Release Notes for IoT Field Network Director, Release 4.12.x

First Published: 2024-05-15

Release Notes for IoT Field Network Director, Release 4.12.x

This release notes contain the latest information about using the user interface for IoT Field Network Director (IoT FND), Release 4.12.x to configure and manage IPv6 mesh endpoints, Cisco 1000 Series Connected Grid Routers (CGR1120 or CGR1240), Cisco LoRaWAN IXM Gateway, Cisco 500 WPAN Industrial Routers (IR500), and Cisco 800 Series Industrial Integrated Services Routers (IR807, IR809, and IR829), Cisco Industrial Compute Gateway IC3000, Cisco 1101 Integrated Services Router, Cisco Catalyst IR8100 Heavy-Duty Series Router, and Cisco Catalyst IR1800 Rugged Series Routers.

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.

Cisco IoT FND Documentation

Listed below are the user documents that support this release:

- Cisco IoT FND Postgres and Influx DB Deployment with Integrated Application Management on OVA, Release 4.3.1 and Later
- Cisco IoT FND Deployment on an Open Virtual Appliance
- Cisco IoT Field Network Director Installation Guide-Oracle Deployment, Releases 4.3.x and Later
- Cisco IoT Field Network Director User Guide, Release 4.12.x
- Release Notes for Cisco Resilient Mesh Release 6.7
- Release Notes for Cisco Resilient Mesh Release 6.2.35
- Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and Cisco Resilient Mesh Configuration Guide (Cisco IOS)

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

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

Conventions

This document uses the following conventions.

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

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

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

Warning **IMPORTANT SAFETY INSTRUCTIONS**

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for

preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Regulatory:

Provided for additional information and to comply with regulatory and customer requirements.

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 Catalyst IR1800 Rugged Series Routers are secure, 5G routers designed with a high level of modularity that supports private LTE, FirstNet, Wi-Fi6, and Gigabit Ethernet. These routers offer enterprise-grade security from the hardware to the network communications all the way to the industrial assets. The routers are powered by Cisco IOS® XE, Cisco's fully programmable next-generation operating system. Automotive certifications and features such as Controller Area Network (CAN) bus support, dead reckoning and Global Navigation Satellite System (GNSS), and ignition power management make it ideal for secure, reliable connectivity in transit and public safety applications.
- The IP 67-rated Cisco Catalyst IR8100 Heavy-Duty Series routers is a modular, secure, rugged and outdoor router that is suitable for harsh physical environments. It has multiple WAN (LTE, LTE-Advanced, LTE Advanced Pro, 5G Sub-6GHz1, RJ45/SFP Ethernet) and storage options. The router supports wireless and wired connectivity such as 5G, public, or private LTE, Wi-SUN, LoRaWAN, and has more connectivity options making it more adaptable. It runs on Cisco IOS XE and Cisco IOS XE provides both autonomous and controller (SD-WAN) mode support.
- 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 Wi-Fi 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 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, 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. See the following sections in the IoT Field Network Director User Guide for more information on: "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 with IR829 platforms. These access points are referred to as FARs in this document and identified by product ID (for example, AP800).
- Cisco ASR 1000 Series Aggregation Services Routers (ASRs), Cisco 8000 Series Routers, 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).

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 FAR, HER, gateways, 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 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 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 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 IR800 devices, DMVPN and Flex VPN do not require IoT FND to apply device-specific tunnel configuration to the HER during tunnel provisioning. HER tunnel provisioning is only required for site-to-site VPN tunnels.
- **Dual PHY Support** — IoT FND can communicate with devices that support Dual PHY (RF and PLC) traffic. IoT FND identifies CGRs running Dual PHY, enables configuration to masters and slaves, and collects metrics from masters. IoT FND also manages security keys for Dual PHY CGRs. On the mesh side, IoT FND identifies Dual PHY nodes using unique hardware IDs, enables configuration pushes and firmware updates, and collects metrics, including RF and PLC traffic ratios.
- **Device Location Tracking** — IoT FND displays real-time location and device location history for CGR 1000, IR1101, IR8100, IR800, and N2450 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 IR800, range extender, or meter (mesh endpoints).
- **High Availability** — To ensure uninterrupted network management and monitoring, you can deploy the Cisco IoT FND solution in a High Availability (HA) configuration. By using clusters of load-balanced IoT FND servers and primary and standby IoT FND databases, Cisco IoT FND constantly monitors the health of the system, including connectivity within clusters and server resource usage. If a server cluster member or database becomes unavailable or a tunnel fails, another takes its place seamlessly. Additionally, you can add reliability to your IoT FND solution by configuring redundant tunnels between a Cisco CGR and multiple Cisco ASRs.
- **Power Outage Notifications** — Cisco Resilient Mesh Endpoints (RMEs) implement a power outage notification service to support timely and efficient reporting of power outages. In the event of a power outage, CGEs perform the necessary functions to conserve energy and notify neighboring nodes of the outage. FARs relay the power outage notification to IoT FND, which then issues push notifications to customers to relate information on the outage.
- **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.

- **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.

New Features in Cisco IoT FND 4.12.x

The table summarizes the new and updated features that are included in this release and tells you where they are documented in the User Guide.

Features	Description
PSK Challenge String	Enhances the security between FND and FAR in the SUDI+PSK based tunnel management.
PSK Rotation	This feature offers the ability to rotate the PSK on FAR and HER to enhance network security.
IPAM for All Interfaces	IP address management is supported for all interfaces. You can define multiple subnets and allocate the IP addresses from those subnets to the interfaces in IoT FND. This removes the dependency of relying on a third-party DHCP server.
Upgrade IOS Image during Bootstrapping – IR1800 and IR8100	Allows to perform firmware image upgrade on IR1800 and IR8100 devices from versions 17.13.01 and above. During bootstrapping, you can enter a different image if the installed image at manufacturing is inappropriate. For PNP skip updates, define the firmware versions separated by commas in the pnp-skip-update-ios-xe-fw-versions property in cgms.properties.
Support Mesh Parent for L+G Endpoints	FND displays the mesh parent value as 1 for L+G endpoints.
Exporting Mesh Routing Tree Data	Supports exporting the mesh routing tree information of the parent and child nodes into an Excel file.
CGMS Certificate Renewal for Routers	Support for automated CGMS and/or CA certificate renewal for router.
Integrating Third-Party Endpoints in IoT FND through CSMP	Periodic metric and configuration push for report interval are supported in the phase 2 of CSMP.

Install and Upgrade Instructions

The release-specific install and upgrade instructions are covered in this section.

Bare Metal Deployment with Oracle

- Use the *--force* option in install and upgrade commands starting from Cisco IoT FND 4.11.0.

  Example:

```
[root@iot-fnd-oracle ~]# rpm -qa | grep cgms
cgms-4.11.0-50.x86_64
cgms-tools-4.11.0-50.x86_64
cgms-oracle-4.11.0-50.x86_64
[root@iot-fnd-oracle ~]#
[root@iot-fnd-oracle programs]# rpm -Uvh cgms-4.11.0-69.x86_64.rpm --force
[root@iot-fnd-oracle programs]# rpm -Uvh cgms-oracle-4.11.0-69.x86_64.rpm --force
[root@iot-fnd-oracle programs]# rpm -Uvh cgms-tools-4.11.0-69.x86_64.rpm --force
[root@iot-fnd-oracle programs]# rpm -ivh cgms-influx-4.11.0-69.x86_64.rpm --force
[root@iot-fnd-oracle programs]# rpm -ivh cgms-ssm-4.11.0-69.x86_64.rpm --force
[root@iot-fnd-oracle programs]# rpm -ivh cgms-tpsproxy-4.11.0-69.x86_64.rpm --force
[root@iot-fnd-oracle programs]# rpm -ivh fnd-ra-4.11.0-69.x86_64.rpm --force
```

- For upgrades, it is recommended that all rpm versions (such as tools, ssm, tpsproxy) align with the FND version.

VM Deployment with Postgres

- **Install**: Download (`CISCO-IOTFND-VPI-K9-<release>-<build number>-SHA256.zip`), which contains both FND and TPS OVA. It is recommended to use the same version of FND and TPS.
- **Upgrade**: Use (`CISCO-IOTFND-VPI-K9-UPGRADE-SCRIPTS-<release>-<build number>.zip`) to upgrade the FND. Delete the older TPS VM and install the TPS OVA for the newer version.

System Requirements

The following table lists the hardware and software versions associated with this release.

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: 150 GB
		• Red Hat Enterprise Linux (RHEL) 8.8, 64-bit with all packages installed (software development and web server) is recommended for Cisco IoT FND version 4.12.x.
		Note FND application software is backward compatible with RHEL versions. For example, Cisco IoT FND version 4.8.1 and above is compatible with earlier versions of RHEL such as 7.7.
		See Bare Metal Mesh Deployment with Oracle for suggested application server resource allocation profiles.
		• Internet connection
		When you access IoT FND from a client browser, the browser connects to the Internet to download the necessary data files from the GIS maps provider.
		• A license to use SafeNet for mesh endpoint security
		Note IoT FND software bundle includes required Java version.

Component	Minimum Hardware Requirement	Software Release Requirements

Cisco IoT FND TPS proxy	• Processor:
	  • 2.27 GHz (64-bit)
	  • 2 CPUs
	• RAM: 4 GB
	• Disk space: 25 GB
		• RHEL 8.8, 64-bit with all packages installed (software development and web server) is recommended for Cisco IoT FND version 4.12.x.
		• Internet connection
		Note IoT FND software bundle includes required Java version.

Database server for IoT FND • Scalability: Up to 25 routers/10,000 endpoints with minimum hardware requirement. See Resource Management Guidelines, on page 13 for additional scale sizes. • High availability: Oracle 19c RAC is supported from IoT FND 4.7 onwards.	• Processor: 3.33 GHz (64-bit) • 4 CPUs • RAM: 16 GB • Disk space: 150 GB	• Cisco IoT FND release 4.7 and later supports the Oracle Database 19c Enterprise Edition. Before installing Oracle, install the Linux packages referenced in “Minimum Hardware and Software Requirements for Oracle Install” in Cisco IoT Field Network Director Installation Guide-Oracle Deployment, Releases 4.3.x and Later. See Bare Metal Mesh Deployment with Oracle of this release notes for suggested Oracle Database server resource allocation profiles. • RHEL 8.8, 64-bit with all packages installed (software development and web server) is recommended for Cisco IoT FND version 4.12.x.

Component	Minimum Hardware Requirement	Software Release Requirements
Cisco IoT FND—RA	• Processor: 2.27 GHz (64-bit) • 2 CPUs • RAM: 4 GB • Disk space: 25 GB	• RHEL 8.8, 64-bit with all packages installed (software development and web server) is recommended for Cisco IoT FND version 4.12.x. • Internet connection **Note** From Cisco IoT FND 4.8.x onwards, only Python version 3.9.5 is supported.
Cisco IoT FND Client	The client must meet the following minimum requirements to connect to the IoT FND application server and view IoT FND displays: • Windows 10 • RAM: 8 GB • Processor: 2 GHz • Resolution: 1024 x 768	Supported browsers: • Microsoft EdgeHTML: 42.17134.1098.0 • Mozilla Firefox: 88 or later

Cisco 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:
		• For CPNR 11.1.1, the recommended operating system is AlmaLinux 8.6
		• For CPNR 10.1, the recommended operating system is Windows Server 2012 R2
		• 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)
		• For Prime Network Registrar license, contact your Cisco partner.

Component	Minimum Hardware Requirement	Software Release Requirements
Hardware Security Module (HSM)	Luna SA appliance, with client software installed on the IoT FND application servers	Luna SA appliance: • Release 7.4 firmware **Note** Contact SafeNet to determine if you can run a higher version. • Release 7.4 software, plus security patches Luna SA client software: • Release 10.2 software with 7.3 patch
Software Security Module (SSM)	• RAM: 8 GB • Processor: 2 GHz • 2 CPUs	• RHEL 8.8, 64-bit with all packages installed (software development and web server) is supported.

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.

Systemctl Command Support for RHEL Version 8.x

If the RHEL version is 8.x or later, then use `systemctl` command instead of the `service` command as given in the table.

RHEL Version	Command
For CGMS	
8.x	`systemctl <status/start/restart/stop> cgms`
7.x	`service cgms <status/start/restart/stop>`
For TPSPROXY	
8.x	`systemctl <status/start/restart/stop> tpsproxy`
7.x	`service tpsproxy <status/start/restart/stop>`
For SSM	
8.x	`systemctl <status/start/restart/stop> ssm`
7.x	`service ssm <status/start/restart/stop>`

RHEL Version	Command
For FND-RA	
8.x	`systemctl <status/start/restart/stop> fnd-ra`
7.x	`service fnd-ra <status/start/restart/stop>`

Supported Device Types in IoT FND

The following device types are supported in the IoT FND:

Device Types	Software Release Requirements
FAR	
1. Cisco Catalyst IR1800 Rugged Series Routers	• Cisco IOS XE Release 17.14.1a • Cisco IOS XE Release 17.13.01a • Cisco IOS XE Release 17.06.07
2. Cisco IR8140 Heavy-Duty Series Routers	• Cisco IOS XE Release 17.14.1a • Cisco IOS XE Release 17.13.01a • Cisco IOS XE Release 17.06.07
3. Cisco 1101 Series Industrial Integrated Services Routers (IR1101)	• Cisco IOS XE Release 17.14.1a • Cisco IOS XE Release 17.13.01a • Cisco IOS XE Release 17.06.07
4. Cisco CGR1000 Series Connected Grid Router (CGR1120 and CGR1240)	• Cisco IOS Release 15.9.3M9(MD) • Cisco IOS Release 15.8.3M9(MD)
5. Cisco 800 Series Industrial Integrated Services Router (IR800)	• Cisco IOS Release 15.9.3M9(MD) • Cisco IOS Release 15.8.3M9(MD)
6. Cisco 800 Series Access Points (AP800) are integrated with IR829 platforms.	• AP803: 15.3.3-JK10 • AP802: 15.3.3-JF15
HER	
1. Cisco 8000 Series Routers	• C8000V: Cisco IOS XE 17.6.7 (MD) • C8500L: Cisco IOS XE 17.6.7 (MD)

Device Types	Software Release Requirements
2. Cisco ASR 1001 or 1002 Aggregation Services Router (ASR) serving as a head-end router	Cisco IOS XE Release 17.6.7 (MD)
3. Cisco 4000 Series Integrated Service Router (ISR)	• Cisco IOS Release 15.4(3)M • Cisco IOS Release 15.4(2)T
4. Cisco Cloud Services Router 1000V Series (CSR)	Cisco IOS XE Release 17.3.4a(MD)
Note C8000, ASRs, and ISRs with different releases can coexist on the network.	
Compute Gateway	
Cisco IC3000 Industrial Compute Gateway	• 1.5.1 • 1.4.2
Long Range Wide Area Network (LoRaWAN) Interface Module for Cisco 800 Series Industrial Integrated Services Routers (IR800)	• LoRa/IXM-LPWA 2.3.1 • LoRa/IXM-LPWA 2.3.0
Mesh Endpoints	• Wi-SUN firmware version 6.8.0 • Dual stack supported version 6.2.35 (MR) • Non-Wi-SUN firmware version 5.6.42
Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR500)	The firmware versions supported for the following router series are: • Cisco IR510 (DA Gateway device) — 6.8.0 and 6.2.35 (MR) • Cisco IR530 (Range Extender) — 6.8.0 and 6.2.35 (MR)

Resource Management Guidelines

This section provides the resource management guidelines for the bare metal and virtual machine deployments. Both bare metal and virtual machine deployment options support mesh management and router management.

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 an 8-CPU host, do not allocate all 8 CPUs to ensure that one (or more) VM does not use all resources.

- Mesh Deployment
- Router-Only Deployment

Mesh Deployment

This section provides the resource management guidelines for the following mesh deployment options.

- Bare Metal Mesh Deployment with Oracle
- VM Mesh Deployment with Oracle

Bare Metal Mesh Deployment with Oracle

This section provides the resource management guidelines for the application and database servers for this deployment.

IoT FND Application Server

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

Nodes (Routers/Endpoints)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
25/10,000	2	16	100
50/50,000	4	16	200
500/500,000	4	16	250
1,000/1,000,000	8	16	250
2,000/2,000,000	8	16	500
6,000/6,000,000	8	16	500
8,000/8,000,000	8	32	500

Note Four application servers are recommended for 8,000/ 8,000,000 routers/endpoints.

Note IoT FND can process approximately 90 CSMP packets per second per node.

Oracle Database Server

The following table lists example Oracle database server usage profiles for important resource parameters such as CPU, memory, and disk space.

Nodes (Routers/Endpoints)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
25/10,000	2	16	100

Nodes (Routers/Endpoints)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
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
8,000/8,000,000	32	160	2000

VM Mesh Deployment with Oracle

The following table lists example server usage profiles for important resource parameters such as CPU, memory, and disk space.

Nodes (Routers/Endpoints)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
2,000/2,000,000	24	96	1500

Router-Only Deployment

This section provides the resource management guidelines for the following router-only deployments.

- Bare Metal Router-Only Deployment with Oracle
- VM Router-Only Deployment with Postgres

Bare Metal Router-Only Deployment with Oracle

IoT FND Application Server

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

Routers	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
25,000	32	64	500
10,000	16	48	500

Oracle Database Server

The following table lists example Oracle database server usage profiles for important resource parameters such as CPU, memory, and disk space.

Routers	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
25,000	96	128	1000
10,000	64	96	1000

VM Router-Only Deployment with Postgres

The following table lists example server usage profiles for important resource parameters such as CPU, memory, and disk space.

Routers	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
25,000	24	96	800
15,000	16	64	500

Note The default value of heap memory is 6GB, which is appropriate for 15,000 routers. The heap memory used in 25,000 routers is 12GB.

To configure the heap memory:

- Open a cmd console and navigate to /opt/fnd/conf folder.
- Edit the fnd-env.list file and modify the value of MAX_JVM_HEAP_SIZE property from 6g to 12g and save the file.
- Restart the FND container.
- Verify the change by logging into IoT FND, and navigating to **Devices** > **Server** > **NMS Server**. Select the device and check the updated heap memory provided as Memory Allocation under IoT-FND Application Information section.

Note When you upgrade your IoT FND, follow the steps mentioned above to update the heap memory from the default value of 6GB.

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 RHEL version 8.8.

Documentation Updates

1. **Troubleshooting IoT FND** —This chapter in the "Cisco IoT Field Network Director User Guide, Release 4.10.x" is moved to the Troubleshooting Guide for Cisco IoT Field Network Director.
2. **Cisco IoT Field Network Director Post-Installation Guide, Release 4.3.x and later**—This guide is no longer available as the chapters of this guide are moved to the following guides:
   a. Managing Tunnel Provisioning—Cisco IoT Field Network User Guide, Release 4.8.x
   b. Managing High Availability Installations—Cisco IoT Field Network Director Installation Guide - Oracle Deployment, Releases 4.3.x and Later

IoT FND Release Upgrade Matrix

This section provides IoT FND upgrade information based on the current and target releases.

Target Release	You Can Upgrade to the Target Release (Left column) from the Following Releases (Right Column)	
4.12.0-xxx	4.11.0-69 (OVA) 4.11.0-69 (ISO)	4.10.0-45 (OVA) 4.10.0-46 (ISO)
4.11.0-xxx	4.10.0-45 (OVA) 4.10.0-46 (ISO)	4.9.0-62 (ISO, OVA) 4.9.1-8 (Postgres OVA) 4.9.2-4 (ISO)
4.10.0-xxx	4.9.1-8 4.9.0-62	4.8.1-72 4.8.0-130 (ISO), 4.8.0-133(OVA)
4.9.1-xxx **Note** This release is only for Postgres OVA deployment.	4.9.0-62 4.8.1-72 4.8.0-130 (ISO), 4.8.0-133 (OVA)	4.7.2-8 4.7.1-60 4.7.0-100
4.9.0-xxx	4.8.1-72 4.8.0-130 (ISO), 4.8.0-133 (OVA)	4.7.2-8 4.7.1-60 4.7.0-100
4.8.1-xxx	4.8.0-xxx	4.7.2-8 4.7.1-60 4.7.0-100

Target Release	You Can Upgrade to the Target Release (Left column) from the Following Releases (Right Column)	
4.8.0-xxx	4.7.2-8 4.7.1-60 4.7.0-100	4.6.2-16 4.6.1-61
4.7.2-8	4.7.1-60 4.7.0-100	4.6.1-61
4.7.1-60	4.7.0-100	4.6.1-61
4.7.0-100	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 4.4.1-10 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	4.1.1-64.1.0-257
4.2.0-123	4.1.0-257	4.0.0-299

Note Sometimes, firmware images are not displayed in GUI while upgrading the IoT FND from earlier versions to 4.8.x. To resolve this issue, we recommend that you clear the browser cache.

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 are required to get to the target release. Use the table above to plan the upgrade paths.

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

Example:

If your network is running IoT FND 4.4.0-79 and your Target Release is 4.8.0-xx, then your best upgrade path is:

- 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 are:

1. Backup IoT FND 4.4.0-79 database.
2. Perform an upgrade to IoT FND 4.6.1-61 using the upgrade instructions in the Installation Guide.
3. Start IoT FND 4.6.1-61 and login to the IoT FND user interface and perform a quick sanity check.
4. Stop IoT FND 4.6.1-61 services.
5. Backup IoT FND 4.6.1-61 database.
6. Upgrade to IoT FND 4.8.0-xx using the upgrade instructions in the Installation Guide.
7. Start IoT FND 4.8.0-xx and log into the GUI.

Hardware Security Module (HSM) Upgrade Table

For Cisco IoT-FND Release 4.6.2 and greater, within the IoT-FND image bundle, there are new subfolders for the jar and API files: `/opt/cgms/safenet/LunaX`.

Note LunaProvider.jar and libLunaAPI files contain the HSM library patch for the defect CSCvs83557.

The table below lists the HSM client versions that are tested and recommended for the corresponding Cisco IoT FND software versions. However, FND application software is backward compatible with HSM client versions. For example, FND version 4.7.1 is compatible with older versions of HSM client such as 5.4, 6.3.

HSM Upgrade Table

FND Software Release	HSM Client	HSM Software
4.7.1 to 4.12.x	10.2	7.4
4.6	7.3 with software patch	7.4
4.5	7.3 with software patch	7.3
4.4	7.3 with software patch	7.0

Install SUDI Certificate with 2099 expiry in FND and TPS keystore

SUDI 2099 has to be installed in FND and TPS for compatibility with newer versions of images for devices.

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 software.

Feature	IoT FND Releases	Upgrade Impact
LDevID: Auto-Renewal of Certs and Saving Configuration	4.9.1	By default, this feature is disabled. However, if required, you can enable the feature. For information on enabling the feature, see LDevID: Auto-Renewal of Certs and Saving Configuration.
	4.9.0	By default, this feature is disabled. We recommend the users "NOT to enable" this feature because it could break the FAR connectivity with FND.
CSMP-Request tool support for L+G endpoints	4.9.0 onwards	Owing to L+G platform limitation, CSMP-Request tool fails for L+G endpoints when passing single TLV. **Workaround**: We recommend that you use minimum two TLVs in the CSMP-Request tool for the L+G endpoints.
Firmware Upgrade during PnP	4.4 to 4.9.0	The PnP workflow supports device upgrade only if the target image version is higher than the running (current) image version. If the target image runs the same or lower version, then the device upgrade is skipped during the PnP workflow. **Note** From Cisco IoT FND 4.9.1 onwards, both device upgrade and downgrade are supported during the PnP workflow.
External DHCP support for tunnel provisioning	Applicable to all IoT FND releases	External DHCP is not supported for tunnel provisioning in the Postgres-OVA deployment.

Feature	IoT FND Releases	Upgrade Impact
DB migration fails due to incorrect incremental size	4.10	The database schema and IoT FND should match in order to avoid the failure during DB migrate, hence the hibernate jars were upgraded in Cisco IoT FND 4.10.0. **Workaround**: Execute the query in order to update the incremental value in the DB. For more information, see Troubleshooting guide.
Cellular MODEM gets powered off during firmware upgrade	4.11	Cellular MODEM gets powered off during firmware upgrade and after the firmware upgrade, the router does not register back with FND. This happens when the certificate renewal date and the firmware upgrade date overlaps. **Workaround**: To avoid this, ensure to complete the firmware upgrade either before or after the automatic certificate renewal date.
PSK rotation on IR829	4.12	For IR829, the PSK tunnels must be configured using the cellular interface. It is not supported on switch port/SVI interfaces. For more information, see CSCwj64906.

Caveats

This section presents the open and resolved caveats in Cisco IoT FND releases and information on using the Bug Search Tool to view details on those caveats.

Open Caveats

The section lists the open caveats in Cisco IoT FND Release 4.12.x.

Table 1: Cisco IoT FND 4.12.x

Caveat ID	Description
CSCwf96300	Factory reprovisioning failed on FND for IR1101 with bootstrapping flag in template.

Resolved Caveats

This section lists the resolved caveats in Cisco IoT FND Release 4.12.x.

Table 2: Cisco IoT FND 4.12.x

Caveat ID	Description
CSCwj79081	Multi license+Multi domain Licence available count shows count with expired license device count.
CSCwi84496	Docker container logs are not getting rotated.
CSCwj32260	IR8140 low battery events are not reported in FND.

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 valid Cisco credentials (user ID and password).

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

End of Life Bulletins for IoT FND Releases

EOL Announcement

End of Sale and End of Life Bulletin for IoT Device Manager

- Cisco IoT Device Manager

Related Products

This section provides links to the Cisco IoT FND related products:

- Cisco Catalyst IR1800 Rugged Series Routers
- Cisco Catalyst IR8100 Heavy Duty Series Routers
- Cisco Catalyst 1101 Rugged Routers
- Cisco 1000 Series Connected Grid Routers
- Cisco 5921 Embedded Services Routers
- Cisco 800 Series Integrated Services Routers
- Cisco 800 Series Industrial Integrated Services Routers
- Cisco 800 Series Access Points
- Cisco 8000 Series Routers
- Cisco ASR 1000 Series Aggregation Services Routers Configuration Guide
- Cisco ISR 4000 Series

- Cisco 4431 Integrated Services Router
- Cisco 500 Series WPAN Industrial Routers
- Cisco 3000 Series Industrial Compute Gateways (IC3000)
- Cisco Wireless Gateway for LoRaWAN