Release Notes for IoT Field Network Director, Release 4.6.x

First Published: 2020-05-26

Last Modified: 2023-04-19

Release Notes for IoT Field Network Director, Release 4.6.x

Last Updated: 2021-04-12

First Published: 2020-03-20

These release notes contain the latest information about using the user interface for IoT Field Network Director (IoT FND), Release 4.6.

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.

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Documentation

Listed below are the documents that support this release:

- Cisco IoT FND 4.3.1 and greater with Integrated Application Management with Postgres and Influx Database Deployment on an OVA, VMware ESXi 5.5/6.0
- Cisco IoT FND Deployment on an Open Virtual Appliance, VMware ESXi 6.5.0
- Cisco IoT FND Deployment on an Open Virtual Appliance, VMware ESXi 5.5/6.0
- Cisco IoT Field Network Director Installation Guide-Oracle Deployment, Release 4.3.x, 4.4.x, 4.5.x and 4.6.x.
- Cisco IoT Field Network Director Post-Installation Guide - Release 4.3.x, 4.4.x, 4.5.x and 4.6.x- High Availability and Tunnel Provisioning

- Cisco IoT Field Network Director User Guide, Release 4.6.x

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

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

Be sure to refer to the following related Cisco Resilient Mesh documentation:

- Release Notes for Cisco Resilient Mesh Release 6.3
- Release Notes for Cisco Resilient Mesh Release 6.2
- Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and Cisco Resilient Mesh Configuration Guide (Cisco IOS)

Organization

Conventions	Conventions used in this document.
New Features	New features in IoT FND Release 4.6.
IoT FND Release 4.x Upgrade Matrix	Description of the IoT FND application.
System Requirements	System requirements for IoT FND Release 4.6.
Important Notes	Notes about IoT FND Release 4.6. Please review before installing software.
Caveats	Open and resolved caveats in IoT FND Release 4.6.
End of Life Announcements for IoT FND and IoT Device Manager Releases	Provides a summary of IoT FND releases that are End of Life (EOL)
Accessing the Bug Search Tool	Provides details on how to access the Bug Search Tool.
Documentation	Links to documentation for products managed or associated with IoT FND Release 4.6.

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.

Conventions	Indication
[ ]	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 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 4.6.x lists new platforms and features that are managed in IoT FND 4.6.x.

Feature	Description	First IoT FND Release Support	Related Documentation
Event Page Navigation Enhancement	You can navigate through Event Pages by entering a valid page number in the Page# text box. Clicking the Go button on the page initiates the search. If you enter an invalid page number, the page number entry in the text box displays a red border around the search text box. A tool tip error also displays when you hover over the text box. OPERATIONS > EVENTS	4.6.2	Cisco IoT Field Network Director, User Guide, Release 4.6.x
Dashboard Enhancement	You can now retain the previous states of some dashlets in the Dashboard page when you refresh the Dashboard page or navigate to the Dashboard from any other FND page. DASHBOARD	4.6.2	Cisco IoT Field Network Director, User Guide, Release 4.6.x
Reload Meter Module Using New Reboot Button for OpenWay RIVA Electric and Gas-Water Endpoints	You can initiate a reboot of specific cg-mesh meters by clicking a Reboot button on the Device Details page for the meter. You will be prompted to confirm the reboot, before the reboot begins. DEVICES > FIELD DEVICES > Browse Devices > ENDPOINT	4.6.2	Cisco IoT Field Network Director, User Guide, Release 4.6.x
Set Time and Page View Preferences for Events	You can retain Time Range and Page View selections across multiple, like devices in the Events tab of the Device Details page. DEVICES > FIELD DEVICES	4.6.2	Cisco IoT Field Network Director, User Guide, Release 4.6.x
Show Truncated View of Open Issues	When more than two of the same Open Issue are reported for a device, a truncated view of the Open Issues column appears and display three dots(...) in that column to indicate multiple entries. To view all of the Open Issues you simply expand the column outward to the right. This feature helps reduce a page view from being over populated by a single Open Issue. DEVICES > FIELD DEVICES > All FAN Devices > Browse Devices > Inventory	4.6.2	Cisco IoT Field Network Director, User Guide, Release 4.6.x
Display PAN ID in Decimal or Hexadecimal	A new ‘Show PAN ID in Hexadecimal’ check box option is available to define as part of <user> Preferences. This option, allows you to request that the format of the value be displayed in either decimal or hexadecimal format. ‘Decimal’ is the default setting of the Show PAN ID check box.	4.6.2	Cisco IoT Field Network Director, User Guide, Release 4.6.x

Feature	Description	First IoT FND Release Support	Related Documentation
Oracle 19c RAC HA Support	IoT FND now supports Oracle 19c RAC High Availability deployments.	4.6.2	RAC Administration and Deployment Guide 19
Increased Number of Allowed Parallel Router Image Downloads	You can initiate up to 400 downloads of router images in parallel within FND, irrespective of group.	4.6.1	Cisco IoT Field Network Director, User Guide, Release 4.6.x
Left Pane Updates to Reflect Search Actions	When you initiate a search in the right pane of FND, any details relevant to the Left Pane content will update automatically.	4.6.1	Cisco IoT Field Network Director, User Guide, Release 4.6.x
Support for more than five simultaneous pings	Configure the ‘ping-traceroute-device-count’ property within cgms.properties with the desired number of devices to be pinged simultaneously.Example command: ping-traceroute-device-count=30	4.6.1	Cisco IoT Field Network Director, User Guide, Release 4.6.x
Auto Retry for Router Upload When Error Conditions Occur for Router Managed Files	Configure the ‘router-file-upload-retries’ property within cgms.properties with the desired value. Example command: router-files-upload-retries=5	4.6.1	Cisco IoT Field Network Director, User Guide, Release 4.6.x
Auto Retry for Router Firmware Install	Configure the ‘router-firmware-install-retries’ property within cgms.properties with the desired value. Example command: router-firmware-install-retries=5	4.6.1	Cisco IoT Field Network Director, User Guide, Release 4.6.x
Auto Retry for Router Firmware Install	Configure the ‘router-firmware-install-retries’ property within cgms.properties with the desired value. Example command: router-firmware-install-retries=5	4.6.1	Cisco IoT Field Network Director, User Guide, Release 4.6.x
Oracle 19c Support	Oracle 19c is the final release of the Oracle 12c family.	4.6.1	Oracle Database 19c
Microsoft Edge Browser Support	Microsoft Edge browser will be used in IoT FND 4.6.x and onwards. (Microsoft Edge Browser Version: 88.0.705.68)	4.6.1	Microsoft Edge

Feature	Description	First IoT FND Release Support	Related Documentation
FND Quick Start for New Installs	Quick Start for New Installs prompts you for information to determine the appropriate deployment. No devices or licenses are added during the Quick Start process. When you first open a new install of FND software, the DASHBOARD page appears and you select QUICK SETUP. Additional actions you can perform are: ADD LICENSE, ADD DEVICES and ADD DASHLET. DASHBOARD	4.6.1	Cisco IoT Field Network Director, User Guide, Release 4.6.x
Avoid Re-ZTD of a Device During a Firmware Upgrade	Avoid config replace and second router reboot when config replacement fails, and avoid Tunnels Reprovisioning after a firmware update, by setting the property enableFwUpdateSequence in cgms.properties. The default value is 'True'. Example: enableFwUpdateSequence = true	4.6.1	Cisco IoT Field Network Director, User Guide, Release 4.6.x
WiSUN Configuration for IR500 and Itron30	When firmware uploads begin, it will collect cellular link quality metrics for the supported device types: CGR1000, IR800 and IR1101. You enable the function by setting the property, 'collect-cellular-link-metrics' to 'true' in cgms.properties. The following metrics are monitored: RSRP, RSRQ, SINR and RSSI. Metric data is found in the Metrics history table in the Database and can be collected by using getMetricHistory NB-API.	4.6.1	Cisco IoT Field Network User Guide, FND 4.6.x
Collect Cellular Link Metrics Interval	Controls how fast, in minutes, CGRs will send cellular metrics to FND during firmware uploads, if 'collect-cellular-link-metrics' is set to 'true'.	4.6.1	Cisco IoT Field Network User Guide, FND 4.6.x
Tunnel Provisioning Optimization	When using FlexVPN/DMVPN tunnels for a FAR, a new property 'optimizeTunnelProv = true' is used to tell FND to avoid HER configuration during Tunnel Provisioning of the Device (router). This property is uploaded for each router using the CSV file.	4.6.1	Cisco IoT Field Network User Guide, FND 4.6

Feature	Description	First IoT FND Release Support	Related Documentation
Ability to Import More Devices Than the License Allows (Classic Licenses Only)	Ensures that should you mistakenly import more devices than your Classic Licenses allows, the import process will not fail. Any devices imported beyond the license limit are marked as 'unmanaged'. ADMIN > SYSTEM MANGEMENT > LICENSE CENTER	4.6.0	Cisco IoT Field Network Director User Guide, Release 4.6.x
Adaptive Modulation Configuration Removed from the Edit Configuration Template page for Endpoints	The Edit Configuration Template tab and subordinate page is no longer available for IR500. You can no longer configure Adaptive Modulation for IR500s using IoT-FND. CONFIG > DEVICE CONFIGURATION > Edit Configuration Template	4.6.0	Cisco IoT Field Network Director User Guide, Release 4.6.x
Pluggable and Expansion Module Support for IR1101	You can manage and view details about IR1101 pluggable and expansion modules (IR-1100-SP, IR1100-SPMI). Each module has a distinct panel on the IR1101. After navigating to the path below, click on Routers and then IR1101. DEVICES > FIELD DEVICES	4.6.0	Cisco IoT Field Network Director User Guide, Release 4.6.x
Application Security tab	You can enable and disable application signature verification and install the signature trust anchor for Fog Director on the Application Security tab on the Certificates page. You can also install the signature trust anchor to the Fog Director. ADMIN > SYSTEM MANAGEMENT > CERTIFICATES	4.6.0	Cisco IoT Field Network Director User Guide, Release 4.6.x
WiSUN 1.x Power Outage and Restoration Message	IR510s running Cisco Resilient Mesh Release 6.2.19, will send the WiSUN outage and restoration notification when running in WiSUN mode. Additionally, IR509, IR529 and IR530 will relay notification messages. OPERATIONS >EVENTS OPERATIONS > ISSUES	4.6.0	Cisco IoT Field Network Director User Guide, Release 4.6.x Release Notes for Cisco Resilient Mesh Release 6.2

Feature	Description	First IoT FND Release Support	Related Documentation
New Dashlet: Network Interfaces Down	Dashlet for: Devices with Interfaces Enabled but Down. This dashlet provides information for the following devices: CGR1000, C800, ESR5000, IR809, IR829, IR1101 and SBR. You can use a filter to select the specific device (such as CGR1000) and corresponding interface(s) to view their respective status. You can enable the dashlet on the Dashlet Settings page. You can view the new dashlet on the Dashboard. DASHBOARD	4.6.0	Cisco IoT Field Network User Guide, FND 4.6
Support for FTT Security Enhancements for work orders on IR510s. Mesh 6.2 Feature	To support this capability, you must create a work order within FND and select type Endpoint and check the FTT Type option for that work order. You will then be able to define the TLV 342 Authorization messages you want sent as the Create Authorization Message panel. After FND syncs with the IoT Device Manager (IoT-DM), the newly created FTT-Work order is visible in the IoT-DM work orders table. Note: The edit operation is not allowed for a FTT work order. OPERATION > WORK ORDER	4.6.0	Cisco IoT Field Network Director User Guide, Release 4.6
Domain Name Support (DNS) Support in the IC3000 Local Manager (LM) User Interface	You can configure and manage the following items for a DNS server in the IC3000 LM user interface: - Add and configure server NTP SETTINGS > NTP SERVER: Add/Edit Settings page	4.6.0	Cisco IC3000 Industrial Compute Gateway Deployment Guide
CA Certificate Configuration for App Signature Verification	Allows you to import and add a trust anchor to the default profile. (Default profile is not seen by user) You enable this capability on the Application Security tab of the Certificate page. The Application Security tab only appears when the user has Application Management permission and there is at least one IOx device being managed such as IC3000 or IR800. ADMIN > SYSTEM MANAGEMENT > CERTIFICATES	4.6.0	Cisco IoT Field Network Director User Guide, Release 4.6

Feature	Description	First IoT FND Release Support	Related Documentation
Oracle 18c and 12cR2 Support	FND 4.6.0 Oracle OVA will have Oracle18c installed in the virtual machine. Oracle 12cR2 will be supported in FND 4.6.0. The database (DB) scripts in cgms-oracle-4.6.0.rpm will be updated to support Oracle 12cR2. Note: End of Support (EoS) for Oracle 11g in 2020.	4.6.0	Oracle Documentation

IoT FND Release 4.x Upgrade Matrix

A Target IoT FND Software Release version supports upgrades from the two prior major releases and their associated maintenance releases.

For example, you can upgrade to IoT FND 4.7.x from 4.6.x and 4.5.x as summarized in IoT FND Software Upgrade Matrix below unless the maintenance release was released after the Target Software version. When the current release is not within the two prior versions of the target release, then multiple hops are required to get to the target software release. Use IoT FND Software Upgrade Matrix to plan your upgrade path.

Table 1: IoT FND Software Upgrade Matrix

Target Release	Upgradeable from Release:	
4.7.0-100	4.6.2-xx, 4.6.1-11	4.5.1-11
4.6.2-xx	4-6.1-61	4.5.1-11
4.6.1-61	4.5.1-11	4.4.4-9 4.4.3-4 4.4.2-11 4.4.1-10 4.4.0-79
4.5.1-11	4.4.2-11 4.4.2-10 4.4.0-79	4.3.2-7 4.3.1-7 4.3.0-133
4.4.x	4.3.1-7 4.3.0-133	4.2.0-123
4.3.x	4.2.0-123	4.1.1-6 4.1.0-257

Target Release	Upgradeable from Release:	
4.2.0-123	4.1.0-257	4.0.0-299

Note Target Release versions allow upgrades from the two prior major releases and its maintenance releases unless the maintenance release was released after the Target version.

If the current version is not within the two prior versions of the target release, then multiple upgrade hops will be required to get to the target release. Use IoT FND Software Upgrade Matrix above to plan the upgrade paths.

The system must be upgraded to each intermediate version(s) followed by starting the FND application and allowing it to stabilize. This allows the FND application to perform necessary modifications of databases during startup. The ability to log on to FND is the best indication of completion of these startup modifications.

EXAMPLE:

If your network is running FND 4.4.0-79 and your Target Release is 4.7.0-100, then your best upgrade path would be:

- Upgrade 4.4.0-79 to 4.6.1-61 and then upgrade to 4.7.0-100

Recommended steps for the multi-hop upgrade noted above are:

1. Backup FND 4.4.0-79 database.
2. Perform an upgrade to FND 4.6.1-61 using the upgrade instructions in the Install Guide.
3. Start FND 4.6.1-61 and login to the FND user interface and perform a quick sanity check.
4. Stop FND 4.6.1-61 services.
5. Backup FND 4.6.1-61 database.
6. Upgrade to FND 4.7.0-100 using the upgrade instructions in the Install Guide.
7. Start FND 4.7.0-100 and login to the GUI.

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 1101 Series Integrated Services Routers (ISRs) with Cisco IOS XE Software combine Internet access, comprehensive security, and wireless services (LTE Advanced 3.0 wireless WAN and 802.11ac wireless LAN) in a single, high-performance device. The Cisco 1101 Series ISRs are well-suited for deployment as Customer Premises Equipment (CPE) in enterprise branch offices, in service provider managed environments as well as smaller form factor and M2M use cases.

- Cisco 800 Series Industrial Integrated Services Routers (IR800s) are ruggedized small-form factor cellular routers for mobile/vehicle applications. IR829 includes WiFi providing connectivity in non-carpeted IT spaces, industrials, utilities, transportation, infrastructure, industrial M2M application, asset monitoring, Smart Grid, and utility applications. These devices are referred to as FARs in this document and identified by product ID (for example, IR800) on the Field Devices page. You can use IoT FND to manage the following IR800 models: IR809 and IR829.
- Cisco 800 Series Integrated Services Routers (C800s) are used in most networks as edge routers or gateways to provide WAN connectivity (cellular, satellite over Ethernet, and WiFi) to an end device (energy-distribution automation devices, other verticals such as ATMs, and mobile deployments). These devices are referred to as FARs in this document and identified by product ID (for example, C800 or C819) on the Field Devices page.
- Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR500) supply RF mesh connectivity to IPv6 and serial Internet of Things (IoT) devices (for example, recloser control, cap bank control, voltage regulator controls, and other remote terminal units).

Note CGRs, C800s, 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 4000 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, C800s, 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, IR500, and mesh endpoint firmware images. Use Cisco IoT FND to upgrade the firmware on groups of similar devices by loading the firmware image file onto the Cisco IoT FND server, and then uploading the image to the devices in the group. Once uploaded, use IoT FND to install the firmware image directly on the devices.
- **Zero Touch Deployment** – Ease of deployment at scale with Zero-Touch Deployment (ZTD) of gateways and routers.
- **Tunnel Provisioning** – Protects data exchanged between Cisco ASRs and Cisco CGRs and C800s, and prevents unauthorized access to Cisco CGRs to provide secure communication between devices. Cisco IoT FND can execute CLI commands to provision secure tunnels between Cisco CGRs, Cisco C800s, Cisco IR800s and Cisco ASRs. Use Cisco IoT FND to bulk-configure tunnel provisioning using groups.
- **IPv6 RPL Tree Polling** – The IPv6 Routing Protocol for Low-power and Lossy Networks (RPL) finds neighbors and establishes routes using ICMPv6 message exchanges. RPL manages routes based on the relative position of the endpoint to the CGR that is the root of the routing tree. RPL tree polling is available through the mesh nodes and CGR periodic updates. The RPL tree represents the mesh topology, which is useful for troubleshooting. IoT FND maintains a periodically updated snapshot of the RPL tree.
- **Dynamic Multipoint VPN and Flex VPN** – For Cisco C800s and Cisco IR800s, 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 1000s, C800s, and IR800s, 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 CGRs, Cisco C800s, Cisco IR800s, 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.
- **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 2: 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: • 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 (RHEL) 7.7, 64-bit with all packages installed (software development and web server) See Table 5 for suggested application server resource allocation profiles. Note: End of Support (EOS) for RHEL 7.5 in April 2020. • 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: • 2.27 GHz (64-bit) • 2 CPUs • RAM: 4 GB • Disk space: 25 GB	• Red Hat Enterprise Linux (RHEL) 7.7, 64-bit 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: • 3.33 GHz (64-bit) • 2 CPUs • RAM: 16 GB • Disk space: 100 GB	**Note** IoT FND 4.6 supports both of the Oracle releases listed below. • Oracle Database 18c Enterprise Edition (formerly named 12.2c) • Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64-bit Production (with Patch 20830993) **Note** Before installing Oracle, install the Linux packages referenced in “Table 1: Minimum Hardware and Software Requirements for Oracle Install” in the following guide: • Red Hat Enterprise Linux (RHEL) 7.7, 64-bit with all packages installed (software development and web server) **Note** End of Support in April 2020 for Red Hat Linux 7.5, 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 viewIoT FND displays: • Windows 7 or Win2000 R2 Server • RAM: 8 GB • Processor: 2 GHz • Resolution: 1024 x 768	Supported browser: • Microsoft EdgeHTML: 42.17134.1098.0 • Mozilla Firefox: 63 or later
Prime Network Registrar(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 Prime 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 (Microsoft Edge 42.17134.1098.0) and command-line interface (CLI). • Prime Network Registrar 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 10, Windows 7 Enterprise or Microsoft Windows Professional • 2 GHz or faster processor • 2 GB RAM minimum (for potential large log file processing) • WiFi or Ethernet interface • 4 GB disk storage space • Windows login enabled • Utility-signed Certificate Authority (CA) and Client Certificate for router authentication (obtained from your IT department) • Customer-specific IT security hardening to keep the Device Manager laptop secure	• IoT-DM 5.5 • IoT-DM 5.6 • Both versions are compatible with IoT- FND 4.6.x
Cisco 1000 Series Connected Grid Router (CGR)	–	• Cisco IOS Release 15.8(3)M2
Cisco 5921 (C5921) Embedded Service Routers		• Cisco IOS Release 15.8(3)M2
Cisco ISR 800 Series Integrated Services Router (C800)	–	• Cisco IOS Release 15.9(3)M2
Cisco 800 Series Access Points (AP800)	–	• AP802: ap802-k9w7-tar.153-3.JD.tar • AP803: ap1g3-k9w7-tar.153-3.JD.tar
Cisco 800 Series Industrial Integrated Services Router (IR800)	–	• Cisco IOS Release 15.8(3)M2
Cisco 1101 Series Industrial Integrated Services Routers (IR1101)	–	• Cisco IOS-XE 17.2.1

Component	Minimum Hardware Requirement	Software Release Requirements
Cisco 4000 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 16.9.3 for Flex tunnels (IOS)
Note ASRs and ISRs with different releases can co-exist on the network.		
Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR500)	–	• Cisco IR509 and IR510, DA Gateway device: Firmware version 6.2.19 • Cisco IR529 and IR530 Range Extender: Firmware version 6.2.19
Cisco Resilient Mesh Module and supported endpoints	–	• Firmware version 6.2.19 when communicating with CGR 1000s or Cisco ASRs and the minimumCisco IOS software versions recommended for these routers in these release notes
Cisco RF Mesh endpoints	–	• Firmware version 6.2.19 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 (RHEL) 7.7, 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 4 lists example Oracle database server usage profiles for important resource parameters such as CPU, memory, and disk space.

Table 3: 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
6,000/6,000,000	20	96	1000

Table 5 lists example IoT FND Application server usage profiles for important resource parameters such as CPU, memory, and disk space.

Table 4: 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

Nodes(Routers/Endpoints)	CPU(Virtual Cores)	Memory(RAM GB)	Disk Space (GB)
2,000/2,000,000 [1]	8	16	500
5,000/5,000,000 [1]	8	16	500
6,000/6,000,000	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 5: 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 6: Database Server Hardware Requirements Example Profile For Routers and LoRa Modules

(IR800/LoRa modules)	CPU(Virtual Cores)	Memory(RAM GB)	Disk Space (GB)
10,000/30,000	6	32	500

Important Notes

Note At the first login to the FND OVA, the root user will be forced to change the password.

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 version (7.7).

Caveats

This section presents open and resolved caveats in this release and information on using the Bug Search Tool to view details on those caveats. Section topics are:

- Open Caveats
- Resolved Caveats

Open Caveats

There are no known Open Caveats for IoT FND 4.6.2.

Resolved Caveats

Table 7: IoT FND 4.6.2 Resolved Caveats

Caveat Number	Description
CSCvn44512	Used count not matching for legacy CGNMS licenses
CSCvt38501	FND CGNMS setup script corrupts RAC setup
CSCvu84222	Unable to upload file with.tar.gz extension
CSCvv09570	Unexpected EOF error during metric retrieval failures intermittently
CSCvv32393	DB migrate fails when using custom db connection string
CSCvv44554	Upgrade status stuck at 35% for a few IR829 during bulk IOS installation with FND instance in GMM
CSCvv85453	GPS script “fnd-push-gps.td” pushed from GMM impacting user traffic
CSCvv94534	Event notification is not sending events to subscribers
CSCvw07363	Unable to move devices with domain’s firmware groups
CSCvw27368	ZTD provisioning settings - no verification and cgnms.properties check
CSCvw63745	IOT-FND 4.6.1 the Terrain view in the map view is missing
CSCvw70168	Negative Key Index values in FND DB tables (Sync SQL hibernation ID issues)

Table 8: IoT FND 4.6.1 Resolved Caveats

Caveat Number	Description
CSCvo03741	Monitor Only User: Permission denied for ISR3900 and ISR4000 device details page
CSCvr12356	FND Export certificates, wrong file extensions
CSCvr41352	FND 4.1.2-19 PRN got ignored when less than 1 minute PON/PRN outage
CSCvs00562	Provisioning Settings don’t allow multiple servers
CSCvs44179	COAP Server thread killed with a java.lang.NullPointerException
CSCvs53841	Issues with deploying IXM when FND is in Easy Mode
CSCvs83557	FND Connection to HSM - Wrong length for a GeneralizedTime
CSCvu55518	Pruning of tables is not happening (4.6.1)
CSCvu56453	DB server has high CPU usage during S&P test (4.6.0)
CSCvu72491	Not able to add devices in FND when it is partially initialized
CSCvu73044	Unable to delete device files from FND GUI
CSCvu74200	Error handling for not found interface type
CSCvu74218	Memory leak issue observed in FND 4.6.1
CSCvu74222	GMM issue with FND restart

Limitations and Restrictions

Cisco recommends that you review this section before you begin working with IoT FND. These are known limitations, and there is not always a workaround for these issues. Some features might not work as documented, and some features might be affected by recent changes to the software.

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

End of Life Announcements for IoT FND and IoT Device Manager Releases

The following Cisco IoT FND releases are End of Life (EOL):

- Cisco IoT Field Network Director, Release 4.4.x
- Cisco IoT Field Network Director, Release 4.3.x
- Cisco IoT Field Network Releases 4.0.x, 4.1.x and 4.2.x
- Cisco IoT Field Network Releases 3.0, 3.1 and 3.2

The following Cisco IoT Device Manager releases are End of Life (EOL):

- Cisco IoT Device Manager versions 5.0 to 5.4

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:

- 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 devices or applications referenced in this release note, see the following documentation on Cisco.com:

- Cisco IoT Device Manager
- Cisco ASR 1000 Series Aggregation Services Routers Configuration Guide
- Cisco 5921 Embedded Services Router
- Cisco 3000 Series Industrial Compute Gateways (IC3000)
- Cisco 3945 Series Integrated Services Router
- Cisco 800 Series Integrated Services Routers
- Cisco 800 Series Industrial Integrated Services Routers
- Cisco 800 Series Access Points
- Cisco 500 Series WPAN Industrial Routers
- Cisco LoRaWAN Interface Module Hardware Installation Guide
- Cisco Wireless Gateway for LoRaWAN