Introduction to Cisco IoT Field Network Director

First Published: 2024-07-16

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Full Cisco Trademarks with Software License

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.

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 of this document are considered uncontrolled. See the current online version for the latest version.

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

CHAPTER 1

IoT FND Overview

Cisco IoT Field Area Network Director (FND) is a network management system for the Cisco Field Area Network (FAN).

The FAN is a communication network overlay that provides an end-to-end, IP-based reference architecture from data centers responsible for grid operations to homes and industries. It seamlessly connects IoT devices and services in a power grid infrastructure and provides multiservice enablement, security, fog computing, and more. It also serves as a communication platform for a variety of advanced applications, including Distribution Automation, Advanced Metering Infrastructure, and renewable energy.

IoT FND is a core component of a FAN. Through an intuitive user interface, it provides features for managing, monitoring, and troubleshooting supported devices and network operations in FANs of almost any size. Supported devices include various models of field area routers (FARs), headend routers (HERs), gateways, and endpoints. IoT FND ensures smooth device setup through zero-touch deployment (ZTD), secure communication, seamless scalability, and increased network efficiency. It provides real-time visibility of devices and assets, proactive fault detection, and many other important features for the management of the FAN.

For data protection and security, IoT FND uses digital certificates that undergo stringent authentication process based on 802.1x standards. Use of multiple IP encryptions and a standard FlexVPN solution establishes a secure data transmission environment that implements hop-by-hop encryption to safeguard data integrity and confidentiality.

Key features of IoT FND include the following:

- **Lifecycle management**:
  - On-premises network management system for FAN devices
  - Secure zero-touch provisioning for enrollment and deployment of devices
  - Device inventory
  - Secure tunnel provisioning
  - Rich APIs for third-party application integration
- **Network optimization**:
  - Configuration and firmware management
  - Network management for constrained bandwidth
  - Multitenancy and RBAC support

    - Network troubleshooting

- **Real-time monitoring**:
    - Enterprise-class visibility for routers and endpoints
    - Device status, health, and performance metrics
    - Alerts for critical events
    - Location tracking of all network assets and geofencing
    - Dynamic and customizable dashboard

CHAPTER 2

IoT FND in a FAN Solution

As the network management system, IoT FND lets you manage other components in a FAN, and perform various monitoring and administrative operations. Key FAN components include IoT FND itself, routers, endpoints, gateways, and security hardware and software. This chapter provides an overview of the roles and interactions of these key FAN components.

IoT FND Components

This section explains the role and function of the following IoT FND core components in the FAN solution:

- IoT FND Application Server
- IoT FND Database Server
- Tunnel Provisioning Server
- Load Balancer
- Software Security Module

IoT FND Application Server

The IoT FND application server resides in the data center and performs the functions that are needed to monitor and manage the FAN and devices. It hosts the IoT FND application and interacts with many of the components in the headend, including the IoT FND database server, DHCP server, headend routers (HER), and tunnel provisioning server (TPS). This server hosts the IoT FND user interface from which you perform IoT FND operations and management procedures and view information about the network, devices, and related items, and it stores the IoT FND log files.

The IoT FND application server runs under the Red Hat Enterprise Linux (RHEL) operating system and can be installed on a bare metal server or a virtual machine (VM).

IoT FND Database Server

The IoT FND database server resides in the headend and is the storage repository for the data that IoT FND generates and collects. This data includes metrics, device properties such as firmware images, configuration templates, and event notifications.

The IoT FND database server runs under the Red Hat Enterprise Linux (RHEL) operating system and can run the Oracle or Postgres database. When running Oracle, the IoT FND database server can be installed on a bare metal server or a VM. When running Postgres, this server can be installed only on a VM.

The IoT FND application server is the only component that interacts directly with the IoT FND database server.

Tunnel Provisioning Server

The tunnel provisioning server (TPS) resides in the DMZ and is a proxy server for IoT FND. The TPS provides a bridge for the communication between IoT FND and FARs. It relays tunnel requests from FARs to IoT FND and provides FARs with the configuration for the tunnel to the headend.

When they first start up, routers communicate with IoT FND through the TPS. After IoT FND provisions tunnels, routers communicate with IoT FND directly.

Load Balancer

An optional load balancer provides IoT FND server high availability. You can connect multiple IoT FND servers to a load balancer.

Load balancing is configured using a third-party device and is supported only in an IoT FND bare metal server deployment.

Software Security Module

The software security module (SSM) is an optional component of IoT FND. It is used to sign CSMP messages that IoT FND sends to meters and to Cisco IR500 endpoints. The SSM is bundled with the IoT FND image.

The SSM has a limited scaling capability and does not support high availability. We recommend that a hardware security module be used instead of the SSM in production environments.

Devices Managed by IoT FND

IoT FND lets you manage and monitor the following types of devices in a FAN:

- Field Area Routers
- Headend Routers
- Endpoints
- Gateways

Field Area Routers

Field area routers (FARs) reside in the FAN. They communicate with headend routers through tunnels that are provisioned by the TPS.

IoT FND provides options for managing the lifecycle activities of FARs, and for monitoring and troubleshooting.

You can use IoT FND to manage the following FARs:

- Cisco Catalyst IR1800 Rugged Series Router
- Cisco Catalyst IR8100 Heavy-Duty Series Router
- Cisco Catalyst IR1100 Rugged Series Router
- Cisco 1000 Series Connected Grid Router
- Cisco 800 Series Industrial Integrated Services Router
- Cisco 800 Series Router

Headend Routers

Headend routers (HERs) reside in the DMZ and provide routing connectivity between FARs and other headend components in the DMZ and data center. These headend components include IoT FND, the AAA server, the DHCP server, and utility application servers, such as SCADA and MDMS servers.

IoT FND does not provide options for managing lifecycle activities of headend routers, but it does provide options for monitoring their status and configuration. It also provides options for provisioning tunnels between HERs and FARs and for viewing the status of tunnels.

Headend routers include the following devices:

- Cisco 8000 Series Router
- Cisco ASR 1000 Series Aggregation Services Routers (ASR 1001 or 1002)
- Cisco 4000 Series Integrated Services Router (ISR)
- Cisco Cloud Services Router 1000V Series (CSR)

Endpoints

Endpoints are Cisco and third-party devices, including meters from Itron and Landis+Gyr, range extenders, cameras, battery endpoints, and cellular endpoints.

IoT FND provides options for managing lifecycle activities of endpoints, and for monitoring and troubleshooting.

You can use IoT FND to manage the following endpoints:

- Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR500)
    - Cisco IR510 (DA Gateway)
    - Cisco IR530 Series Resilient Mesh Range Extenders
- Mesh endpoints (from Itron and Landis+Gyr)

Gateways

Gateways provide connections between the FAN and other networks or the internet.

IoT FND provides options for managing lifecycle activities of gateways, and for monitoring and troubleshooting.

You can use IoT FND to manage the following gateways:

- Cisco IC3000 Industrial Compute Gateway
- Long Range Wide Area Network (LoRaWAN) Interface Module for Cisco 800 Series Industrial Integrated Services Routers (IR800)
- Landis+Gyr N2450 Network Gateway

Security Components in a FAN Solution

This section explains the key security components and their roles and interaction with IoT FND in the FAN solution.

- Public Key Infrastructure, on page 6
- Registration Authority
- Hardware Security Module, on page 6
- Authentication, Authorization, and Accounting

Public Key Infrastructure

A public key infrastructure (PKI) includes hardware and software for managing and controlling digital certificates and public-key encryption. In the FAN solution, digital certificates are issued to IoT FND and FARs so that they can authenticate and securely communicate with each other and with other FAN components.

The PKI includes a certificate authority (CA) server that issues RSA certificates for routers, ECC certificates for endpoints, and web certificate for IoT FND. Routers use Simple Certificate Enrollment Protocol (SCEP) to request and receive certificates. Endpoints use Enrollment over Secure Transport (EST) to request and receive certificates.

Registration Authority

A registration authority (RA) is a proxy that FARs use when requesting a digital certificate. Because a CA server cannot be in a public network, FARs use the RA to communicate with the CA to obtain digital certificates for secure communication. The RA proxies requests between public and private networks.

Hardware Security Module

A hardware security module (HSM) is a third-party appliance that is used to sign CSMP messages that IoT FND sends to meters and Cisco IR500 endpoints.

An HSM scales to support large FANs and supports high availability. We recommend that an HSM be used instead of the SSM in production environments.

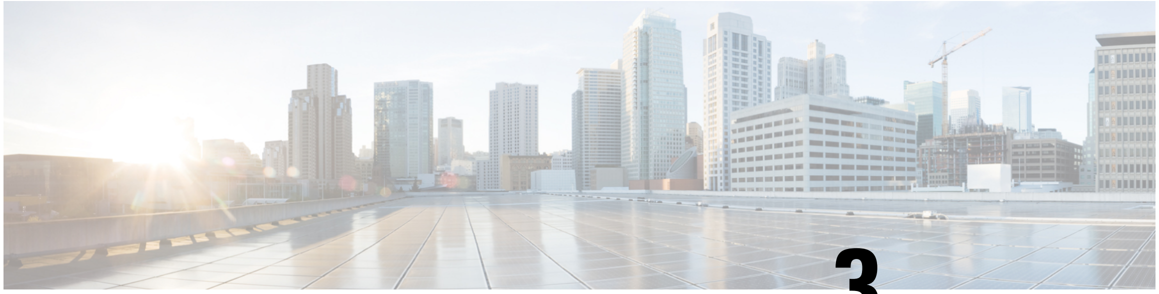
Authentication, Authorization, and Accounting

Authentication, authorization, and accounting (AAA) is a security framework that authenticates (verifies) FARs and endpoints before they can join the FAN, authorizes (grants access) for these devices to join the

FAN, and provides accounting (tracking) of the activities of these devices. The RADIUS protocol is used for authorization.

DHCP Server

The dynamic host configuration protocol (DHCP) server allocates IPv4 and IPv6 IP address to FARs. During tunnel provisioning, IoT FND sends requests to the DHCP server for the IP address on behalf of FARs, compiles the addresses that it receives as part of the tunnel provisioning configuration, and pushes the addresses to FARs through the TPS.



CHAPTER 3

IoT FND Managed Devices

IoT FND offers lifecycle management for Cisco and third-party devices. Lifecycle management includes automated deployment, firmware updates, and real-time visualization of device operations.

Cisco Devices

IoT FND can manage the following Cisco devices:

- Field Area Routers
- Headend Routers
- Endpoints
- Gateways

Field Area Routers

- Cisco Catalyst IR1800 Rugged Series Routers
- Cisco Catalyst IR8100 Heavy-Duty Series Routers (IR8140)
- Cisco 1101 Series Industrial Integrated Services Routers (IR1101)
- Cisco 1000 Series Connected Grid Routers (CGR1120 and CGR1240)
- Cisco 800 Series Industrial Integrated Services Routers (IR800)
- Cisco 800 Series Access Points (AP800) when integrated with C800 and IR829 devices

Headend Routers

- Cisco 8000 Series Routers
- Cisco ASR 1000 Series Aggregation Services Routers (ASR 1001 or 1002) serving as a head-end router
- Cisco 4000 Series Integrated Services Routers (ISR)
- Cisco Cloud Services Router 1000V Series (CSR)

Endpoints

- Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR500)
  - Cisco IR510 (DA Gateway)
  - Cisco IR530 Series Resilient Mesh Range Extenders
- Mesh endpoints

Note IoT FND can manage third-party endpoints only if the endpoints are running Cisco CSMP agent.

Gateways

- Cisco IC3000 Industrial Compute Gateway
- Long Range Wide Area Network (LoRaWAN) Interface Module for Cisco 800 Series Industrial Integrated Services Routers (IR800)

Third-Party Devices

IoTFND can manage the following third-party devices:

Vendors	Products
ITRON	• OpenWay Riva ACT • OpenWay Riva ACT Gateway • OpenWay Riva ACT Extender • OpenWay Riva BACT • OpenWay Riva BACT Controller • OpenWay Riva CAM
Landis+Gyr (L+G)	• Landis+Gyr Series 6 N2450 Network Gateway N2450 Gateway • Revelo E360/E660 • M125 RF Residential Gas Communications Module • M225 RF Commercial & Industrial Gas and Communications Module • Landis+Gyr R651 Network Router

Vendors	Products
MMB Networks	• Nansen/Sanxing • Hexing • Grupo Union (AMS) • Seltic (Donsun)

CHAPTER 4

IoT FND Deployment Options

Cisco IoT FND can be deployed in one of three ways. The deployment that you choose depends on a variety of factors, including your operational requirements, features needed, and devices that are to be managed.

Deployment options are:

- Bare metal server deployment: IoT FND is installed on a bare metal server and integrated with your existing Oracle database.

  After installing IoT FND, you manually configure the connection to your database, install database certificates, and configure related items. This option provides for the management of all supported devices.

- VM deployment with Oracle: A virtual machine (VM) that includes IoT FND and the Oracle database preinstalled and preconfigured is deployed on VMware ESXi 6.5.

  With this deployment, you do not need to manually integrate the database with IoT FND. This option provides for the management of all supported devices.

- VM deployment with Postgres: A VM that includes IoT FND and the Postgres database preinstalled and preconfigured is deployed on VMware ESXi 6.5.

  With this deployment, you do not need to manually integrate the database with IoT FND. This option provides for the management of routers only.

Note The VM deployment with Oracle and the VM deployment with Postgres options include a distribution license for the database. A support license for the database is not included.

The following table describes key elements of the IoT FND deployment options.

Element	**Deployment Option**		
	Bare Metal Server Deployment	**VM Deployment with Oracle**	**VM deployment with Postgres**
Database	Requires an existing Oracle database in your deployment.	Oracle database included, preinstalled and preconfigured on the provided VM.	Postgres database included, preinstalled, and preconfigured on the provided VM.

Element	**Deployment Option**		
	Bare Metal Server Deployment	**VM Deployment with Oracle**	**VM deployment with Postgres**
Installation and configuration process	Install IoT FND and manually configure the connection to your database, install database certificates, and configure related items.	Deploy the VM on which the IoT FND application and the database are preinstalled and preconfigured.	Deploy the VM on which the IoT FND application and the database are preinstalled and preconfigured.
Upgrade process	An upgrade script is not provided for new releases. Install the ISO package for the upgraded software.	An upgrade script is not provided for new releases. Install the OVA package for the upgraded software.	An upgrade script is provided for new releases.
Software host	The IoT FND application and the Oracle database run on a dedicated server.	The IoT FND application and the Oracle database run on the same VM.	The IoT FND application and the Postgres database run on the same VM.
Image distribution	ISO file that contains the RPM installation files. Provided as a ZIP file.	VM with IoT FND and the Oracle database preinstalled. Provided as a ZIP file.	VM with IoT FND and the Postgres database preinstalled. Provided as a ZIP file.
Example image filename	iot-fnd-*release_number-build_number*-signed.zip	CISCO-IOT-FND-V-K9-*release_number-build_number*-SHA256.zip	CISCO-IOT-FND-VPI-K9-*release_number-build_number*-SHA256.zip
Devices managed	All supported devices.	All supported devices.	Routers only.
High availability	High availability and load balancing are supported for the IoT FND application server and IoT FND database server. Load balancing is configured using a third-party load balancing device.	Not supported.	Not supported.
IOx app management	Not supported.	Not supported.	Supported.

- Bare Metal Server Deployment , on page 14
- VM Deployment with Oracle, on page 16
- VM Deployment with Postgres, on page 16

Bare Metal Server Deployment

With the bare metal server deployment option, you can install IoT FND on a bare metal server and then manually integrate it with your existing Oracle database. This deployment is a large-scale Advanced Metering Infrastructure (AMI) deployment that supports up to 8,000 routers and 8,000,000 endpoints. It provides for the management of all supported routers, gateways, and endpoints. For information about managed devices, see IoT FND Managed Devices, on page 9.

This deployment supports high availability for the IoT FND application server and the IoT FND database server in single or cluster IoT FND server deployments.

On the IoT FND application server, high availability is achieved by connecting multiple IoT FND servers to a load balancer. Traffic that originates at routers and endpoints goes to the load balancer, which uses a load balancing algorithm to distribute the load among the IoT FND servers.

On the IoT FND database server, high availability is achieved by configuring two IoT FND database servers: a primary database server and a standby (or secondary) database server. When the primary database server receives new data, it sends a copy to the standby database server. The Observer, a program that monitors the IoT FND database servers, runs on a separate server or the standby server. If the primary database server fails, the Observer configures the standby database server as the new primary database server.

The following steps provide an overview of the implementation procedure for the bare metal server deployment. For detailed installation information and complete steps, see Cisco IoT Field Network Director Installation Guide – Oracle Deployment.

1. Ensure that your environment meets the requirements for installation and obtain the required licenses.
2. Download the IoT FND packages that you need from the Cisco Software Download page and verify the images.
3. Generate and install certificates for secure communications between IoT FND and devices.
4. Install and configure the IoT FND database.
5. Install and configure the IoT FND.
6. Install and configure the IoT FND TPS proxy.
7. Optionally configure high availability for IoT FND.

The following table describes the files that are included in the distribution for the bare metal server deployment.

File	Description
cgms-*release_number-build_number*86_64.rpm	Contains the IoT FND installer. Install this package on the IoT FND application server.
cgms-oracle-*release_number-build_number*86_64.rpm	Contains database template and management tools for the Oracle database. Install this package on the IoT FND database server.
cgms-ssm-*release_number-build_number*86_64.rpm	Contains the Software Security Module (SSM). Install this package on the IoT FND application server. **Note** This rpm is required only when you are managing mesh endpoints.
cgms-tools-*release_number-build_number*86_64.rpm	Contains optional command line tools. If needed, install this package on the IoT FND application server.

File	Description
cgms-tpsproxy-*release_number-build_number*86_64.rpm	Contains the tunnel provisioning server (TPS) proxy application. Install this package on the IoT FND TPS proxy server.
fnd-ra-*release_number- build_number*86_64.rpm	Contains the installation file for the registration authority (RA). Install this package on the IoT FND application server.

VM Deployment with Oracle

With the VM deployment with Oracle option, you deploy an OVA file on VMware ESXi 6.5, a VM in which IoT FND and the Oracle database are preinstalled and preconfigured. This deployment does not require manual integration of the database with IoT FND. In this deployment, both the IoT FND application and database servers run on the same VM.

This deployment is a large-scale AMI deployment for mesh management and supports up to 2,000 routers and 2,000,000 endpoints. It provides for the management of all supported routers, gateways, and endpoints. For information about managed devices, see IoT FND Managed Devices, on page 9.

This deployment does not support high availability.

The following steps provide an overview of the implementation procedure for the VM deployment with Oracle.

1. Ensure that your environment meets the requirements for installation and obtain the required licenses.
2. Download the IoT FND packages that you need from the Cisco Software Download page and verify the images.
3. Install the OVA file.
4. Install CA certificates and import SUDI certificates.
5. Configure IoT FND.

The following table describes the files that are included in the distribution for the VM deployment with Oracle.

File	Description
iot-fnd-oracle-*release_number-build_number*_SHA256_signed.ova	Contains the files for deploying the VM with the preinstalled IoT FND application and Oracle database.
iot-tps-*release_number-build_number*_SHA256_signed.ova	Contains the TPS proxy application.

VM Deployment with Postgres

With the VM deployment with Postgres option, you deploy an OVA file on VMware ESXi 6.5, a VM in which IoT FND and the Postgres database are preinstalled and preconfigured. This deployment does not require manual integration of the database with IoT FND. In this deployment, both the IoT FND application and database servers run on the same VM.

This option is a small-scale deployment for router management and supports up to 25,000 routers. It provides for the management of all supported gateways and IOx application management. For information about managed devices, see IoT FND Managed Devices, on page 9.

This deployment includes Influx, an open-source time series database that provides real-time insights on device data. It also includes the Cisco IOx application management service. This service allows you to deploy and manage applications on devices with built-in security for application signing and verification.

This deployment does not support high availability.

The following steps provide an overview of the implementation procedure for the VM deployment with Postgres. For detailed installation information and complete steps, see Cisco IoT FND Postgres and Influx DB Deployment with Integrated Application Management on OVA.

1. Ensure that your environment meets the requirements for installation and obtain the required licenses.
2. Download the IoT FND packages that you need from the Cisco Software Download page and verify the images.
3. Install the OVA file.
4. Install CA certificates and import SUDI certificates.
5. Configure IoT FND.

The following table describes the files that are included in the distribution for the VM deployment with Postgres.

File	Description
Install scripts (greenfield deployment)	
iot-fnd-*release_number-build_number*_SHA256_signed.ova	Contains the files for deploying the VM with the preinstalled IoT FND application and database.
iot-tps-*release_number-build_number*_SHA256_signed.ova	Contains the TPS proxy application.
Upgrade scripts (brownfield deployment)	
CISCO-IOTFND-VPI-K9-UPGRADE-SCRIPTS-*release_number-build_number*.zip	Contains upgrade scripts for IoT FND application and Postgres database.

CHAPTER 5

Resource Requirements for Deployments

This section provides the CPU, memory, and disk space requirements for the IoT FND application, database, and tunnel provisioning servers for each of the IoT FND deployment types.

- Bare Metal Server Deployment Resource Requirements, on page 19
- VM Deployment with Oracle Resource Requirements, on page 21
- VM Deployment with Postgres Resource Requirements , on page 22

Bare Metal Server Deployment Resource Requirements

The following table shows the CPU, memory (RAM), and disk space requirements for the IoT FND application server in a bare metal server deployment for:

- Resource Requirements in a BM Deployment for Mesh Management
- Resource Requirements in a BM Deployment for Router Management

Resource Requirements in a BM Deployment for Mesh Management

For improved device scalability and device performance, we recommend that you cluster application servers as follows:

- For deployments with between 2,000 routers/2,000,000 endpoints and 6,000 routers/6,000,000 endpoints: Two application servers
- For deployments with more than 6, 000 routers and 6,000,000 endpoints: Four application servers

Table 1: IoT FND Application Server Resource Requirements in a Bare Metal Server Deployment

Nodes Deployed	CPU	Memory (RAM GB)	Disk Space (GB)
Up to 25 routers and 10,000 endpoints	2	16	100
Up to 50 routers and 50,000 endpoints	4	16	200
Up to 500 routers and 500,000 endpoints	4	16	250

Nodes Deployed	CPU	Memory (RAM GB)	Disk Space (GB)
Up to 1,000 routers and 1,000,000 endpoints	8	16	250
Up to 2,000 routers and 2,000,000 endpoints	8	16	500
Up to 6,000 routers and 6,000,000 endpoints	8	16	500
Up to 8,000 routers and 8,000,000 endpoints	8	32	500

The following table shows the CPU, memory (RAM), and disk space requirements for the IoT FND database server in a bare metal server IoT FND deployment.

Table 2: IoT FND Database Server Resource Requirements in a Bare Metal Server Deployment

Nodes Deployed	CPU	Memory (RAM GB)	Disk Space (GB)
Up to 25 routers and 10,000 endpoints	2	16	100
Up to 50 routers and 50,000 endpoints	4	16	200
Up to 500 routers and 500,000 endpoints	8	32	500
Up to 1,000 routers and 1,000,000 endpoints	12	48	1000
Up to 2,000 routers and 2,000,000 endpoints	16	64	1000
Up to 6,000 routers and 6,000,000 endpoints	20	96	1000
Up to 8,000 routers and 8,000,000 endpoints	32	160	2000

The following table shows the CPU, memory (RAM), and disk space requirements for the TPS in a bare metal server IoT FND deployment.

Table 3: Tunnel Provisioning Server Resource Requirements in a Bare Metal Server Deployment

Nodes Deployed	CPU	Memory (RAM GB)	Disk Space (GB)
Up to 25 routers and 10,000 endpoints	2	4	50
Up to 50 routers and 50,000 endpoints	2	4	100
Up to 500 routers and 500,000 endpoints	2	4	100
Up to 1,000 routers and 1,000,000 endpoints	2	4	100
Up to 2,000 routers and 2,000,000 endpoints	2	4	100

Nodes Deployed	CPU	Memory (RAM GB)	Disk Space (GB)
Up to 6,000 routers and 6,000,000 endpoints	2	4	100
Up to 8,000 routers and 8,000,000 endpoints	2	4	100

Resource Requirements in a BM Deployment for Router Management

Table 4: IoT FND Application Server Resource Requirements a Bare Metal Deployment

Nodes Deployed	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
Up to 25,000 routers	24	32	500
Up to 10,000 routers	16	24	500

Table 5: IoT FND Database Server Resource Requirements for a Bare Metal Deployment

Nodes Deployed	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
Up to 25,000 routers	48	64	1000
Up to 10,000 routers	24	48	1000

VM Deployment with Oracle Resource Requirements

The following table shows the CPU, memory (RAM), and disk space requirements in a VM deployment with Oracle.

Table 6: Resource Requirements in a VM Deployment with Oracle

Nodes Deployed	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
Up to 2,000 routers and 2,000,000 endpoints	24	96	1500

VM Deployment with Postgres Resource Requirements

The following table shows the CPU, memory (RAM), and disk space requirements in a VM deployment with Postgres.

Table 7: Resource Requirements in a VM Deployment with Postgres

Nodes Deployed	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
Up to 25,000 routers	24	64	800
Up to 15,000 routers	16	48	500
Up to 10,000 routers	10	32	500

CHAPTER 6

IoT FND Licensing

IoT FND is licensed through software package licenses for application software and device licenses for the devices to be managed.

Device licenses are offered in either a perpetual or subscription licensing model.

Subscription device licenses are valid for a specific period. You can choose a period of 1, 3, 5, or 10 years.

Perpetual device licenses do not expire.

Subscription licensing includes IoT FND maintenance and support. With perpetual licensing, IoT FND maintenance and support can be purchased separately.

Note New device licenses that become available are offered through subscription licensing only.

Obtaining Licenses

To obtain licenses for IoT FND, you purchase the following:

- A software package license for the IoT FND application.

  One software package license is required for each IoT FND instance that you are deploying. Sofware package licenses do not expire.

- Either of the following for managing devices:
  - A set of perpetual device licenses.

    Perpetual device licenses do not expire.

  - A set of subscription device licenses.

    Subscription device licenses are valid for 1, 3, 5, or 10 years.

- Optionally, a software package license for a Geographic Information System (GIS) map.

  This license does not expire.

License Product IDs

The following table describes the licenses that are available for IoT FND and provides the Cisco product ID (PID) for each license. Use this information to determine the licenses that you need for your deployment.

For example, to obtain IoT FND subscription licensing for managing Cisco Catalyst IR8100 Heavy-Duty Series Routers for 3 years in a bare metal server deployment, purchase the following licenses:

- Software package license: R-IOTFND-K9, under the IOT-FND license
- Subscription device license: IOTFND-IR8100, under the IOTFND-SOFTWARE-K9 license

Similarly, to obtain IoT FND perpetual licensing for managing a Cisco 1000 Series Connected Grid Router in a VM deployment with Postgres, purchase the following licenses:

- Software package license: R-IOTFND-VPI-K9, under the IOT-FND license
- Device license: L-IOTFND-CGR1K, under the IOT-FND license

Table 8: IoT FND Licenses and PIDs

License Type and Description	PID		Supported Deployments
	Subscription Licensing	Perpetual Licensing	
Top-Level Licenses			
For software package licenses and perpetual device licenses	IOT-FND		—
For subscription device licenses	IOTFND-SOFTWARE-K9	—	—
Software Package Licenses (under IOT-FND)			
For a bare metal server deployment	R-IOTFND-K9		Bare metal server deployment
For a VM deployment with Oracle	R-IOTFND-V-K9		VM deployment with Oracle
For a VM deployment with Postgres	R-IOTFND-VPI-K9		VM deployment with Postgres
For GIS map	L-IOTFND-GIS-3YRS		• Bare metal server deployment • VM deployment with Oracle • VM deployment with Postgres

License Type and Description	PID		Supported Deployments
	Subscription Licensing	Perpetual Licensing	
Device Licenses • Subscription license PIDs are under IOTFND-SOFTWARE-K9 • Perpetual license PIDs are under IOT-FND			
For managing up to 100 endpoints, other than battery and cellular endpoints	IOTFND-EP-100	—	• Bare metal server deployment • VM deployment with Oracle
For managing up to 1,000 endpoints, other than battery and cellular endpoints	IOTFND-EP-1K	L-IOTFND-EP-1K	• Bare metal server deployment • VM deployment with Oracle
For managing up to 1,000 battery endpoints	IOTFND-BEP-1K	L-IOTFND-BEP-1K	• Bare metal server deployment • VM deployment with Oracle
For managing up to 1,000 cellular endpoints	IOTFND-CEP-1K	—	• Bare metal server deployment • VM deployment with Oracle
For managing a Cisco 500 WPAN Industrial Router	IOTFND-IR509	L-IOTFND-IR509	• Bare metal server deployment • VM deployment with Oracle
For managing a Cisco 1000 Series Connected Grid Router	IOTFND-CGR1000	L-IOTFND-CGR1K	• Bare metal server deployment • VM deployment with Oracle
For managing a Cisco 800 Series Industrial Integrated Services Router	IOTFND-IR800	L-IOTFND-IR800	• Bare metal server deployment • VM deployment with Oracle • VM deployment with Postgres
For managing a Cisco 800 Series Router	IOTFND-C800	L-IOTFND-C800	• Bare metal server deployment • VM deployment with Oracle • VM deployment with Postgres
For managing a Cisco Catalyst IR1100 Rugged Series Router	IOTFND-IR1100	—	• Bare metal server deployment • VM deployment with Oracle • VM deployment with Postgres

License Type and Description	PID		Supported Deployments
	Subscription Licensing	Perpetual Licensing	
For managing a Cisco Catalyst IR8100 Heavy-Duty Series Router	IOTFND-IR8100	—	• Bare metal server deployment • VM deployment with Oracle
For managing a Cisco Catalyst IR1800 Rugged Series Router	IOTFND-IR1800	—	• Bare metal server deployment • VM deployment with Oracle • VM deployment with Postgres
For managing a Long Range Wide Area Network (LoRaWAN) Interface Module for Cisco 800 Series Industrial Integrated Services Router (IR800)	IOTFND-LORAWAN	L-IOTFND-LORAWAN	• Bare metal server deployment • VM deployment with Oracle • VM deployment with Postgres
For managing a Cisco IC3000 Industrial Compute Gateway	IOTFND-IC3000	—	• Bare metal server deployment • VM deployment with Oracle • VM deployment with Postgres
For managing a Landis+Gyr N2450 Network Gateway	IOTFND-N2450	—	• Bare metal server deployment • VM deployment with Oracle

CHAPTER 7

IoT FND User Interface

This chapter provides an overview of the IoT FND user interface. From the user interface, you can manage, monitor, and troubleshoot devices, events, and issues in your FAN, and perform a variety of other administrative and management tasks.

To access the IoT FND user interface, enter the following URL in your web browser and log in with your IoT FND username and password. Replace *fnd-ip* with the IP address of your IoT FND system.

https://*fnd-ip*/login.seam

The FND user interface includes the following menus. Use these menus to access the pages in the IoT FND user interface.

- Dashboard
- Devices
- Operations
- Config
- Admin
- Apps

For more detailed information about the IoT FND user interface and the activities you can perform, see Cisco IoT Field Network Director User Guide.

Dashboard

The **Dashboard** appears when you log in to IoT FND. You also can click **DASHBOARD** to display the Dashboard.

This page displays dashlets that provide information about the FAN, including the operational states and operational trends of routers, endpoints, and gateways. Actions that you can perform on this page include:

- Use the configurable and customizable dashlets to view information in various formats, such as pie charts, bar charts, or line graphs.
- Add, minimize, refresh, export, reposition, and remove dashlets as needed.
- Use the **Filter** option to view information for a specific time or time period.
- Export selected information in Excel format for archiving and analysis.
- Use the **Series Selector** option to display information by device status.

Devices Menu

The **Devices** menu provides access to pages that list and provide information about the devices and assets that you can manage with IoT FND. The pages also provide options for performing most onboarding and lifecycle management activities, including adding items, deleting items, and changing item properties.

To display the Devices menu, click **DEVICES**. This menu includes the following options:

- **Field Devices**: Displays information about the field area routers, endpoints, and gateways that are managed in IoT FND and provides options for managing devices.

  You can add devices for IoT FND to manage, remove devices from IoT FND management, manage labels that identify a set of devices, modify device properties, refresh the display of device metrics, block devices from accessing IoT FND, remove devices from IoT FND management, troubleshoot devices, and perform other related tasks. You also can monitor devices in real-time, obtain information about the health of devices, and view detailed hardware, software, and metrics information for a device. The Map view displays the geographical location of each device.

- **Head End Routers**: Displays information about the HERs that are managed with IoT FND and provides options for managing these devices.

  You can add HERs for IoT FND to manage, remove HERs from IoT FND management, manage labels for devices, trace routes to a device, and perform other related tasks. You also can view detailed hardware, software, and metrics information for a HER, and view information about tunnels that are established between HERs and FARs.

- **Servers**: Displays information about the IoT FND application and database servers and provides options for managing these servers.

  You can ping servers, remove servers, and add or remove labels for servers. You also can view detailed hardware, software, and metrics information for a server.

- **Assets**: Displays information about third-party equipment that is associated with IoT FND managed devices and provides options for managing this equipment. Assets can include routers, meters, extenders, access points, cameras, and other similar devices.

  You can add assets to be managed by IoT FND, remove assets from IoT FND management, change the properties of assets, and add files such as images to assets.

Operations Menu

The **Operations** menu provides access to pages with options for monitoring events, issues, and tunnel status in your network.

To display the **Operations** menu, click **OPERATIONS**. This menu includes the following options:

- **Events**: Displays notifications about events that are associated with IoT FND-managed devices. Events include activities, warnings, state changes, or errors that IoT FND detects on devices. An event can be the result of a user action, for example, provisioning a tunnel. It also can be the result of a problem with a device, for example, a low battery, expired certificate, or metric retrieval failure. An event notification includes the time period in which the event occurred, and other related information that can help you address an issue.
- **Issues**: Displays information about the overall health of the network, and displays a list of issues, which are unresolved events. Major and critical issues appear at the top of the screen, and you can view issues for the periods of your choice.
- **Tunnel Status**: Provides information about tunnels that have been provisioned between HERs and FARs.

Config Menu

The **Config** menu provides access to pages with options for configuring devices, installing firmware on devices, managing device files, provisioning tunnels, managing rules, and managing groups.

To display the **Config** menu, click **CONFIG**. This menu includes the following options:

- **Device Configuration**: IoT FND lets you configure devices by using configuration templates and configuration groups. A configuration template contains configuration settings for devices, and a configuration group is a collection of similar devices. By pushing a configuration template to a configuration group, you can apply the same settings to all devices that are in that configuration group. This approach is an efficient way to configure many devices with a single operation.

  You can view and access configuration templates and configuration groups, add devices to configuration groups, edit configuration templates, push configuration templates to devices, and manage configuration group properties.
- **Firmware Update**: Provides options for installing a firmware image on a router or endpoint. This page also displays information about the firmware that is installed on devices, firmware images that are available for devices, and information about subnets for endpoints.

  You can install a firmware image on a single device or use predefined or user defined firmware groups to install a firmware image on several devices with a single operation. You can also upload WPAN images to IoT FND.
- **Device File Management**: Provides options for viewing and managing device files. These files include configuration files, log files, and debug files on devices.
- **Rules**: Provides options for adding, activating, deactivating, and deleting rules, and displays information about existing rules. A rule defines actions that IoT FND performs after specified events occur or when it receives metrics that match criteria that you define. Use a rule to specify a message and severity to include in the log entry for an event.

- **Tunnel Provisioning**: Provides options for provisioning tunnels between HERs and FARs. You also can configure the bootstrap configuration templates for HERs and FARs and view the bootstrap status of a router during plug and play (PNP) operation.
- **Groups**: Provides options for managing endpoint groups, which are a logical groupings of devices. You can add endpoints to groups, remove endpoints from groups, and move an endpoint to another group.

  Groups provide a convenient way to manage several endpoints at one time. For example, when you push a configuration to a group, IoT FND pushes the configuration to all the endpoints in that group.

Admin Menu

The **Admin** menu provides access to the **Access Management** pages and the **System Management** pages.

The **Access Management** pages provide options for configuring various user access and device domain settings and display related information. The **System Management** pages provide options for configuring various user login, security, logging, provisioning, and server options, and display related information.

To display the **Admin** menu, click **ADMIN**. This menu includes the following options:

Access Management Pages

- **Users**: Provides options for managing IoT FND user accounts, including adding users, deleting users, activating users, deactivating users, and updating user roles.
- **Roles**: Provides options for managing roles that you can assign to IoT FND users.

  Each user is assigned a role, and the role determines what IoT FND operations the user can perform based on permissions that are enabled for a role. You can view existing roles, modify the permissions that are enabled for default roles, create new roles and enable permissions for them as needed, and delete non-default roles.
- **Domains**: Provides options for managing domains.

  A domain is a logical grouping of devices within the network, and it is used in multi-tenancy environments where a single deployment of IoT FND can support multiple customers. You also add and delete domains, update domain configuration, configure the hierarchy for a domain, and designate the IoT FND users who can modify information in a domain.
- **Password Policy**: Provides options for configuring the conditions that valid IoT FND user passwords must meet. This page also provides an option for setting the number of consecutive unsuccessful log in after which the user is locked out from IoT FND. An administrator must grant a locked out user permission to log in again.
- **Authentication**: Provides options for configuring the type of authentication that IoT FND uses to verify a user before the user can log in, and for configuring parameters for user authentication methods. You can configure local authentication, local or remote authentication, or single sign-on (SSO) authentication.

  With local authentication, user credentials stored in the IoT FND database. With remote authentication, user credentials are stored in a RADIUS server. With SSO authentication, user credentials are stored in an identify provider (IdP).

System Management Pages

- **Active Sessions**: This screen displays information about each user who is logged in to IoT FND, including the IP address of the user device, the date and time that the user logged in, and the date and time that the user last accessed IoT FND. The root user can force logout other users from IoT FND.
- **Audit Trail**: Provides information about the IoT FND activities that each user performed, including when the user logged in and what operations the user performed.
- **Certificates**: Provides options for viewing and downloading CoAP Simple Management Protocol (CSMP), router certificates, or web certificates. Devices use these certificates to ensure secure communication in the network. You also can add a trust anchor to the default profile for a Cisco IOx device that is managed by IoT FND.
- **Data Retention**: Provides options for designating the number of days that IoT FND stores information about events, issues, and metrics. Data is permanently deleted after the designated retention period.
- **License Center**: Provides options for viewing and managing IoT FND license files.
- **Logging**: Provides options for downloading IoT FND log files and for configuring the log level for logging categories. Log files capture information about events that occur on devices that are managed by IoT FND.
- **Syslog Settings**: Provides options for enabling IoT FND to send information about events to a syslog server, and for designating the syslog server to which events are sent.
- **Provisioning Settings**: Provides options for configuring the DHCPv4 and DHCPv6 proxy client settings that IoT FND requires to create tunnels between FARs and HERs and for configuring the URL of the IoT FND server.
- **Server Settings**: Provides options for viewing and managing IoT FND server settings. Items that you can configure include keystore settings for downloading log files, the timeout period after which IoT FND terminates web sessions, the period after which IoT FND moves unreachable devices to the Down state, the start day of monthly billing periods for cellular and ethernet (satellite) services, RPL tree settings, and map settings.
- **Jobs**: Displays the state and execution status of IoT FND jobs. A job is an IoT FND operation that you performed. Examples of jobs include provisioning a tunnel, updating firmware, or pushing a configuration file to devices.

Apps Menu

The **Apps** menu provides access to pages with options for managing Docker applications that are installed on Cisco 1800 Series Industrial Integrated Services Routers and Cisco Catalyst IR1100 Rugged Series Routers. Activities that you can perform include installing, uninstalling, starting, stopping, and exporting applications.

Note This menu is available only for the IoT FND VM deployment with Postgres.

CHAPTER 8

IoT FND Documentation

The following documents are available for IoT FND:

- Release Notes for IoT Field Network Director, Release 4.12.x
- Cisco IoT Field Network Director User Guide, Release 4.12.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