



Installing Cisco IoT FND

This chapter provides an overview of the steps required to install Cisco IoT Field Network Director (Cisco IoT FND) in your network.

Note: For an overview of the features and functionality of the application and details on how to configure features and manage the Cisco IoT Field Network Director after its installation, refer to the [Cisco IoT Field Network Director User Guide, Release 4.0.x](#).

How to install IoT FND and related software:

- [Before You Install IoT FND](#)
- [Installing and Setting Up the IoT FND Database](#)
- [Installing and Setting Up IoT FND](#)
- [Installing and Configuring the IoT FND TPS Proxy](#)
- [Configuring IoT FND for Dual-PHY](#)
- [Backing Up and Restoring the IoT FND Database](#)
- [Deploying IoT FND/Oracle/TPS Virtual Machines on ESXi 5.x or ESXi 6.x](#)

Before You Install IoT FND

Use the procedures in the following sections to prepare for your IoT FND installation:

- [IoT FND Map View Requirements](#)
- [System Requirements](#)
- [Obtaining IoT FND and CNR Licenses](#)
- [Installing the Linux Packages Required for Installing Oracle](#)
- [Obtaining IoT FND RPM Packages](#)
- [Configuring NTP Service](#)
- [IoT FND Installation Overview](#)

IoT FND Map View Requirements

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 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 tile servers. Only IoT FND operator browsers are allowed access to the GIS map tile 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 ask-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 tiles. No utility operational data or asset information is ever used (that is, sent over Internet) to retrieve Google map tiles. Map tiles are retrieved only using geographic location information.

FQDN INFORMATION EXAMPLE

For example, your non-cluster installation has a domain named UtilityA.com, and cgnms1 as the hostname with an FQDN of cgnms1.UtilityA.com. You would email ask-fnd-pm-external@cisco.com and include the FQDN, cgnms1.UtilityA.com.

In a cluster deployment with one or more IoT FND servers and a load balancer with the FQDN of loadbalancer-vip, which directs traffic to the cgnms-main or cnms-dr cluster (DR installations). You would email ask-fnd-pm-external@cisco.com and include the FQDN, loadbalancer-vip.UtilityA.com.

System Requirements

[Table 1](#) lists the required hardware and software versions associated with this release.

Note: For a large scale system, refer to [Table 2](#) and [Table 3](#) for scale requirements.

Table 1 Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems

Component	Minimum Hardware Requirement	Minimum Software Release
Cisco IoT FND application server (or comparable system that meets the minimum hardware and software requirements)	<ul style="list-style-type: none"> ■ Processor: <ul style="list-style-type: none"> – Intel Xeon x5680 2.27 GHz (64-bit) – 4 CPUs – RAM: 16 GB ■ Disk space: 100 GB ■ Hardware Security Module (HSM) or Software Security Module (SSM) 	<ul style="list-style-type: none"> ■ Red Hat Enterprise Linux 6.4 and above, 64-bit with all packages installed (software development and web server) See Table 3 on page 12 for suggested application server resource allocation profiles. ■ Internet connection When you access IoT FND from a client browser, the browser connects to the Internet to download the necessary data files from the GIS maps provider. ■ A license to use SafeNet for mesh endpoint security <p>Note: IoT FND software bundle includes the required Java version.</p>

Table 1 Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems (continued)

Component	Minimum Hardware Requirement	Minimum Software Release
Cisco IoT FND TPS proxy	<ul style="list-style-type: none"> ■ Processor: <ul style="list-style-type: none"> – Intel Xeon x5680 2.27 GHz (64-bit) – 2 CPUs ■ RAM: 4 GB ■ Disk space: 25 GB 	<ul style="list-style-type: none"> ■ Red Hat Enterprise Linux 6.4 and above with all packages installed (software development and web server) ■ Internet connection <p>Note: IoT FND software bundle includes required Java version.</p>
<p>Database server for IoT FND</p> <p>Scalable to 25 routers/10,000 endpoints with minimum hardware requirement. See Resource Management Guidelines for additional scale sizes.</p>	<ul style="list-style-type: none"> ■ Processor: <ul style="list-style-type: none"> – Intel Xeon x5680 3.33 GHz (64-bit) ■ 2 CPUs ■ RAM: 16 GB ■ Disk space: 100 GB (120 GB when installing Oracle 12c) 	<p>Note: IoT FND 3.2.x supports both of the Oracle releases listed below.</p> <ul style="list-style-type: none"> ■ Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production (with Patch 20830993) ■ Oracle 11g Enterprise Edition (11.2.0.3 64-bit version only) <p>Note: Before installing Oracle, install the Linux packages referenced in Installing the Linux Packages Required for Installing Oracle.</p> <p>See Table 2 on page 12 for suggested Oracle Database server resource allocation profiles.</p> <ul style="list-style-type: none"> ■ Red Hat Linux 6.4 and above, 64-bit with all packages installed (software development and web server)
Cisco IoT FND Client	<p>The client must meet the following minimum requirements to connect to the IoT FND application server and view IoT FND displays:</p> <ul style="list-style-type: none"> ■ Windows 7 or Win2000 R2 Server ■ RAM: 8 GB ■ Processor: 2 GHz ■ Resolution: 1024 x 768 	<ul style="list-style-type: none"> ■ Adobe Flash Version 9.0.115 or later (required for viewing charts) ■ Supported browsers: <ul style="list-style-type: none"> – Internet Explorer (IE): 11.0 – Mozilla Firefox: 3.5 or higher – Windows 7 works with IE 11.0

Table 1 Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems (continued)

Component	Minimum Hardware Requirement	Minimum Software Release
Cisco Network Registrar (CNR) (used as a DHCP server)	Server must have the following minimum requirements: <ul style="list-style-type: none"> ■ Free disk space: 146 GB ■ RAM: 4 GB (small network), 8 GB (average network), 16 GB (large network) ■ Hard drives: <ul style="list-style-type: none"> – SATA drives with 7500 RPM drive > 500 leases/second <li style="text-align: center;"><i>or</i> – SAS drives with 15K RPM drive > 1000 leases/second 	The following software environment must exist before installing Cisco Network Registrar, software release 8.2 on the server: <ul style="list-style-type: none"> ■ Operating System: Windows Server 2000 ■ 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 and command-line interface (CLI) (Browser versions listed below): <ul style="list-style-type: none"> – Internet Explorer (IE) 11.0, Mozilla Firefox 3.0 or later ■ CNR license. Contact your Cisco partner for the necessary license.
IoT Device Manager (IoT-DM or Device Manager)	Laptop running Device Manager must have the following: <ul style="list-style-type: none"> ■ Microsoft Windows 7 Enterprise or Windows 10 ■ 2 GHz or faster processor ■ 1 GB RAM minimum (for potential large log file processing) ■ WiFi or Ethernet interface ■ 4 GB disk storage space ■ Windows login enabled ■ Utility-signed Certificate Authority (CA) and Client Certificate for router authentication (obtained from your IT department) ■ Customer-specific IT security hardening to keep the Device Manager laptop secure 	<ul style="list-style-type: none"> ■ Version 5.0.0.16
Cisco 1000 Series Connected Grid Router	–	<ul style="list-style-type: none"> ■ Cisco IOS Release 15.7(3)M ■ Cisco CG-OS Release CG4(5)
Cisco ISR 800 Series Integrated Services Routers (C800)	–	<ul style="list-style-type: none"> ■ Cisco IOS Release 15.7(3)M

Table 1 Minimum Hardware and Software Requirements for Cisco IoT FND and Supporting Systems (continued)

Component	Minimum Hardware Requirement	Minimum Software Release
Cisco 800 Series Access Points (AP800)	-	<ul style="list-style-type: none"> ■ AP802: ap802-k9w7-tar.153-3.JBB.tar ■ AP803: ap1g3-k9w7-tar.153-3.JBB2.tar
Cisco 800 Series Industrial Integrated Services Routers (IR800)	-	<ul style="list-style-type: none"> ■ Cisco IOS Release 15.7(3)M
Cisco 3900 Series Integrated Service Router (ISR)	-	<ul style="list-style-type: none"> ■ Cisco IOS Release 15.4(3)M ■ Cisco IOS Release 15.4(2)T
Cisco ASR 1001 or 1002 Aggregation Services Router (ASR) serving as a head-end router	-	<ul style="list-style-type: none"> ■ Cisco IOS XE Release 3.17.02.S for Flex tunnels (IOS) ■ Cisco IOS XE Release 3.11S for Point to Point tunnels (CG-OS)
Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR500)	-	<ul style="list-style-type: none"> ■ Cisco IR509, DA Gateway device: Firmware version 5.6.10 ■ Cisco IR529, Range Extender: Firmware version 5.6.10
Note: ASRs and ISRs with different releases can co-exist on the network.		
Cisco Connected Grid CG-Mesh Module and supported endpoints	-	<ul style="list-style-type: none"> ■ Firmware version 5.6.10 when communicating with CGR 1000s or Cisco ASRs and the minimum Cisco IOS software versions recommended for these routers in these release notes
Cisco Connected Grid RF Mesh endpoints		<ul style="list-style-type: none"> ■ Firmware version 5.6.10 when communicating with IR500
Long Range Wide Area Network (LoRAWAN) Interface Module for Cisco 800 Series Industrial Integrated Services Routers (IR800)	-	<ul style="list-style-type: none"> ■ Cisco IOS 15.6(3)M1b
Hardware Security Module (HSM)	Luna SA appliance, with client software installed on the IoT FND application servers	<p>Luna SA appliance:</p> <ul style="list-style-type: none"> ■ Release 6.10.2 firmware <p>Note: Contact SafeNet to determine if you can run a higher version.</p> <ul style="list-style-type: none"> ■ Release 5.4.7-1 software, plus security patches <p>Luna SA client software:</p> <ul style="list-style-type: none"> ■ Release 5.4.7-1 software
Software Security Module (SSM)	<ul style="list-style-type: none"> ■ RAM: 8 GB ■ Processor: 2 GHz ■ 2 CPUs 	<ul style="list-style-type: none"> ■ Red Hat Enterprise Linux 6.4 or 7.1, 64-bit with all packages installed (software development and web server)

Note: If deploying a IoT FND server cluster, all nodes in the cluster should run on similar hardware. Additionally, all nodes must run the same version of IoT FND.

Resource Management Guidelines

Virtual machine configuration workload characterization is important. When using multiple VMs on the same physical host, allocate resources so that individual VMs do not impact the performance of other VMs. For example, to allocate 4 VMs on a 8-CPU host, do not allocate all 8 CPUs to ensure that one (or more) VM does not use all resources.

[Table 2 on page 12](#) lists example Oracle database server usage profiles for important resource parameters such as CPU, memory, and disk space.

Note: Please note the following with respect to [Table 2](#), when you install the IOTFND SKU (R-IOTFND-V-K9) that has Oracle bundled into the Virtual Machine (VM), the maximum number of supported routers is 1000 and the maximum number of endpoints supported is 250,000.

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

[Table 3 on page 12](#) lists example IoT FND Application Server usage profiles for important resource parameters such as CPU, memory, and disk space.

Table 3 Application Server Hardware Requirements Example Profiles

Nodes (Routers/Endpoints)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
25/10,000	2	16	100
50/50,000	4	16	200
500/500,000	4	16	250
1,000/1,000,000	8	16	250
2,000/2,000,000 ¹	8	16	500
5,000/5,000,000 ¹	8	16	500

1. Clustered installations.

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

For Router Only Deployments

Information in [Table 4](#) and [Table 5](#) applies to Router Only deployments.

Table 4 Application Server Hardware Requirements Example Profile For Routers and LoRa Modules

Nodes (IR800/LoRa modules)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
10,000/30,000	4	24	100

Table 5 Database Server Hardware Requirements Example Profile For Routers and LoRa Modules

Nodes (IR800/LoRa modules)	CPU (Virtual Cores)	Memory (RAM GB)	Disk Space (GB)
10,000/30,000	6	32	500

Obtaining IoT FND and CNR Licenses

- Contact your Cisco partner to obtain the necessary licenses to use IoT FND and CNR.
- Obtain a license to use SafeNet as your HSM for mesh endpoint security.

Installing the Linux Packages Required for Installing Oracle

Note: You must contact Red Hat directly to obtain the Linux packages listed below:

Install these packages in this order 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

When you purchase IoT FND from Cisco or a Cisco partner, you will receive a link to download an ISO file that contains the following five RPM packages. Before you install and set up your IoT FND system, ensure that you have the following five RPM packages:

RPM Package	Description
<code>cgms-version_number.x86_64.rpm</code>	This is the main RPM that contains the IoT FND application server itself. Install this package on the IoT FND application servers.
<code>cgms-oracle-version_number.x86_64.rpm</code>	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.
<code>cgms-tools-version_number.x86_64.rpm</code>	Contains a few optional command-line tools. If needed, install this package on the system running the IoT FND application server.
<code>cgms-ssm-version_number.x86_64.rpm</code>	Contains the Software Security Module (SSM). Install this package on the system running the IoT FND application server.
<code>cgms-tpsproxy-version_number.x86_64.rpm</code>	Contains the TPS proxy application. Install this package on the IoT FND TPS proxy system.

Configuring NTP Service

Configure all Red Hat Enterprise Linux (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.

To configure NTP on your RHEL servers:

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

For 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
...
```

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

```
service ntpd restart
chkconfig ntpd on
```

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.

```
# 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 Installation Overview

Complete the following procedures to install IoT FND:

1. [Installing and Setting Up the IoT FND Database.](#)
2. [Installing and Setting Up IoT FND.](#)
3. [Installing and Configuring the IoT FND TPS Proxy.](#)

Installing and Setting Up the IoT FND Database

Complete the following procedures to finish your IoT FND installation:

- [Installation and Setup Overview](#)
- [Downloading and Unpacking Oracle Database](#)
- [Running the Oracle Database Installer](#)
- [Setting Up the IoT FND Database](#)
- [Additional IoT FND Database Topics](#)

Installation and Setup Overview

The following topics provide an overview of IoT FND deployment:

- [Single-Server Deployment](#)
- [High Availability Deployment](#)

Single-Server Deployment

To install and set up IoT FND database for a single-server database deployment:

1. Log in to the database server.
2. [Downloading and Unpacking Oracle Database.](#)
3. [Running the Oracle Database Installer.](#)
4. [Setting Up the IoT FND Database.](#)

High Availability Deployment

To install and set up IoT FND database for HA:

1. Log in to the primary IoT FND database server.
2. [Downloading and Unpacking Oracle Database.](#)
3. [Running the Oracle Database Installer.](#)
4. Log in to the standby database server.
5. [Downloading and Unpacking Oracle Database.](#)
6. [Running the Oracle Database Installer.](#)

7. Setting Up IoT FND Database for HA.

Downloading and Unpacking Oracle Database

To download the Oracle database:

1. Log in to your server as root.
2. Download Oracle 11g Enterprise Edition (11.2.0.3 64-bit) or Oracle12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production (with Patch 20830993).
3. To avoid display-related errors when installing the Oracle Database software, as root run this command:

```
# xhost + local:oracle
```

4. Create the **oracle** user and **dba** group:

```
# groupadd dba
# adduser -d /home/oracle -g dba -s /bin/bash oracle
```

5. Unpack the Oracle Database zip archives.

```
p10404530_112030_Linux-x86-64_1of7.zip
p10404530_112030_Linux-x86-64_2of7.zip
p10404530_112030_Linux-x86-64_3of7.zip
p10404530_112030_Linux-x86-64_4of7.zip
p10404530_112030_Linux-x86-64_5of7.zip
p10404530_112030_Linux-x86-64_6of7.zip
p10404530_112030_Linux-x86-64_7of7.zip
```

Running the Oracle Database Installer

Note: Before running the Oracle installer, disable the firewall.

To install the Oracle database:

1. Switch to user **oracle** and run the Oracle database installer:

```
# su - oracle
# setenv DISPLAY <desktop>
# path_to_DB_installation_folder/database/runInstaller
```

2. Click **Yes**, and then click **Next**.
3. Click **Install database software only**, and then click **Next**.
4. Click **Single instance database installation**, and then click **Next**.
5. Select **English** as the language in which the database runs, and then click **Next**.
6. Click **Enterprise Edition (4.29GB (Oracle 11g))** or **6.4GB (Oracle12c)**, and then click **Next**.
7. Select the following two default installation values, Oracle Base and Software Location (**11.2.0** or **12.1.0**), and then click **Next**.
 - Oracle Base—**/home/oracle/app/oracle**
 - Software Location—**/home/oracle/app/oracle/product/11.2.0/dbhome_1**
 - Software Location—**/home/oracle/app/oracle/product/12.1.0/dbhome_1**

Later you will create the environment variables ORACLE_BASE and ORACLE_HOME based on the values of the Oracle Base and Software Location properties.

8. On the **Create Inventory** page, keep the default values, and then click **Next**.

- Inventory Directory—**/home/oracle/app/oralInventory**
- oralInventory_Group Name—**dba**

9. On the **Privileged Operating System Groups** page, keep the default values, and then click **Next**.

- Database Administrator (OSDBA) group—**dba**
- Database Operator (OSOPER) group—**dba**
- Database Backup and Recovery (OSBACKUPDBA) group—**dba** (12c only)
- Data Guard administrative (OSDGDBA) group—**dba** (12c only)
- Encryption Key Management administrative (OSKMDBA) group—**dba** (12c only)

10. (optional) On the **Perform Prerequisite Checks** page, install any required software or run supplied scripts.

The installer might require the installation of additional software based on your system kernel settings, and may also instruct you to run scripts to configure your system and complete the database installation.

Note: If no missing packages are noted or you see the message “This is a prerequisite condition to test whether the package “ksh” is available on the system, check the **Ignore All** box.

11. After installing any missing packages, click **Fix & Check Again**.

Keep doing this until all requirements are met.

Caution: Do not ignore errors on this page. If there are errors during database installation, IoT FND may not function properly.

12. Click **Next**.

13. On the **Summary** page, verify the database settings, and then click **Finish** (11g) or **Install** (12c) to start the installation process.

14. At the prompts, run the supplied configuration scripts.

Because the installer runs as the user *oracle*, it cannot perform certain installation operations that require root privileges. For these operations, you will be prompted to run scripts to complete the installation process. When prompted, open a terminal window and run the scripts as root.

15. If the installation succeeds, click **Close** on the **Finish** page.

Note: If performing a new installation of Oracle 12c or upgrading from Oracle 11g, you **must** install the Oracle 12c Patch 20830993. Go to [\(Mandatory\) Installing 12c Patch](#).

(Mandatory) Installing 12c Patch

For all new Oracle 12c database installations and all Oracle 11g upgrades, you must install the 12c patch.

To install the patch:

1. Stop IoT FND application if running.

2. Stop Oracle service if running.**3. Run the following commands to verify inventory of installed Oracle software components and patches. No patches applied at this stage. The following displays at the end: *There are no interim patches installed in this Oracle Home.***

```
/home/oracle/app/oracle/product/12.1.0/dbhome_1/OPatch/opatch lsinventory -details
```

```
Oracle Interim Patch Installer version 12.1.0.1.3
Copyright (c) 2016, Oracle Corporation. All rights reserved.
```

```
Oracle Home      : /home/oracle/app/oracle/product/12.1.0/dbhome_1
Central Inventory : /home/oracle/app/oraInventory from           :
                  /home/oracle/app/oracle/product/12.1.0/dbhome_1/oraInst.loc
OPatch version   : 12.1.0.1.3
OUI version      : 12.1.0.2.0
Log file location: /home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/opatch2016-02-25_10-37-50AM_1.log
```

```
Lsinventory Output file location :
/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/lsinv/lsinventory2016-02-25_10-37-50
AM.txt
```

```
-----
Installed Top-level Products (1):
Oracle Database 12c                               12.1.0.2.0
There are 1 products installed in this Oracle Home.
Installed Products (135):
Assistant Common Files                           12.1.0.2.0
Buildtools Common Files                          12.1.0.2.0
Cluster Verification Utility Common Files         12.1.0.2.0
Database Configuration and Upgrade Assistants    12.1.0.2.0
Database Migration Assistant for Unicode         12.1.0.2.0
Database SQL Scripts                             12.1.0.2.0
Database Workspace Manager                       12.1.0.2.0
DB TOOLS Listener                               12.1.0.2.0
Deinstallation Tool                              12.1.0.2.0
Enterprise Edition Options                       12.1.0.2.0
Expat libraries                                  2.0.1.0.2
Generic Connectivity Common Files                 12.1.0.2.0
Hadoopcore Component                             12.1.0.2.0
HAS Common Files                                 12.1.0.2.0
HAS Files for DB                                 12.1.0.2.0
Installation Common Files                        12.1.0.2.0
Installation Plugin Files                        12.1.0.2.0
Installer SDK Component                          12.1.0.2.0J
Accelerator (COMPANION)                         12.1.0.2.0
Java Development Kit                             1.6.0.75.0
LDAP Required Support Files                       12.1.0.2.0
OLAP SQL Scripts                                 12.1.0.2.0
Oracle Advanced Security                         12.1.0.2.0
Oracle Application Express                       12.1.0.2.0
Oracle Bali Share                                11.1.1.6.0
Oracle Call Interface (OCI)                      12.1.0.2.0
Oracle Clusterware RDBMS Files                   12.1.0.2.0
Oracle Configuration Manager                     10.3.8.1.1
Oracle Configuration Manager Client              10.3.2.1.0
Oracle Configuration Manager Deconfiguration     10.3.1.0.0
Oracle Containers for Java                       12.1.0.2.0
Oracle Context Companion                         12.1.0.2.0
Oracle Core Required Support Files                12.1.0.2.0
Oracle Core Required Support Files for Core DB   12.1.0.2.0
Oracle Core XML Development Kit                  12.1.0.2.0
Oracle Data Mining RDBMS Files                   12.1.0.2.0
Oracle Database 12c                              12.1.0.2.0
```

Oracle Database 12c	12.1.0.2.0
Oracle Database 12c Multimedia Files	12.1.0.2.0
Oracle Database Deconfiguration	12.1.0.2.0
Oracle Database Gateway for ODBC	12.1.0.2.0
Oracle Database Plugin for Oracle Virtual Assembly Builder	12.1.0.2.0
Oracle Database User Interface	11.0.0.0.0
Oracle Database Utilities	12.1.0.2.0
Oracle Database Vault option	12.1.0.2.0
Oracle DBCA Deconfiguration	12.1.0.2.0
Oracle Extended Windowing Toolkit	11.1.1.6.0
Oracle Globalization Support	12.1.0.2.0
Oracle Globalization Support	12.1.0.2.0
Oracle Globalization Support For Core	12.1.0.2.0
Oracle Help for Java	11.1.1.7.0
Oracle Help Share Library	11.1.1.7.0
Oracle Ice Browser	11.1.1.7.0
Oracle Internet Directory Client	12.1.0.2.0
Oracle Java Client	12.1.0.2.0
Oracle Java Layout Engine	11.0.0.0.0
Oracle JDBC Server Support Package	12.1.0.2.0
Oracle JDBC/OCI Instant Client	12.1.0.2.0
Oracle JDBC/THIN Interfaces	12.1.0.2.0
Oracle JFC Extended Windowing Toolkit	11.1.1.6.0
Oracle JVM	12.1.0.2.0
Oracle JVM For Core	12.1.0.2.0
Oracle Label Security	12.1.0.2.0
Oracle LDAP administration	12.1.0.2.0
Oracle Locale Builder	12.1.0.2.0
Oracle Message Gateway Common Files	12.1.0.2.0
Oracle Multimedia	12.1.0.2.0
Oracle Multimedia Client Option	12.1.0.2.0
Oracle Multimedia Java Advanced Imaging	12.1.0.2.0
Oracle Multimedia Locator	12.1.0.2.0
Oracle Multimedia Locator Java Required Support Files	12.1.0.2.0
Oracle Multimedia Locator RDBMS Files	12.1.0.2.0
Oracle Net	12.1.0.2.0
Oracle Net Java Required Support Files	12.1.0.2.0
Oracle Net Listener	12.1.0.2.0
Oracle Net Required Support Files	12.1.0.2.0
Oracle Net Services	12.1.0.2.0
Oracle Netca Client	12.1.0.2.0
Oracle Notification Service	12.1.0.2.0
Oracle Notification Service (eONS)	12.1.0.2.0
Oracle Notification Service for Instant Client	12.1.0.2.0
Oracle ODBC Driver	12.1.0.2.0
Oracle ODBC Driverfor Instant Client	12.1.0.2.0
Oracle OLAP	12.1.0.2.0
Oracle OLAP API	12.1.0.2.0
Oracle OLAP RDBMS Files	12.1.0.2.0
Oracle One-Off Patch Installer	12.1.0.1.2
Oracle Partitioning	12.1.0.2.0
Oracle Programmer	12.1.0.2.0
Oracle Quality of Service Management (Client)	12.1.0.2.0
Oracle R Enterprise Server Files	12.1.0.2.0
Oracle RAC Deconfiguration	12.1.0.2.0
Oracle RAC Required Support Files-HAS	12.1.0.2.0
Oracle Real Application Testing	12.1.0.2.0
Oracle Recovery Manager	12.1.0.2.0
Oracle Security Developer Tools	12.1.0.2.0
Oracle Spatial and Graph	12.1.0.2.0
Oracle SQL Developer	12.1.0.2.0
Oracle Starter Database	12.1.0.2.0
Oracle Text	12.1.0.2.0

Oracle Text ATG Language Support Files	12.1.0.2.0
Oracle Text for Core	12.1.0.2.0
Oracle Text Required Support Files	12.1.0.2.0
Oracle Universal Connection Pool	12.1.0.2.0
Oracle Universal Installer	12.1.0.2.0
Oracle USM Deconfiguration	12.1.0.2.0
Oracle Wallet Manager	12.1.0.2.0
Oracle XML Development Kit	12.1.0.2.0
Oracle XML Query	12.1.0.2.0
oracle.swd.oui.core.min	12.1.0.2.0
Parser Generator Required Support Files	12.1.0.2.0
Perl Interpreter	5.14.1.0.0
Perl Modules	5.14.1.0.0
PL/SQL	12.1.0.2.0
PL/SQL Embedded Gateway	12.1.0.2.0
Platform Required Support Files	12.1.0.2.0
Precompiler Common Files	12.1.0.2.0
Precompiler Common Files for Core	12.1.0.2.0
Precompiler Required Support Files	12.1.0.2.0
Precompilers	12.1.0.2.0
RDBMS Required Support Files	12.1.0.2.0
RDBMS Required Support Files for Instant Client	12.1.0.2.0
RDBMS Required Support Files Runtime	12.1.0.2.0
Required Support Files	12.1.0.2.0
Sample Schema Data	12.1.0.2.0
Secure Socket Layer	12.1.0.2.0
SQL*Plus	12.1.0.2.0
SQL*Plus Files for Instant Client	12.1.0.2.0
SQL*Plus Required Support Files	12.1.0.2.0
SQLJ Runtime	12.1.0.2.0
SSL Required Support Files for InstantClient	12.1.0.2.0
Tracle File Analyzer	12.1.0.2.0
XDK Required Support Files	12.1.0.2.0
XML Parser for Java	12.1.0.2.0
XML Parser for Oracle JVM	12.1.0.2.0

There are 135 products installed in this Oracle Home.

There are no Interim patches installed in this Oracle Home.

4. Apply the patch.

a. On the database machine. Copy the patch file: "p20830993_121020_Linux-x86-64.zip"

b. Run a prerequisite check. It should pass.

```
$ cd /home/oracle/patches/20830993/
$ /home/oracle/app/oracle/product/12.1.0/dbhome_1/OPatch/opatch prereq
CheckConflictAgainstOHWithDetail -ph ./
Oracle Interim Patch Installer version 12.1.0.1.3
Copyright (c) 2016, Oracle Corporation. All rights reserved.

PREREQ session

Oracle Home      : /home/oracle/app/oracle/product/12.1.0/dbhome_1
Central Inventory : /home/oracle/app/oraInventory
   from           : /home/oracle/app/oracle/product/12.1.0/dbhome_1/oraInst.loc
OPatch version   : 12.1.0.1.3
OUI version      : 12.1.0.2.0
Log file location : /home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtool
logs/opatch/opatch2016-02-25_10-48-48AM_1.log

Invoking prereq "checkconflictagainsthwithdetail"

Prereq "checkConflictAgainstOHWithDetail" passed.
```

OPatch succeeded.

c. Apply the patch.

```
$ /home/oracle/app/oracle/product/12.1.0/dbhome_1/OPatch/opatch apply
Oracle Interim Patch Installer version 12.1.0.1.3
Copyright (c) 2016, Oracle Corporation. All rights reserved.

Oracle Home      : /home/oracle/app/oracle/product/12.1.0/dbhome_1
Central Inventory : /home/oracle/app/oraInventory   from           :
                  /home/oracle/app/oracle/product/12.1.0/dbhome_1/oraInst.loc
OPatch version   : 12.1.0.1.3
OUI version      : 12.1.0.2.0
Log file location:
/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/20830993_Feb_25_2016_10_53_25/ap
ply2016-02-25_10-53-25AM_1.log

Applying interim patch '20830993' to OH '/home/oracle/app/oracle/product/12.1.0/dbhome_1'
Verifying environment and performing prerequisite checks...
All checks passed.

Please shutdown Oracle instances running out of this ORACLE_HOME on the local system.
(Oracle Home = '/home/oracle/app/oracle/product/12.1.0/dbhome_1')

Is the local system ready for patching? [y|n]
y
User Responded with: Y
Backing up files...

Patching component oracle.rdbms, 12.1.0.2.0...

Verifying the update...
Patch 20830993 successfully applied
Log file location:/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/
20830993_Feb_25_2016_10_53_25/apply2016-02-25_10-53-25AM_1.log

OPatch succeeded.
```

d. Run Opatch utility to verify that the patch is now recognized. Notice the mention of "Interim Patch" at the end of following output.

```
$ /home/oracle/app/oracle/product/12.1.0/dbhome_1/OPatch/opatch lsinventory -details
Oracle Interim Patch Installer version 12.1.0.1.3
Copyright (c) 2016, Oracle Corporation. All rights reserved.

Oracle Home      : /home/oracle/app/oracle/product/12.1.0/dbhome_1
Central Inventory : /home/oracle/app/oraInventory
                  from           : /home/oracle/app/oracle/product/12.1.0/dbhome_1/oraInst.loc
OPatch version   : 12.1.0.1.3
OUI version      : 12.1.0.2.0
Log file location:
/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/opatch2016-02-25_11-05-19AM_1.lo
g
Lsinventory Output file location :
/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/lsinv/lsinventory2016-02-25_11-0
5-19AM.txt

-----
Installed Top-level Products (1):
Oracle Database 12c                               12.1.0.2.0
There are 1 products installed in this Oracle Home.
```

Installed Products (135):

Assistant Common Files	12.1.0.2.0
Buildtools Common Files	12.1.0.2.0
Cluster Verification Utility Common Files	12.1.0.2.0
Database Configuration and Upgrade Assistants	12.1.0.2.0
Database Migration Assistant for Unicode	12.1.0.2.0
Database SQL Scripts	12.1.0.2.0
Database Workspace Manager	12.1.0.2.0
DB TOOLS Listener	12.1.0.2.0
Deinstallation Tool	12.1.0.2.0
Enterprise Edition Options	12.1.0.2.0
Expat libraries	2.0.1.0.2
Generic Connectivity Common Files	12.1.0.2.0
Hadoopcore Component	12.1.0.2.0
HAS Common Files	12.1.0.2.0
HAS Files for DB	12.1.0.2.0
Installation Common Files	12.1.0.2.0
Installation Plugin Files	12.1.0.2.0
Installer SDK Component	12.1.0.2.0
JAccelerator (COMPANION)	12.1.0.2.0
Java Development Kit	1.6.0.75.0
LDAP Required Support Files	12.1.0.2.0
LAP SQL Scripts	12.1.0.2.0
Oracle Advanced Security	12.1.0.2.0
Oracle Application Express	12.1.0.2.0
Oracle Bali Share	11.1.1.6.0
Oracle Call Interface (OCI)	12.1.0.2.0
Oracle Clusterware RDBMS Files	12.1.0.2.0
Oracle Configuration Manager	10.3.8.1.1
Oracle Configuration Manager Client	10.3.2.1.0
Oracle Configuration Manager Deconfiguration	10.3.1.0.0
Oracle Containers for Java	12.1.0.2.0
Oracle Context Companion	12.1.0.2.0
Oracle Core Required Support Files	12.1.0.2.0
Oracle Core Required Support Files for Core DB	12.1.0.2.0
Oracle Core XML Development Kit	12.1.0.2.0
Oracle Data Mining RDBMS Files	12.1.0.2.0
Oracle Database 12c	12.1.0.2.0
Oracle Database 12c	12.1.0.2.0
Oracle Database 12c Multimedia Files	12.1.0.2.0
Oracle Database Deconfiguration	12.1.0.2.0
Oracle Database Gateway for ODBC	12.1.0.2.0
Oracle Database Plugin for Oracle Virtual Assembly Builder	12.1.0.2.0
Oracle Database User Interface	11.0.0.0.0
Oracle Database Utilities	12.1.0.2.0
Oracle Database Vault option	12.1.0.2.0
Oracle DBCA Deconfiguration	12.1.0.2.0
Oracle Extended Windowing Toolkit	11.1.1.6.0
Oracle Globalization Support	12.1.0.2.0
Oracle Globalization Support	12.1.0.2.0
Oracle Globalization Support For Core	12.1.0.2.0
Oracle Help for Java	11.1.1.7.0
Oracle Help Share Library	11.1.1.7.0
Oracle Ice Browser	11.1.1.7.0
Oracle Internet Directory Client	12.1.0.2.0
Oracle Java Client	12.1.0.2.0
Oracle Java Layout Engine	11.0.0.0.0
Oracle JDBC Server Support Package	12.1.0.2.0
Oracle JDBC/OCI Instant Client	12.1.0.2.0
Oracle JDBC/THIN Interfaces	12.1.0.2.0
Oracle JFC Extended Windowing Toolkit	11.1.1.6.0
Oracle JVM	12.1.0.2.0
Oracle JVM For Core	12.1.0.2.0
Oracle Label Security	12.1.0.2.0

Oracle LDAP administration	12.1.0.2.0
Oracle Locale Builder	12.1.0.2.0
Oracle Message Gateway Common Files	12.1.0.2.0
Oracle Multimedia	12.1.0.2.0
Oracle Multimedia Client Option	12.1.0.2.0
Oracle Multimedia Java Advanced Imaging	12.1.0.2.0
Oracle Multimedia Locator	12.1.0.2.0
Oracle Multimedia Locator Java Required Support Files	12.1.0.2.0
Oracle Multimedia Locator RDBMS Files	12.1.0.2.0
Oracle Net	12.1.0.2.0
Oracle Net Java Required Support Files	12.1.0.2.0
Oracle Net Listener	12.1.0.2.0
Oracle Net Required Support Files	12.1.0.2.0
Oracle Net Services	12.1.0.2.0
Oracle Netca Client	12.1.0.2.0
Oracle Notification Service	12.1.0.2.0
Oracle Notification Service (eONS)	12.1.0.2.0
Oracle Notification Service for Instant Client	12.1.0.2.0
Oracle ODBC Driver	12.1.0.2.0
Oracle ODBC Driverfor Instant Client	12.1.0.2.0
Oracle OLAP	12.1.0.2.0
Oracle OLAP API	12.1.0.2.0
Oracle OLAP RDBMS Files	12.1.0.2.0
Oracle One-Off Patch Installer	12.1.0.1.2
Oracle Partitioning	12.1.0.2.0
Oracle Programmer	12.1.0.2.0
Oracle Quality of Service Management (Client)	12.1.0.2.0
Oracle R Enterprise Server Files	12.1.0.2.0
Oracle RAC Deconfiguration	12.1.0.2.0
Oracle RAC Required Support Files-HAS	12.1.0.2.0
Oracle Real Application Testing	12.1.0.2.0
Oracle Recovery Manager	12.1.0.2.0
Oracle Security Developer Tools	12.1.0.2.0
Oracle Spatial and Graph	12.1.0.2.0
Oracle SQL Developer	12.1.0.2.0
Oracle Starter Database	12.1.0.2.0
Oracle Text	12.1.0.2.0
Oracle Text ATG Language Support Files	12.1.0.2.0
Oracle Text for Core	12.1.0.2.0
Oracle Text Required Support Files	12.1.0.2.0
Oracle Universal Connection Pool	12.1.0.2.0
Oracle Universal Installer	12.1.0.2.0
Oracle USM Deconfiguration	12.1.0.2.0
Oracle Wallet Manager	12.1.0.2.0
Oracle XML Development Kit	12.1.0.2.0
Oracle XML Query	12.1.0.2.0
oracle.swd.oui.core.min	12.1.0.2.0
Parser Generator Required Support Files	12.1.0.2.0
Perl Interpreter	5.14.1.0.0
Perl Modules	5.14.1.0.0
PL/SQL	12.1.0.2.0
PL/SQL Embedded Gateway	12.1.0.2.0
Platform Required Support Files	12.1.0.2.0
Precompiler Common Files	12.1.0.2.0
Precompiler Common Files for Core	12.1.0.2.0
Precompiler Required Support Files	12.1.0.2.0
Precompilers	12.1.0.2.0
RDBMS Required Support Files	12.1.0.2.0
RDBMS Required Support Files for Instant Client	12.1.0.2.0
RDBMS Required Support Files Runtime	12.1.0.2.0
Required Support Files	12.1.0.2.0
Sample Schema Data	12.1.0.2.0
Secure Socket Layer	12.1.0.2.0

```
SQL*Plus                                12.1.0.2.0
SQL*Plus Files for Instant Client        12.1.0.2.0
SQL*Plus Required Support Files         12.1.0.2.0
SQLJ Runtime                             12.1.0.2.0
SSL Required Support Files for InstantClient 12.1.0.2.0
Tracle File Analyzer                     12.1.0.2.0
XDK Required Support Files               12.1.0.2.0
XML Parser for Java                      12.1.0.2.0
XML Parser for Oracle JVM                12.1.0.2.0
There are 135 products installed in this Oracle Home.
```

Interim patches (1) :

```
Patch 20830993      : applied on Thu Feb 25 10:53:50 PST 2016
Unique Patch ID: 18912657
Created on 13 May 2015, 00:37:38 hrs PST8PDT
  Bugs fixed:      20830993
Files Touched:
  /qksvc.o --> ORACLE_HOME/lib/libserver12.a
  ins_rdbms.mk --> ORACLE_HOME/rdbms/lib/ioracle
Patch Location in Inventory:
  /home/oracle/app/oracle/product/12.1.0/dbhome_1/inventory/oneoffs/20830993
Patch Location in Storage area:
  /home/oracle/app/oracle/product/12.1.0/dbhome_1/.patch_storage/20830993_May_13_2015_00_37_38
-----
```

Process complete.

Continue to [Setting Up the IoT FND Database](#)

Setting Up the IoT FND Database

Complete the following procedures to set up the IoT FND database:

- [IoT FND Database Setup Overview](#)
- [Defining Oracle Database Environment Variables](#)
- [Installing IoT FND Oracle Database Scripts](#)
- [Creating the IoT FND Oracle Database](#)
- [Starting the IoT FND Oracle Database](#)

IoT FND Database Setup Overview

To set up the IoT FND database:

1. [Defining Oracle Database Environment Variables.](#)
2. [Installing IoT FND Oracle Database Scripts.](#)
3. [Creating the IoT FND Oracle Database.](#)
4. [Starting the IoT FND Oracle Database.](#)

Defining Oracle Database Environment Variables

Before installing the IoT FND Oracle database, switch to the **oracle** user account and define the following Oracle database environment variables.

Table 6 Oracle Database Environment Variables

Variable	Description
ORACLE_BASE	<p>Defines the path to the Oracle root directory on your system. For example:</p> <pre>\$ export ORACLE_BASE=/home/oracle/app/oracle</pre> <p>If this variable is not set, the IoT FND setup script displays an error.</p>
ORACLE_HOME	<p>Defines the path to the Oracle home of the IoT FND database. For example:</p> <pre>\$ export ORACLE_HOME=/home/oracle/app/oracle/product/11.2.0/dbhome_1</pre> <p>Note: Do not have any trailing backslashes in the ORACLE_HOME environment variable.</p>
PATH	<p>Defines the path to the Oracle binaries. For example:</p> <pre>\$ export PATH=\$PATH:\$ORACLE_HOME/bin</pre>
LD_LIBRARY_PATH	<p>Defines the path to the libraries. For example:</p> <pre>\$ export LD_LIBRARY_PATH=\$ORACLE_HOME/lib:\$LD_LIBRARY_PATH</pre>
ORACLE_SID	<p>Defines the Oracle System ID (SID).</p> <p>If you are only using one database server or installing an HA deployment, set this variable on the <i>primary</i> database server to cgms:</p> <pre>\$ export ORACLE_SID=cgms</pre> <p>If deploying a standby database server, set this variable on the <i>standby</i> database server to cgms_s:</p> <pre>\$ export ORACLE_SID=cgms_s</pre> <p>If this variable is not set, the IoT FND setup script displays an error.</p>

You can set these variables manually, as shown in the following example:

On a Single or Primary Database Server	On a Standby Database Server
<pre>\$ su - oracle \$ export ORACLE_BASE=/home/oracle/app/oracle \$ export ORACLE_HOME=/home/oracle/app/oracle/product/11.2.0/db home_1 \$ export PATH=\$PATH:\$ORACLE_HOME/bin \$ export LD_LIBRARY_PATH=\$ORACLE_HOME/lib:\$LD_LIBRARY_PATH \$ export ORACLE_SID=cgms</pre>	<pre>\$ su - oracle \$ export ORACLE_BASE=/home/oracle/app/oracle \$ export ORACLE_HOME=/home/oracle/app/oracle/product/11.2.0/db home_1 \$ export PATH=\$PATH:\$ORACLE_HOME/bin \$ export LD_LIBRARY_PATH=\$ORACLE_HOME/lib:\$LD_LIBRARY_PATH \$ export ORACLE_SID=cgms_s</pre>

You can also use a .bashrc file to define these variables.

Installing IoT FND Oracle Database Scripts

IoT FND is packaged with scripts and Oracle database templates.

To install the Oracle scripts on your Oracle server:

1. Log in as the root user.
2. Securely copy the IoT FND Oracle script RPM to your Oracle server:

```
$ scp cgms-oracle-version_number.x86_64.rpm root@oracle-machine:~
$ rpm -ivh cgms-oracle-version_number.x86_64.rpm
```

3. Create the cgms directory and download the scripts and templates to it:

```
$ cd $ORACLE_BASE/app/oracle
$ mkdir cgms
$ cd cgms
$ cp -R /opt/cgms-oracle/scripts .
$ cp -R /opt/cgms-oracle/templates .
$ cp -R /opt/cgms-oracle/tools .
$ cd ..
$ chown -R oracle:dba cgms
```

Creating the IoT FND Oracle Database

To create the IoT FND Oracle database in a single-database-server deployment, run the `setupCgmsDb.sh` script as the user `oracle`. This script starts the Oracle Database and creates the IoT FND database.

This script creates the user `cgms_dev` used by IoT FND to access the database. The default password for this user account is `cgms123`.

The default password for the sys DBA account is `cgmsDba123`.

Note: We strongly recommend that you change all default passwords. Do not use special characters such as `@`, `#`, `!`, or `+` when using the `encryption_util.sh` script. The script cannot encrypt special characters.

Note: This script might run for several minutes. To check the setup progress, run the command:

```
$ tail -f /tmp/cgmsdb_setup.log
```

```
$ su - oracle
$ export DISPLAY=localhost:0
$ cd $ORACLE_BASE/cgms/scripts
$ ./setupCgmsDb.sh
09-13-2012 10:38:07 PDT: INFO: ===== CGMS Database Setup Started =====
09-13-2012 10:38:07 PDT: INFO: Log file: /tmp/cgmsdb_setup.log
```

```
Are you sure you want to setup CG-NMS database (y/n)? y
```

```
09-13-2012 10:38:08 PDT: INFO: User response: y
09-13-2012 10:38:08 PDT: INFO: CGMS database does not exist.
Enter new password for SYS DBA:
Re-enter new password for SYS DBA:
09-13-2012 10:38:14 PDT: INFO: User entered SYS DBA password.
```

```
Enter new password for CG-NMS database:
Re-enter new password CG-NMS database:
09-13-2012 10:38:18 PDT: INFO: User entered CG-NMS DB password.
09-13-2012 10:38:18 PDT: INFO: Stopping listener ...
09-13-2012 10:38:18 PDT: INFO: Listener already stopped.
09-13-2012 10:38:18 PDT: INFO: Deleting database files ...
09-13-2012 10:38:18 PDT: INFO: Creating listener ...
09-13-2012 10:38:19 PDT: INFO: Listener creation completed successfully.
09-13-2012 10:38:19 PDT: INFO: Configuring listener ...
09-13-2012 10:38:19 PDT: INFO: Listener successfully configured.
09-13-2012 10:38:19 PDT: INFO: Creating database. This may take a while. Please be patient ...
09-13-2012 10:42:55 PDT: INFO: Database creation completed successfully.
```

```

09-13-2012 10:42:55 PDT: INFO: Updating /etc/oratab ...
09-13-2012 10:42:55 PDT: INFO: /etc/oratab updated.
09-13-2012 10:42:55 PDT: INFO: Configuring database ...
09-13-2012 10:42:56 PDT: INFO: Starting listener ...
09-13-2012 10:42:56 PDT: INFO: Listener start completed successfully.
09-13-2012 10:42:56 PDT: INFO: Starting database configuration ...
09-13-2012 10:43:17 PDT: INFO: Database configuration completed successfully.
09-13-2012 10:43:17 PDT: INFO: Starting Oracle ...
09-13-2012 10:43:17 PDT: INFO: Starting Oracle in mount state ...
ORACLE instance started.

Total System Global Area 1.6836E+10 bytes
Fixed Size      2220032 bytes
Variable Size 8589934592 bytes
Database Buffers 8187281408 bytes
Redo Buffers   56487936 bytes
Database mounted.
09-13-2012 10:43:26 PDT: INFO: Opening database for read/write ...

Database altered.

09-13-2012 10:43:29 PDT: INFO: ===== CGMS Database Setup Completed Successfully =====

```

Starting the IoT FND Oracle Database

To start the IoT FND Oracle database:

1. Run the script:

```

$ su - oracle
$ cd $ORACLE_BASE/cgms/scripts
$ ./startOracle.sh

```

2. Configure a cron job that starts IoT FND database at bootup by running this script:

```

./installOracleJob.sh

```

Additional IoT FND Database Topics

The following procedures discuss database management:

- [Stopping the IoT FND Oracle Database](#)
- [Removing the IoT FND Database](#)
- [Upgrading the IoT FND Database](#)
- [Changing the SYS DBA and IoT FND Database Passwords](#)
- [IoT FND Database Helper Scripts](#)

Stopping the IoT FND Oracle Database

Typically, you do not have to stop the Oracle database during the installation procedure. However, if it becomes necessary to stop the Oracle database, use the stop script in the scripts directory:

```

su - oracle
cd $ORACLE_BASE/cgms/scripts
./stopOracle.sh
...

```

```
SQL> Database closed.
Database dismounted.
ORACLE instance shut down.
...
```

Removing the IoT FND Database

Caution: The following script is destructive. Do not use this script during normal operation.

To remove the IoT FND database, run this script:

```
cd $ORACLE_BASE/cgms/scripts
./deleteCgmsDb.sh
```

Upgrading the IoT FND Database

To upgrade the IoT FND database:

1. Add the database files (a total of 15 files).

```
ALTER TABLESPACE USERS ADD DATAFILE '&oracle_base/oradata/&sid_caps/users<02 to 15>.dbf'
SIZE 5M AUTOEXTEND ON;
```

This is required for scaling the system.

2. Enable block-change tracking (required for incremental backup):

```
ALTER DATABASE ENABLE BLOCK CHANGE TRACKING USING FILE
'&oracle_base/oradata/&sid_caps/rman_change_track.f' REUSE;
```

3. Disable parallel execution:

```
set parallel_max_servers = 0 scope=both
```

Caution: The incremental IoT FND backup script enables the Oracle block-change tracking feature to improve backup performance. To take advantage of this feature, delete your IoT FND database and run the setupCgmsDb.sh script before performing the first incremental backup. To avoid losing data, run these commands:

```
sqlplus sys/password@cgms as sysdba
ALTER DATABASE ENABLE BLOCK CHANGE TRACKING USING FILE
'/home/oracle/app/oracle/oradata/CGMS/rman_change_track.f' REUSE;
exit;
```

Changing the SYS DBA and IoT FND Database Passwords

To change default IoT FND database password for the cgms_dba user:

1. On the IoT FND server, run the setupCgms.sh script and change the password for the cgms_dba user.

Caution: The password for the IoT FND database and the cgms_dba user password must match or IoT FND cannot access the database.

```
# cd /opt/cgms/bin
# ./setupCgms.sh
...
Do you want to change the database password (y/n)? y
09-13-2012 17:15:07 PDT: INFO: User response: y
Enter database password:
Re-enter database password:
09-13-2012 17:15:31 PDT: INFO: Configuring database password. This may take a while. Please wait
...
09-13-2012 17:15:34 PDT: INFO: Database password configured.
...
```

For information about running the setupCgms.sh script, see [Setting Up IoT FND](#).

2. On the Oracle server, run the change_password.sh script and change the password for the cgms_dba user:

```
$ ./change_password.sh
09-13-2012 10:48:32 PDT: INFO: ===== Database Password Util Started =====
09-13-2012 10:48:32 PDT: INFO: Log file: /tmp/cgms_oracle.log

Are you sure you want to change CG-NMS database password (y/n)? y
09-13-2012 10:48:33 PDT: INFO: User response: y

Enter current password for SYS DBA:
Re-enter current password for SYS DBA:
09-13-2012 10:48:41 PDT: INFO: User entered current SYS DBA password.
Enter new password for SYS DBA:
Re-enter new password for SYS DBA:
09-13-2012 10:48:54 PDT: INFO: User entered SYS DBA password.

Enter new password for CG-NMS database:
Re-enter new password CG-NMS database:
09-13-2012 10:49:03 PDT: INFO: User entered CG-NMS DB password.
User altered.
...
```

Note: As root, you can also use this script to change the password for the sys user (SYS DBA).

3. On the IoT FND server, run the cgms_status.sh script to verify the connection between IoT FND and the IoT FND database:

```
# service cgms status
09-06-2012 18:51:20 PDT: INFO: CG-NMS database server: localhost
09-06-2012 18:51:21 PDT: INFO: CG-NMS database connection verified.
```

IoT FND Database Helper Scripts

Table 7 describes helper IoT FND database scripts available in the \$ORACLE_BASE/cgms/scripts/ directory:

Table 7 IoT FND Database Helper Scripts

Script	Description
change_password.sh	Use this script to change the passwords for the database administration and IoT FND database user accounts. The IoT FND database user account is used by IoT FND to access the database.
backup_archive_log.sh	Use this script to back up the archive logs.
backupCgmsDb.sh	Use this script to back up the IoT FND database. This script supports full and incremental backups.
restoreCgmsDb.sh	Use this script to restore the IoT FND database from a backup.
setupCgmsDb.sh	Use this script to set up IoT FND database.
startOracle.sh	Use this script to start the IoT FND database.
stopOracle.sh	Use this script to stop the IoT FND database.
setupStandbyDb.sh	(IoT FND database HA installations only) Use this script to set up the standby database server.
setupHaForPrimary.sh	(IoT FND database HA installations only) Use this script to set up the primary database server.
getHaStatus.sh	Run this script to verify that the database is set up for HA.

Installing and Setting Up the SSM

The Software Security Module (SSM) is a low-cost alternative to a Hardware Security Module (HSM). IoT FND uses the CSMP protocol to communicate with meters, DA Gateway (IR500 devices), and range extenders. SSM uses [CiscoJ](#) to provide cryptographic services such as signing and verifying CSMP messages, and CSMP Keystore management. SSM ensures Federal Information Processing Standards (FIPS) compliance, while providing services. You install SSM on the IoT FND application server or other remote server. SSM remote-machine installations use HTTPS to securely communicate with IoT FND.

This section describes SSM installation and set up, including:

- [Installing or Upgrading the SSM Server](#)
- [Uninstalling the SSM Server](#)
- [Integrating SSM and IoT FND](#)

With the SSM server installed, configured, and started and with IoT FND configured for SSM, you can view the CSMP certificate on **Admin > Certificates > Certificate for CSMP**.

Note: See [Setting Up an HSM Client](#) for information on the Hardware Security Module (HSM).

BEFORE YOU BEGIN

Ensure that the installations meets the hardware and software requirements listed in [Table 1](#).

Installing or Upgrading the SSM Server

To install the SSM server:

1. Run the `cgms-ssm-<version>-<release>.<architecture>.rpm rpm script`:

```
[root@VMNMS demosm]# rpm -Uvh cgms-ssm-<version>.x86_64.rpm
Preparing...                               ##### [100%]
 1:cgms-ssm                                ##### [100%]
```

2. Get the IoT FND configuration details for the SSM. SSM ships with following default credentials:

- `ssm_csmp_keystore` password: **ciscossm**
- `csmp` alias name: **ssm_csmp**
- `key` password: **ciscossm**
- `ssm_web_keystore` password: **ssmweb**

```
[root@VMNMS demosm]# cd /opt/cgms-ssm/bin/
[root@VMNMS bin]# ./ssm_setup.sh
```

```
Software Security Module Server
1. Generate a new keyalias with self signed certificate for CSMP
2. Generate a new keypair & certificate signing request for CSMP
3. Import a trusted certificate
4. Change CSMP keystore password
5. Print CG-NMS configuration for SSM
6. Change SSM server port
7. Change SSM-Web keystore password
Select available options.Press any other key to exit
Enter your choice :
```


3. Enter 5 at the prompt, and complete the following when prompted:

```
Enter current ssm_csmp_keystore password :ciscossm
Enter alias name : ssm_csmp
Enter key password :ciscossm

security-module=ssm
ssm-host=<Replace with IPv4 address of SSM server>
ssm-port=8445
ssm-keystore-alias=ssm_csmp
ssm-keystore-password=NQ1/zokip4gtUeUyQnUuNw==
ssm-key-password=NQ1/zokip4gtUeUyQnUuNw==
```

4. To connect to this SSM server, copy paste the output from 3. into the cgms.properties file.

Note: You must include the IPv4 address of the interface for IoT FND to use to connect to the SSM server.

5. (Optional) Run the ssm_setup.sh script to:

- Generate a new key alias with self-signed certificate for CSMP
- Change SSM keystore password
- Change SSM server port
- Change SSM-Web keystore password

Note: If you perform any of the above operations, you must run the SSM setup script, select “Print CG-NMS configuration for SSM,” and copy and paste all details into the cgms.properties file.

6. Start the SSM server:

```
[root@VMNMS ~]# service ssm start
Starting Software Security Module Server: [ OK ]
```

Monitoring SSM Log Files

You can monitor SSM logs in /opt/cgms-ssm/log/ssm.log

The default metrics report interval is 900 secs (15 min.), which is the minimum valid value. Only servicing metrics are logged. If there are no metrics to report, no messages are in the log.

You can change the metrics report interval by setting the **ssm-metrics-report-interval** field (in secs) in the /opt/cgms-ssm/conf/ssm.properties file.

Note: Your SSM must server is up and running before starting the IoT FND server.

Uninstalling the SSM Server

This section presents steps to completely uninstall the SSM server, including the steps for a fresh installation.

Note: Do not use this procedure for upgrades. Use the procedure in [Installing or Upgrading the SSM Server](#).

To uninstall the SSM server:

1. Stop the SSM server:

```
service ssm stop
```

2. Copy and move the /opt/cgms-ssm/conf directory and contents to a directory outside of /opt/cgms-ssm.

3. Uninstall the `cgms-ssm` rpm:

```
rpm -e cgms-ssm
```

Fresh installations only

4. Install a new SSM server.
5. Copy and overwrite the `/opt/cgms-ssm/conf` directory with the contents moved in 2..

Integrating SSM and IoT FND

Note: You must install and start the SSM server before switching to SSM.

To switch from using the Hardware Security Module (HSM) for CSMP-based messaging and use the SSM:

1. Stop IoT FND.

```
service cgms stop
```

2. Run the `ssm_setup.sh` script on the SSM server.
3. Select option 3 to print IoT FND SSM configuration.
4. Copy and paste the details into the `cgms.properties` to connect to that SSM server.

EXAMPLE

```
security-module=ssm
ssm-host=127.107.155.85
ssm-port=8445
ssm-keystore-alias=ssm_csmp
ssm-keystore-password=NQ1/zokip4gtUeUyQnUuNw==
ssm-key-password=NQ1/zokip4gtUeUyQnUuNw==
```

5. To set up the HSM, specify the following properties in the `cgms.properties` file (see also, [Setting Up an HSM Client](#)):

```
security-module=ssm/hsm (required; hsm : Hardware Security Module default.)
hsm-keystore-name=testGroup1 (optional; hsm partition name; testGroup1 default)
hsm-keystore-password=TestPart1 (optional; encrypted hsm partition password; TestPart1 default)
```

6. Ensure that the SSM up and running and you can connect to it.
7. Start IoT FND.

Installing and Setting Up IoT FND

Complete the following procedures to finish your IoT FND installation:

- [Installation and Setup Overview](#)
- [Installing IoT FND](#)
- [Generating and Installing Certificates](#)
- [Setting Up IoT FND](#)
- [Starting IoT FND](#)
- [Checking IoT FND Status](#)
- [Running the IoT FND Database Migration Script](#)

- [Accessing the IoT FND Web GUI](#)

BEFORE YOU BEGIN

To install IoT FND, first obtain the IoT FND installation RPM:

```
cgms-version_number.x86_64.rpm
```

Note: Ensure that `/etc/hosts` and `/etc/resolv.conf` files are correctly configured on the IoT FND server.

Installation and Setup Overview

These topics provide an overview of the two types of IoT FND installations:

- [Single-Server Deployment](#)
- [Cluster Deployment \(HA\)](#)

Single-Server Deployment

To install and set up IoT FND for a single-server deployment:

1. [Log in to the RHEL server that will host IoT FND.](#)
2. [Installing IoT FND.](#)
3. [Setting Up IoT FND.](#)
4. [Running the IoT FND Database Migration Script.](#)
5. [Checking IoT FND Status.](#)
6. [Accessing the IoT FND Web GUI](#)

Cluster Deployment (HA)

To install and set up IoT FND for HA deployments, repeat the steps in [Single-Server Deployment](#), but only run the IoT FND database migration script once.

Installing IoT FND

To install the IoT FND application:

1. Run the IoT FND installation RPM:

```
$ rpm -ivh cgms-version.x86_64.rpm
```

2. Verify installation and check the RPM version:

```
$ rpm -qa | grep -i cgms  
cgms-1.0
```

Setting Up IoT FND

To set up IoT FND, run the `setupCgms.sh` script.

Note: If deploying a IoT FND server cluster, the `setupCgms.sh` script must be run on every node in the cluster.

Caution: The IoT FND certificate encrypts data in the database. The setupCgms.sh script runs database migration, which requires access to the IoT FND certificate in the keystore. You must set up certificates must before running setupCgms.sh. The script results in an error if it migrates the database and cannot access the certificate (see [Generating and Installing Certificates](#)).

Caution: Ensure that the database password entered while running the setupCgms.sh script is valid. If you enter an invalid password multiple times, Oracle might lock your user account. You can unlock your account on the database server. For more information about unlocking your password, see “Unlocking the IoT FND Database Password” in the Troubleshooting chapter of the [IoT Field Network Director User Guide, Release 4.0.x](#).

This example uses the setupCgms.sh script to set up a single-server IoT FND system that uses one database.

```
# cd /opt/cgms/bin
# ./setupCgms.sh
09-13-2012 17:10:00 PDT: INFO: ===== CG-NMS Setup Started - 2012-09-13-17-10-00 =====
09-13-2012 17:10:00 PDT: INFO: Log file: /opt/cgms/bin/./server/cgms/log/cgms_setup.log

Are you sure you want to setup CG-NMS (y/n)? y

09-13-2012 17:10:02 PDT: INFO: User response: y

Do you want to change the database settings (y/n)? y

09-13-2012 17:10:05 PDT: INFO: User response: y

Enter database server IP address [example.com]: 128.107.154.246
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.246

Enter database server port [1522]:
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522

Enter database SID [cgms]:
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms

Do you wish to configure another database server for this CG-NMS ? (y/n)? n

09-13-2012 17:11:18 PDT: INFO: User response: n
09-13-2012 17:11:18 PDT: INFO: Configuring database settings. This may take a while. Please wait ...
09-13-2012 17:11:19 PDT: INFO: Database settings configured.

Do you want to change the database password (y/n)? y
09-13-2012 17:15:07 PDT: INFO: User response: y

Enter database password:
Re-enter database password:

09-13-2012 17:15:31 PDT: INFO: Configuring database password. This may take a while. Please wait ...
09-13-2012 17:15:34 PDT: INFO: Database password configured.

Do you want to change the keystore password (y/n)? n

09-13-2012 17:16:18 PDT: INFO: User response: n

Do you want to change the web application 'root' user password (y/n)? n
09-13-2012 17:16:34 PDT: INFO: User response: n

Do you want to change the FTP settings (y/n)? n
09-13-2012 17:16:45 PDT: INFO: User response: n
09-13-2012 17:16:45 PDT: INFO: ===== CG-NMS Setup Completed Successfully =====
```

The setupCgms.sh script lets you configure these settings:

- [Configuring Database Settings](#)

- [Configuring Database HA](#)
- [Configuring the IoT FND Database Password](#)
- [Configuring the Keystore Password](#)
- [Configuring the Web root User Password](#)
- [Configuring FTPS Settings](#)

Configuring Database Settings

To configure the database settings, the setupCgms.sh script prompts you for this information:

- IP address of the primary IoT FND database server
- Port number of the IoT FND database server
Press Enter to accept the default port number (1522).
- Database System ID (SID), which is cgms for the primary database server
Press Enter to accept the default SID (cgms). This SID identifies the server as the primary database server.

```
Do you want to change the database settings (y/n)? y
09-13-2012 17:10:05 PDT: INFO: User response: y

Enter database server IP address [example.com]: 128.107.154.246
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.246

Enter database server port [1522]:
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522

Enter database SID [cgms]:
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms
```

Configuring Database HA

To configure the standby database settings, the setupCgms.sh script prompts you for the following information:

- IP address of the standby IoT FND database server
- Port number of the standby IoT FND database server
Enter **1522**.
- Database System ID (SID), which is cgms for the primary database server
Enter **cgms_s**. This SID identifies the server as the standby database server.

```
Do you wish to configure another database server for this CG-NMS ? (y/n)? y

09-13-2012 17:11:18 PDT: INFO: User response: y
Enter database server IP address []: 128.107.154.20
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.20
Enter database server port []: 1522
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522
Enter database SID []: cgms_s
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms_s
09-13-2012 17:11:18 PDT: INFO: Configuring database settings. This may take a while. Please wait ...
09-13-2012 17:11:19 PDT: INFO: Database settings configured.
```

For information about setting up database HA, see [Setting Up IoT FND Database for HA](#).

Configuring the IoT FND Database Password

When prompted to change the IoT FND database password, enter the password of the `cgms_dba` user account on the database server. If using the default password, do not change the database password now.

```
Do you want to change the database password (y/n)? y
09-13-2012 17:15:07 PDT: INFO: User response: y

Enter database password:
Re-enter database password:

09-13-2012 17:15:31 PDT: INFO: Configuring database password. This may take a while. Please wait ...
09-13-2012 17:15:34 PDT: INFO: Database password configured.
```

Configuring the Keystore Password

To configure the keystore password:

```
Do you want to change the keystore password (y/n)? y
09-13-2012 10:21:52 PDT: INFO: User response: y

Enter keystore password: keystore_password
Re-enter keystore password: keystore_password

09-13-2012 10:21:59 PDT: INFO: Configuring keystore password. This may take a while. Please wait ...
09-13-2012 10:22:00 PDT: INFO: Keystore password configured.
```

Configuring the Web root User Password

To change the password of the root user account that lets you access the IoT FND browser-based interface, enter **y** and provide the password:

```
Do you want to change the web application 'root' user password (y/n)? n
09-13-2012 17:16:34 PDT: INFO: User response: n
```

Configuring FTPS Settings

If deploying a cluster, provide the FTPS settings required for downloading logs. FTPS securely transfers files between cluster nodes. If the FTPS settings are not configured, you can only download logs from the IoT FND node where you are currently logged in.

```
Do you want to change the FTP settings (y/n)? y
09-13-2012 17:16:45 PDT: INFO: User response: y

Enter FTP user password:
Re-enter FTP user password:

09-13-2012 17:16:49 PDT: INFO: Configuring FTP settings. This may take a while. Please wait ...
09-13-2012 17:16:57 PDT: INFO: FTP settings configuration completed successfully
```

Checking IoT FND Status

Before you can start IoT FND, check its connection to the IoT FND database by running this command:

```
# service cgms status
09-06-2012 18:51:20 PDT: INFO: CG-NMS database server: localhost
09-06-2012 18:51:21 PDT: INFO: CG-NMS database connection verified.
```

This command provides the IP address or hostname and status of the IoT FND database, and also verifies the connection to the IoT FND database. If the connection is not verified, you cannot start IoT FND.

Running the IoT FND Database Migration Script

IoT FND uses a special database migration system that lets you quickly migrate your IoT FND database without having to perform a database dump and restore. Each database migration creates or modifies some of the tables in the IoT FND database so that IoT FND can keep a record of migrations already performed.

Before launching IoT FND the first time, run the database migration script to set up the IoT FND tables in the database:

```
# cd /opt/cgms/bin
# ./db-migrate
```

Note: This script runs for a few minutes before launching IoT FND for the first time. Running this script after upgrading to a new version of IoT FND takes longer depending on the amount of data in the IoT FND database.

Note: If deploying a IoT FND server cluster, run the db-migrate script on only one cluster node.

The **db-migrate** command prompts you for the database password. The default password is **cgms123**.

Caution: Ensure that the password entered while running the db-migrate script is the correct password. If you enter an incorrect password multiple times, Oracle might lock your user account. If so, you have to unlock your account on the database server. Follow the steps below to unlock your password:

- If you enter an incorrect IoT FND Database password multiple times, Oracle locks your user account. Unlock your password using the Oracle software, as shown in this example:

```
# su - oracle
# sqlplus sys/<database_password>@cgms as sysdba
alter user cgms_dev account unlock;
exit;.
```

Accessing the IoT FND Web GUI

IoT FND has a self-signed certificate for its Web GUI. You must add a security exception in your browser to access the IoT FND GUI. Once you start IoT FND, you can access its web GUI at:

https://nms_machine_IP_address/

The initial default username is root; the password is **root123**.

IoT FND uses the default password of **root123** unless the password was changed when the setup script ran.

For more information on the setup script, see [Setting Up IoT FND](#).

Note: If the IoT FND includes the Hardware Security Module (HSM), the Firefox browser will not connect to IoT FND. To work around this issue, open Firefox Preferences, navigate to **Advanced**, and click the **Encryption** tab. Under Protocols, clear the **Use TLS 1.0** check box. Reconnect to IoT FND and ensure that the page loaded properly.

HTTPS Connections

IoT FND only accepts TLSv1.2 based HTTPS connections. To access the IoT FND GUI, you must enable the TLSv1.2 protocol to establish an HTTPS connection with the IoT FND.

Note: IoT FND Release 2.1.1-54 and later do not support TLSv1.0 or TLSv1.1 based connections.

First-Time Log In Actions

Changing the Password

When you log in to IoT FND for the first time, a popup window prompts you to change the password.

Note: IoT FND supports a maximum 32-character password length.

1. Enter your New password.
2. Re-enter the new password in the Confirm Password field.
3. Click **Change Password**.

Configuring the Time Zone

To configure the time zone, follow these steps:

1. From the *username* drop-down menu (top right), choose **Time Zone**.
2. Select a time zone.
3. Click **Update Time Zone**.
4. Click **OK**.

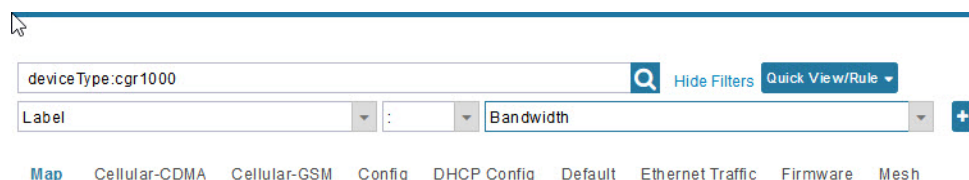
Changing the Sorting Order of Columns

For pages that display lists under a column heading (such as a list of routers) you can change the sort order (ascending or descending) by toggling the triangle icon in the column heading,

Filtering Lists

IoT FND lets you define filters on the DEVICES and OPERATIONS pages.

- To define a filter, click **Show Filters** to the right of the search field to open a filter definition panel (shown below). After you define the search parameters in the field, click the magnifying glass icon to start search. Results display beneath the filter field.



- Click **Hide Filters** to close the search field.

In the following example, typing the search string **deviceType:cgmesh status:up** in the Search Devices field lists the mesh endpoint devices with an Up status.

Setting User Preferences for User Interface

You can define what items display in the user interface by selecting the Preferences option under the *<user name>* drop-down menu (top right).

In the User Preferences panel that displays, you can select those items (listed below) that you want to display by checking the box next to that option. Click **Apply** to save.

User Preference options include:

- Show chart on events page
- Show summary counts on events/issues page
- Enable map:
 - Default to map view
- Show device type and function on device pages: Routers, Endpoints, Head End Routers, Servers

Logging Out

Click **Log Out** in the *<user name>* drop-down menu (top right).

IoT FND CLIs

This section addresses key command-line interface (CLI) commands used to manage IoT FND:

- [Starting IoT FND](#)
- [Checking IoT FND Status](#)
- [Stopping IoT FND](#)
- [IoT FND Log File Location](#)
- [IoT FND Helper Scripts](#)
- [Upgrading IoT FND](#)
- [Uninstalling IoT FND](#)

Starting IoT FND

To start IoT FND, run this command:

```
service cgms start
```

To configure IoT FND so that it runs automatically at boot time, run this command:

```
chkconfig cgms on
```

Checking IoT FND Status

To check IoT FND status, run this command:

```
service cgms status
```

Stopping IoT FND

To stop IoT FND, run this command:

```
service cgms stop
```

Note: The application typically takes approximately 10 seconds to stop. Run **ps | grep java** to verify that no Java processes are running.

IoT FND Log File Location

The IoT FND log file (server.log) is located in the /opt/cgms/server/cgms/log directory.

IoT FND Helper Scripts

[Table 8](#) describes the helper IoT FND scripts in the /opt/cgms/bin/ directory.

Table 8 IoT FND Helper Scripts

Script	Description
deinstall_cgms_watchdog.sh	Uninstalls the watchdog script.
install_cgms_watchdog.sh	Installs the watchdog script.
mcast_test.sh	Tests the communication between cluster members.
password_admin.sh	Changes or resets the user password used to access IoT FND.
print_cluster_view.sh	Prints cluster members.

Upgrading IoT FND

Note: It is not necessary to stop the database during normal upgrades. All upgrades are in-place.

Note: For virtual IoT FND installations using custom security certificates, see [Managing Custom Certificates](#) before performing this upgrade.

Caution: Run the following steps sequentially.

To upgrade the IoT FND application:

1. Obtain the new IoT FND RPM.
2. Stop IoT FND:

```
service cgms stop
```

Note: The application typically takes approximately 10 seconds to stop. Run **ps | grep java** to verify that no Java processes are running.

3. Upgrade the IoT FND RPM:

```
rpm -Uvh new_cgms_rpm_filename
```

Note: These files overwrite the files in /opt/cgms.

4. Run the database migrations to upgrade the database from the /opt/cgms directory:

```
cd /opt/cgms
bin/db-migrate
```

Note: You must run the db-migrate script after each upgrade.

5. When prompted, enter the database password. The default password is **cgms123**.

6. Start IoT FND:

```
# service cgms start
```

You can also use the RHEL (Red Hat Enterprise Linux) GUI to start the IoT FND service (**ADMIN > System Management > Server Settings > Services**). For information, see the RHEL documentation.

Uninstalling IoT FND

Note: This deletes all IoT FND local installation configuration settings and installation files (for example, the keystore with your certificates).

Tip: If you plan to reinstall IoT FND, copy your current keystore and certificate files to use to overwrite the keystore and certificate files included with the install package.

To remove the IoT FND application, run these commands:

```
# rpm -e cgms
# rm -rf /opt/cgms
```

Cleaning up the IoT FND Database

To clean up the IoT FND database:

1. (HA database configurations) Stop the Observer server.
2. (HA database configurations) Run the `$ORACLE_BASE/cgms/scripts/ha/deleteStandbyDb.sh` script to delete the standby database.
3. (HA database configurations) Run the `$ORACLE_BASE/cgms/scripts/ha/deletePrimaryDbHa.sh` script to delete the HA configuration from primary database.
4. Run the `$ORACLE_BASE/cgms/scripts/deleteCgmsDb.sh` script to delete primary database.

Installing and Configuring the IoT FND TPS Proxy

The first use of the optional TPS proxy is typically when a CGR sends an inbound request to initialize the portion of Zero Touch Deployment (ZTD) handled by IoT FND. IoT FND operates behind a firewall and does not have a publicly reachable IP address. When field area routers (CGRs) contact IoT FND for the first time, IoT FND requires that they use the TPS proxy. This server lets these routers contact the IoT FND application server to request tunnel provisioning (see [Managing Tunnel Provisioning](#)).

The TPS proxy does not have its own GUI. You must edit the properties in the **cgms.properties** and **tpsproxy.properties-template** files for HTTPS outbound tunnel provisioning requests so that IoT FND recognizes them as requests from the TPS proxy.

After provisioning the tunnel(s), the field area routers can contact IoT FND directly without using the TPS proxy. IoT FND is notified of the exact certificate subject from the proxy certificate, and then authenticates that the HTTPS inbound requests are coming from the TPS proxy.

Setting Up the TPS Proxy

Install the `cgms-tpsproxy` RPM package Java application on a separate (TPS proxy) server to act as a stateless extension of IoT FND outside the firewall. The TPS proxy can be a Red Hat Enterprise Linux (RHEL) server (see TPS proxy system requirements in [Table 1](#)). The `cgms-tpsproxy` application runs as a daemon on the server and requires the following configuration parameters:

- URL of the IoT FND server (to forward inbound requests).
- IP address of the IoT FND server, as part of a whitelist (approved list) for forwarding outbound requests.

Before you install the TPS proxy, obtain the TPS proxy installation package:

```
cgms-tpsproxy-version_number.x86_64.rpm
```

To configure the proxy-server settings:

1. Configure a RHEL server to use as the TPS proxy.
2. Connect this RHEL server so that it can be reached while outside the firewall.
3. Configure the TPS proxy using the template file:

```
ssh root@tps_proxy_server
cd /opt/cgms-tpsproxy/conf
cp tpsproxy.properties-template tpsproxy.properties
```

Note: Edit the `cgms.properties` and `tpsproxy.properties` files after running the `encryption_util.sh` script during [IoT FND TPS Proxy Enrollment](#).

4. Edit the `tpsproxy.properties` file to add the following lines defining the inbound and outbound addresses for the IoT FND application server:

```
[root@cgr-centos57 conf]# cat tpsproxy.properties-template
inbound-proxy-destination=https://nms_domain_name:9120
outbound-proxy-allowed-addresses=nms_ip_address
cgms-keystore-password-hidden=<obfuscated password>
```

Note: You must edit the properties in the `cgms.properties` and `tpsproxy.properties-template` files for HTTPS outbound tunnel provisioning requests so that IoT FND recognizes them as requests from the TPS proxy.

Configuring the TPS Proxy Firewall

To configure the TPS proxy firewall:

- Set up a firewall rule to allow HTTPS connections from the TPS proxy to the IoT FND server on port 9120 (for HTTPS inbound requests).
- Set up a firewall rule to allow HTTPS connections from the IoT FND server to the TPS proxy on port 9122 (for HTTPS outbound requests).

IoT FND TPS Proxy Enrollment

The enrollment process for the TPS proxy is the same as the IoT FND enrollment process. The certification authority (CA) that signs the certificate of the IoT FND application server must also sign the certificate of the TPS proxy. The certificate of the TPS proxy is stored in a Java keystore and is similar to the IoT FND certificate.

For the enrollment process, consider these scenarios:

- Fresh installation
 - If the keystore password is the same as the default password, change the default password.

Note: We **strongly recommend** that you change all default passwords. Do not use special characters such as, @, #, !, or + as the `encryption_util.sh` script cannot encrypt special characters.

- If the keystore password is different from default password, run the `encryption_util.sh` script and copy the encrypted password to the properties file.

Note: Edit the `cgms.properties` and `tpsproxy.properties` files after running the `encryption_util.sh` script.

- Upgrade

Regardless of whether you are using the default password or a custom one, the upgrade process encrypts the password in the `/opt/cgms-tpsproxy/conf/tpsproxy.properties` file.

For information on IoT FND enrollment, see: [Generating and Exporting Certificates](#).

To enroll the terminal TPS proxy:

1. Create a `cgms_keystore` file.
2. Add your certifications to this file.
3. Copy the file to the `/opt/cgms-tpsproxy/conf` directory.

Configuring IoT FND to Use the TPS Proxy

You must edit the properties in the `cgms.properties` and `tpsproxy.properties-template` files for HTTPS outbound tunnel provisioning requests so that IoT FND recognizes them as requests from the TPS proxy. The TPS proxy logs all inbound and outbound requests.

Note: If the properties in the `cgms.properties` and `tpsproxy.properties-template` files are not set, IoT FND does not recognize the TPS proxy, drops the forwarded request, and considers it from an unknown device.

Note: The following examples employ variable not mandatory values, and are provided as examples only.

To configure IoT FND to use the TPS proxy:

1. Open an SSH connection to the IoT FND server:

```
ssh root@nms_machine
cd /opt/cgms/server/cgms/conf/
```

Note: Edit the `cgms.properties` and `tpsproxy.properties` files after running the `encryption_util.sh` script during [IoT FND TPS Proxy Enrollment](#).

2. Edit the `cgms.properties` file to add lines identifying the TPS proxy IP address, domain name, and user subjects in the `cgdm-tpsproxy-subject` property:

Note: The `cgdm-tpsproxy-subject` property must match the installed TPS proxy certificate.

```
cgdm-tpsproxy-addr=proxy_server_IP_address
cgdm-tpsproxy-subject=CN="common_name", OU="organizational_unit", O="organization", L="location",
ST="state", C="country"
```

Note: Use quotes around comma-separated strings.

Starting the IoT FND TPS Proxy

Start the TPS proxy after it is installed, configured, and enrolled.

To start the TPS proxy, run the start script:

```
service tpsproxy start
```

The TPS proxy log file is located at:

```
/opt/cgms-tpsproxy/log/tpsproxy.log
```

Note: For information, see [TPS Proxy Validation](#).

TPS Proxy Validation

The TPS proxy logs all HTTPS inbound and outbound requests in the TPS proxy log file located at `/opt/cgms-tpsproxy/log/tpsproxy.log`

The following entry in the TPS proxy `tpsproxy.log` file defines inbound requests for a CGR:

```
73: cgr-centos57: May 21 2014 01:05:20.513 -0700: %CGMS-6-UNSPECIFIED:
%[ch=TpsProxyServlet-49dc423f][eid=CGR1240/K9+JAF1732ARCJ][ip=192.168.201.5][sev=INFO][tid=qtp46675819-29]: Inbound proxy request from [192.168.201.5] with client certificate subject
[CN=CGRJAF1732ARCJ.example.com, SERIALNUMBER=PID:CGR1240/K9 SN:JAF1732ARCJ]
```

This message entry in the TPS proxy `tpsproxy.log` file indicates that the TPS successfully forwarded the message to IoT FND:

```
74: cgr-centos57: May 21 2014 01:05:20.564 -0700: %CGMS-6-UNSPECIFIED:
%[ch=TpsProxyServlet-49dc423f][sev=INFO][tid=com.cisco.cgms.tpsproxy.TpsProxyServlet-49dc423f-22]:
Completed inbound proxy request from [192.168.201.5] with client certificate subject
[CN=CGRJAF1732ARCJ.example.com, SERIALNUMBER=PID:CGR1240/K9 SN:JAF1732ARCJ]
```

The following entry in the IoT FND server log file identifies the TPS proxy:

```
Request came from proxy
Using forwarded client subject (CN=cg-cgr-1, SERIALNUMBER=PID:CGR1240/K9 SN:JSJ15220047) for
authentication
```

The following entry in the TPS proxy `tpsproxy.log` file defines outbound requests:

```
%CGMS-6-UNSPECIFIED: %[ch=TpsProxyOutboundHandler][ip=192.168.205.5][sev=INFO][tid=qtp257798932-15]:
Outbound proxy request from [192.168.205.5] to [192.168.201.5:8443]
```

The following entry in the IoT FND server log file identifies the HTTPS connection:

```
Using proxy at 192.168.201.6:9122 to send to https://192.168.201.4:8443/cgdm/mgmt commands:
```

Configuring IoT FND for Dual-PHY

For Dual-PHY CGRs, you must configure all Dual-PHY WPAN modules—master and slaves—by setting the Dual-PHY WPAN Properties (see Table 13) in the *Managing Devices* chapter of the [IoT FND 4.0 User Guide](#). The parameters to set in the appropriate device addition file are **masterWpanInterface** and **slaveWpanInterface**. For slave Dual-PHY WPAN devices, you must also set the **slave-mode** parameter.

Note: See the [Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide \(Cisco IOS\)](#) for Dual-PHY CGR configuration information.

EXAMPLE

The following instructs IoT FND which WPAN devices to allocate as the master interface and slave interface during the configuration push:

```
deviceType,eid,ip,meshPrefixConfig,meshPrefixLengthConfig,meshPanidConfig,meshAddressConfig,
dhcpV4LoopbackLink,dhcpV4TunnelLink,dhcpV6LoopbackLink,dhcpV6TunnelLink,tunnelSrcInterfacel,
tunnelHerEid,adminUsername,adminPassword,certIssuerCommonName,ipsecTunnelDestAddr1,
masterWpanInterface,slaveWpanInterface,lat,lng
cgr1000,CGR1240/K9+JAF1741BFQS,2.2.56.253,2319:EXTRA:BEEF:CAFE::,64,1233,
2319:EXTRA:BEEF:CAFE::,20.211.0.1,20.211.0.1,2001:420:7bf:7e8::1,
2001:420:7bf:7e8::1,GigabitEthernet2/1,cg-isr900,cg-nms-administrator,
0ERIF+cKsLwyT0YTFd0k+NpVAAPxcIvFfoX1sogAXVksOAczUFT8TG0U58ccJuhds52KXL4dtu5iljZsQNH+
pEQ1aIQvIGuIas9wp9MKUARYpNERXriHEnpeH044Rfa4uSgsWXEyrVnXHyuvSefB5j6H0uA7tIQwEHDxOiq
/d0yxvfd4IYos7NzPX1JNiR+Cp6bwx7dG+d9Jo+JuNXLXpi8Fo5n88usjMoXPNbyrqvgn7SS4f+VYgXxliyDNP0k
+70EE8uSTVeUJXe7UXkndz5CaU17yk94UxOxamv2i1KEQxTFgw/UvrkCwPQoDMijPstDBXpFv8dqtA0xDGKuaRg
==,cenbursaca-cenbu-sub-ca,2.2.55.198,Wpan3/1,Wpan5/1,41.413324,-120.920315
```

The following is a typical template for configuring the master/slave interface on CGR WPAN modules:

```
interface ${device.masterWpanInterface}
  no shut
  ipv6 address ${device.meshAddressConfig}/${device.meshPrefixLengthConfig}
  ieee154 panid ${device.meshPanidConfig}
  outage-server ${device.relayDest}
exit

interface ${device.slaveWpanInterface}
  no ip address
  ip broadcast-address 0.0.0.0
  no ip route-cache
  ieee154 beacon-async min-interval 10 max-interval 10 suppression-coefficient 0
  ieee154 ssid cisco_muruga_dual
  ieee154 txpower 21
  slave-mode 3
  rpl dag-lifetime 240
  rpl dio-min 21
  rpl version-incr-time 240
  authentication host-mode multi-auth
  authentication port-control auto
  ipv6 dhcp relay destination global 2001:420:7BF:5F::705
  dot1x pae authenticator
  ieee154 panid ${device.meshPanidConfig}
exit
end
```

Mesh Security Keys for Dual-PHY Devices

Note: Do not configure mesh security keys on slave WPAN devices.

With master/slave mode configured correctly in IoT FND, IoT FND automatically detects the master WPAN and sets its the mesh security keys. When configuring an existing CGR and adding another WPAN interface, remove all mesh security keys from both interfaces, and then configure master/slave mode through IoT FND. If CGRs are connected, all meters go through re-authentication.

You can remove mesh keys using the command:

```
mesh-security expire mesh-key interface wpan <slot>/<slot number>
```

Configuration Example

The following examples retrieve the current Dual-PHY WPAN device RPL slot tree, RPL slot table, RPL IP route info table, and configuration information for slots 4/1 and 3/1.

```
cisco-NXT-FAR5#show wpan 4/1 rpl stree
```

```
----- WPAN RPL SLOT TREE [4] -----
[2001:RTE:RTE:64::4]
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1800 // SY RF nodes
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1801
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A00
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1802
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1803
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1804
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1805
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A03
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A07
```

```

\--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1806
\--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1807
\--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1808
\--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1809
\--(RF )-- 2001:RTE:RTE:64:207:8108:3C:180A
\--(RF )-- 2001:RTE:RTE:64:207:8108:3C:180B
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A01
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C05
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C06
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C07
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A02
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A04
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A05
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C03
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C08
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C09
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C0A
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A06
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C02
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C04
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A08
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A09
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A0A
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C00
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C01
    \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C0B
  \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A0B
\--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E00 // CY PLC nodes
\--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E01
\--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E02
\--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E03
\--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E04
\--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E05
\--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E06
\--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E07

```

RPL SLOT TREE: Num.DataEntries 44, Num.GraphNodes 45 (external 0) (RF 36) (PLC 8)

```

cisco-NXT-FAR5#ping 2001:RTE:RTE:64:217:3BCD:26:4E01
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:RTE:RTE:64:217:3BCD:26:4E01, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 254/266/294 ms

```

```

cisco-NXT-FAR5#ping 2001:RTE:RTE:64:207:8108:3C:1C00
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:RTE:RTE:64:207:8108:3C:1C00, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 272/441/636 ms
cisco-NXT-FAR5#

```

cisco-NXT-FAR5#show wpan 4/1 rpl stable

```

----- WPAN RPL ROUTE SLOT TABLE [4] -----
NODE_IPADDR          NEXTHOP_IP          SSLOT LAST_HEARD
2001:RTE:RTE:64:207:8108:3C:1800      2001:RTE:RTE:64::4      3      17:49:12
// SY RF nodes
2001:RTE:RTE:64:207:8108:3C:1801      2001:RTE:RTE:64::4      3      18:14:05
2001:RTE:RTE:64:207:8108:3C:1802      2001:RTE:RTE:64::4      3      18:14:37
2001:RTE:RTE:64:207:8108:3C:1803      2001:RTE:RTE:64::4      3      17:56:56
2001:RTE:RTE:64:207:8108:3C:1804      2001:RTE:RTE:64::4      3      17:48:53
2001:RTE:RTE:64:207:8108:3C:1805      2001:RTE:RTE:64::4      3      17:47:52
2001:RTE:RTE:64:207:8108:3C:1806      2001:RTE:RTE:64::4      3      17:49:54
2001:RTE:RTE:64:207:8108:3C:1807      2001:RTE:RTE:64::4      3      17:46:38

```



```

2001:RTE:RTE:64:207:8108:3C:1808      2001:RTE:RTE:64:::4      3      18:22:01
2001:RTE:RTE:64:207:8108:3C:1809      2001:RTE:RTE:64:::4      3      17:50:02
2001:RTE:RTE:64:207:8108:3C:180A      2001:RTE:RTE:64:::4      3      17:50:02
2001:RTE:RTE:64:207:8108:3C:180B      2001:RTE:RTE:64:::4      3      18:24:00
2001:RTE:RTE:64:207:8108:3C:1A00      2001:RTE:RTE:64:207:8108:3C:1801      3      17:56:34
2001:RTE:RTE:64:207:8108:3C:1A01      2001:RTE:RTE:64:207:8108:3C:180B      3      18:27:34
2001:RTE:RTE:64:207:8108:3C:1A02      2001:RTE:RTE:64:207:8108:3C:180B      3      18:03:06
2001:RTE:RTE:64:207:8108:3C:1A03      2001:RTE:RTE:64:207:8108:3C:1805      3      18:25:18
2001:RTE:RTE:64:207:8108:3C:1A04      2001:RTE:RTE:64:207:8108:3C:180B      3      17:57:15
2001:RTE:RTE:64:207:8108:3C:1A05      2001:RTE:RTE:64:207:8108:3C:180B      3      18:23:39
2001:RTE:RTE:64:207:8108:3C:1A06      2001:RTE:RTE:64:207:8108:3C:180B      3      18:04:16
2001:RTE:RTE:64:207:8108:3C:1A07      2001:RTE:RTE:64:207:8108:3C:1805      3      17:55:00
2001:RTE:RTE:64:207:8108:3C:1A08      2001:RTE:RTE:64:207:8108:3C:180B      3      18:19:35
2001:RTE:RTE:64:207:8108:3C:1A09      2001:RTE:RTE:64:207:8108:3C:180B      3      18:02:02
2001:RTE:RTE:64:207:8108:3C:1A0A      2001:RTE:RTE:64:207:8108:3C:180B      3      18:18:00
2001:RTE:RTE:64:207:8108:3C:1A0B      2001:RTE:RTE:64:207:8108:3C:180B      3      18:02:46
2001:RTE:RTE:64:207:8108:3C:1C00      2001:RTE:RTE:64:207:8108:3C:1A0A      3      18:22:03
2001:RTE:RTE:64:207:8108:3C:1C01      2001:RTE:RTE:64:207:8108:3C:1A0A      3      18:24:03
2001:RTE:RTE:64:207:8108:3C:1C02      2001:RTE:RTE:64:207:8108:3C:1A06      3      18:25:03
2001:RTE:RTE:64:207:8108:3C:1C03      2001:RTE:RTE:64:207:8108:3C:1A05      3      18:15:05
2001:RTE:RTE:64:207:8108:3C:1C04      2001:RTE:RTE:64:207:8108:3C:1A06      3      18:24:05
2001:RTE:RTE:64:207:8108:3C:1C05      2001:RTE:RTE:64:207:8108:3C:1A01      3      18:10:02
2001:RTE:RTE:64:207:8108:3C:1C06      2001:RTE:RTE:64:207:8108:3C:1A01      3      18:05:03
2001:RTE:RTE:64:207:8108:3C:1C07      2001:RTE:RTE:64:207:8108:3C:1A01      3      18:11:03
2001:RTE:RTE:64:207:8108:3C:1C08      2001:RTE:RTE:64:207:8108:3C:1A05      3      18:15:05
2001:RTE:RTE:64:207:8108:3C:1C09      2001:RTE:RTE:64:207:8108:3C:1A05      3      18:15:04
2001:RTE:RTE:64:207:8108:3C:1C0A      2001:RTE:RTE:64:207:8108:3C:1A05      3      18:15:04
2001:RTE:RTE:64:207:8108:3C:1C0B      2001:RTE:RTE:64:207:8108:3C:1A0A      3      18:24:03
2001:RTE:RTE:64:217:3BCD:26:4E00      2001:RTE:RTE:64:::4      4      18:21:40

// CY PLC nodes
2001:RTE:RTE:64:217:3BCD:26:4E01      2001:RTE:RTE:64:::4      4      17:47:23
2001:RTE:RTE:64:217:3BCD:26:4E02      2001:RTE:RTE:64:::4      4      18:20:16
2001:RTE:RTE:64:217:3BCD:26:4E03      2001:RTE:RTE:64:::4      4      17:49:07
2001:RTE:RTE:64:217:3BCD:26:4E04      2001:RTE:RTE:64:::4      4      18:21:49
2001:RTE:RTE:64:217:3BCD:26:4E05      2001:RTE:RTE:64:::4      4      18:22:06
2001:RTE:RTE:64:217:3BCD:26:4E06      2001:RTE:RTE:64:::4      4      18:22:51
2001:RTE:RTE:64:217:3BCD:26:4E07      2001:RTE:RTE:64:::4      4      18:24:04

```

Number of Entries in WPAN RPL ROUTE SLOT TABLE: 44 (external 0)

cisco-NXT-FAR5#show wpan 4/1 rpl itable

```

----- WPAN RPL IPROUTE INFO TABLE [4] -----
NODE_IPADDR      RANK  VERSION  NEXTHOP_IP      ETX_P  ETX_LRSSIR  RSSIF  HOPS  PARENTS  SSSLOT
2001:RTE:RTE:64:207:8108:3C:1800      835   1      2001:RTE:RTE:64:::4      0      0      762   -67   -71   1   1   3
// SY RF nodes
2001:RTE:RTE:64:207:8108:3C:1801      692   2      2001:RTE:RTE:64:::4      0      547   -68   -67   1   1   3
2001:RTE:RTE:64:207:8108:3C:1802      776   2      2001:RTE:RTE:64:::4      0      711   -82   -83   1   1   3
2001:RTE:RTE:64:207:8108:3C:1803      968   2      2001:RTE:RTE:64:::4      0      968   -72   -63   1   1   3
2001:RTE:RTE:64:207:8108:3C:1804      699   1      2001:RTE:RTE:64:::4      0      643   -71   -66   1   1   3
2001:RTE:RTE:64:207:8108:3C:1805      681   1      2001:RTE:RTE:64:::4      0      627   -70   -64   1   1   3
2001:RTE:RTE:64:207:8108:3C:1806      744   1      2001:RTE:RTE:64:::4      0      683   -69   -68   1   1   3
2001:RTE:RTE:64:207:8108:3C:1807      705   1      2001:RTE:RTE:64:::4      0      648   -76   -63   1   1   3
2001:RTE:RTE:64:207:8108:3C:1808      811   2      2001:RTE:RTE:64:::4      0      811   -68   -69   1   2   3
2001:RTE:RTE:64:207:8108:3C:1809      730   1      2001:RTE:RTE:64:::4      0      692   -68   -70   1   1   3
2001:RTE:RTE:64:207:8108:3C:180A      926   1      2001:RTE:RTE:64:::4      0      926   -66   -68   1   1   3
2001:RTE:RTE:64:207:8108:3C:180B      602   2      2001:RTE:RTE:64:::4      0      314   -74   -69   1   1   3
2001:RTE:RTE:64:207:8108:3C:1A00      948   1      2001:RTE:RTE:64:207:8108:3C:1801      692   256   -73   -75   2   1   3
2001:RTE:RTE:64:207:8108:3C:1A01      646   2      2001:RTE:RTE:64:207:8108:3C:180B      323   256   -73   -75   2   3   3
2001:RTE:RTE:64:207:8108:3C:1A02      948   1      2001:RTE:RTE:64:207:8108:3C:180B      602   256   -73   -75   2   2   3
2001:RTE:RTE:64:207:8108:3C:1A03      803   2      2001:RTE:RTE:64:207:8108:3C:1805      503   256   -68   -78   2   3   3
2001:RTE:RTE:64:207:8108:3C:1A04      858   1      2001:RTE:RTE:64:207:8108:3C:180B      602   256   -65   -69   2   1   3
2001:RTE:RTE:64:207:8108:3C:1A05      646   2      2001:RTE:RTE:64:207:8108:3C:180B      323   256   -71   -69   2   2   3
2001:RTE:RTE:64:207:8108:3C:1A06      858   1      2001:RTE:RTE:64:207:8108:3C:180B      602   256   -73   -75   2   2   3
2001:RTE:RTE:64:207:8108:3C:1A07      979   1      2001:RTE:RTE:64:207:8108:3C:1805      627   352   -71   -73   2   1   3
2001:RTE:RTE:64:207:8108:3C:1A08      646   2      2001:RTE:RTE:64:207:8108:3C:180B      390   256   -75   -70   2   3   3
2001:RTE:RTE:64:207:8108:3C:1A09      948   1      2001:RTE:RTE:64:207:8108:3C:180B      602   256   -70   -69   2   3   3
2001:RTE:RTE:64:207:8108:3C:1A0A      646   2      2001:RTE:RTE:64:207:8108:3C:180B      390   256   -75   -71   2   2   3
2001:RTE:RTE:64:207:8108:3C:1A0B      858   1      2001:RTE:RTE:64:207:8108:3C:180B      602   256   -68   -68   2   2   3
2001:RTE:RTE:64:207:8108:3C:1C00      902   2      2001:RTE:RTE:64:207:8108:3C:1A0A      646   256   -70   -74   3   1   3

```

```

2001:RTE:RTE:64:207:8108:3C:1C01      902  2    2001:RTE:RTE:64:207:8108:3C:1A0A      646  256  -71  -72  3    1    3
2001:RTE:RTE:64:207:8108:3C:1C02      1114  1    2001:RTE:RTE:64:207:8108:3C:1A06      858  256  -74  -73  3    1    3
2001:RTE:RTE:64:207:8108:3C:1C03      1114  1    2001:RTE:RTE:64:207:8108:3C:1A05      858  256  -76  -77  3    1    3
2001:RTE:RTE:64:207:8108:3C:1C04      902  2    2001:RTE:RTE:64:207:8108:3C:1A06      646  256  -75  -68  3    2    3
2001:RTE:RTE:64:207:8108:3C:1C05      1114  1    2001:RTE:RTE:64:207:8108:3C:1A01      858  256  -66  -74  3    1    3
2001:RTE:RTE:64:207:8108:3C:1C06      1114  1    2001:RTE:RTE:64:207:8108:3C:1A01      858  256  -74  -72  3    1    3
2001:RTE:RTE:64:207:8108:3C:1C07      1114  1    2001:RTE:RTE:64:207:8108:3C:1A01      858  256  -70  -75  3    1    3
2001:RTE:RTE:64:207:8108:3C:1C08      1114  1    2001:RTE:RTE:64:207:8108:3C:1A05      858  256  -74  -70  3    1    3
2001:RTE:RTE:64:207:8108:3C:1C09      1114  1    2001:RTE:RTE:64:207:8108:3C:1A05      858  256  -70  -74  3    1    3
2001:RTE:RTE:64:207:8108:3C:1C0A      1114  1    2001:RTE:RTE:64:207:8108:3C:1A05      858  256  -70  -69  3    1    3
2001:RTE:RTE:64:207:8108:3C:1C0B      902  2    2001:RTE:RTE:64:207:8108:3C:1A0A      646  256  -76  -74  3    1    3
2001:RTE:RTE:64:217:3BCD:26:4E00      616  2    2001:RTE:RTE:64::4                      0    616  118  118  1    1    4 // CY PLC
nodes
2001:RTE:RTE:64:217:3BCD:26:4E01      702  1    2001:RTE:RTE:64::4                      0    646  118  118  1    1    4
2001:RTE:RTE:64:217:3BCD:26:4E02      557  2    2001:RTE:RTE:64::4                      0    557  118  118  1    1    4
2001:RTE:RTE:64:217:3BCD:26:4E03      626  1    2001:RTE:RTE:64::4                      0    579  118  118  1    1    4
2001:RTE:RTE:64:217:3BCD:26:4E04      609  2    2001:RTE:RTE:64::4                      0    609  118  118  1    1    4
2001:RTE:RTE:64:217:3BCD:26:4E05      602  2    2001:RTE:RTE:64::4                      0    602  118  118  1    1    4
2001:RTE:RTE:64:217:3BCD:26:4E06      594  2    2001:RTE:RTE:64::4                      0    594  118  118  1    1    4
2001:RTE:RTE:64:217:3BCD:26:4E07      584  2    2001:RTE:RTE:64::4                      0    584  118  118  1    1    4

```

Number of Entries in WPAN RPL IPRROUTE INFO TABLE: 44

```
cisco-NXT-FAR5#
```

```
cisco-NXT-FAR5#show run int wpan 4/1
```

```
Building configuration...
```

```
Current configuration : 320 bytes
```

```
!
```

```
interface Wpan4/1
```

```
no ip address
```

```
ip broadcast-address 0.0.0.0
```

```
no ip route-cache
```

```
ieee154 beacon-async min-interval 100 max-interval 600 suppression-coefficient 1
```

```
ieee154 panid 5552
```

```
ieee154 ssid ios_far5_plc
```

```
ipv6 address 2001:RTE:RTE:64::4/64
```

```
ipv6 enable
```

```
ipv6 dhcp relay destination 2001:420:7BF:5F::500
```

```
end
```

```
cisco-NXT-FAR5#show run int wpan 3/1
```

```
Building configuration...
```

```
Current configuration : 333 bytes
```

```
!
```

```
interface Wpan3/1
```

```
no ip address
```

```
ip broadcast-address 0.0.0.0
```

```
no ip route-cache
```

```
ieee154 beacon-async min-interval 120 max-interval 600 suppression-coefficient 1
```

```
ieee154 panid 5551
```

```
ieee154 ssid ios_far5_rf
```

```
slave-mode 4
```

```
ipv6 address 2001:RTE:RTE:65::5/64
```

```
ipv6 enable
```

```
ipv6 dhcp relay destination 2001:420:7BF:5F::500
```

```
end
```

Backing Up and Restoring the IoT FND Database

The following topics demonstrate how IoT FND supports both full and incremental database backups:

- [Before You Begin](#)
- [Creating a Full Backup of the IoT FND Database](#)
- [Scheduling a Full IoT FND Backup](#)
- [Restoring a IoT FND Backup](#)

Before You Begin

Before backing up your IoT FND database:

1. Download and install the latest `cgms-oracle-version_number.x86_64.rpm` package.
2. Copy the scripts, templates, and tools folders from the `/opt/cgms-oracle` folder to the `$ORACLE_BASE/cgms` folder.
3. Set the ownership of the files and folders you copied to `oracle:dba`.

Creating a Full Backup of the IoT FND Database

Full backups back up all the blocks from the data file. Full backups are time consuming and consume more disk space and system resources than partial backups.

IoT FND lets you perform full hot backups of IoT FND database. In a hot backup, IoT FND and the IoT FND database are running during the backup.

Note: The destination backup directory must be writable by the oracle user and have enough space for the IoT FND data.

To create a backup file of the IoT FND software:

1. On the IoT FND database server, open a CLI window.
2. Switch to the user `oracle`:

```
su - oracle
```

3. Change directory to the location of the IoT FND backup script (`backupCgmsDb.sh`):

```
cd /home/oracle/app/oracle/cgms/scripts
```

4. Run the backup script and specify the destination folder. For example, to store the backup data in the `/home/oracle/bkp` folder, enter this command:

```
./backupCgmsDb.sh full /home/oracle/bkp
08-03-2012 15:54:10 PST: INFO: ===== CGMS Database Backup Started =====
08-03-2012 15:54:10 PST: INFO: Log file: /tmp/cgms_backup_restore.log
Are you sure you want to backup CG-NMS database (y/n)? y
```

5. Enter `y` to begin the backup process.

Scheduling a Full IoT FND Backup

To schedule a full IoT FND backup to run daily at 1:00 AM (default setting):

Note: The destination backup directory must be writable by the oracle user and have enough space for the IoT FND data.

1. On the IoT FND database server, open a CLI window.
2. Switch to the user `oracle`:

```
su - oracle
```

3. Change directory to the location of the IoT FND backup script (`backupCgmsDb.sh`):

```
cd /home/oracle/app/oracle/cgms/scripts
```

4. Run the backup script and specify the destination folder.

To change the backup scheduling interval, edit the `installCgmsBackupJob.sh` script before running it. For example, to store the backup data in `/home/oracle/bkp`, enter this command:

```
./installCgmsBackupJob.sh /home/oracle/bkp
```

To delete the backup job, enter these commands:

```
cd /home/oracle/app/oracle/cgms/scripts
./deinstallCgmsBackupJob.sh
```

Backing Up the IoT FND Database Incrementally

Incremental backups only back up data file blocks that changed since the previous specified backup. IoT FND supports two incremental backup levels, and an hourly log backup:

- **incr0**—Base backup for subsequent incremental backups. This is similar to a full backup. For large deployments (millions of mesh endpoints and several thousand routers such as CGR1000 and IR800). Run `incr0` backups twice a week.
- **incr1**—Differential backup of all blocks changed since the last incremental backup. For large deployments (millions of mesh endpoints and several thousand routers), run `incr1` backups once a day.

Note: An `incr0` backup must run before an `incr1` backup to establish a base for the `incr1` differential backup.

- **Hourly archivelog backup**—The Oracle Database uses archived logs to record all changes made to the database. These files grow over time and can consume a large amount of disk space. Schedule the `backup_archive_log.sh` script to run every hour. This script backs up the database archive (`.arc`) log files, stores them on a different server, and deletes the source archivelog files to free space on the database server.

Tip: Before performing any significant operation that causes many changes in the IoT FND database (for example, importing a million mesh endpoints or uploading firmware images to mesh endpoints), perform an `incr0` backup. After the operation completes, perform another `incr0` backup, and then resume the scheduled incremental backups.

Performing an Incremental Backup

Note: The destination backup directory must be writable by the `oracle` user and have enough space for the IoT FND data.

To perform an incremental backup:

1. On the IoT FND database server, open a CLI window.
2. Switch to the user `oracle` and change directory to the location of the IoT FND backup script:

```
su - oracle
cd /home/oracle/app/oracle/cgms/scripts
```

3. Run the backup script and specify the incremental backup level and the destination folder where the backup data is stored (for example, `/home/oracle/bkp`). For example, to perform an `incr0` backup to `/home/oracle/bkp`, enter the command:

```
./backupCgmsDb.sh incr0 /home/oracle/bkp
```

To perform an `incr1` backup, enter the command:

```
./backupCgmsDb.sh incr1 /home/oracle/bkp
```

Restoring a IoT FND Backup

Perform database backups and restores using the scripts provided in the `cgms-oracle.rpm` package. If using the supplied scripts, backups and restores only work if performed on the same Oracle database version.

Note: Backups from Oracle version 11.2.0.1 can only be restored on v11.2.0.1 if using the supplied scripts. Backups do not work across different versions of Oracle, for example, a backup taken on 11.2.0.1 cannot be restored on 11.2.0.3 using the supplied scripts. If a database upgrade from 11.2.0.1 to 11.2.0.3 is required, follow the Oracle upgrade procedure. Refer to the Oracle upgrade document and Web site.

IoT FND supports restoring IoT FND backups on the same host or different host. If you choose to restore IoT FND backups on a different host, ensure that the host runs the same or a higher version of the Oracle database software and that IoT FND database on the destination host was created using the `setupCgmsDb.sh` script.

Note: IoT FND does not support cross-platform backups.

To restore a IoT FND backup:

1. Stop IoT FND.

```
service cgms stop
```

2. Switch to the user oracle, change directories to the script location, and stop Oracle:

```
su -oracle
cd /home/oracle/app/oracle/cgms/scripts
./stopOracle.sh
```

3. To restore the IoT FND database, run the command:

```
./restoreCgmsDb.sh full-backup-file
```

Tip: Performing a restore from a full backup can be time consuming. For large deployments, we recommend restoring the database from incremental backups.

To restore IoT FND database from an incremental backup, run these commands and specify the path to last incremental backup file:

```
su -oracle
cd /home/oracle/app/oracle/cgms/scripts
./restoreCgmsDb.sh last-incrl-backup-file
```

The restore script might display these errors:

```
06-08-2012 13:12:56 PDT: INFO: Import completed successfully
06-08-2012 13:12:56 PDT: INFO: Shared memory file system. Required (1K-blocks): 6084456,
Available (1K-blocks): 4083180
06-08-2012 13:12:56 PDT: ERROR: Insufficient shared memory file system. Increase your
shared memory file system before restoring this database.
06-08-2012 13:12:56 PDT: ERROR: ===== CGMS Database Restore Failed =====
06-08-2012 13:12:56 PDT: ERROR: Check log file for more information.
```

To avoid these errors, increase the size of the shared memory file system:

```
##### as "root" user
##### Following command allocates 6G to shm. Adjust size as needed.
# umount tmpfs
# mount -t tmpfs tmpfs -o size=6G /dev/shm

##### Edit /etc/fstab and replace defaults as shown below
tmpfs /dev/shm tmpfs size=6G 0 0
```

4. Start Oracle:

```
./startOracle.sh
```

5. Change directories to `/opt/cgms` and run the `db-migrate` script:

```
$ cd /opt/cgms
```

```
$ bin/db-migrate
```

When you restore a IoT FND database, the restore script restores the database to the IoT FND version the database was using. An error returns if you restore an old database to a newer version of IoT FND. Run the migrate script to ensure that the database runs with the current version of IoT FND.

6. Start IoT FND:

```
service cgms start
```

For disaster recovery, perform a clean restore. The script starts by deleting the current IoT FND database:

```
$ su -oracle
$ cd /home/oracle/app/oracle/cgms/scripts
$ ./deleteCgmsDb.sh
INFO: ===== CGMS Database Deletion Started - 2011-10-16-07-24-09 =====
INFO: Log file: /tmp/cgmsdb_setup.log
INFO: Deleting database. This may take a while. Please be patient ...
INFO: Delete database completed successfully
INFO: ===== CGMS Database Deletion Completed Successfully - 2011-10-16-07-25-01 =====
```

If a clean restore is not required, use the Oracle tool to restore the database.

Deploying IoT FND/Oracle/TPS Virtual Machines on ESXi 5.x or ESXi 6.x

You use the VMware vSphere client to import OVA files into ESXi 5.x or ESXi 6.x.

BEFORE YOU BEGIN

- Install the VMware vSphere Client for the ESXi 5.x or ESXi 6.x server.
- Locate the VMware ESXi 5.x or ESXi 6.x credentials to create virtual machines in ESXi 5.x or ESXi 6.x, respectively.
- Ensure that you meet the VMware server machine requirements.

These are the VM CPU and memory requirements for a small scale deployment:

NMS OVA

- 16 GB Memory
- 1 core and 4 virtual sockets
- 150 GB of virtual storage

Oracle OVA

- 24 GB of Memory
- 2 virtual sockets with 2 cores per socket
- 300 GB of virtual Storage

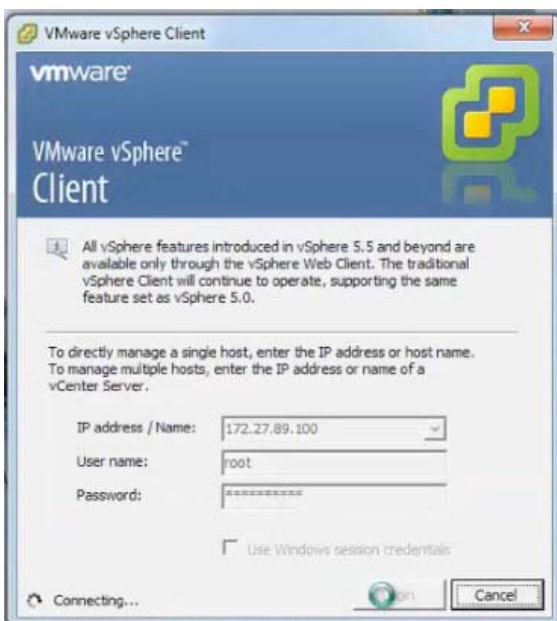
TPS OVA

- 4 GB of Memory
- 1 virtual socket with 1 core
- 50 GB of virtual storage

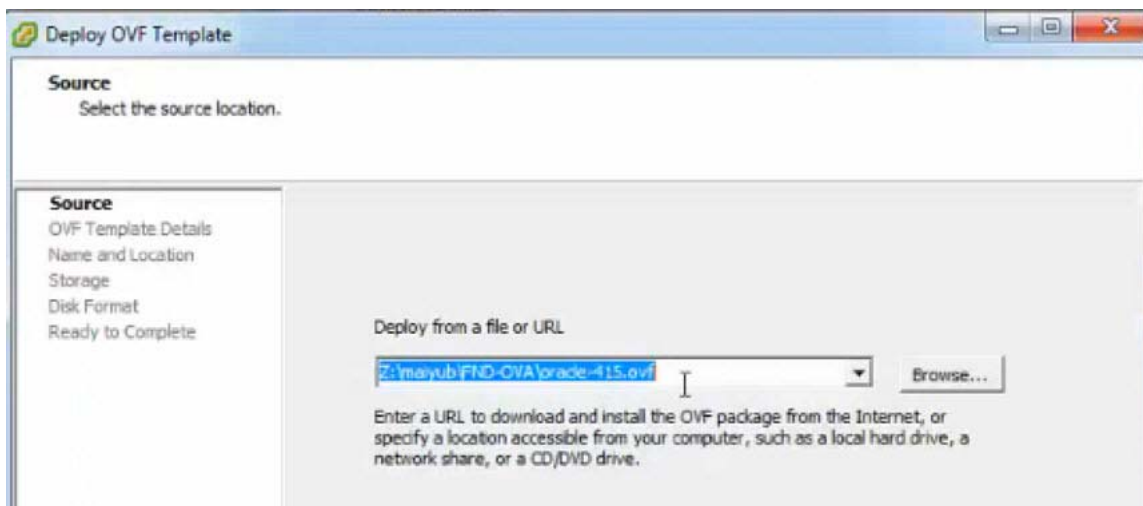
DETAILED STEPS

To import the IoT FND, Oracle, and TPS virtual appliances into ESXi 5.x or ESXi6.x using VMware vSphere Client version 5.0.0 or 6.0.0, respectively:

1. Select the **Network Adapter > NAT** setting for the server.
2. At the VMware vSphere Client window enter the IP address, username and password of the server where VMware resides. Click **Login**.

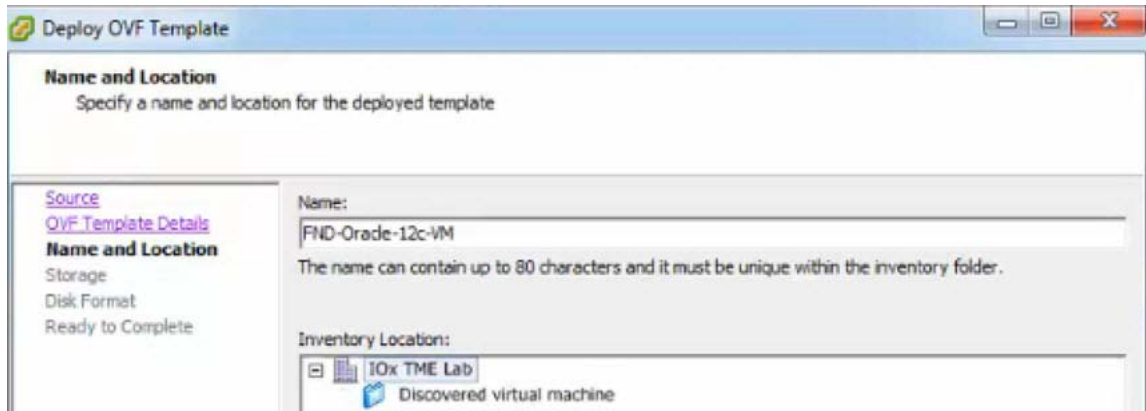


3. Select **File > Deploy OVF Template...**
4. Browse to the FND-OVA\oracle-415.ovf file.

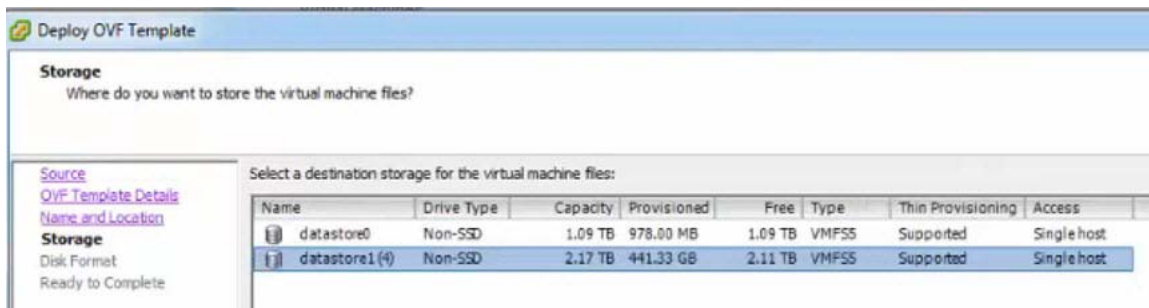


5. Ensure that the correct OVA file displays in the Source location window, and then click **Next**. (**Note:** The Next button, not shown, is found in the bottom, right-hand portion of the window.)

6. In the OVF Template Details window, enter the Name and Inventory Location of the deployed template (for example, FND-Oracle-12c-VM) Click **Next**.
7. In the next window that appears, verify the OVA file name matches what you entered in the previous window. If no issues, click **Next**. If the OVA file name does **not** match, click **Back** and reenter the information.



8. Select a Storage destination for the VM deployed template.



9. In the Disk Format window (not shown), select the **Thin Provision** option, and then click **Next**.

Note: Thin Provision allows the VM disk to grow as needed.

10. In the Ready to Complete window, confirm your deployment settings, and then click **Finish**. Deployment of the FND-Oracle-12C-VM templates begins.
11. After completion of the FND-Oracle-12c-VM install, a window displays.
 - In the left panel, select the FND-Oracle-12c-VM server.
 - In the right panel, Under Basic Task, select Edit virtual machine settings to confirm CPU and MEM settings.
 - Click **OK** to close the window.



What is a Virtual Machine?

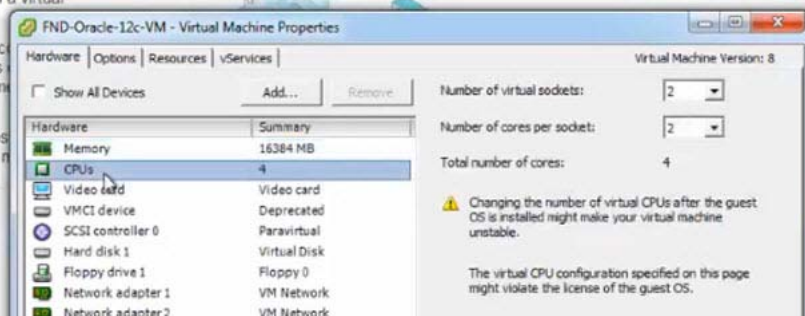
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated environment, you can use virtual machines as workstation environments, as testing environments, or to consolidate server applications.

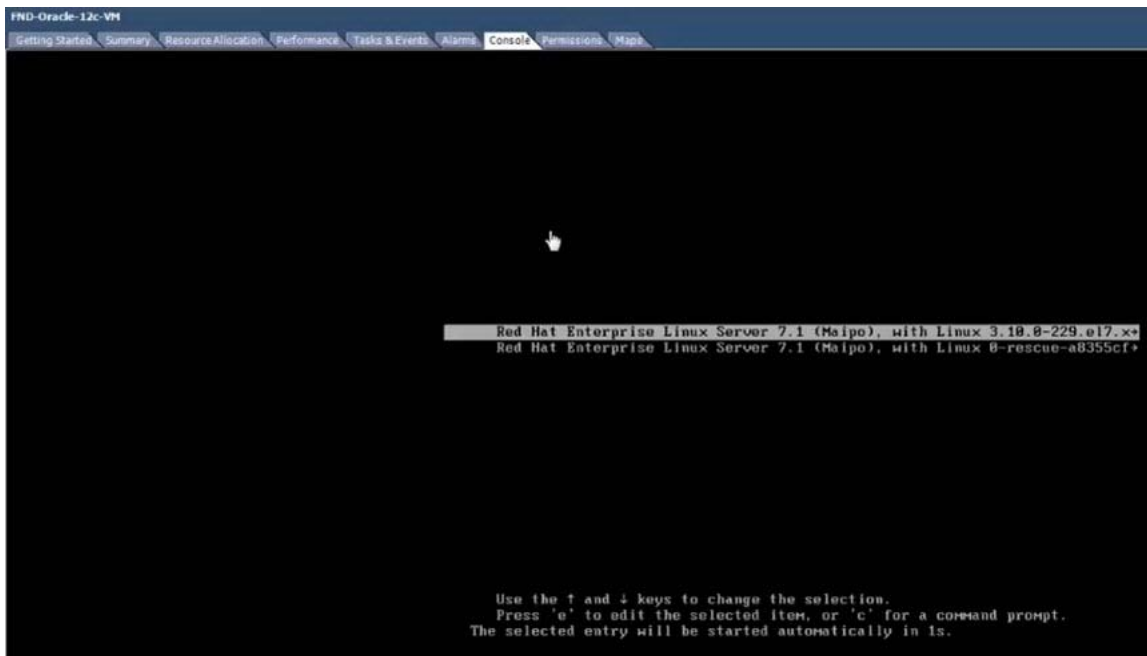
In vCenter Server, virtual machines run on hosts and clusters. The same host can run many virtual machines.

Basic Tasks

-  **Power on the virtual machine**
-  **Edit virtual machine settings**



12. Click **Power on the virtual machines** and select **Console** tab in the window that opens. The console opens showing possible RHEL server versions to select.



13. After you select a RHEL option, you will be prompted for your username and password.
14. Click **Sign In** and select the **GNOME Classic** option.



15. Click Sign In.
16. At the Welcome screen, select the default language (such as English-United States) for the interface, Click **Next**.
17. Continue through the install script until you reach the final screen that indicates that “Your computer is ready to use.” Click Start using **Red Hat Enterprise Linux Server** button.
18. Close **Getting Started** window, right-click to open.
19. At the Application Places window, right-click in the window to display a menu panel. Select **Open in Terminal**. The VM is now in your Datastore.