



Release Notes for IoT Field Network Director, Release 3.0.1-36

Last Updated: March 15, 2016

First Published: August 14, 2015

This release note contains the latest information about using the Release 3.0 user interface for the IoT Field Network Director (IoT FND), IPv6 mesh endpoints, Cisco 1000 Series Connected Grid Routers (CGR 1000 or CGR), Cisco 800 Series Integrated Services Routers (C800s), Cisco 500 Series WPAN Industrial Routers (IR 500), and Cisco 800 Series Industrial Integrated Services Routers (IR 800s).

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

Organization

This guide includes the following sections:

Conventions	Conventions used in this document.
New Features	New features in Release 3.0.
IoT FND Licenses	Summary of supported licenses for Release 3.0.
About Cisco IoT FND	Description of the IoT FND application.
System Requirements	System requirements for Release 3.0.
Installation Notes	Procedures for downloading software.
Important Notes	Notes about Release 3.0.
Limitations and Restrictions	Known limitations in IoT FND.
Caveats	Open and resolved caveats in Release 3.0.
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.
<i>italic</i> font	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic</i> font.
[]	Elements in square brackets are optional.

New Features

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 translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

New Features

Table 1 lists new features in IoT FND 3.0.

IoT FND Licenses

Table 1 New Features in IoT FND 3.0

Feature	Description	First released	Related Documentation
Oracle 12c	IoT FND supports new Oracle 12c installations and upgrades from Oracle 11g.	3.0.1-36	For more information, see <i>Cisco IoT Field Network Director User Guide, Release 3.x</i> at: http://www.cisco.com/go/fnd
Enhancements to the Config > Firmware Update page for Endpoints	<ul style="list-style-type: none"> ■ Subnet List View: Users can filter and view subnets by PAN identifier (PAN ID) and Group. (Group details include number of nodes within the group, hops away from the router, and operation status). ■ Subnet progress histogram 	3.0.1-36	
Enhancement to the Config > Device Configuration page for Endpoints	Push Configuration tab now supports a Subnet view.	3.0.1-36	
IR800 Industrial Integrated Services Routers	IoT FND manages IR809 and IR829, which offer support for integrated 4G LTE wireless WAN (both 809 and 829 models) and wireless LAN capabilities (829 model only).	3.0.0-69	
CG-OS to Cisco IOS software migration	IoT FND supports migrating CGRs running CG-OS software to Cisco IOS software.	3.0.0-69	
Embedded access point (AP) management	IoT FND provides management of embedded APs on C819 and IR829 routers.	3.0.0-69	
4G LTE module support	IoT FND supports management of the CGR 1000 4G LTE module.	3.0.0-69	
Custom EAC certificates	Users can import their ECC certificates for IoT FND CSMP signing instead of employing self-signed certificates.	3.0.0-69	
User Interface enhancements	<ul style="list-style-type: none"> ■ Device Info page: Lists the <i>First Heard date and time</i> for all devices. ■ RPL Tree page: Added Meter ID and serial number for that meter in the Name column. ■ Operations > Events page: Added the ability to enter a start and end time for events. 	3.0.0-69	
Hyper-V support	IoT FND can now operate with Hyper-V and VMware.	3.0.0-69	
North Bound API enhancements	IoT FND supports a new bulk data retrieval API: <ul style="list-style-type: none"> ■ <code>exportDevices</code>: Call returns a list of devices found by the query. This is an asynchronous call. Unlike other device management APIs, this call is blocking until all results are consumed by the caller. 	3.0.0-69	For more information, see the <i>North Bound API User Guide for the Cisco IoT FND Release 3.x</i> . http://www.cisco.com/go/fnd

IoT FND Licenses

Table 2 provides a summary of licenses supported on IoT FND, Release 3.0. Contact your Cisco partner to obtain the necessary licenses.

About Cisco IoT FND

Table 2 Summary of IoT FND Licenses and Associated PIDs

PID	License
L-IOTFND-C800	IoT FND device license for managing the Cisco 800 Series Integrated Services Routers.
L-IOTFND-CGR1K	IoT FND device license for managing CGR 1000 Series Connected Grid Routers.
L-IOTFND-IR509	IoT FND device license for managing Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers.
L-IOTFND-IR800	IoT FND device license for managing the IR800 Industrial Integrated Services Routers.
L-IOTFND-EP-1K	IoT FND device license for managing 1000 endpoints.
L-IOTFND-K9	IoT FND software license for bare-metal deployment (RPMs).
L-IOTFND-V-K9	IoT FND software license for virtual deployments (VMs)

About Cisco IoT FND

The IoT Field Network Director (IoT FND) is a software platform to manage a multi-service network and security infrastructure for IoT applications such as smart grid applications including advanced metering infrastructure (AMI). IoT FND is a scalable, highly secure, modular, and open-platform with an extensible architecture. IoT FND is a multi-vendor, multi-service, communications network management platform that enables network connectivity to an open ecosystem of power grid devices.

Through the browser-based interface, utility operators manage and monitor devices in a Cisco Connected Grid Field Area Network (FAN) solution, using IPv6 over Low-power Wireless Personal Area Networks (6LoWPANs). The FAN includes the following devices:

- Cisco 1000 Series Connected Grid Routers (CGRs), also called pole-top or DIN-rail-mount routers. These devices are identified by model (for example, CGR1000, CGR1120, or CGR1240) on the Field Devices page.
- Cisco 800 Series Industrial Integrated Services Routers (IR 800s) are ruggedized small-form factor cellular routers for mobile/vehicle applications. IR829 include 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 IR 800 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:

- C819HG-4G-V-K9
- C819HG-4G-A-K9
- C819HG-U-K9
- C819HW-S-A-K9
- C819H-K9
- C819G-B-K9

About Cisco IoT FND

- 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, C800s, IR800s, IR 500s 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 with the *IoT Field Network Director User Guide, Release 3.0* for more information: “*Creating Device Groups and Working with Mesh Endpoint Firmware Images*” and “*Configuring Firmware Group Settings*.”
- Cisco 800 Series Access Points are integrated access points on the Cisco 800 Series Integrated Services Routers (C800s). 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 ISR 3900 Series Integrated Service Routers (ISRs), 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, IR 500s and other types of mesh endpoint devices can coexist on a network, but cannot be in the same device group or firmware management group.

The software features enterprise-class fault, configuration, accounting, performance, and security (FCAPS) functionality, as defined in the OSI Network Management reference model.

Cisco IoT Features and Capabilities

- **Configuration Management** – Cisco IoT FND facilitates configuration of large numbers of Cisco CGRs, Cisco C800s, Cisco ASRs, and MEs. Use Cisco IoT FND to bulk-configure devices by placing them into configuration groups, editing settings in a configuration template, and then pushing the configuration to all devices in the group.
- **Device and Event Monitoring** – Cisco IoT FND displays easy-to-read tabular views of extensive information generated by devices, allowing you to monitor your network for errors. Cisco IoT FND provides integrated Geographic Information System (GIS) map-based visualization of FAN devices such as routers and smart meters. Use IoT FND to create CGR-specific work orders that include the required certificates to access the router.
- **Firmware Management** – Cisco IoT FND serves as a repository for Cisco CGR, Cisco C800s, Cisco IR800 (which has a different group for firmware management) and ME firmware images. Use Cisco IoT FND to upgrade the firmware running on groups of devices by loading the firmware image file onto the Cisco IoT FND server, and then uploading the image to the devices in the group. Once uploaded, use IoT FND to install the firmware image directly on the devices.
- **Zero Touch Deployment** – This ease-of-use feature automatically registers (enrolls) and distributes X.509 certificates and provisioning information over secure connections within a connected grid network.
- **Tunnel Provisioning** – Protects data exchanged between Cisco ASRs and Cisco CGRs and C800s, and prevents unauthorized access to Cisco CGRs, to provide secure communication between devices. Cisco IoT FND can execute CLI commands to provision secure tunnels between Cisco CGRs, Cisco C800s, Cisco IR800s and Cisco ASRs. Use Cisco IoT FND to bulk-configure tunnel provisioning using groups.

About Cisco IoT FND

- **IPv6 RPL Tree Polling** – The IPv6 Routing Protocol for Low-power and Lossy Networks (RPL) finds its neighbors and establishes routes using ICMPv6 message exchanges. RPL manages routes based on the relative position of the ME 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.
- **Guest OS (GOS) Support** – For Cisco IOS CGR 1000 devices that support Guest OS, IoT FND allows approved users to manage applications running on the supported operating systems. IoT FND supports all phases of application deployment, and displays application status and the Hypervisor version running on the device.
- **Device Location Tracking** – For CGR 1000, C800, and IR800 devices, IoT FND displays real-time location and device location history.
- **Software Security Module (SSM)** – This is a low-cost alternative to the Hardware Security Module (HSM), and is used for signing CSMP messages sent to meters and IR500 devices.
- **Diagnostics and Troubleshooting** – The IoT FND rule engine infrastructure provides effective monitoring of triage-based troubleshooting. Device troubleshooting runs on-demand device path trace and ping on any CGR, Cisco C800, Cisco IR800, range extender, or meter (mesh endpoints).
- **High Availability** – To ensure uninterrupted network management and monitoring, you can deploy the Cisco IoT FND solution in a High Availability (HA) configuration. By using clusters of load-balanced IoT FND servers and primary and standby IoT FND databases, Cisco IoT FND constantly monitors the health of the system, including connectivity within clusters and server resource usage. If a server cluster member or database becomes unavailable or a tunnel fails, another takes its place seamlessly. Additionally, you can add reliability to your IoT FND solution by configuring redundant tunnels between a Cisco CGR and multiple Cisco ASRs.
- **Power Outage Notifications** – Connected Grid Endpoints (CGEs) implement a power outage notification service to support timely and efficient reporting of power outages. In the event of a power outage, CGEs perform the necessary functions to conserve energy and notify neighboring nodes of the outage. FARs relay the power outage notification to IoT FND, which then issues push notifications to customers to relate information on the outage.
- **Mesh Upgrade Support** – 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

System Requirements

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 with the Cisco 1000 Series Connected Grid Routers:

Command Line Interface

Use the command line interface (CLI) to configure, manage, and monitor Cisco 1000 Series Connected Grid Routers. Learn more at www.cisco.com/go/cgr1000-docs

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 Cisco CGR. IoT-DM uses a local Ethernet or WiFi link to connect to the CGR. Learn more at www.cisco.com/go/cgr1000-docs

System Requirements

Table 3 lists the hardware and software versions associated with this release.

Note: For a large scale system, refer to [Table 4](#) and [Table 5](#) for scale requirements.

Table 3 Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems

Component	Minimum Hardware Requirement	Minimum Software Release and Requirements
Cisco IoT FND application server (or comparable system that meets the minimum hardware and software requirements)	<ul style="list-style-type: none"> ■ Processor: <ul style="list-style-type: none"> — Intel Xeon x5680 2.27 GHz (64-bit) — 2 cores, 2 sockets (2 virtual CPUs) ■ RAM: 16 GB ■ Disk space: 100 GB ■ Hardware Security Module (HSM) or Software Security Module (SSM) 	<ul style="list-style-type: none"> ■ Red Hat Enterprise Linux 6.4 and above, 64-bit with all packages installed (software development and web server) ■ See Table 5 on page 11 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 <p>Note: IoT FND software bundle includes required Java version.</p>

System Requirements

Table 3 Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems (continued)

Component	Minimum Hardware Requirement	Minimum Software Release and 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.	<ul style="list-style-type: none"> ■ Processor: Intel Xeon x5680 3.33 GHz (64-bit) ■ 2 CPUs ■ RAM: 16 GB ■ Disk space: 100 GB 	<ul style="list-style-type: none"> ■ 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) <p>Note: Before installing Oracle, install the Linux packages referenced in Installing the Linux Packages Required for Installing Oracle.</p> <p>See Table 4 on page 11 for suggested Oracle Database server resource allocation profiles.</p> <ul style="list-style-type: none"> ■ Red Hat Linux 6.4 and above, 64-bit with all packages installed (software development and web server)
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"> ■ Windows 7 or Win2000 R2 Server ■ RAM: 8 GB ■ Processor: 2 GHz ■ Resolution: 1024 x 768 	<ul style="list-style-type: none"> ■ Adobe Flash Version 9.0.115 or later (required for viewing charts) ■ Supported browsers: <ul style="list-style-type: none"> – Internet Explorer (IE): 10.0 or 11.0 – Mozilla Firefox: 3.5 or later – Windows 7 works with IE 10.0 with 128-bit cipher and IE 11.0
Cisco Network Registrar (CNR) (used as a DHCP server)	<p>Server must have the following minimum requirements:</p> <ul style="list-style-type: none"> ■ Free disk space: 146 GB ■ RAM: 4 GB (small network), 8 GB (average network), 16 GB (large network) ■ Hard drives: <ul style="list-style-type: none"> – SATA drives with 7500 RPM drive > 500 leases/second or – SAS drives with 15K RPM drive > 1000 leases/second 	<p>The following software environment must exist before installing Cisco Network Registrar, software release 8.2 on the server:</p> <ul style="list-style-type: none"> ■ Operating System: Windows Server 2008 ■ Java Runtime Environment (JRE) 7.0 (1.7.0_60) or equivalent Java Development Kit (JDK) ■ User interfaces: Web browser and command-line interface (CLI) (Browser versions listed below): <ul style="list-style-type: none"> – Internet Explorer (IE) 8.0, 9.0 (with 9.0.x Flash plug-in) and later – Mozilla Firefox 3.0 or later ■ CNR license. Contact your Cisco partner for the necessary license.

System Requirements

Table 3 Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems (continued)

Component	Minimum Hardware Requirement	Minimum Software Release and Requirements
IoT Device Manager (IoT-DM or Device Manager)	Laptop running Device Manager must have the following: <ul style="list-style-type: none">■ Microsoft Windows 7 Enterprise■ 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	<ul style="list-style-type: none">■ Version 5.0.0.16
Cisco 1000 Series Connected Grid Router (CGR)	-	<ul style="list-style-type: none">■ Cisco IOS Release 15.5(3)M■ Cisco CG-OS Release CG4(3) and later
Cisco ISR 800 Series Integrated Services Router (C800)	-	<ul style="list-style-type: none">■ Cisco IOS Release 15.5(3)M
Cisco 800 Series Access Points (AP800)	-	<ul style="list-style-type: none">■ AP802: ap802-k9w7-tar.153-3.JBB.tar■ AP803: ap1g3-k9w7-tar.153-3.JBB2.tar
Cisco 800 Series Industrial Integrated Services Router (IR800)	-	<ul style="list-style-type: none">■ Cisco IOS Release 15.5(3)M
Cisco 3900 Series Integrated Service Router (ISR)	-	<ul style="list-style-type: none">■ 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	-	<ul style="list-style-type: none">■ Cisco IOS XE Release 3.140S 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.		

System Requirements

Table 3 Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems (continued)

Component	Minimum Hardware Requirement	Minimum Software Release and Requirements
Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR500)	-	<ul style="list-style-type: none"> ■ Cisco IR509, DA Gateway device: Firmware version 5.5.80 ■ Cisco IR529, Range Extender: Firmware version 5.5.80 ■ RF mesh endpoints: Firmware version 5.5.80
Cisco Connected Grid CG-Mesh Module and supported endpoints	-	<ul style="list-style-type: none"> ■ Firmware version 5.5.80 when communicating with CGR 1000s or Cisco ASRs and the minimum Cisco IOS software versions recommended for these routers in these release notes ■ Firmware version 5.2.82 is the minimum requirement for meters; however, 5.5.80 is recommended
Cisco IoT FND TPS proxy	<ul style="list-style-type: none"> ■ Processor: <ul style="list-style-type: none"> — Intel Xeon x5680 2.27 GHz (64-bit) — 4 cores, 2 sockets (2 CPUs) ■ RAM: 4 GB ■ Disk space: 25 GB 	<ul style="list-style-type: none"> ■ Red Hat Enterprise Linux 6.4 and above with all packages installed (software development and web server) ■ Internet connection <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> <p>Note: IoT FND software bundle includes required Java version.</p>
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"> ■ Release 6.10.2 firmware <p>Note: Contact SafeNet to determine if you can run a higher version.</p> <ul style="list-style-type: none"> ■ Release 5.4.7-1 software, plus security patches <p>Luna SA client software:</p> <ul style="list-style-type: none"> ■ Release 5.4.7-1 software
Software Security Module (SSM)	<ul style="list-style-type: none"> ■ RAM: 8 GB ■ Processor: 2 GHz 	<ul style="list-style-type: none"> ■ Red Hat Enterprise Linux 6.4 or 7.1, 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.

Installation Notes

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 on page 11](#) lists example Oracle database server usage profiles for important resource parameters such as CPU, memory, and disk space.

Table 4 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
1000/1,000,000	12	48	1000
2000/2,000,000	16	64	1000
5000/5,000,000	20	96	1000

[Table 5 on page 11](#) lists example IoT FND Application server usage profiles for important resource parameters such as CPU, memory, and disk space.

Table 5 Application 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	4	16	250
1000/1,000,000	8	16	250
2000/2,000,000 ¹	8	16	500
5000/5,000,000 ¹	8	16	500

1. Clustered installations.

Note: We strongly recommend RAID 10 for deployments of 2 million endpoints and above.

Installation Notes

The installation procedure for IoT FND comprises several tasks, as described in the *Cisco IoT Field Network Director User Guide, Release 3.x*. 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 User Guide.

Important Notes

Important Notes

In [Limitations and Restrictions, page 12](#) and [Caveats, page 12](#), 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).

Limitations and Restrictions

Cisco recommends that you review this section before you begin working with IoT FND. These are known limitations that will not be fixed, 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.

■ CSCui54154

Symptom: On the **Device > Routers or Devices > Field Devices** page in List view with routers selected, on the Config tab the Config Error Details column may contain a hyperlink to the error description. If the Config tab is exported using the Export CSV option, the Config Error Details column is not included in the exported CSV file.

Conditions: This issue occurs when trying to export the Config tab with routers selected.

Workaround: There is no workaround for this issue.

■ CSCui54221

Symptom: On the **Device > Routers or Devices > Field Devices** page in List view with routers selected, on the Firmware tab the Firmware Error Details column may contain a hyperlink to the error description. If the Firmware tab is exported using the Export CSV option, Firmware Error Details column is not included in the exported CSV file.

Conditions: This issue occurs when trying to export the Firmware tab with routers selected.

Workaround: There is no workaround for this issue.

■ CSCuy49541

Symptom: When navigating to the Firmware page, the left pane and right pane do not show correct data.

Conditions: Navigating to the images tab before the firmware tab has finished loading.

Workaround: Wait for firmware tab to complete loading before navigating to the images tab.

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 17](#)
- [Accessing the Bug Search Tool, page 19](#)

Caveats

Open Caveats

■ CSCtx50284

Symptom: CG-NMS failed to shut down cleanly. The Cisco CG-NMS `server.log` file included exceptions.

Conditions: Occurred when the Cisco CG-NMS server was shut down or restarted using the Red Hat service commands `service cgms stop` or `service cgms restart` and Cisco CG-NMS internal server components shut down in an incorrect sequence.

Exceptions might have also appeared in the `server.log` file if any Cisco CG-NMS logging category is set to “Debug” level, as at this level, exceptions that represent normal internal activity might have been logged.

If the Cisco CG-NMS server was not commanded to shut down using the service commands, then check the `cgms_watchdog.log` to see if watchdog restarted Cisco CG-NMS. If watchdog restarted Cisco CG-NMS, then there was a notation in `cgms_watchdog.log` providing the reason watchdog was triggered.

If the shutdown cannot be explained, then the exceptions might have indicated why the server shut down, and should be reviewed by the Cisco Technical Assistance Center (TAC).

Workaround: There is no workaround for this issue.

■ CSCty78770

Symptom: If two or more devices have the same GPS coordinate (which is likely if two Cisco CGRs are on the same pole), the icon in the map shows the devices as a cluster even at maximum zoom in.

Conditions: This issue occurs when two devices of the same type have the same GPS location.

Workaround: There is no workaround for this issue.

■ CSCtz29999

Symptom: On the Devices List page under “WiMAX Link Info”, the Base Station Identifier (BSID) field is not populated.

Conditions: The issue only occurs for WiMAX links.

Workaround: There is no workaround for this issue.

■ CSCub90976

Symptom: When configuring high availability (HA) on the secondary database at initial setup, the entire output of the database content copy is unexpectedly seen in the log output. Logging is inconsistent with logs when a new database is set up.

Conditions: The issue occurs when configuring or setting up a secondary CG-NMS database.

Workaround: There is no workaround for this issue.

■ CSCuc17916

Symptom: When reprovisioning or creating workorders for the Cisco CGR, a Cisco CGR SSID entry greater than 31 characters in the CSV import file does not throw an error during import, but creates other issues.

Conditions: The issue occurs when an SSID entry with more than 31 characters is found.

Workaround: Limit the number of characters to less than or equal to 31.

Caveats

■ CSCuf95076, CSCuf95834

Symptom: During tunnel reprovisioning on a cluster failover, a System Error appears in the Reprovisioning Status column. Exceptions are listed in the log on the active NMS server when the CGR contacts it to complete the reprovisioning. Tunnel reprovisioning fails and snippets of exceptions display in the Error Message and Error Details columns, but the CGR can successfully register with the active NMS server.

Conditions: This issue occurs during CG-NMS cluster failovers.

Workaround: There is no workaround for this issue.

■ CSCug77724

Symptom: When using RPDON in the CG mesh solution, outage and registration messages from the smart meters are not handled correctly.

Conditions: This issue occurs when one meter in the mesh is powered off and the RPDON heartbeat frequency and peer down count are set to maximum. On meter power-up the meter status and restore messages are not reported correctly.

Workaround: There is no workaround for this issue.

■ CSCuj70073

Symptom: Deleting a large number of elements from CG-NMS takes a long time.

Conditions: This issue occurs when you delete a large number of elements from CG-NMS and devices with issues are included in the operation. CG-NMS must lock all devices. Devices with issue rows in the NMS database increase the time of the delete operation.

Workaround: There is no workaround for this issue.

■ CSCul02893

Symptom: The Confirm dialog box does not display to start an SD Card Password push.

Conditions: This issue occurs during an SD card password enable or disable operation.

Workaround: There is no workaround for this issue.

■ CSCul05847

Symptom: On the **Config > Device Configuration > Push Configuration** page during a push SD card password operation, the start and end times displayed are the same.

Conditions: This issue occurs during an SD card password enable or disable operation.

Workaround: There is no workaround for this issue.

■ CSCul51424

Symptom: The same SSID is assigned to all CGRs in a group during reprovisioning.

Conditions: This issue occurs when generating a random SSID using the factory reprovisioning template and the prefix length is 31 characters, which is the valid length for the entire SSID. CG-NMS does not check the prefix length.

Workaround: There is no workaround for this issue.

■ CSCuo96336

Symptom: A success message displays on metrics refresh although WSMA was timed out. No WSMA error displays.

Caveats

Conditions: This issue occurs when you click Refresh Metrics and CG-NMS successfully refreshes, but WSMA was timed out.

Workaround: There is no workaround for this issue.

■ CSCuo96482

Symptom: A CGR module hot swap causes a CG-NMS metric retrieval failure, and an error displays in CG-NMS during **show interfaces** command processing.

Conditions: This issue occurs during CGR reprovisioning where a module in the CGR was just swapped.

Workaround: There is no workaround for this issue. Avoid removing modules during CGR provisioning.

■ CSCuq38133

Symptom: Rule event severity is not consistent for certain event categories.

Conditions: This issue occurs when you select **Operations > Events > Rule Events** and you see a mix of event severities grouped into the Rule Event category.

Workaround: In order to view Events with a specific Severity, add "eventSeverity:<desired severity>" to the search query. An example query would be - eventName:ruleEvent eventSeverity:INFO

■ CSCur38441

Symptom: On the **Field Devices** page, in Map view with the Overlay option and a group selected, clicking a cluster icon displays the device count either as zero or an incorrect number.

Conditions: This issue occurs with the overlay feature enabled and set to All or Associated Endpoints/Routers, and the zoom level set so that a single marker denotes a group of devices.

Workaround: To display an accurate device count, zoom in until the icons no longer appear clustered and display as individual icons on the map.

■ CSCur44911

Symptom: During the ZTD process, illegal state exceptions display in the server logs indicating tunnel interface change traps occurred.

Conditions: This issue occurs when you add a new interface on the router that CG-NMS did not detect. Exceptions display in the server log when CG-NMS receives traps from that interface.

Workaround: There is no workaround for this issue. Exceptions are not logged after CG-NMS detects the interface either during periodic inventory polling or user-triggered refresh metrics.

■ CSCut65807

Symptom: This bug is applicable only when CG-NMS is installed on a Red Hat Enterprise Linux 7.x server. CG-NMS fails to obtain DHCP leases (both IPv4 and IPv6) from the DHCP server during router configuration. You can observe the DHCP calls timing out in the CG-NMS log files. This affects router provisioning.

Conditions: This issue occurs when CG-NMS is configured to bind to all interfaces (that is, set to "0.0.0.0" for IPv4, and ":" for IPv6) for DHCP IPv4 and IPv6 client purposes, and CG-NMS fails to start client services on ports 67 and 547. As a result, CG-NMS fails to obtain leases for routers, which leads to router configuration failures.

Workaround: You must configure specific IPv4 and IPv6 addresses from the CG-NMS Linux host server to which to bind DHCP IPv4 and IPv6 clients by setting the following values in CG-NMS:

Caveats

- **Admin > Provisioning Settings > DHCPv6 Proxy Client > Client Listen Address:** Set the value to the IPv6 address of the interface to use to obtain IPv6 DHCP leases from the DHCP server. The default value is “::”. Change the default setting to an actual IPv6 address on the Linux host machine.
- **Admin > Provisioning Settings > DHCPv4 Proxy Client > Client Listen Address:** Set the value to the IPv4 address of the interface to use to obtain IPv4 DHCP leases from the DHCP server. The default value is “0.0.0.0”. Change the default setting to an actual IPv4 address on the Linux host machine.

■ CSCuv32208

Symptom: IoT FND GUI shows the database (DB) server in “down” state when checked under "Servers" section. All FND operations work correctly and no side effects are observed as a consequence of this apparent “down” state of the DB server. The database is marked “up” on the IoT FND application server restart but is soon marked “down” after 15 minutes of startup.

Conditions: This is caused under certain circumstances when periodic jobs responsible for updating the DB server status are stuck in the ACQUIRED state and never recover. This prevents the IoT FND application from updating the status of the DB server.

Workaround: The following workaround requires access to the DB server.

1. Stop the IoT FND application server.
2. Log in to the DB server as *cgms_dev_user*.
3. Update the State column for the CgnmsDbJobTrigger row in the QRTZ_TRIGGER tables from ACQUIRED to WAITING.
4. Commit the transaction.
5. Start the IoT FND application server.

■ CSCuw44833

Symptom: When making a request for a getJob function call, from the SOAP UI, the user will get an empty response.

Conditions: Occurs when using SOAP UI to query for getJob function within the NB API.

Workaround: There is no workaround for this type of call.

■ CSCuw62985

Symptom: User expects two events for each cluster for an HSM down issue/event, but only receives one.

Conditions: When HSM is unreachable or down only one issue/event is raised

Workaround: No workarounds exist, only one event is used to determine if the HSM is down.

■ CSCuy68887

Symptom: Mesh firmware update histogram does not display small values.

Conditions: During mesh firmware update, the histogram depicting upload progress does not show bars for buckets with smaller device counts as compared to large values. An example would be if the 100% bucket has 50,000 devices and the bucket for 60-70% has only 200 devices, the bar for 200 is not shown.

Workaround: Go to the **Devices** tab for the firmware group on which operation is being performed; and, order by Update Progress column. This list will report progress for all devices in the group.

■ CSCuy74922

Symptom: Mesh Operator User does not see option in the GUI to upload meter/mesh image to IoT FND.

Caveats

Conditions: User with Mesh Operator privileges.

Workaround: Create a custom role and add 'Router Firmware Update' privileges to the existing set of privileges that a 'Mesh Operator' role has.

Resolved Caveats

■ CSCuv85990

Symptom: NBAPI search and device tool queries are not working.

Conditions: NBAPI search and device tool queries are not working.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.

■ CSCuw51087

Symptom: EOF exceptions are seen due to timeout at the TPS server when applying large templates at CGR.

Conditions: Trigger a dual homing request with a large template.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.

■ CSCuw79955

Symptom: CSV file cannot be generated when the uptime column is selected.

Conditions: Export devices using the uptime column.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.

■ CSCuw82504

Symptom: Monitor user is not able to create Quick Views.

Conditions: Try to create Quick view and Tab view as monitor user.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.

■ CSCuw84635

Symptom: If an NBAPI query is made for a larger count of devices than is available, then the DB connection pool will ultimately be exhausted.

Conditions: Heavy NBI usage with queries that are not using queryIDs and are using counts larger than total number of devices present.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.

■ CSCuw86435

Symptom: NBAPI search query was given without specifying any additional parameters such as FieldNames. Query returned output unsuccessfully as it did not default to EID.

Conditions: Made search queries without any field names.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.

■ CSCuw88183

Symptom: Tunnel UP events are not seen in Events UI.

Caveats

- Conditions:** ASR is polled and the tunnel status moves to UP. NMS should generate a TUNNEL UP event.
- Workaround:** This issue is resolved in IoT FND Release 3.0.1-36.
- **CSCux13788**

Symptom: When making calls as non-root user, the connection opened to validate permissions is not closed once the task is completed.

Conditions: Occurs when making NB API calls as non-root user.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.
 - **CSCux14011**

Symptom: Outages are being processed for unheard devices, when they should only be processed for down or up devices.

Conditions: Trigger outages and observe unheard mesh device state.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.
 - **CSCux22730**

Symptom: When a large number of issues are generated, some may be dropped.

Conditions: Generate a large number of issues on CG-NMS and observe.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.
 - **CSCux27440**

Symptom: Authorization proceeded in error for an NB API user that was in a disabled state.

Conditions: Made NB API calls from a user in a disabled state,

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.
 - **CSCux29355**

Symptom: Audit trail entries are not recorded for successful and unsuccessful NBAPI login attempts.

Conditions: NB API calls are generated.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.
 - **CSCux31111**

Symptom: NBAPI request for user with expired password still works.

Conditions: Make NBAPI request as a user whose password has expired.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.
 - **CSCux37411**

Symptom: Monitor user is able to view password policy.

Conditions: Navigating to password policies page as a user that only has monitor/read-only permissions.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.
 - **CSCux57905**

Related Documentation

Symptom: If the user executes multiple file upload operation one after another, a DB connection pool will be exhausted after some time.

Conditions: Seen under heavy file upload operations.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.

■ CSCux61413

Symptom: Only 50 of the first 100 archived logs are visible.

Conditions: Up to 100 logs can be archived.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.

■ CSCuy20218

Symptom: Spelling errors visible in logs for a PRN event.

Conditions: Spelling errors visible in logs for a PRN event.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.

■ CSCuy34572

Symptom: Google Maps Javascript API not supported on Internet Explorer 11 (IE 11)when working .

Conditions: When opening IoT FND 3.0 in IE 11, a message appears indicating an incompatible browser instead of the expected maps.

Workaround: This issue is resolved in IoT FND Release 3.0.1-36.

Accessing the Bug Search Tool

You can use the Bug Search Tool to find information about caveats for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To access the Bug Search Tool, use the following URL: <https://tools.cisco.com/bugsearch/search>

To search using a specific bug ID, use the following URL: <https://tools.cisco.com/bugsearch/bug/<BUGID>>

Related Documentation

Find Cisco 1000 Series Connected Grid Routers and IoT Device Manager documentation at:

www.cisco.com/go/cgr1000-docs

For information on additional systems referenced in this release note, see the following documentation on Cisco.com:

- [Cisco ASR 1000 Series Aggregation Services Routers Configuration Guide](#)

Related Documentation

- [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](#)

Related Documentation

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

No combinations are authorized or intended under this document.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015-2016 Cisco Systems, Inc. All rights reserved.

Related Documentation