only required for site-to-site VPN tunnels.
- **Dual PHY Support** – IoT FND can communicate with devices that support Dual PHY (RF and PLC) traffic. IoT FND identifies CGRs running Dual PHY, enables configuration to masters and slaves, and collects metrics from masters. IoT FND also manages security keys for Dual PHY CGRs. On the mesh side, IoT FND identifies Dual PHY nodes using unique hardware IDs, enables configuration pushes and firmware updates, and collects metrics, including RF and PLC traffic ratios.

- **Device Location Tracking** – For CGR 1000, C800, and IR800 devices, IoT FND displays real-time location and device location history.
- **Diagnostics and Troubleshooting** – The IoT FND rule engine infrastructure provides effective monitoring of triage-based troubleshooting. Device troubleshooting runs on-demand device path trace and ping on any CGR, Cisco C800, Cisco IR800, range extender, or meter (mesh endpoints).
- **High Availability** – To ensure uninterrupted network management and monitoring, you can deploy the Cisco IoT FND solution in a High Availability (HA) configuration. By using clusters of load-balanced IoT FND servers and primary and standby IoT FND databases, Cisco IoT FND constantly monitors the health of the system, including connectivity within clusters and server resource usage. If a server cluster member or database becomes unavailable or a tunnel fails, another takes its place seamlessly. Additionally, you can add reliability to your IoT FND solution by configuring redundant tunnels between a Cisco CGR and multiple Cisco ASRs.
- **Power Outage Notifications** – Cisco Resilient Mesh Endpoints (RMEs) implement a power outage notification service to support timely and efficient reporting of power outages. In the event of a power outage, CGEs perform the necessary functions to conserve energy and notify neighboring nodes of the outage. FARs relay the power outage notification to IoT FND, which then issues push notifications to customers to relate information on the outage.
- **Mesh Upgrade Support** – Allows over-the-air software and firmware upgrades to field devices such as 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 7: 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	**Note** IoT FND 4.3 supports both of the Oracle releases listed below. • Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production (with Patch 20830993) • Oracle 11g Enterprise Edition (11.2.0.3 64-bit version only) **Note** Before installing Oracle, install the Linux packages referenced in "Installing the Linux Packages Required for Installing Oracle" in the "Before You Install Field Network Director" chapter of the: Cisco IoT Field Network Director Installation Guide - Oracle Deployment, Release 4.3.x and 4.4.x See Table 7 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)

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	When using FND 4.2 and higher, use Zingcharts for viewing charts. • Supported browser: • Mozilla Firefox: 63 or later **Note** IE 11.0 is not supported in FND 4.4.x, and 4.5.x. 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 5.4
Cisco 1000 Series Connected Grid Router (CGR)	–	• Cisco IOS Release 15.8(3)M1 • Cisco CG-OS Release CG4(5)
Cisco 5921 (C5921) Embedded Service Routers	-	• Cisco IOS Release 15.8(3)M1
Cisco ISR 800 Series Integrated Services Router (C800)	–	• Cisco IOS Release 15.8(3)M1
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 IR510, DA Gateway device: Firmware version 6.0.20 • Cisco IR529, Range Extender: Firmware version 6.0.20
Cisco Resilient Mesh Module and supported endpoints	–	• Firmware version 6.0.20 when communicating with CGR 1000s or Cisco ASRs and the minimum • Cisco IOS software versions recommended for these routers in these release notes
Cisco RF Mesh endpoints	-	• Firmware version 6.0.20 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 8: 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 9: 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 10: 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 11: 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 4.3.* 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,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
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

Table 12: Open Caveats in 4.4.3

Caveat Number	Description
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 device to groups via import file fails prior to creating groups.

Resolved Caveats

Table 13: Resolved Caveats for 4.4.4

Caveat	Description
CSCvr12356	FND Export certificates, wrong files extensions
CSCvr20909	Intermittent: FND occasionally clears the IPV6 addresses on all CGR interfaces

Caveat	Description
CSCvs00562	Provisioning Settings don’t allow multiple servers
CSCvs37815	Maps on Issue page do not show devices on the map
CSCvs53841	Issues with deploying IXM when FND is in Easy Mode
CSCvs60239	Label management drop-down.
CSCvt05570	Firmware upload completed in the FND but only part of the image is copied to the device.
CSCvt08217	PNP stuck Multi-file in transferring image state for IR1100 and IR800 devices.
CSCvt21704	Image version check failing between 16.x and 17.x for IR1100 device during PnP
CSCvt22795	Consolidated issue faced while device stuck in transferring firmware to 4.4.0.
CSCvt52642	App server not starting
CSCvt67517	[File Transfer] Multi-file selection should be restricted to one in FND to delete.
CSCvt73513	Improve logging for CoAP packets sent with incorrect options and incorrect message.

Table 14: Resolved Caveats for 4.4.3

Caveat Number	Description
CSCvq09661	//SR 686314268: Clustered nodes do not fully start//CGR cache syncing issue with FND cluster nodes
CSCvq11552	First config push after registration doesn't correctly set tbit
CSCvq83749	Geo fencing notifications not working
CSCvq86541	Tunnel provisioning failing - ORA-01795 list > 1000

Table 15: Resolved Caveats in 4.4.2

Caveat Number	Description
CSCvg09726	FND goes back to first profile category regardless of any profile creation
CSCvo56725	Getting “java.lang.NullPointerException" when removing bulk
CSCvp63798	FND Ioxclient Processes hang

Table 16: Resolved Caveats in 4.4.1

Caveat Number	Description
CSCvn46601	FND's Router Factory Reprovision template should have “license smart reservation" for Default-Ir1101
CSCvn80790	vault.sh is not using fnd bundled jre
CSCvn95720	Error seen in HER poll when certain VRF config
CSCvo00969	NullPointerException for virtual WPAN
CSCvo64812	Kinetic displays the incorrect connectivity type
CSCvp02178	CSV upload with multiple config groups creating duplicate
CSCvp30353	Firmware Upgrade fails with timeout exceptions on a slow
CSCvp32823	Add support for disabling reverse dns lookup on TPS proxy

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 1100 Series Industrial Integrated Services Routers
- 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.