Revised: January 24, 2025

Release Notes for Cisco IoT Field Network Director, Release 5.0.x

Introduction To Cisco IoT Field Network Director

Cisco IoT FND offers high security, scalability, and modularity. Its pluggable architecture allows network connectivity to a multi-vendor ecosystem of Cisco and third-party IoT devices.

The Cisco IoT FND software platform enables a clear separation between communications network management and operational applications, such as distribution management systems, outage management systems, and meter data management in utilities. You can manage a multi-service network of routers or a combination of routers and endpoint devices with end-to-end security tailored to your specific use case using Cisco IoT FND. For more information, see the Introduction to Cisco IoT FND.

What's New In Cisco IoT FND Release 5.0.x

New Features

Feature Name	Description	Business Outcome
Achieve Scale Beyond 25,000 Routers	Starting from Cisco IoT FND Release 5.0, you can manage up to 50,000 routers using Cisco IoT FND on a VM using Postgres + Influx database.	Scale your network operations significantly, accommodating growth without the need for additional hardware investments.
Autosync of CGMS Properties Files	Cisco IoT FND ensures that any changes made to the CGMS properties file, whether inside or outside the container, are automatically mirrored in the corresponding file. This synchronization maintains consistency across configurations, reducing the risk of errors and ensuring seamless application performance.	Maintain consistent configurations across Cisco IoT FND deployments. This reduces the likelihood of configuration errors that could disrupt operations, leading to fewer application downtimes and improved performance reliability.
Bootflash Space Cleanup	Check the **Remove unused firmware images from bootflash** check box to remove unused firmware bin files from the bootflash when Cisco IoT FND uploads the image to the router. The check box is enabled for the following devices running Cisco IOS-XE: • Cisco Catalyst IR1100 • Cisco Catalyst IR8100 • Cisco Catalyst IR1800	Clears up space in the bootflash when there is no more space available for an efficient firmware upload.

Feature Name	Description	Business Outcome
Enhancement to Firmware Update Page for Down and Active Device Status	Cisco IoT FND includes two additional device statuses in the **Firmware Update** page: **Down Devices** and **All Devices**.	Filter your search based on the device statuses for routers running a firmware group. View the count of all devices that are part of a given firmware group of routers.
Improved Audit Trail	When you add or remove or edit files using .CSV files on Cisco IoT FND, a log is generated in the **Audit Trail** page. You can download the .CSV file that you used to change the devices.	Provides a clear and detailed record of all changes made to devices via .CSV files, enhancing accountability and traceability. You can download the .CSV file used for these changes, it facilitates easier audits and ensures that you can verify and review modifications.
Manage Router Firmware Upgrades	Manage Router Firmware upload, install and retry counts using Cisco IoT FND, instead of editing the CGMS properties file.	Automating the firmware upgrade process and tracking install counts with Cisco IoT FND reduces the time and effort required for manual updates.
Manage Firmware Upgrade Properties For A Router Group	Cisco IoT FND includes a **Router Firmware Upload Retry Count** in the **Firmware Update** page. Customize the retry count at the router group level, allowing for tailored firmware update strategies for specific groups of routers.	Customizing the retry count at the router group level in Cisco IoT FND's Firmware Update page enhances the efficiency of firmware update strategies, resulting in improved operational uptime and reduced network downtime for specific groups of routers.
Manage Router Push Configuration Count	Define the number of router configuration changes or updates that you want to apply to routers within a specific group. Manage and track the number of configuration changes applied to a group of routers during the configuration push using Cisco IoT FND.	Defining and managing the number of router configuration changes for specific groups using Cisco IoT FND ensures precise control over network configurations, enhancing network stability and streamlining operations.
Search in the **Device Configuration** page	The **Device Configuration** page has a new search bar for you to search through the various device configurations.	The search bar on the **Device Configuration** page allows you to search through various device configurations, helping you narrow down your scope to easily identify a device.
Search Firmware Updates	Search through the existing firmware updates using the filters introduced in this release	The filters introduced allow you to search through the existing firmware updates, making the firmware updates page searchable.
Username and Password Validation	Cisco IoT FND includes username and password validation check for CSV file input.	The username and password validation helps in enhancing the security standards for usernames and passwords.

Modified Features

Feature Name	Description	Business Outcome
Additonal HER Support	The Cisco IoT FND supports Cisco Catalyst 8500 and 8300 series HER platforms: Cisco Catalyst 8500-12X and Cisco Catalyst 8300-1N1S-4T2X.	The additional HER platforms enhance network scalability and reliability, enabling more efficient management and monitoring of Cisco IoT devices. The additional HER support improves operational efficiency and reduces downtime.
User Experience Enhancements	The Cisco IoT FND dashboard includes pre-defined dashlets, where an additional **Name** field is added along with the Element Identifier (**EID**). You can delete the default views of the devices you select in the **Devices** > **Field Devices** page. You can also add the user-defined properties in the customized tab in the **Field Devices** page.	Easy to use dashlets which are more accessible, enhance your experience. The intuitive tab navigation facilitates faster task completion, allowing you to seamlessly switch between different tasks and functionalities. Additionally, you can also customize the dashboard to suit your specific needs, providing a more personalized and efficient workflow.
Device-Level Configuration Push	You can push the configurations at the device level using the **Push Configuration** tab in the **Field Devices** page when you click the device using two options: Config push without-rollback or Config push with-rollback.	You can manage configuration at the device level, providing more flexibility for managing siloed devices and reducing the time it takes to push new configuration
Show Registration Config vs Running Config	In the **Running Config** tab of a device page, you can see both the Registration Config and the active running config of the device.	You can track configuration changes at the device level which helps in managing and reducing configuration drift and provides better visibility to your network devices.
Admin Password Rotation	The Cisco IoT FND tools package includes a new script `rotate_admin_password.sh` with CSV input file. This script enables the seamless rotation of administrator passwords across Cisco IoT FND devices, supporting both Cisco IOS and Cisco IOS XE device types.	This enhancement streamlines the process of updating administrator credentials periodically, ensuring consistent security practices, and simplifying password management across your network infrastructure.

Feature Name	Description	Business Outcome
Full Open CoAP Simple Management Protocol Support	A Vendor TLV 127 value support is added to the Full Open CoAP Simple Management Protocol (CSMP) for the Cisco IoT FND devices. A new tab **Vendor TLV Info** is introduced where you can add the TLV details for a selected device. You can modify and retrieve Vendor TLV details and push the modified configuration to new endpoints. You can also upgrade and manage the firmware with supported TLVs.	This feature allows customization and flexibility, improves control over device settings and behaviors, enhances operational efficiency, and provides better visibility and monitoring.
EID Field	EID field is added in most of the Cisco IoT FND pages for you to access the **Device Info** of the devices which are associated with the EID.	The EID hyperlinks enhance your experience by allowing easy access to device information from any page which has device details in Cisco IoT FND.
Update Target Firmware Versions For All Users	In Cisco IoT FND Release 4.12.x and earlier releases, when you change the target firmware versions in the **Router Bootstrap Configuration** tab, the target firmware changes don't reflect in Cisco IoT FND. Starting from Cisco IoT FND Release 5.0, when you make changes to the target firmware version, the changes reflects for all the other associated Cisco IoT FND users.	Starting from Cisco IoT FND Release 5.0, you experience seamless synchronization of target firmware version changes across all associated accounts.

Important Notes For Cisco IoT FND Release 5.0.x

Install SUDI Certificate with 2099 expiry in FND and TPS keystore. The SUDI 2099 has to be installed in FND and TPS for compatibility with newer versions of images for devices.

GUI Changes In Cisco IoT FND Release 5.0.x

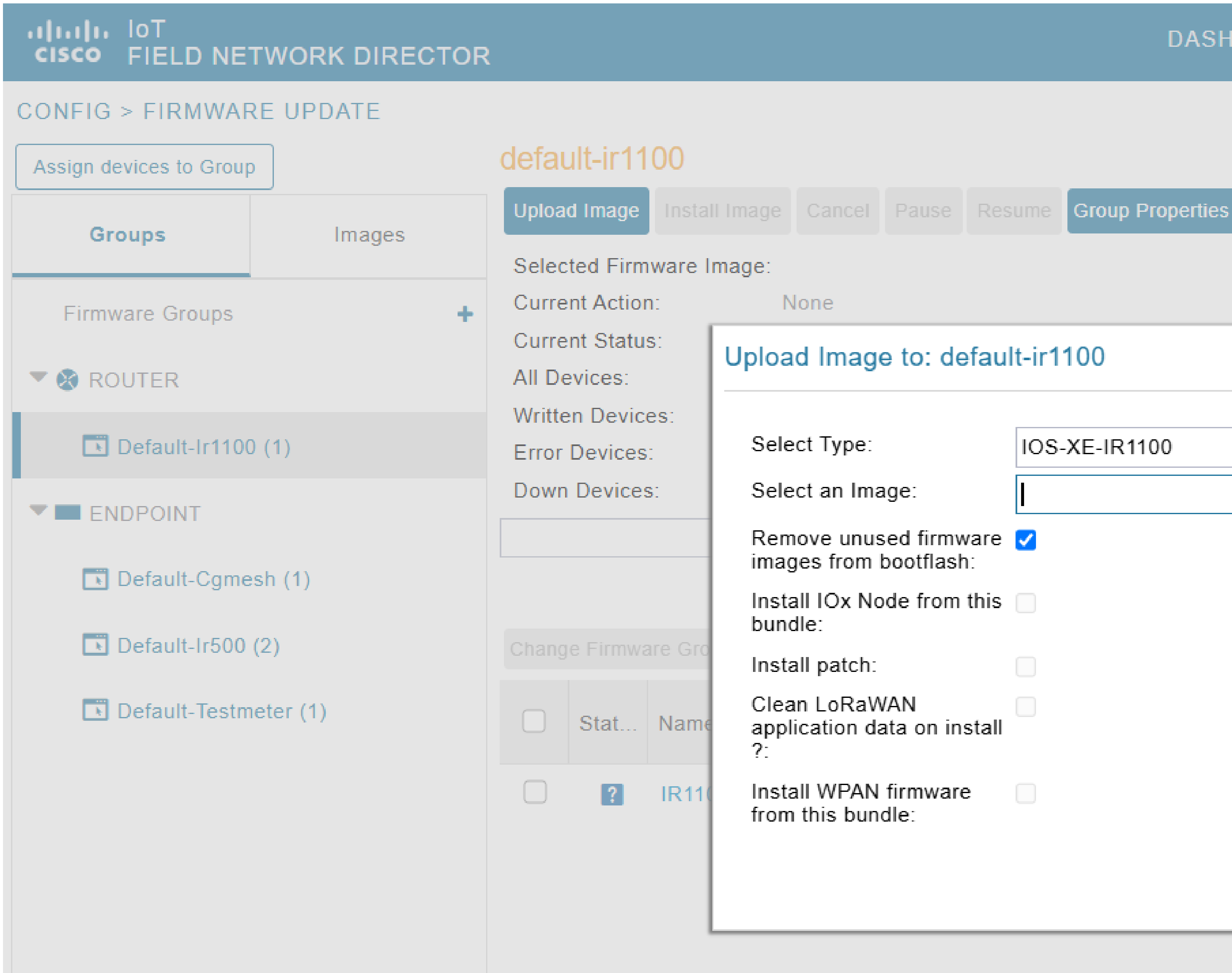
This section presents a summary of the significant GUI changes between Cisco IoT FND Release 4.12.1 and Cisco IoT FND Release 5.0.

- Search bar in the **Device Configuration** page

- Search bar in the **Firmware Update** page

- New property settings in the **Server Settings** page.

- The **Remove unused firmware images from bootflash** check box is added to the upload firmware image pane.



Selected Firmware Image:

Current Action: None

Current Status:

All Devices:

Written Devices:

Error Devices:

Down Devices:

Upload Image to: default-ir1100

Select Type: IOS-XE-IR1100

Select an Image:

Remove unused firmware images from bootflash: ☑

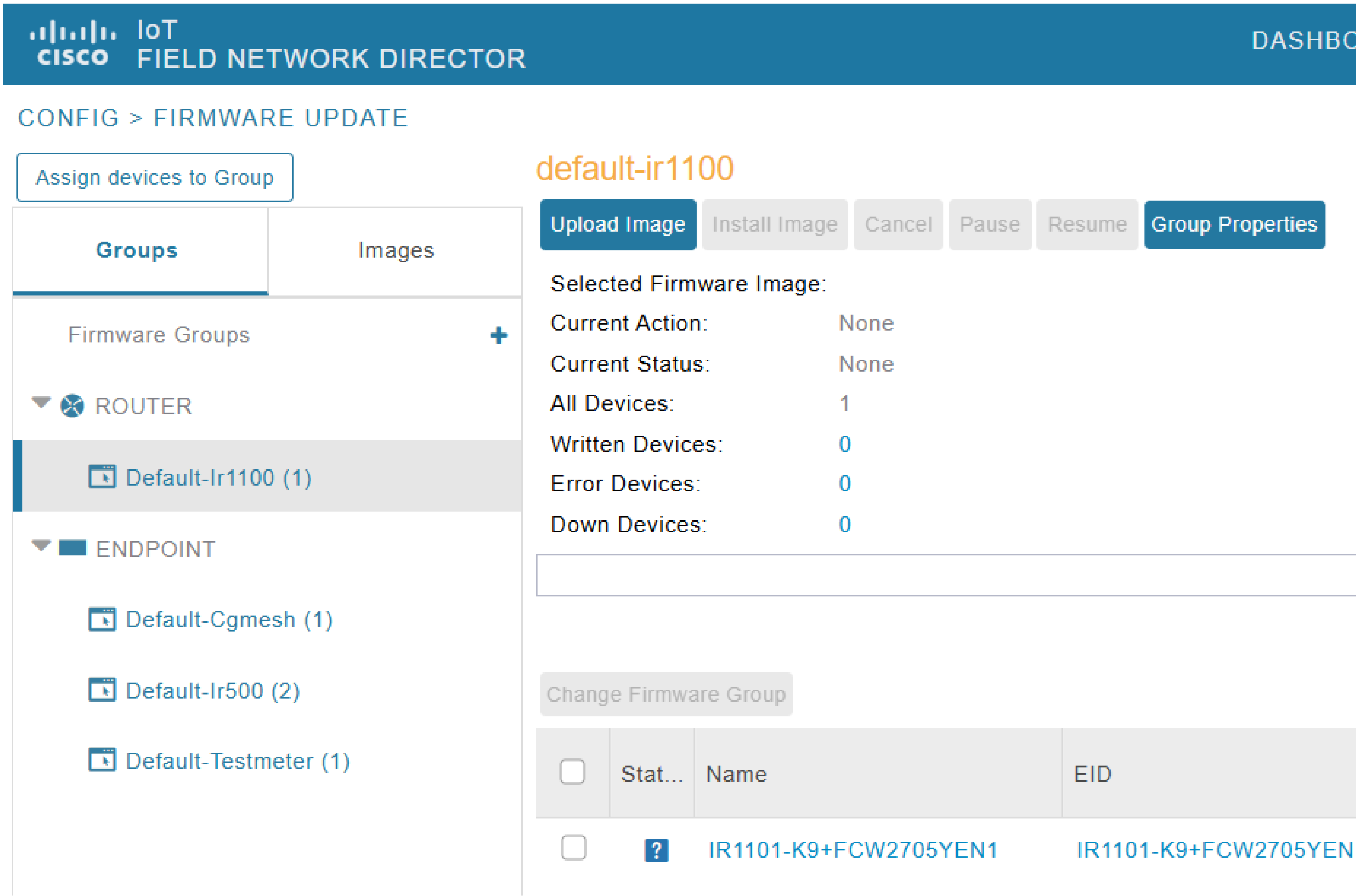
Install IOx Node from this bundle: □

Install patch: □

Clean LoRaWAN application data on install ?: □

Install WPAN firmware from this bundle: □

- **Firmware Update** page adds two new device statuses in addition to existing ones: **All Devices** and **Down Devices**.



Selected Firmware Image:

Current Action: None

Current Status: None

All Devices: 1

Written Devices: 0

Error Devices: 0

Down Devices: 0

□	Stat...	Name	EID
□	?	IR1101-K9+FCW2705YEN1	IR1101-K9+FCW2705YEN

Supported Devices And Device Types

Supported Devices

Device Name	Description
Routers	

Device Name	Description
Cisco Catalyst IR1800 Rugged Series Routers	The 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.
Cisco Catalyst IR8100 Heavy-Duty Series routers	The IP 67-rated Cisco Catalyst IR8100 Heavy-Duty Series Router 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)	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	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 Cisco IoT FND to manage the following IR800 models: IR809 and IR829.

Device Name	Description
Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers	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)	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	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 ASR 1000 Series Aggregation Services Routers, Cisco 8000 Series Routers, and Cisco 4000 Series Integrated Service Routers	These routers are referred to as *head-end routers* or HERs in this document.
Access Points and Endpoints	
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).

Device Name	Description
Cisco IPv6 RF mesh endpoints (smart meters and range extenders)	Cisco IPv6 RF mesh endpoints, including smart meters and range extenders, are designed to enhance smart grid networks by providing reliable, scalable, and secure communication for utility management. These devices leverage IPv6 technology to ensure efficient data transmission and robust connectivity across extensive utility infrastructures.

Supported Device Types And Versions

Device Types	Software Release Requirements
FAR	
Cisco Catalyst IR1800 Rugged Series Routers	• Cisco IOS XE Release 17.16.1 • Cisco IOS XE Release 17.15.2 • Cisco IOS XE Release 17.9.5b
Cisco IR8140 Heavy-Duty Series Routers	• Cisco IOS XE Release 17.16.1 • Cisco IOS XE Release 17.15.2 • Cisco IOS XE Release 17.9.5b
Cisco 1101 Series Industrial Integrated Services Routers (IR1101)	• Cisco IOS XE Release 17.16.1 • Cisco IOS XE Release 17.15.2 • Cisco IOS XE Release 17.9.5b
Cisco CGR1000 Series Connected Grid Router (CGR1120 and CGR1240)	• Cisco IOS Release 15.9.3M9(MD) • Cisco IOS Release 15.9-3M10(MD)
Cisco 800 Series Industrial Integrated Services Router (IR800)	• Cisco IOS Release 15.9.3M9(MD) • Cisco IOS Release 15.9-3M10(MD)
Cisco 800 Series Access Points (AP800) are integrated with IR829 platforms.	• AP803: 15.3.3-JK10 • AP802: 15.3.3-JF15
HER	
Cisco 8000 Series Routers	• C8000V: Cisco IOS XE 17.6.7 (MD) • C8500L: Cisco IOS XE 17.6.7 (MD)
Cisco ASR 1001 or 1002 Aggregation Services Router (ASR) serving as a head-end router	Cisco IOS XE Release 17.6.7 (MD)

Device Types	Software Release Requirements
Cisco 4000 Series Integrated Services Router (ISR)	• Cisco IOS Release 15.4(3)M • Cisco IOS Release 15.4(2)T
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)

System Requirements and Recommended Computing Resources

Validated Browsers

- Microsoft Edge
- Firefox 3.5 or higher

Note

All the listed browsers require the Adobe Flash Player 11 plug-in.

Supported Cisco IoT FND Deployment Methods

- Bare Metal with Oracle DB

- OVA with Oracle DB
- OVA with Postgres + Influx DB

System Requirements For Mesh Deployments

Mesh Deployments Using Bare Metal With Oracle

Using Cisco IoT FND Application Server

Nodes (Routers/Endpoints)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
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.
- We recommend you to use the cluster method for application server if you are using over 2,000/20,000 routers/endpoints.

Note

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

Using Oracle Database Server

Nodes (Routers/Endpoints)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
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

Mesh Deployments Using Virtual Machines With Oracle

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

System Requirements For Router-Only Deployments

Router-Only Deployments Using Bare Metal With Oracle

Using Cisco IoT FND Application Server

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

Using Oracle Database Server

Routers	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
25,000	32	96	1000
10,000	16	96	1000

Router-Only Deployments Using Virtual Machines With Postgres

Routers	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
50,000	24 (cores per socket: 4 and sockets: 6)	96	800
25,000	24 (cores per socket: 4 and sockets: 6)	96	800
15,000	16	64	500

Note

Set the Java Heap memory to 12 GB to achieve a 25,000 scale, and increase the heap memory to 18 GB for anything greater than a 25,000 scale. For more information see, Achieve Scale Beyond 25,000 Routers.

OpenSSH Version

Since Cisco 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 Cisco IoT FND server is up-to-date. On initial installation, upgrade the OpenSSH package in the Cisco IoT FND server to RHEL version 8.8 and later versions.

Caveats

The Caveats section includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a specific caveat, use the Cisco Bug Search Tool (BST).

Open Caveats

There are no open caveats captured in the Cisco IoT FND Release 5.0.

Resolved Caveats

Bug ID	**Description**
CSCwk77651	ERROR: duplicate key value violates unique constraint "net_tunnels_pkey" Detail
CSCwf79373	FND[4.9.0-62] UI with IR8140 Scrolling issue on Mesh Router Tree tab
CSCwm61478	DHCPv4 and DHCPv6 Loopback Link address not used in DHCP DISCOVER message
CSCwn37460	Target FW version under pnp not updating across all the users
CSCwk33955	Meters mesh tree map links stop at the first hop
CSCwn24188	FW upload MD5 checksum is not occurring for IR8100 and IR1800 device types
CSCwm06020	Increase CPU and Memory notices when Router Upgrade / Downgrade triggered as part of PNP
CSCwm75885	FND UI does not include Last GPS Heard for the IR8140
CSCwm75882	FND IR8140 lat and long are overwritten by 0,0 coordinates
CSCwm03426	UI Error rendering view - failed with NullPointerException
CSCwm39996	Metric Retrieval Failure - java.lang.NullPointerException

Upgrade Cisco IoT FND

Cisco IoT FND Release Upgrade Matrix

Current Release	**Target Release**
4.12.0-69 (OVA), 4.12.0-69 (ISO), 4.11.0-69 (OVA), and 4.11.0-69 (ISO)	5.0-xxx

Current Release	Target Release
4.11.0-69 (OVA), 4.11.0-69 (ISO), 4.10.0-45 (OVA), and 4.10.0-46 (ISO)	4.12.0-xxx
4.10.0-45 (OVA), 4.10.0-46 (ISO), 4.9.0-62 (ISO, OVA), 4.9.1-8 (Postgres OVA), and 4.9.2-4 (ISO)	4.11.0-xxx
4.9.1-8, 4.9.0-62, 4.8.1-72, 4.8.0-130 (ISO), and 4.8.0-133(OVA)	4.10.0-xxx
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, and 4.7.0-100	4.9.1-xxx **Note** This release is only for Postgres OVA deployment.
4.8.1-72, 4.8.0-130 (ISO), 4.8.0-133 (OVA), 4.7.2-8, 4.7.1-60, and 4.7.0-100	4.9.0-xxx
4.8.0-xxx, 4.7.2-8, 4.7.1-60, and 4.7.0-100	4.8.1-xxx
4.7.2-8, 4.7.1-60, 4.7.0-100, 4.6.2-16, and 4.6.1-61	4.8.0-xxx
4.7.1-60, 4.7.0-100, and 4.6.1-61	4.7.2-8
4.7.0-100 and 4.6.1-61	4.7.1-60
4.6.1-61 and 4.5.1-11	4.7.0-100
4.5.1-11, 4.4.4-9, 4.4.3-4, 4.4.2-11, 4.4.1-10, and 4.4.0-79	4.6.1-61
4.4.2-11, 4.4.1-10, 4.4.0-79, 4.3.2-7, 4.3.1-7, and 4.3.0-133	4.5.1-11
4.3.1-7, 4.3.0-133, and 4.2.0-123	4.4.x
4.2.0-123 and 4.1.1-64.1.0-257	4.3.x
4.1.0-257 and 4.0.0-299	4.2.0-123

Note

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

Note

- The 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 your upgrade.

  Upgrade each intermediate version(s) and initiate the Cisco IoT FND application. If you are able to login to Cisco IoT FND, it is the best indication that your upgrade is successful.

Upgrading Hardware Security Module (HSM)

Starting from Cisco IoT FND Release 4.6.2 and later, within the Cisco IoT FND image bundle, there are new subfolders for the .jar and API files, here's the filepath: `/opt/cgms/safenet/LunaX`.

Note

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

Cisco IoT FND application software is backward compatible with the HSM client versions. For example, Cisco IoT FND version 4.7.1 is compatible with older versions of HSM clients such as 5.4, 6.3.

Cisco IoT FND Software Release	HSM Client	HSM Software
5.0.0	10.12 with software patch	7.4
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

Cisco IoT FND Documentation

The following documents are available for Cisco IoT FND:

- Cisco IoT Field Network Director User Guide, Release 5.0.x
- Cisco IoT FND 4.3.1 and Later Postgres and Influx DB Deployment with Integrated Application Management on OVA
- Cisco IoT FND Deployment on an Open Virtual Appliance, VMware ESXi 5.5/6.0
- Cisco IoT Field Network Director Installation Guide-Oracle Deployment, Releases 4.3.x and Later
- Cisco IoT Field Network Director—Oracle DB Installation and Upgrade Guide
- North Bound API User Guide for Cisco IoT Field Network Director, Release 4.x
- Troubleshooting Guide for Cisco IoT Field Network Director

End of Life and End of Sale Bulletins

- EOL Announcement
- Cisco IoT Device Manager EOL and EOS