Before You Install Field Network Director

When installing an Oracle database, review this chapter as preparation for your IoT Field Network Director installation.

This chapter provides details on the hardware and software you must have within your network to support the Cisco IoT Field Network Director (FND) 4.3 application and greater that employs an Oracle deployment:

Note Oracle 18c is supported from Cisco IoT FND Releases 4.4.4, 4.5.x and later. Oracle 19c is supported on Cisco IoT FND Releases 4.6.1 and later.

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

Minimum System Requirements for Oracle Installation

Note Before downloading and installing the Oracle Database, ensure that the /tmp folder can handle, at a minimum, a 5GB file. After you complete the full installation and are working with the FND user interface, you may need to zip up log files sets and the larger /tmp folder will be of value.

Table 1: Minimum Hardware and Software Requirements in IoT FND and Supporting Systems

Component	Minimum Hardware Requirement	Minimum Software Requirements

Cisco IoT FND application server (or comparable system that meets the hardware and software requirements)	• Processor:
	
	  • Intel Xeon x5680 2.27 GHz (64-bit)
	
	  • 4 CPUs
	
	• RAM: 16 GB
	
	• Disk space: 100 GB
	
	• Hardware Security Module
	
	  or
	
	  Software Security Module
		• Red Hat Enterprise Linux (RHEL) 7.5 and above, 64-bit with all packages installed (software development and web server)
		
		See Table 4: Application Server Hardware Requirements Example Profiles For Routers and Endpoints, on page 4 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.

Cisco IoT FND TPS Proxy
 	
See Table 3: Tunnel Provisioning Server (TPS), on page 4
	• Processor:
	
	  • Intel Xeon x5680 2.27 GHz (64-bit)
	
	  • 2 CPUs (virtual cores)
	
	• RAM: 4 GB
	
	• Hard Disk space: 100 GB
		• RHEL 7.5 and above with all packages installed (software development and web server)
		
		• Internet connection
		
		Note IoT FND software bundle includes required Java version.

Component	Minimum Hardware Requirement	Minimum Software Requirements
Database server for IoT FND Scalable to 5,000/5,000,000 endpoints with minimum hardware requirements. See Table 2: Oracle DB Server Hardware Requirements Example Profiles, on page 4 for additional deployment sizes.	• Processor: Intel Xeon x5680 3.33 GHz (64-bit) • 4 CPUs • RAM: 32 GB • Disk space: 150 GB	You will install both Linux and Oracle software on the Database server. Install Linux packages on the Database server before you install Oracle: • RHEL 7.5 and above, 64-bit with all packages installed (software development and web server) **Note** RHEL 8.5 is supported in Cisco IoT FND 4.8.1 release. • Oracle Database 19c Enterprise Edition for IoT FND 4.6.1 and greater. • Oracle Database 18c Enterprise Edition (formerly identified as 12.2c) for IoT FND 4.5.x. 4.6.x and greater. • Oracle Database 12c2 Enterprise Edition Release for IoT FND 4.3.x, 4.4.x, and 4.5.x. • Oracle Database 12cR2 Enterprise Edition Release for IoT FND 4.6.x
Hardware Security Module (HSM)	Luna SA appliance, with client software installed on the IoT FND application servers	Luna SA appliance: • Release 6.10.2 firmware **Note** Contact SafeNet to determine if you can run a higher version. • Release 5.4.7-1 software, plus security patches. Luna SA client software: • Release 5.4.7-1 software.

Component	Minimum Hardware Requirement	Minimum Software Requirements
Software Security Module (SSM)	• RAM: 8 GB • Processor: 2 GHz • 2 CPUs	• RHEL 7.5, 64-bit with all packages installed (software development and web server).

Table 2: Oracle DB Server Hardware Requirements Example Profiles

Nodes (Routers/Endpoints)	CPU (virtual cores)	Memory (RAM GB)	Disk Space (GB)
25/10,000	2	16	100
50/50,000	4	16	200
500/500,000	8	32	500
1,000/1,000,000	12	48	1000
2,000/2,000,000	16	64	1000
5,000/5,000,000	20	96	1000
6,000/6,000,000	20	96	1000

Table 3: Tunnel Provisioning Server (TPS)

Nodes (Routers/Endpoints)	CPU (virtual cores)	Memory (RAM GB)	Disk Space (GB)
25/10,000	2	4	50
50/50,000	2	4	100
500/500,000	2	4	100
1,000/1,000,000	2	4	100
2,000/2,000,000	2	4	100
5,000/5,000,000	2	4	100
6,000/6,000,000	2	4	100

Table 4: Application Server Hardware Requirements Example Profiles For Routers and Endpoints

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	4	16	250
1,000/1,000,000	8	16	250
2,000/2,000,000[1]	8	16	500
5,000/5,000,000 [1]	8	32	500
6,000/6,000,000 [1]	8	32	500

[1]

IR800 Router Only Deployment Requirements

When installing IR800 router only deployments, we recommend using OVA deployments:

Cisco IoT FND Deployment on an Open Virtual Appliance

Table 5: Application Server Hardware Requirements Example Profile for Routers and LoRa Modules

Nodes(IR800)	CPU (Virtual Cores)	Memory (RAM)	Disk Space (GB)
10,000	10	32	500

Table 6: Database Server Hardware Requirements Example Profile For Routers and LoRa Modules

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

Obtaining IoT FND and Cisco Network Register Licenses

• Contact your Cisco partner to obtain the necessary licenses to use IoT FND and Cisco Network Register (CNR).

• Obtain a license to use SafeNet as your Hardware Security Module (HSM) for mesh endpoint security.

---

[1] [1.]Clustered installations RAID 10 is mandatory for deployments of 2 million endpoints and above.

Installing the Linux Packages Required for Installing Oracle

If you are installing a new IoT FND deployment that requires Oracle, you will need to first install the following Linux packages on your FND server, in the order listed, before you install the Oracle database:

1. libaio-devel-0.3.106-5.i386.rpm

2. libaio-devel-0.3.106-5.x86_64.rpm

3. sysstat-7.0.2-11.el5.x86_64.rpm

4. unixODBC-libs-2.2.11-10.el5.i386.rpm

5. unixODBC-libs-2.2.11-10.el5.x86_64.rpm

6. unixODBC-2.2.11-10.el5.i386.rpm

7. unixODBC-2.2.11-10.el5.x86_64.rpm

8. unixODBC-devel-2.2.11-10.el5.i386.rpm

9. unixODBC-devel-2.2.11-10.el5.x86_64.rpm

Obtaining IoT FND RPM Packages

Before you install and set up your IoT FND system, ensure that you have the following packages:

RPM Package	Description
cgms-*version_buildnumber* .x86_64.rpm	Contains the IoT FND installer. This is the main RPM that contains the IoT FND application server itself. Install this package on the IoT FND application servers.
cgms-oracle-*version_number* .x86_64.rpm	Contains the scripts and tools to create the IoT FND Oracle database. This package contains the Oracle database template and management scripts. Install this package on the IoT FND database server system.
cgms-tools-*version_number* .x86_64.rpm	Contains a few optional command-line tools. If needed, install this package on the system running the IoT FND application server.
cgms-ssm-*version_number* .x86_64.rpm	Contains the Software Security Module (SSM). Install this package on the system running the IoT FND application server.
cgms-tpsproxy-*version_number* .x86_64.rpm	Contains the TPS proxy application. Install this package on the IoT FND TPS proxy system.

Important Ensure to configure Network Time Protocol (NTP) before you install the certificates. For more information, refer to .

Configuring NTP Service

To configure NTP on your RHEL servers:

Before you begin

Configure all RHEL servers (including all servers that run IoT FND) in your IoT FND deployment to have their NTP service enabled and configured to use the same time servers as the rest of the system.

⚠️
Caution   Before certificates are generated, synchronize the clocks of all system components.

Step 1   Configure the /etc/ntp.conf file.

For example:

Example:

```
cat /etc/ntp.conf
...
# Use the same NTP servers on all our Connected Grid systems.
server 0.ntp.example.com
server 1.ntp.example.com
server 2.ntp.example.com
...
```

Step 2   Restart the NTP daemon and ensure that it is set to run at boot time.

Example:

```
service chrony restart
chkconfig chrony on
```

Step 3   Check the configuration changes by checking the status of the NTP daemon.

This example shows that the system at 192.0.2.1 is configured to be a local NTP server. This server synchronizes its time using the NTP server at 10.0.0.0.

Example:

```
# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*192.0.2.1      198.51.100.1    3 u   309 1024  377     0.694    0.899   0.435
 LOCAL(0)        .LOCL.         10 l    36   64  377     0.000    0.000   0.001
```

For information about configuring NTP on RHEL servers, refer to RHEL documentation.

IoT FND Map View Requirements

When your IoT FND installation is complete, you will need to do the following to ready the Map within the application window.

Note On any device tab, click the Map button in the main pane to display a GIS map of device locations. In its Map View pane, IoT FND uses a Geographic Information System (GIS) map to display device locations. However, before you can use this feature, you must configure your firewall to enable access for all IoT FND operator systems to Cisco-provided GIS map file servers.Note: Only IoT FND operator systems have access to the GIS map file servers.

Note The operator browsers will not have access to other Google sites. No Internet access is required for the IoT FND application server.

You must also assign a fully qualified domain name (FQDN) for each IoT FND server installation and provide Cisco at mailto:%20ask-fnd-pm-external@cisco.com with the following:

- The number of IoT FND installation environments (test and production)

- The FQDN of the IoT FND server

- For cluster deployments, the FQDN of any load balancer in the deployment

Note The FQDN is only used to provision and authorize access to the licensed Cisco IoT FND installation and make API calls to Enterprise Google Map to download the map files. No utility operational data or asset information is ever used (that is, sent over Internet) to retrieve Google map files. Map files are retrieved only using geographic location information.