

Cisco IoT FND Postgres and Influx DB Deployment with Integrated Application Management on OVA, Release 4.3.1 and Later

First Published: 2018-08-31

Last Modified: 2025-10-17

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

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Overview** 1

CHAPTER 2 **OVA Images and Upgrade Scripts Verification** 3

- Introduction 3
- Verifying the OVA Signature 4
- Verifying the Upgrade-Scripts RPM Signature 5
- Verifying the CGMS Tools RPM for Postgres Signature 6

CHAPTER 3 **Installing the OVA** 9

- Configuring Hostnames in Cisco IoT FND and TPS Servers 16
- Configure NTP Server and IP Host Entries on HER Devices 17

CHAPTER 4 **Install custom CA certificates and import SUDI certificate** 19

- Changing Password 23
- Managing Custom Web Certificates 24
- Installing Custom Browser Certificates 24
  - Install custom certificates in the browser client for Cisco IoT FND release 5.1 and later 25
  - Retain custom certificates during Cisco IoT FND upgrades 27
  - Install custom certificates in the browser client 28
  - Use keytool to create the cgms_keystore file 32
- Properties Used in Cisco IoT FND and TPS Configuration 33

CHAPTER 5 **Configuring IoT FND for IPv6 Tunnel Provisioning and Registration** 37

CHAPTER 6 **Starting and Stopping FND** 39

CHAPTER 7 Starting and Stopping Fog Director 41

CHAPTER 8 Upgrade Cisco IoT FND on OVA 43

Device compatibility check 43

Check the Postgres DB status 43

Cisco IoT FND on OVA upgrade matrix 46

Verify and reset the expired root password 47

Upgrade the database and docker server image 48

Upgrade Cisco IoT FND container images 51

Check DB and status post upgrade 53

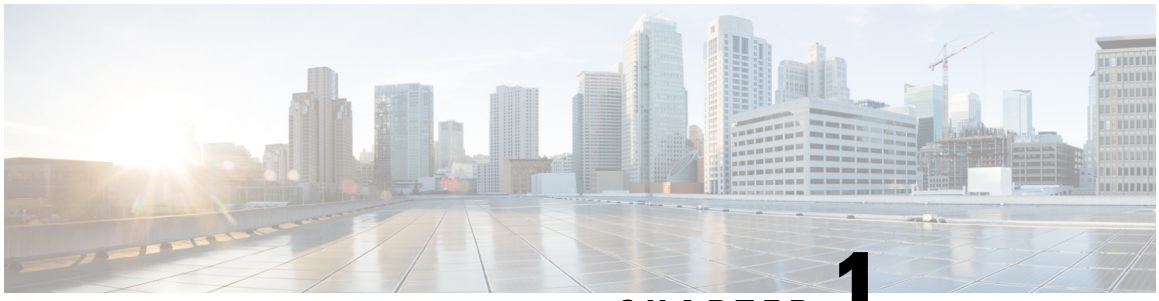
Upgrade RHEL version 55

CHAPTER 9 Obtaining Status of All Services Running on the Host 57

CHAPTER 10 Backup and Restore 59

CHAPTER 11 Setting the Time and Timezone Using NTP Service 61

Configuring NTP Server 62



CHAPTER 1

Overview

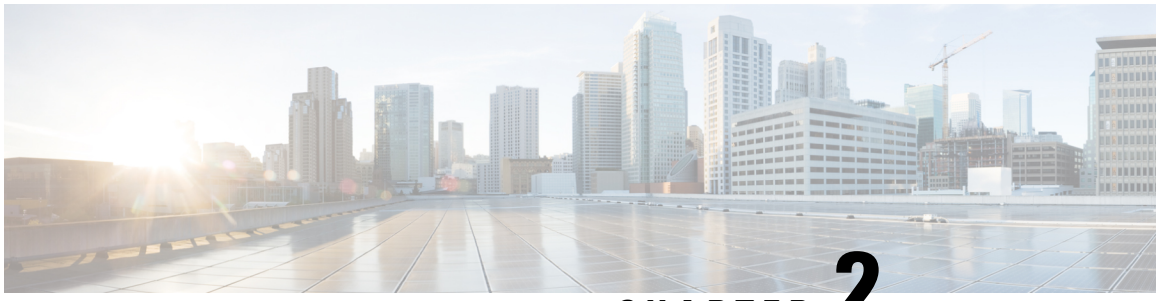
This document provides the steps required to install the Cisco IoT Field Network Director (Cisco IoT FND) Release 4.3.1 and Later application with Integrated Application Management (Fog Director) on an Open Virtual Appliance (OVA), VMware ESXi 5.5 or 6.0. You use the same instructions to install both VMware versions.

Note For information about installing Cisco IoT FND and Oracle on an OVA for Release 4.3 and Later, refer to the following guides:

- Cisco IoT FND Deployment on an Open Virtual Appliance, VMware ESXi 5.5/6.0
- Cisco IoT Field Network Director Installation Guide-Oracle Deployment, Release 4.3.x and Later

For an overview of the features and functionality of the IoT FND application and details on how to configure features and manage Cisco IoT FND after its installation, refer to the Cisco IoT Field Network Director User Guide.

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



CHAPTER 2

OVA Images and Upgrade Scripts Verification

- Introduction, on page 3
- Verifying the OVA Signature, on page 4
- Verifying the Upgrade-Scripts RPM Signature, on page 5
- Verifying the CGMS Tools RPM for Postgres Signature, on page 6

Introduction

Starting from Cisco IoT FND 4.9.0, you can verify the integrity of the OVA images and upgrade scripts before the installation or upgrade of IoT FND.

For more information, refer to:

- Verifying the OVA Signature, on page 4
- Verifying the Upgrade-Scripts RPM Signature, on page 5
- Verifying the CGMS Tools RPM for Postgres Signature, on page 6

Note From FND release 4.12 onwards, the Secure Hash Algorithm is SHA256 and the earlier FND releases use SHA1.

Table 1: OVA Images and Upgrade Scripts Zip File Contents

Zip File Contents	Description
CISCO-IOTFND-V-K9-<release>-<build number>.zip	Includes Oracle for Mesh management (CGR, IR5xx) use case.
1. iot-fnd-oracle-<release>-<build number>_SHA1_signed.ova 2. iot-tps-<release>-<build number>_SHA1_signed.ova	
CISCO-IOTFND-VPI-K9-<release>-<build number>.zip	Includes Postgres / Influx for gateway management (IR8xx, IR1101, IC3K) use case.

Zip File Contents	Description
1. iot-fnd-<release>-<build number>_SHA256_signed.ova 2. iot-tps-<release>-<build number>_SHA256_signed.ova	
CISCO-IOTFND-VPI-K9-CGMS-TOOLS-<release>-<build number>.zip **Attention** The CGMS tools file is bundled with `CISCO-IOTFND-VPI-K9-UPGRADE-SCRIPTS-<release>-<build number>.zip`.	Includes cgms tools rpm for Postgres deployments.
1. cgms-tools-<release>-<build number>.x86_64.rpm 2. FND_RPM_SIGN-CCO_RELEASE.pem — Cisco signed x.509 end-entity certificate containing public key that is used to verify the signature. This certificate is chained to Cisco root CA and sub CA posted on https://www.cisco.com/security/pki/. 3. cisco_openpgp_verify_release.py — Signature verification program for verifying the Open-pgp Complaint Public Key against x.509 end-entity certificate. 4. cisco_openpgp_verify_release.py.signature — Signature generated for the script cisco_openpgp_verify_release.py. 5. FND-rel-binary.gpg — Open-pgp public key is used for verification of signed RPM. 6. FND-rel-ascii.gpg — Open-pgp public key is used for verification of signed RPM.	
CISCO-IOTFND-VPI-K9-UPGRADE-SCRIPTS-<release>-<build number>.zip	Includes upgrade scripts for upgrading FND-Postgres / Influx OVA.
1. upgrade-ova-<release>-<build number>.rpm — Signature embedded RPM image. 2. FND_RPM_SIGN-CCO_RELEASE.pem — Cisco signed x.509 end-entity certificate containing public key that is used to verify the signature. This certificate is chained to Cisco root CA and sub CA posted on https://www.cisco.com/security/pki/. 3. cisco_openpgp_verify_release.py — Signature verification program for verifying the Open-pgp Complaint Public Key against x.509 end-entity certificate. 4. cisco_openpgp_verify_release.py.signature — Signature generated for the script cisco_openpgp_verify_release.py. 5. FND-rel-binary.gpg — Open-pgp public key is used for verification of signed RPM. 6. FND-rel-ascii.gpg — Open-pgp public key is used for verification of signed RPM.	

Verifying the OVA Signature

To verify the OVA signature:

Procedure

Step 1 Install the `ovftool`.

Step 2 Run the command to verify the signed `ova` file.

```
ovftool iot-fnd-<release>-<build number>_SHA256_signed.ova
```

Verifying the Upgrade-Scripts RPM Signature

Prerequisites:

- Python 2.7.x
- OpenSSL
- Verification scripts running on customer-premises need internet connection to reach Cisco to download root and sub-CA certs

To verify the upgrade-scripts RPM signature:

Procedure

Step 1 Unzip the file `CISCO-IOTFND-VPI-K9-UPGRADE-SCRIPTS-<release>-<build number>.zip`.

Step 2 Change directory (cd) to `CISCO-IOTFND-VPI-K9-UPGRADE-SCRIPTS-<release>-<build number>` folder.

Step 3 Extract the public key from the public cert:

```
openssl x509 -pubkey -noout -in FND_RPM_SIGN-CCO_RELEASE.pem > FND-EE-cert.pubkey
```

Expected Result:

```
FND-EE-cert.pubkey is created under the same folder
```

Step 4 Verify the verification script using the public key and the signature files.

```
openssl dgst -sha512 -verify FND-EE-cert.pubkey -signature
cisco_openpgp_verify_release.py.signature cisco_openpgp_verify_release.py
```

Expected Result:

```
Verified OK
```

Step 5 Verify if the delivered binary and ASCII keys have matching fingerprints.

a) `gpg FND-rel-binary.gpg`

Expected Result:

```
pub 2048R/F7D5ED29 2017-01-01 identity-name  (FND.rel) identity-name@cisco.com
```

b) `gpg FND-rel-ascii.gpg`

Expected Result:

```
pub 2048R/F7D5ED29 2017-01-01 identity-name (FND.rel) identity-name@cisco.com
```

Step 6 Verify the binary GPG key against EE cert.

```
./cisco_openpgp_verify_release.py -e FND_RPM_SIGN-CCO_RELEASE.pem -G
FND-rel-binary.gpg
```

Expected Result:

```
 Downloading CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...

Successfully downloaded crcam2.cer.

Downloading SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...

Successfully downloaded innerspace.cer.

Successfully verified Cisco root, subca and end-entity certificate chain.

Successfully fetched a public key from FND_RPM_SIGN-CCO_RELEASE.pem.

Successfully authenticated FND-rel-binary.gpg key using Cisco X.509 certificate trust chain.
```

Step 7 Verify the RPM Signature using the GPG ASCII key.

```
sudo rpm --import FND-rel-ascii.gpg

rpm -K upgrade-ova-<release>-<build number>.rpm
```

Expected Result:

```
upgrade-ova-<release>-<build number>.rpm: rsa sha1 (md5) pgp md5 OK
```

Step 8 Once the RPM is verified, you can upgrade OVA using the RPM.

Verifying the CGMS Tools RPM for Postgres Signature

Prerequisites:

- Python 2.7.x
- OpenSSL
- Verification scripts running on customer-premises need an internet connection to reach Cisco to download root and sub-CA certs

To verify the cgms tools rpm for Postgres signature:

Procedure

Step 1 Unzip the file `CISCO-IOTFND-VPI-K9-CGMS-TOOLS-<release>-<build number>.zip .`

Step 2 Change directory (cd) to `CISCO-IOTFND-VPI-K9-CGMS-TOOLS-<release>-<build number>.zip` folder.

Step 3 Extract the public key from the public cert:

```
openssl x509 -pubkey -noout -in FND_RPM_SIGN-CCO_RELEASE.pem > FND-EE-cert.pubkey
```

Expected Result:

```
FND-EE-cert.pubkey is created under the same folder
```

Step 4 Verify the verification script using the public key and the signature files.

```
openssl dgst -sha512 -verify FND-EE-cert.pubkey -signature
cisco_openpgp_verify_release.py.signature cisco_openpgp_verify_release.py
```

Expected Result:

```
Verified OK
```

Step 5 Verify if the delivered binary and ASCII keys have matching fingerprints.

a) `gpg FND-rel-binary.gpg`

Expected Result:

```
pub 2048R/F7D5ED29 2017-01-01 identity-name  (FND.rel) identity-name@cisco.com
```

b) `gpg FND-rel-ascii.gpg`

Expected Result:

```
pub 2048R/F7D5ED29 2017-01-01 identity-name (FND.rel) identity-name@cisco.com
```

Step 6 Verify the binary GPG key against EE cert.

```
./cisco_openpgp_verify_release.py -e FND_RPM_SIGN-CCO_RELEASE.pem -G
FND-rel-binary.gpg
```

Expected Result:

```
 Downloading CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...

Successfully downloaded crcam2.cer.

Downloading SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...

Successfully downloaded innerspace.cer.

Successfully verified Cisco root, subca and end-entity certificate chain.

Successfully fetched a public key from FND_RPM_SIGN-CCO_RELEASE.pem.

Successfully authenticated FND-rel-binary.gpg key using Cisco X.509 certificate trust chain.
```

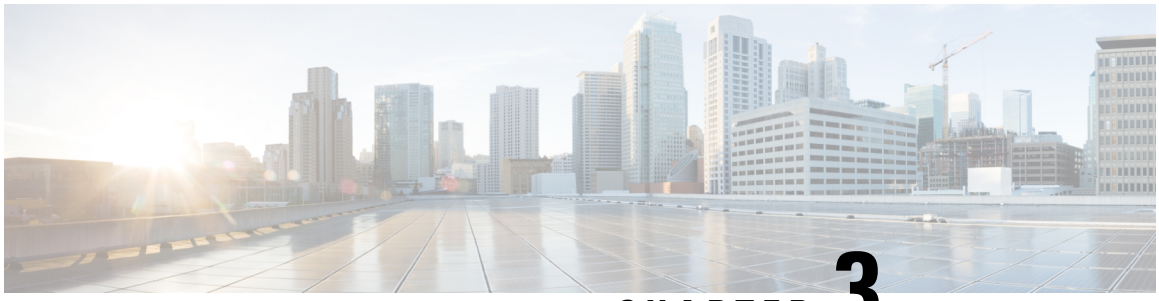
Step 7 Verify the RPM Signature using the GPG ASCII key.

```
sudo rpm --import FND-rel-ascii.gpg
rpm -K cgms-tools-<release>-<build number>.x86_64.rpm
```

Expected Result:

```
upgrade-cgms-tools-<release>-<build number>.x86_64.rpm: rsa sha1 (md5) pgp md5 OK
```

Step 8 Once the RPM is verified, you can upgrade cgms-tools using the RPM.



CHAPTER 3

Installing the OVA

Prerequisites

- Log in to the IP address of a VMware ESXi server running 6.5 and above via a web browser with your user credentials (username and password).
- Ensure that you meet the VMware server machine (VM CPU and memory) requirements as listed below.
  - 24 GB memory
  - 4 vCPUs
  - Hard disk: 450 GB

To install the OVA:

Attention From IoT FND 4.12 onwards, use the following credentials for SSH access after installing OVA. The existing credentials username/password (root/cisco123) is disabled for 4.12 and later releases:

- Username: fnduser
- Password: C!sco123

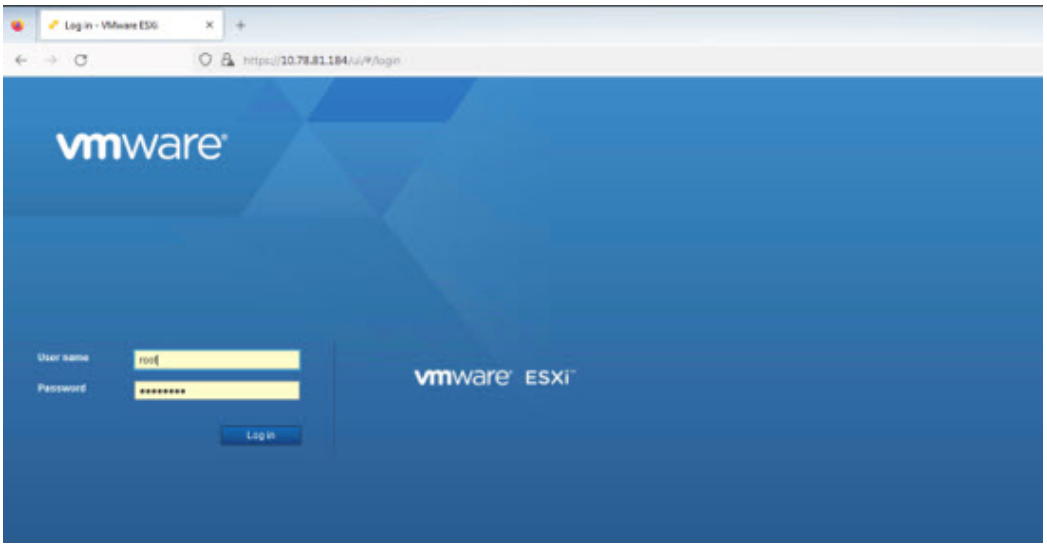
See Step 10 for guidelines to reset the default password.

Procedure

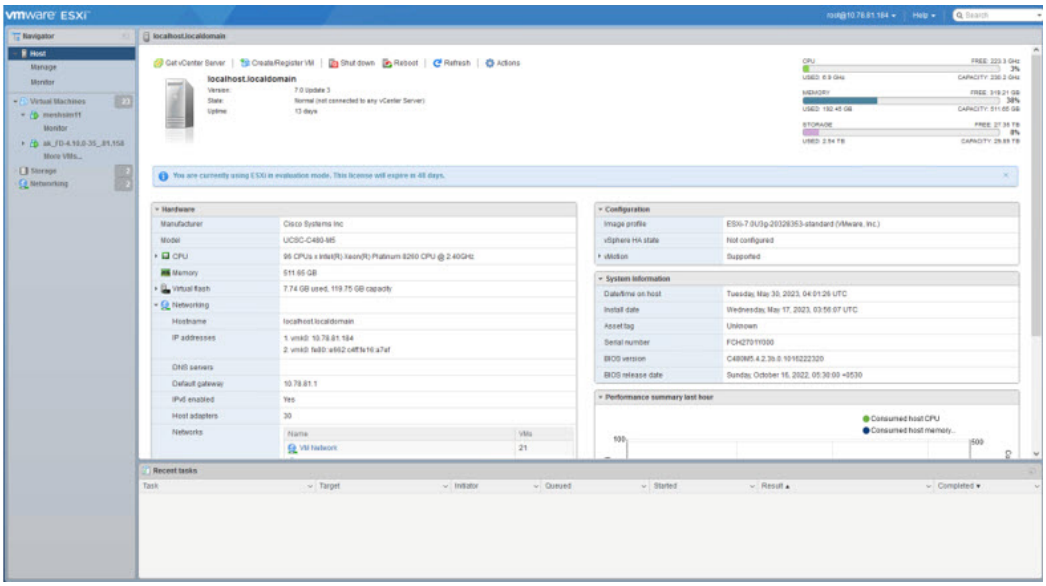
Step 1 Log in to the IP address of a VMware ESXi server running 6.5 and above via a web browser with your user credentials (username and password).

a) Enter the ESXi IP address in the URL.

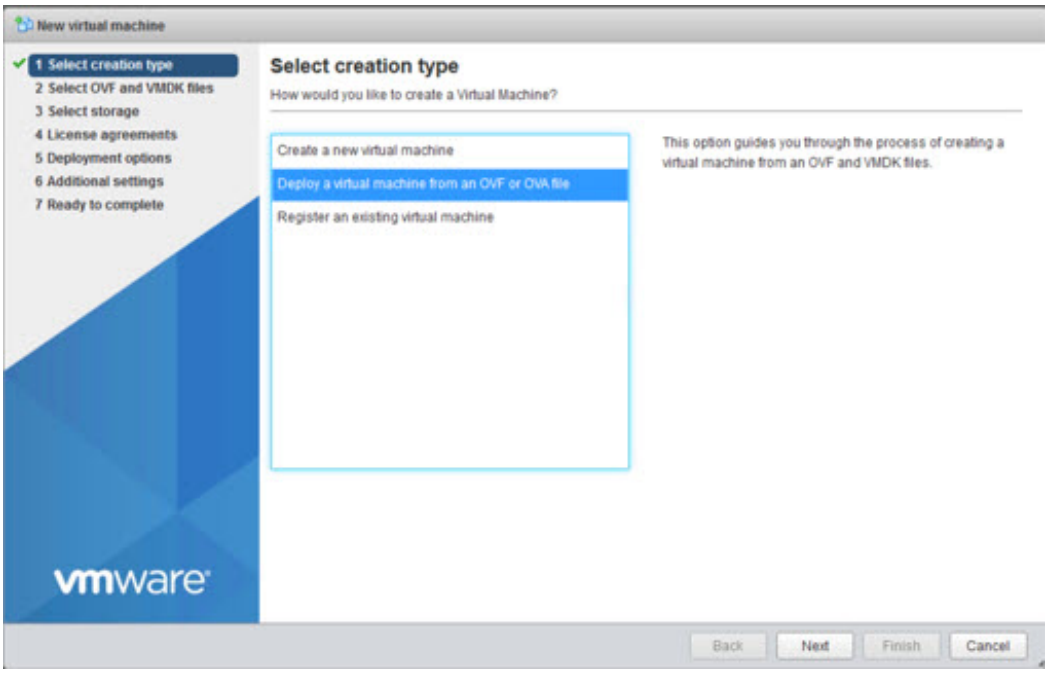
b) Provide the ESXi root login credentials and click **Log In**.



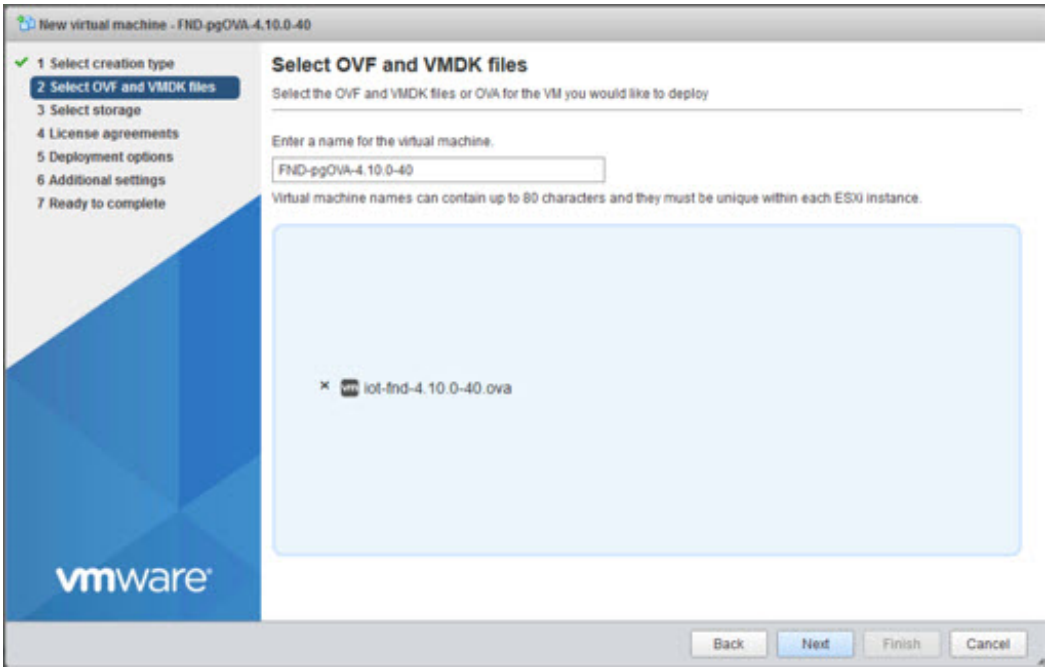
Step 2 In the Host page, select **Create/ Register VM**.



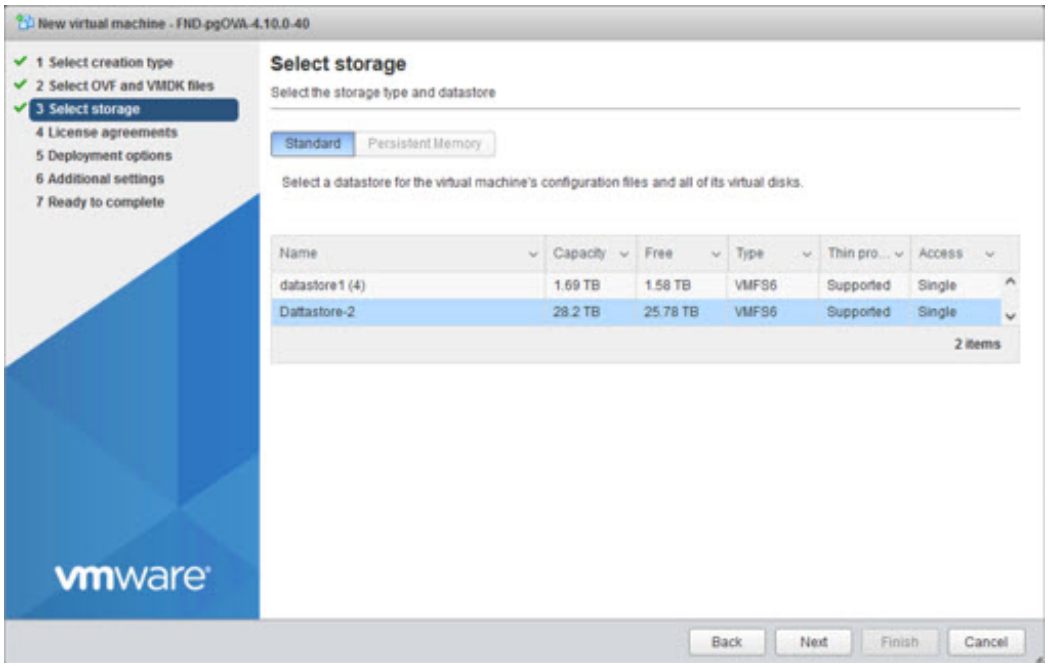
Step 3 In the New virtual machine window, select **Deploy a virtual machine from an OVF or OVA file** in Select creation type tab and click **Next**.



Step 4 In the Select OVF and VMDK files tab, provide a name for the virtual machine and browse to an OVF package from the internet or a file accessible from your computer (for example, iot-fnd-4.10.0-40.ova). Click **Next**.



Step 5 Select a storage location for the virtual machines from the listed options (example - Datastore-2).



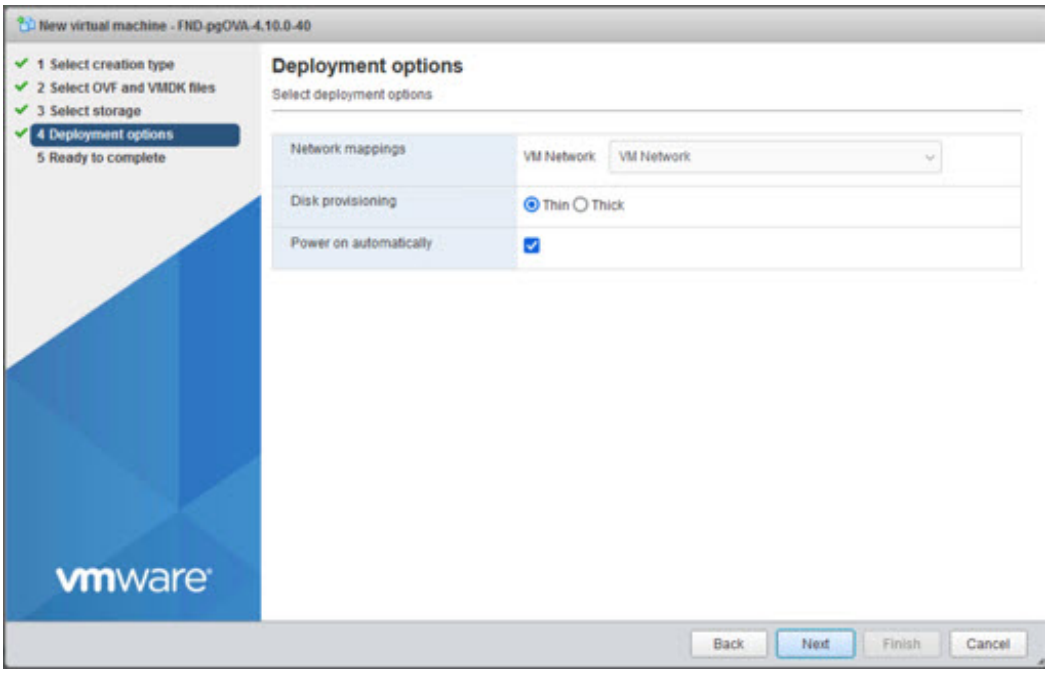
Step 6 After selecting the data store, select the provisioning type and enable the **Power on automatically** option. This ensures to power on the virtual machine once the deployment process is complete. Click **Next**.

Note

- Thick Provisioning — Absolute reservation on the disk space. For the IoT FND OVA deployment, the disk space required is 600 GB on the ESXi server.
- Thin Provisioning — The disk space grows on demand. For the IoT FND OVA deployment, the disk space is approximately 50 GB initially and the disk space occupied by VM will grow as per the scale of deployment.

Note

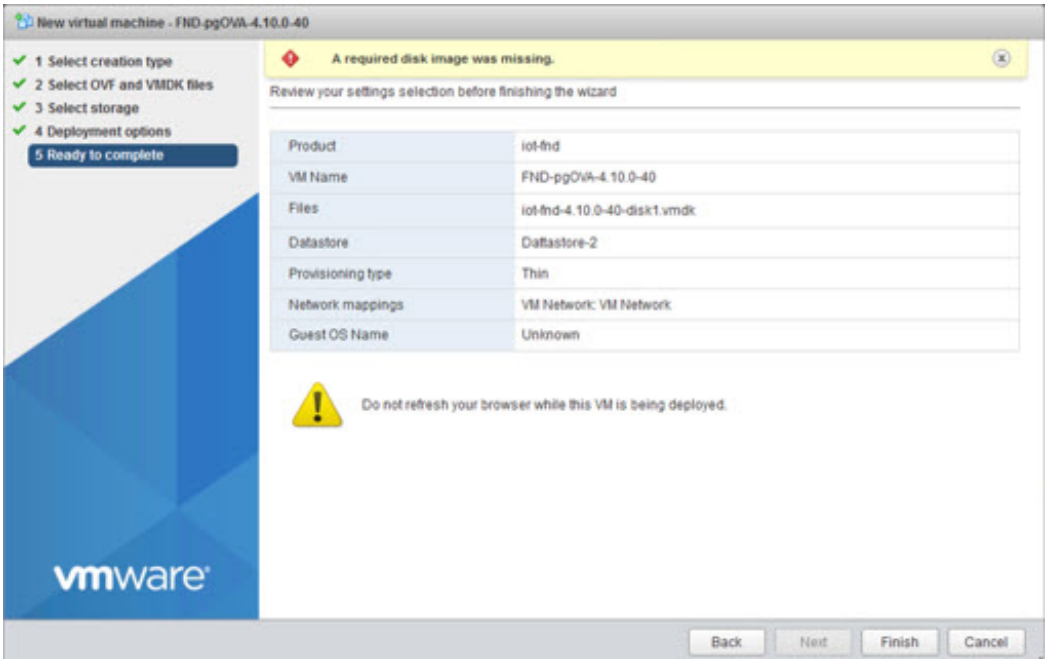
If the selected storage location does not have sufficient storage for the largest file installation option, a message displays noting insufficient storage. If the warning message appears, select another storage resource with greater capacity and click **Next**.



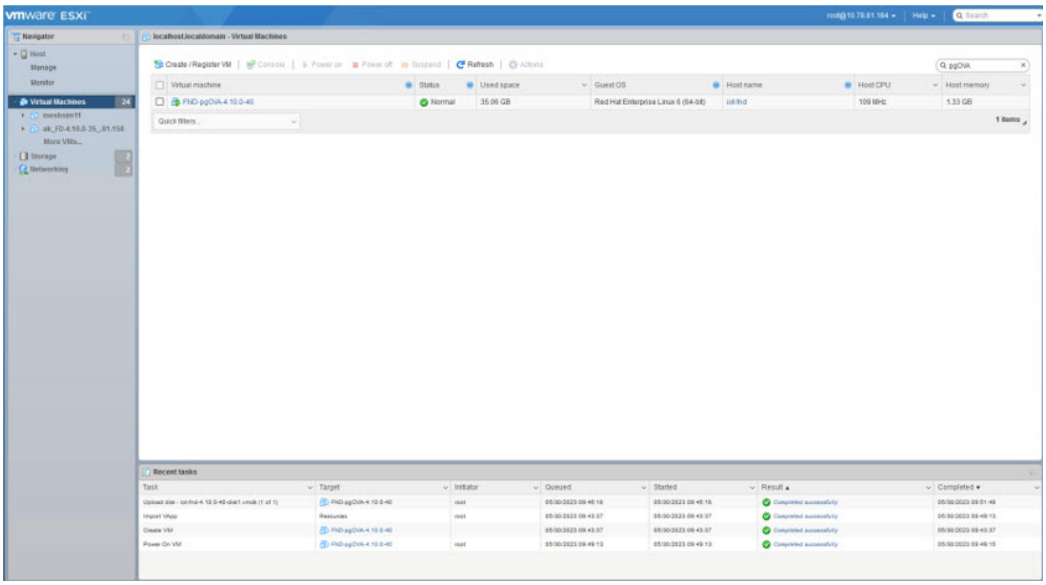
Step 7 Do a final review of the **Ready to Complete** window. If you do not want to change any settings, click **Finish**.

Note
If you see the following warning message while deployment, then cancel the upload, disconnect the Esxi from vCenter Server (**Actions** > **Disconnect from vCenter Server**) and then re-upload OVA. The upload will be successful.

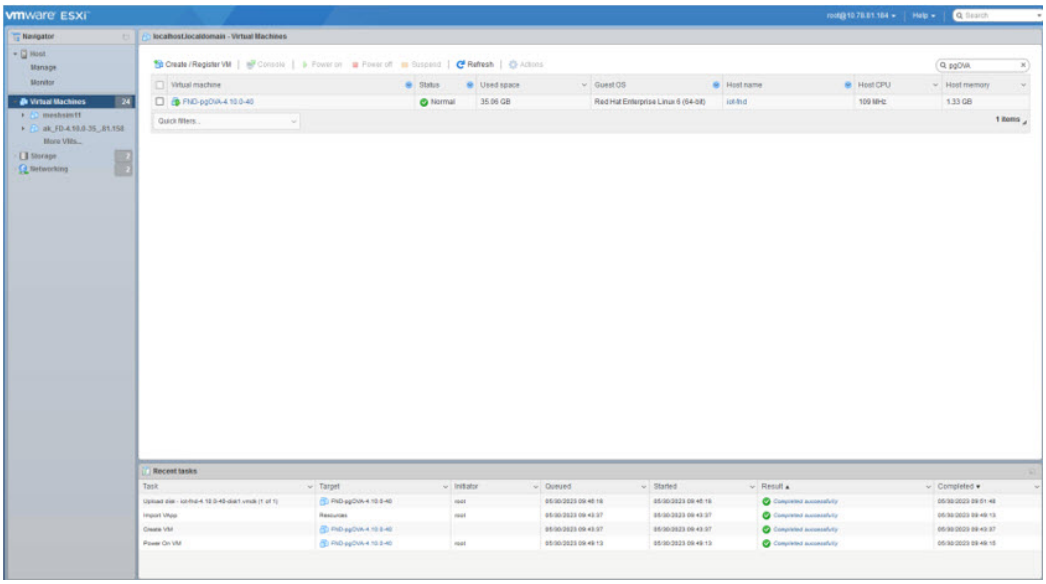
"Failed: Access to resource settings on the host is restricted to the server that is managing it 'vCenter Server IP'"



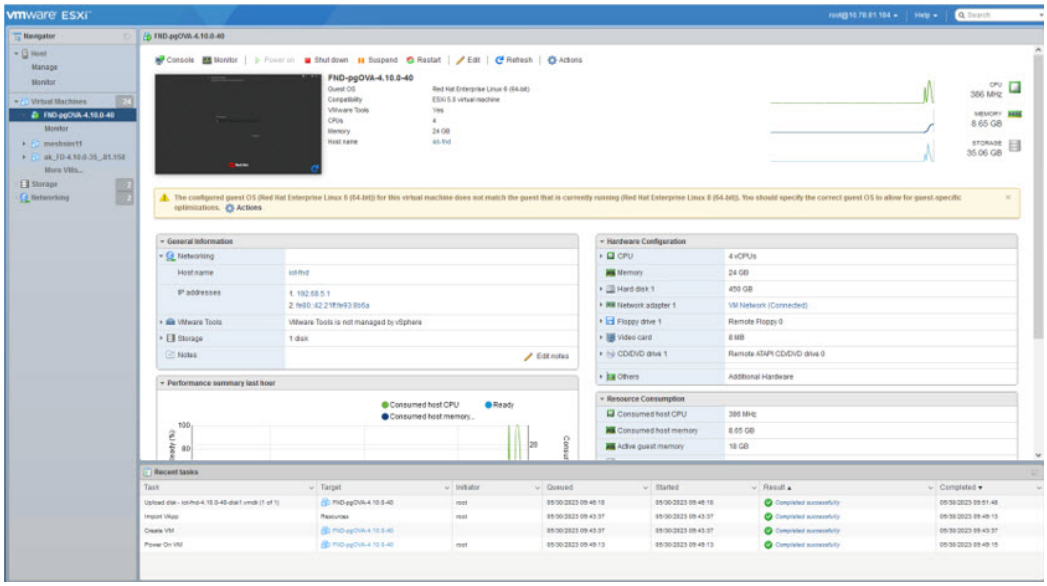
The virtual machine deployment is initiated. After completion of the install, the "Completed successfully" message appears in the Recent tasks pane at the bottom of the install window.



Step 8 Click Virtual Machines in the left pane and select the newly deployed VM.



Step 9 The deployed VM gets listed in the left pane. Select the IoT FND machine name.



Step 10 Click **Console** and login with root/cisco123 once the OS is up. Once you enter the default password, you are prompted to reset your password.

Important
From IoT FND release 4.12 onwards:

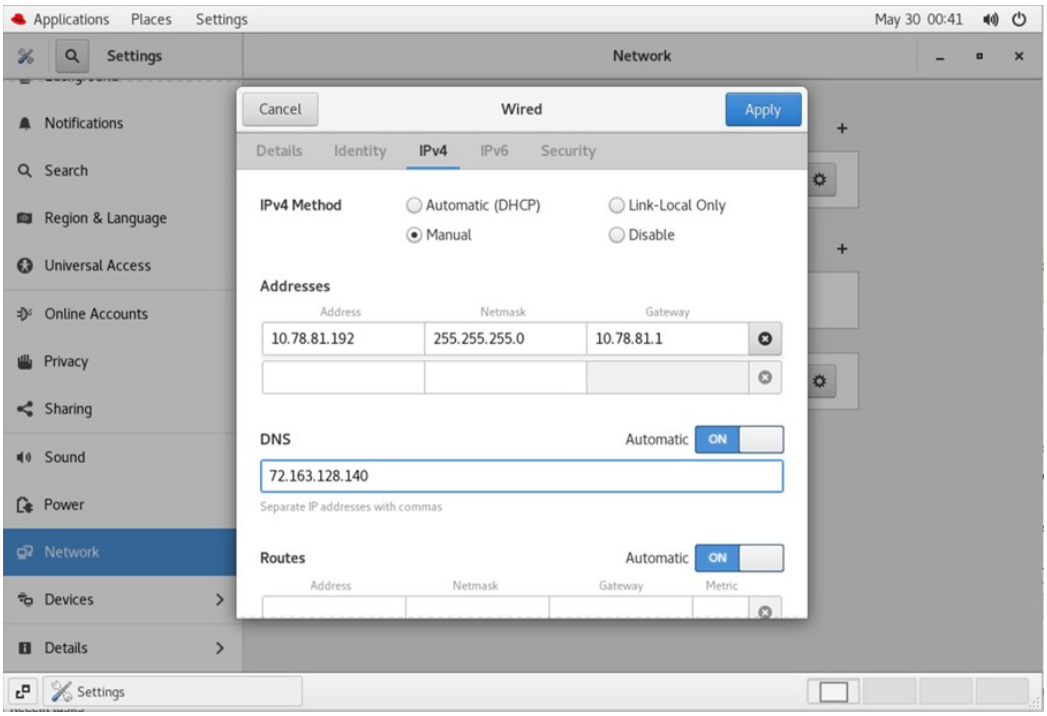
- The default root user password is C!sco123.
- The following conditions are applicable to reset the default password.
  - The password must be at least 8 characters in length
  - The password must have at least 1 uppercase character
  - The password must have at least 1 lowercase character
  - The password must have at least 1 special character
  - The password must have at least 1 digit
  - The password cannot be the same as any of the previous 5 passwords used

Step 11 Reset the default root password. After you complete the password reset, IoT FND is fully deployed. From FND 4.12 release, the conditions mentioned in Step 10 are applicable to reset the default password.

Step 12 Once logged in, navigate to **Applications > System Tools > Settings > Network**.

Step 13 Click the cog icon under Wired, navigate to IPv4 tab to assign a static IP address or set up a DHCP server in the network.

- Under IPv4 tab, select the method as Manual and provide the IPv4 address as below and click **Apply**.
- Set up a valid, reachable working DNS server on the Host VM. (mandatory) Use this IP address to access the FND GUI.



Important
Follow the same steps for TPS OVA installation as well. In order to upgrade the TPS OVA, delete the existing TPS and reinstall the TPS OVA `iot-tps-version_number.ova` with the updated version number.

Step 14 Open a terminal window, and set up Health Monitoring for the Fog Director Container from FND.

```
[root@iot-fnd ~]# cd /opt/monitor/
```

```
[root@iot-fnd monitor]# ./setup.sh
Setup health metrics monitor for App Management Servers
Enter FND Username: root
Enter FND Password:
Successfully configured health metrics monitor for App Management Servers
```

After completing these steps, IoT FND starts monitoring the Fog Director container on the **ADMIN > SERVERS** page.

- Configuring Hostnames in Cisco IoT FND and TPS Servers, on page 16
- Configure NTP Server and IP Host Entries on HER Devices, on page 17

Configuring Hostnames in Cisco IoT FND and TPS Servers

During onboarding Cisco IoT FND. you can configure domain names in the */etc/hosts* file. Use this configuration for the Zero Touch Deployment (ZTD) and Plug and Play (PNP) of FAR devices. The domain name helps in resolving FND or TPS hostname with an IP address. They help in communicating with FND.

To configure hostnames in FND and TPS servers follow the steps given.

Procedure

Step 1 Edit hostname in the */etc/hosts* file.

Example:

```
root@iot-fnd ~]# nano /etc/hosts
```

This will display the */etc/hosts* file which you can edit by adding or updating hostnames with corresponding IP addresses.

Step 2 Enter the domain name for the host IP address separated by a space or a tab.

Example:

```
209.165.200.225  fnd.iot.cisco.com
209.165.201.1  tps.iot.cisco.com
```

Step 3 Save the changes by selecting **Y** and exit.

Step 4 Validate the updated hostname using the command given in the example.

Example:

```
[root@iot-fnd-oracle ~]# ping fnd.iot.cisco.com
64 bytes from fnd.iot.cisco.com (209.165.200.225): icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from fnd.iot.cisco.com (209.165.200.225): icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from fnd.iot.cisco.com (209.165.200.225): icmp_seq=3 ttl=64 time=0.048 ms
```

The updated hostname is displayed along with the corresponding IP address.

Step 5 To view the hostnames with the corresponding IP addresses, use the command given in the example.

Example:

```
[root@iot-fnd ~]# cat /etc/hosts
127.0.0.1  iot-fnd-oracle localhost localhost.localdomain localhost4 localhost4.localdomain4
::1        iot-fnd-oracle localhost localhost.localdomain localhost6 localhost6.localdomain6
209.165.200.225  fnd.iot.cisco.com
209.165.201.1  tps.iot.cisco.com
```

Configure NTP Server and IP Host Entries on HER Devices

Configure the NTP server and IP host entries on a HER device to enhance manageability of your network infrastructure. Here are the instructions to configure NTP server and IP host entries on HER devices:

Configure NTP Server

1. Access the HER device using the SSH terminal.
2. Enter the global configuration mode:

   ```
   config t
   ```

3. Use the `ntp server` command to specify the IP address or hostname of the NTP server. Here are some examples:

   ```
   ntp server 192.168.1.100
   ```

```
ntp server ntp.example.com
```

4. Exit the configuration.

   Here's an example output:

```
config t
ntp server 192.168.1.100
exit
```

Configure IP Host Entries

1. Access the HER device using the SSH terminal.
2. Enter the global configuration mode:

```
config t
```

3. To remove an existing IP host entry, use the `no` form of the `ip host` command:

```
no ip host caserver.fnd.iot.com 192.168.1.100
```

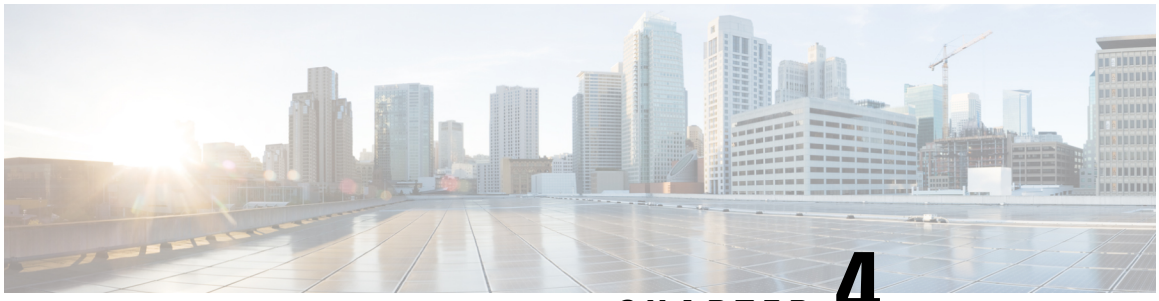
4. Add the new IP address for the hostname:

```
ip host caserver.fnd.iot.com 192.168.1.100
```

5. Repeat steps 3 and 4 for any other host entries you need to update.
6. Exit the configuration.

   Here's an example output:

```
config t
ip host fndserver.fndiot.com 192.168.1.100
exit
```



CHAPTER 4

Install custom CA certificates and import SUDI certificate

The Cisco IoT FND OVA is bundled with keys and certificates which is stored in a keystore. The following values are the default values of the keys and certificates:

- On the Cisco IoT FND OVA Linux Host:

  Keystore Location: /opt/fnd/data/

  Keystore Name: cgms_keystore.selfsigned

- On Cisco IoT FND container:

  Keystore Location: /opt/cgms/server/cgms/conf/

  Keystore Name: cgms_keystore

- **Default Password: Public123!**



Important

- This is the default password for both the files.
- Both these files have the same content.
- When Cisco IoT FND container is restarted, the values of /opt/cgms/server/cgms/conf/cgms_keystore file in Cisco IoT FND container is overwritten by /opt/fnd/data/cgms_keystore file. If /opt/fnd/data/cgms_keystore file is not present in host, then /opt/fnd/data/cgms_keystore.selfsigned file is used.
- When using passwords in shell commands, especially those containing special characters like '$', it is crucial to enclose the password in single quotes, for example, `'your$password!'`. This ensures that the shell treats the password literally and prevents issues caused by variable expansion.

When Cisco IoT FND OVA is a new installation, each certificate/key entry is referenced by an alias name in the keystore. The default alias are:

- cisco_sudi (cisco root CA certificate with 2029 expiry)
- jmarconi (cisco certificate)

- cgms (self signed certificate that is used by Cisco IoT FND when communicating with devices it has to manage)

Note This keystore is specific for certificates used for Cisco IoT FND communication with its managed devices. There is a different keystore for web certificate.

Custom cgms_keystore

The cgms certificate in /opt/cgms/server/cgms/conf/cgms_keystore file in Cisco IoT FND container and /opt/fnd/data/cgms_keystore.selfsigned file of the linux host has by default self signed certificate of Cisco IoT FND. There are two options to build a custom cgms_keystore in /opt/fnd/data location on linux host, where the Cisco IoT FND certificate of the customer organisation can be imported and stored.

We can either copy the existing /opt/fnd/data/cgms_keystore.selfsigned file on the Linux host or build it from scratch. After the cgms_keystore file is present on the linux host, if both /opt/fnd/data/cgms_keystore.selfsigned and /opt/fnd/data/cgms_keystore files are present, then /opt/fnd/data/cgms_keystore takes precedence.

Note NTP is a mandatory requirement for Public Key Infrastructure. Hence NTP should be in sync between the issuing Certificate Authority (CA) server, Cisco IoT FND, TPS, and FAR/HER. If hostname or IP address has to be changed for the Cisco IoT FND host, it has to be done before certificate for Cisco IoT FND is issued and hence it should be done before starting to build cgms_keystore.

The SAN field in Cisco IoT FND certificate is a mandatory requirement and contains the hostname of the Cisco IoT FND server. Any change in hostname or IP address is listed in SAN field (if IP address is also present in the SAN field), then the certificate should be reissued. Depending on the PnP type used, the SAN field contains the hostname of the Cisco IoT FND or the IP address or both.

The cgms_keystore should contain the below mandatory certificates/keys:

- Issuing CA certificate of the organisation – This is the certificate of the issuing CA server of the organisation. The issuing CA server can be a root CA server or intermediate CA server. If it is an intermediate CA, it is recommended to import root CA and also intermediate CA certificates into the keystore.
- Cisco IoT FND device certificate is issued for Cisco IoT FND by issuing CA server.
- Cisco SUDI with 2029 expiry date – This is the cisco manufacturer certificate for Cisco IoT FND issued by Cisco with expiry date 2029.
- Cisco SUDI with 2099 expiry date – This is the cisco manufacturer certificate for Cisco IoT FND issued by Cisco with expiry date 2099.

The below option shows how to build cgms_keystore file from scratch that contains the required certificates and keys.

Procedure

Step 1 Change directory to /opt/fnd/data on linux host.

```
# cd /opt/fnd/data
```

Importing Root/Issuing CA Certificate

Step 2 Importing any certificate using keytool command creates the keystore file, if keystore file does not exist. Note that the name of the file has to be cgms_keystore as Cisco IoT FND refers the file with this name. Copy the issuing CA certificate of your organisation to any location (using scp or any other file transfer method). In this illustration, it is copied to /root/rootca.pem. The certificate can be of the format .cer or .crt or .pem. In this illustration, the issuing CA is the root CA and hence the alias name root is used.

```
# keytool -import -trustcacerts -keystore /opt/fnd/data/cgms_keystore -alias
 root -file /root/rootca.pem
```

Convert the keystore from jks to pkcs12.

```
# keytool -importkeystore -srckeystore /opt/fnd/data/cgms_keystore
-destkeystore /opt/fnd/data/cgms_keystore -deststoretype pkcs12
```

Verify that the file has been created by listing the contents of the keystore.

```
# keytool -list -keystore /opt/fnd/data/cgms_keystore
```

Importing Cisco IoT FND Certificate

Step 3 Import the Cisco IoT FND certificate.

Note
Cisco IoT FND certificate has to be imported only with alias name of cgms.

The below steps tells how to generate a key pair .csr file that can be presented to the issuing CA server for a certificate to be granted for Cisco IoT FND server. The .csr file is required by few issuing CA servers of few PKI vendors. If the .csr certificate is given to the issuing CA server, then a certificate is generated based on the contents of the .csr file. If a certificate of Cisco IoT FND has already been issued, use the following steps, if the Cisco IoT FND certificate issued has .pem or .cer or .crt extension. If the Cisco IoT FND certificate has .pfx extension, follow step 4.

a) Generate a key pair and .csr file .

```
# keytool -genkeypair -keyalg RSA -keysize 2048 -alias cgms
-ext "SAN=dns.labfnd.cisco.com, ip:1.0.0.1" -keystore /opt/fnd/data/cgms_keystore
-dname CN=labfnd, OU=iotescblr, O=cisco, L=Bengaluru, ST=Karnataka, C=IN"
```

Note
The key size in this example is 2048, but 4096 can also be used.

```
# keytool -certreq -file labfnd.csr -keystore
/opt/fnd/data/cgms_keystore -alias cgms -ext "SAN=dns:labfnd.cisco.com,ip:1.0.0.1"
```

Note
This .csr file is then presented to the issuing CA server and a certificate is obtained for Cisco IoT FND server.

b) Copy the issued certificate to FND server in any location. In this sample, it is copied to /opt/fnd/data as labfnd.pem file. Import the certificate using below command.

```
# keytool -import -trustcacerts -keystore /opt/fnd/data/cgms_keystore
-alias cgms -file /root/labfnd.pem
```

Step 4 If the Cisco IoT FND issued certificate issued has .pfx format, then we will have a .pfx file instead of the .pem file. If it is a .pfx file, check the alias name of the .pfx file and then import it using the alias cgms in the cgms_keystore.

- Find the alias name of the pfx file. In this case, the nms.pfx is copied to the current location.

```
# keytool -list -v -keystore /opt/fnd/data/nms.pfx -srcstoretype
 pkcs12 | grep Alias
```

- Import the pfx into the cgms_keystore with alias cgms. In this sample, "le-IoT FND-8f0908aa-dc8d-4101-a526-93b4eaad9481" is the alias present in the .pfx file.

```
# keytool -importkeystore -v -srckeystore /opt/fnd/data/nms.pfx
-destkeystore /opt/fnd/data/cgms_keystore -srcalias
 le-IoT FND-8f0908aa-dc8d-4101-a526-93b4eaad9481 -destalias cgms
```

Importing SUDI with 2029 Expiry

Step 5 The SUDI certificate with 2029 expiry is present in /opt/fnd/data directory as cisco-sudi-ca.pem. Import this file to cgms_keystore.

```
# keytool -import -trustcacerts -alias cisco_sudi -file
/opt/fnd/data/cisco-sudi-ca.pem -keystore /opt/fnd/data/cgms_keystore
```

Importing SUDI with 2099 Expiry

Step 6 The updated SUDI certificate with 2099 expiry is present in Cisco IoT FND container as cisco-ca.pem file, copy this to /opt/fnd/data in linux host.

```
docker cp fnd-container:/opt/cgms/server/cgms/conf/ciscosudi/cisco-ca.pem
/opt/fnd/data/
```

Step 7 Import the SUDI with 2099 expiry, that is, cisco-ca.pem to cgms_keystore.

```
# keytool -import -trustcacerts -keystore /opt/fnd/data/cgms_keystore
-alias sudi1 -file /opt/fnd/data/cisco-ca.pem
```

Step 8 Copy the **cisco-sudi-ca.pem** and **cisco-ca.pem** to the TPS server using the following command:

```
# scp ./cisco-ca.pem root@10.0.0.1
```

Here's an example output:

```
The authenticity of host '10.0.0.1 (10.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.1' (ECDSA) to the list of known hosts.
root@10.0.0.1's password:
cisco-ca.pem                                          100%   123KB 123.4KB/s   00:01
```

Step 9 Import certificates into the Java KeyStore using the `keytool` utility on the TPS server:

```
# keytool -import -trustcacerts -keystore /opt/cgms-tpsproxy/conf/cgms_keystore -alias cisco_sudi
-file ./cisco-sudi-ca.pem
keytool -import -trustcacerts -keystore /opt/cgms-tpsproxy/conf/cgms_keystore -alias cisco_sudi1
-file ./cisco-ca.pem
```

Step 10 Restart the container.

```
docker stop fnd-container
docker start fnd-container
```

Important
It is not advised to use the restart command. It is best practice to stop the container and then start the container so the services can stop gracefully. Sometimes restart will not be graceful and can lead to operational issues.

Step 11 After restart, verify that the contents of the cgms_keystore in the Cisco IoT FND container has same contents as that of the cgms_keystore in /opt/fnd/data of linux host using the below command.

```
# keytool -list -v -keystore -/opt/fnd/data/cgms_keystore
```

```
# docker exec -it fnd-container keytool -list -v -keystore /opt/cgms/server/cgms/conf/cgms_keystore
```

Step 12 To configure or change the cgms_keystore password, see Changing Password for more information.

- Changing Password, on page 23
- Managing Custom Web Certificates, on page 24
- Installing Custom Browser Certificates, on page 24
- Properties Used in Cisco IoT FND and TPS Configuration, on page 33

Changing Password

The cgms.properties file should contain the password for cgms_keystore, so that IoT FND application can access the cgms_keystore. Hence the first time cgms_keystore is created, encrypt the password of cgms_keystore and provide this encrypted password in cgms.properties file.

If at any time the password for cgms_keystore is changed, then the changed password has to be encrypted again and updated in the cgms.properties file.

Procedure

Step 1 Run the following command to encrypt the password for the new **cgms_keystore**. The sample is provided below.

```
# docker exec -it fnd-container /opt/cgms/bin/encryption_util.sh
encrypt <keystore password>
```

```
# docker exec -it fnd-container /opt/cgms/bin/encryption_util.sh
encrypt cisco123
#2bVvZsq+vsq94YxuAKdaag--
```

Step 2 Modify the **cgms.properties** file in the `/opt/fnd/data` folder, and edit the following line to set the new encrypted **cgms_keystore** password:

```
cgms-keystore-password-hidden=<encrypted new cgms_keystore password>
```

Note: With OVA 4.3.x and above, you can leave the `cgms_keystore.selfsigned` default bundled keystore untouched.

If both the files (**cgms_keystore** and **cgms_keystore.selfsigned**) are present, the **cgms_keystore** will be used by the container.

Managing Custom Web Certificates

Procedure

Step 1 The web certificate details are not retained after a reboot of Cisco IoT FND. You should perform a back up of the following files before you attempt to reboot Cisco IoT FND.

In the /opt/cgms/server/cgms/conf/ directory:

- jbossas.keystore.password
- jbossas.keystore
- VAULT.dat
- vault.keystore
- standalone.xml
- cgms.conf

Step 2 Copy the above files to their respective folders, and restart the Cisco IoT FND.

Installing Custom Browser Certificates

By default Cisco IoT FND installations use a self-signed certificate for HTTP or HTTPS communication using either a client web browser or the NB API client. If required, you can use certificates signed by your CA servers. This section presents installation procedures for these custom certificates.

BEFORE YOU BEGIN

- Clear the client browser cache.
- Remove existing certificates for the NMS server (by IP and DNS) on the client browser

  In Firefox, for example, select **Preferences** > **Advanced** > **Encryption** > **View Certifications**. Remove the certificates in the list for the respective server.
- Choose a common name to use in the signed certificate.

  This name requires a DNS entry that resolves to the NMS server IP address.
- Generate the new certificates and export them to a.PFX file.

  This file must contain the private keys, public certificate, and CA server certificates.

  See Use keytool to create the cgms_keystore file, on page 32 for the procedure to generate the private and public keys for the cgms_keystore file and export them to a .PFX file.

Install custom certificates in the browser client for Cisco IoT FND release 5.1 and later

This task helps you install custom certificates for a fresh install of Cisco IoT FND running Cisco IoT FND Release 5.1 and later releases.

Procedure

Step 1 Copy the certificate and private key *.pfx file from the host to the container:

Example:

```
docker cp custom_ca_cert.pfx fnd-container:/opt/cgms/server/cgms/conf/
```

a) Run `docker exec -i -t fnd-container /bin/bash` to enter the container.
b) Change the directory to `cd /opt/cgms/server/cgms/conf/`
c) On the NMS server, copy the existing `jbossas.keystore`, `jbossas.keystore.password`, `vault.keystore`, and `VAULT.dat files` from the `/opt/cgms/server/cgms/conf/` directory to a safe location.

Step 2 Determine the alias in the .PFX file that you plan to import into the new jbossas.keystore file:

Example:

```
#keytool -list -v -keystore custom_ca_cert.pfx -storetype pkcs12
```

Step 3 Enter the keystore password that you set when .PFX file was created

Example:

```
Enter the keystore password: keystore_password_when_pfx_file_was_created

Keystore type: PKCS12
Keystore provider: SunJSSE
Your keystore contains 1 entry
Alias name: lab5-win-2mfnersdbr3-ca
Creation date: Feb 23, 2025
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
…
```

a) Delete the existing jbossas.keystore from the `/opt/cgms/server/cgms/conf/` directory.
b) Import the new custom certificate, in .PFX file format into a new jbossas.keystore file; and, at the same time change the alias name to jboss. Follow the prompts:

Example:

```
keytool -importkeystore -v -srckeystore custom_ca_cert.pfx -srcstoretype pkcs12
-destkeystore /opt/cgms/server/cgms/conf/jbossas.keystore -deststoretype jks
-srcalias Alias name -destalias jboss -destkeypass your_keystore_password
```

The keystore password is stored in the `/opt/cgms/server/cgms/conf/VAULT.dat` file.

Step 4 Delete the following files:

a) Delete the **`vault.keystore`** file.
b) Delete the **`vault.dat`** file.
c) Create a new **`vault.keystore`** file:

Example:

```
/opt/cgms/jre/bin/keytool -genseckey -alias vault -storetype jceks
-keyalg AES -keysize 256 -storepass your_keystore_password -dname your_domain_name -keypass
-validity 730 -keystore vault.keystore
```

d) Update the vault.dat file with the new password:

Example:

```
/opt/cgms/bin/vault.sh --keystore /opt/cgms/server/cgms/conf/vault.keystore
 --keystore-password your_keystore_password --alias vault --vault-block keystore_pass
--attribute password --sec-attr your_keystore_password --enc-dir /opt/cgms/server/cgms/conf/
--iteration 50 --salt 12345678 -n
```

The vault.keystore contains the reference to vault.dat and vault.dat stores and hides the jboss keystore password. This command creates a new vault.dat file that contains the new jboss.keytsore password.

e) Copy `/opt/cgms/standalone/configuration/standalone.xml` to a safe location.

Step 5 Update the `/opt/cgms/standalone/configuration/standalone.xml`.

a) Replace the keystore password:

Example:

```
<vault>
<vault-option name="KEYSTORE_URL"
value="/opt/cgms/server/cgms/conf/vault.keystore"/>
<vault-option name="KEYSTORE_PASSWORD" value="MASK-0VKsAwH928fwt.3H2qUwOG"/>
<vault-option name="KEYSTORE_ALIAS" value="vault"/>
<vault-option name="SALT" value="12345678"/>
<vault-option name="ITERATION_COUNT" value="50"/>
<vault-option name="ENC_FILE_DIR" value="/opt/cgms/server/cgms/conf/"/>
</vault>
```

b) Edit `standalone.xml` and replace the existing section with the above.

c) Restart the CGMS service using `/etc/init.d/cgms/restart`.

d) Save and exit.

Step 6 Perform the following steps to retain the certificates upon container reloads.

a) Copy the files from `opt/cgms/server/cgms/conf/` to `/opt/fnd/data`

Note
If you see any of the following files in `/opt/fnd/data`, delete the files and then copy the files from the container using the following commands:

Example:

```
docker cp fnd-container: /opt/cgms/server/cgms/conf/jbossas.keystore /opt/fnd/data
docker cp fnd-container: /opt/cgms/server/cgms/conf/jbossas.keystore.password /opt/fnd/data
docker cp fnd-container: /opt/cgms/server/cgms/conf/vault.dat /opt/fnd/data
docker cp fnd-container: /opt/cgms/server/cgms/conf/vault.keystore /opt/fnd/data
docker cp fnd-container: /opt/cgms/standalone/configuration/stanalone.xml /opt/fnd/data
```

Step 7 Navigate to `/opt/fnd/scripts` and run the **`script upgrade.sh`** and enter option 2 **`custom web certificates`**

Step 8 Choose option 2 **`continer reload`** to reload the container

Step 9 Use your browser to connect to the NMS server.

a) Accept and add the new certificates.

b) Login to Cisco IoT FND.

c) Backup the following files in your local

- jbossas.keystore
- jbossas.keystore.password
- VAULT.dat
- vault.keystore
- standalone.xml

You've succesfully installed the custom certificates in the browser client for Cisco IoT FND 5.1 and later releases.

Retain custom certificates during Cisco IoT FND upgrades

This task helps you retain custom certificates from an older Cisco IoT FND version to the latest Cisco IoT FND version.

The `upgrade.sh` script needs the custom web certificate keystore (`jbossas.keystore`) in `/opt/fnd/data`. You must copy the `jbossas.keystore` to `/opt/fnd/data` so the OVA upgrade can locate and import the custom certificate.

Before you begin

- Ensure that you have custom certificates installed in your Cisco IoT FND. For more information see, Install custom browser certificates.
- Ensure that you are following the steps provided in the Upgrade Cisco IoT FND on OVA to perform an upgrade of your Cisco IoT FND.
- Ensure to login as a root user.

Procedure

Step 1 Get the upgrade package from Cisco and follow the steps in Upgrade Cisco IoT FND on OVA to upgrade your Cisco IoT FND.

Step 2 Run the RPM file.

Example:

```
http://10.78.81.200/fnd-postgres-ova/5.1.0/152/archive/upgrade-ova-5.1.0-152.rpm
rpm -Uvh --force upgrade-ova-5.1.0-152.rpm
```

The RPM verifies, prepares, and begins updating/installing.

Step 3 You change to `/opt/fnd/scripts/` and execute **`./upgrade.sh`**

Example:

```
Select the Type of Web certificate currently used
Option 1: FND Self Signed Certificate
Option 2: Custom Web Certificate
```

Step 4 Select **`Option 2: Custom Web Certificate`**

Example:

```
Enter option (1 or 2): 2
You selected Option 2 (Custom Web Certificate).
```

Step 5 The script reports a missing custom certificate keystore:

Example:

```
jbossas.keystore was not found in /opt/fnd/data.
Copy jbossas.keystore from /tmp to /opt/fnd/data and re-run the upgrade.
```

Step 6 Copy the `jbossas.keystore` from `/tmp/jbossas.keystore` to `/opt/fnd/data`

Example:

```
cp /tmp/jbossas.keystore /opt/fnd/data
```

Step 7 Re-run the **`./upgrade.sh`** script.

You've copied the custom certificates from a temporary directory to `/opt/fnd/data` which results in retaining the custom certificates to the upgraded Cisco IoT FND version.

Install custom certificates in the browser client

These steps assume that the Java environment has been set to use the Java bundled with Cisco IoT FND in `/opt/cgms/jre`.



Note Update the jbossas.keystore in Cisco IoT FND container. The keystore is present in: `/opt/cgms/server/cgms/conf/`. The name of the keystore is jbossas.keystore.

Procedure

Step 1 Copy the certificate and private key *.pfx file from the host to container.

```
docker cp custom_ca_cert.pfx fnd-container:/opt/cgms/server/cgms/conf/
```

Example:

```
docker cp 65_ca_cert.pfx fnd-container:/opt/cgms/server/cgms/conf/
```

Step 2 Run the following command to enter the container.

```
docker exec -i -t fnd-container /bin/bash
```

Step 3 Change directory to `/opt/cgms/server/cgms/conf/` in the container.

```
cd /opt/cgms/server/cgms/conf/
```

Step 4 On the NMS server, copy the existing jbossas.keystore, jbossas.keystore.password, vault.keystore, and VAULT.dat files from the `/opt/cgms/server/cgms/conf/` directory to a safe location.

Step 5 Determine the alias in the .PFX file that you plan to import into the new jbossas.keystore file:

```
#keytool -list -v -keystore custom_ca_cert.pfx -storetype pkcs12
```

Example:

```
#keytool -list -v -keystore 65_ca_cert.pfx -storetype pkcs12
```

Enter the keystore password: keystore_password_when_pfx_file_was_created

```
Keystore type: PKCS12
Keystore provider: SunJSSE

Your keystore contains 1 entry

Alias name: lab5-win-2mfnersdbr3-ca
Creation date: Feb 23, 2025
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
…
```

Step 6 Delete the existing jbossas.keystore from the `/opt/cgms/server/cgms/conf/` directory.

Step 7 Import the new custom certificate, in .PFX file format into a new jbossas.keystore file; and, at the same time change the alias name to **jboss**. Follow the prompts:

```
keytool -importkeystore -v -srckeystore  /opt/cgms/server/cgms/confcustom_ca_cert.pfx -srcstoretype
 pkcs12
-destkeystore /opt/cgms/server/cgms/conf/jbossas.keystore -deststoretype jks
-srcalias Alias name -destalias jboss -destkeypass your_keystore_password
```

Example:

```
keytool -importkeystore -v -srckeystore  /opt/cgms/server/cgms/conf65_ca_cert.pfx -srcstoretype
pkcs12
-destkeystore /opt/cgms/server/cgms/conf/jbossas.keystore -deststoretype jks
-srcalias lab5-win-2mfnersdbr3-ca -destalias jboss -destkeypass keystore
```

Step 8 The keystore password is stored in the `/opt/cgms/server/cgms/conf/VAULT.dat` file.

Perform the following steps to update the keystore password to match the one entered in Step 4 which is **`your_keystore_password`**.

- IoT FND releases 4.9.x and earlier
- IoT FND releases 4.10.x and later

Cisco IoT FND releases 4.9.x and earlier:

a) Delete vault.keystore file.
b) Delete VAULT.dat file.
c) Create a new vault.keystore file.

```
keytool -genseckey -alias vault -storetype jceks -keyalg AES -keysize 128 -storepass
your_keystore_password -keypass your_keystore_password -keystore
/opt/cgms/server/cgms/conf/vault.keystore
```

d) Update the VAULT.dat file with the new password:

```
//opt/cgms/bin/vault.sh -k /opt/cgms/server/cgms/conf/vault.keystore -p your_keystore_password
 -e /opt/cgms/server/cgms/conf -i 50 -s 12345678 -v vault -b keystore_pass -a password -x
your_keystore_password
```

If required you can optionally modify the iteration and salt values.

Example Output:

```
========================================================================
JBoss Vault
JBOSS_HOME:/opt/cgms
JAVA: java
========================================================================

Dec 20, 2018 3:25:29 PM org.picketbox.plugins.vault.PicketBoxSecurityVault init
INFO: PBOX000361: Default Security Vault Implementation Initialized and Ready
Secured attribute value has been stored in vault.
Please make note of the following:
********************************************
Vault Block:keystore_pass
Attribute Name:password
Configuration should be done as follows:
VAULT::keystore_pass::password::1
********************************************
Vault Configuration in AS7 config file:
********************************************
...
</extensions>
<vault>
<vault-option name=="KEYSTORE_URL"
value="/opt/cgms/server/cgms/conf/vault.keystore"/>
<vault-option name="KEYSTORE_PASSWORD" value="MASK-
VKsAwH928fwt.3H2qUwOG"/>
<vault-option name="KEYSTORE_ALIAS" value="vault"/>
<vault-option name="SALT" value="12345678"/>
<vault-option name="ITERATION_COUNT" value="50"/>
<vault-option name="ENC_FILE_DIR" value="/opt/cgms/server/cgms/conf/"/>
</vault><management>...
********************************************
```

The vault.keystore contains the reference to VAULT.dat and VAULT.dat stores and hides the jboss keystore password. This command creates a new VAULT.dat file that contains the new jboss.keytsore password.

Cisco IoT FND releases 4.10.x and later:

a) Delete `vault.keystore` file.
b) Delete VAULT.dat file.
c) Create a new vault.keystore file:

```
/opt/cgms/jre/bin/keytool -genseckey -alias vault -storetype jceks
-keyalg AES -keysize 256 -storepass your_keystore_password -dname your_domain_name -keypass
your_keystore_password -validity 730 -keystore vault.keystore
```

Example:

```
/opt/cgms/jre/bin/keytool -genseckey -alias vault -storetype jceks
-keyalg AES -keysize 256 -storepass keystore -dname
"CN=lab5-WIN-2MFNERSDBR3-CA,DC=lab5,DC=cisco,DC=com" -keypass keystore -validity 730 -keystore
 vault.keystore
```

d) Update the VAULT.dat file with the new password:

```
/opt/cgms/bin/vault.sh --keystore /opt/cgms/server/cgms/conf/vault.keystore
 --keystore-password your_keystore_password --alias vault --vault-block keystore_pass
--attribute password --sec-attr your_keystore_password --enc-dir /opt/cgms/server/cgms/conf/
--iteration 50 --salt 12345678 -n
```

If required you can optionally modify the iteration and salt values.

Expected Output:

```
========================================================
```

```
  JBoss Vault

  JBOSS_HOME: /opt/cgms

  JAVA: /opt/cgms/jre/bin/java

================================================================================

WFLYSEC0047: Secured attribute value has been stored in Vault.
Please make note of the following:
********************************************
Vault Block:keystore_pass
Attribute Name:password
Configuration should be done as follows:
VAULT::keystore_pass::password::1
********************************************
WFLYSEC0048: Vault Configuration commands in WildFly for CLI:
********************************************
For standalone mode:
/core-service=vault:add(vault-options=[("KEYSTORE_URL" =>
"/opt/cgms/server/cgms/conf/vault.keystore"),
("KEYSTORE_PASSWORD" => "MASK-0VKsAwH928fwt.3H2qUwOG"),("KEYSTORE_ALIAS" => "vault"),
("SALT" => "12345678"),("ITERATION_COUNT" => "50"),("ENC_FILE_DIR" =>
"/opt/cgms/server/cgms/conf/")])
********************************************
For domain mode:
/host=the_host/core-service=vault:add(vault-options=[("KEYSTORE_URL" =>
"/opt/cgms/server/cgms/conf/vault.keystore"),
("KEYSTORE_PASSWORD" => "MASK-0VKsAwH928fwt.3H2qUwOG"),("KEYSTORE_ALIAS" => "vault"),
("SALT" => "12345678"),("ITERATION_COUNT" => "50"),("ENC_FILE_DIR" =>
 "/opt/cgms/server/cgms/conf/")])
********************************************
```

The vault.keystore contains the reference to VAULT.dat and VAULT.dat stores and hides the jboss keystore password. This command creates a new VAULT.dat file that contains the new jboss.keytsore password.

Step 9 Copy `/opt/cgms/standalone/configuration/standalone.xml` and standalone-cluster.xml to a safe location.

Step 10 Update the `/opt/cgms/standalone/configuration/standalone.xml` or standalone-cluster.xml file.

Depending on whether the Cisco IoT FND server is standalone or clustered, you can update the respective file.

a) Replace the keystore password with the output in Step 5.

```
<vault>
<vault-option name="KEYSTORE_URL"
value="/opt/cgms/server/cgms/conf/vault.keystore"/>
<vault-option name="KEYSTORE_PASSWORD" value="0"/>
<vault-option name="KEYSTORE_ALIAS" value="vault"/>
<vault-option name="SALT" value="12345678"/>
<vault-option name="ITERATION_COUNT" value="50"/>
<vault-option name="ENC_FILE_DIR" value="/opt/cgms/server/cgms/conf/"/>
</vault>
```

b) Edit standalone.xml or standalone-cluster.xml and replace the existing <vault> section with the above. Save and exit.

Step 11 Restart the CGMS service by running the command:

```
/etc/init.d/cgms restart
```

Note

If your Cisco IoT FND is running Cisco IoT FND Release 5.0 and earlier releases, your certificate information gets lost when you perform the CGMS restart. You must install the custom certificates once again.

Step 12 Use your browser to connect to the NMS server.

Step 13 Accept and add the new certificates.

Step 14 Use your browser to log in to Cisco IoT FND.

Note
Back up the following files to the local host before you restart or upgrade the container to prevent it from replacing the custom web certificates with self-signed certificates.

- jbossas.keystore,
- jbossas.keystore.password,
- VAULT.dat,
- vault.keystore,
- standalone.xml, and
- standalone-cluster.xml.

Use keytool to create the cgms_keystore file

Use the instructions provided in this section to create the cgms_keystore file for both Cisco IoT FND and the TPS proxy.

Procedure

Step 1 Enter the following command on the Cisco IoT FND or TPS proxy server as root to view the contents of the .PFX file.

```
[root@ tps_server
~]# keytool -list -v -keystore nms_cert.pfx -srcstoretype pkcs12
```

Note
You can get the alias name from the .PFX file during import.

Step 2 Enter the keystore password when prompted.

The password is the same as the one you used for creating the .PFX file.

The alias name is displayed as part of the information as given in this Example 1. You can use this alias name in the command to import the certificates into the cgms_keystore file.

Step 3 Enter the following command to import the certificates into the cgms_keystore file:

```
keytool -importkeystore -v -srckeystore
filename.pfx -srcstoretype pkcs12
-destkeystore cgms_keystore -deststoretype jks -srcalias alias_name
-destalias cgms
```

```
-destkeypass
'keystore_password'
```

Step 4 Enter the destination keystore password when prompted.

Step 5 Re-enter the keystore password when prompted.

Step 6 Enter the password you used earlier while creating the .PFX file (either *nms_cert.pfx* or *tps_cert.pfx*) when prompted for the source keystore password.

Example 1:

To view the *nms_cert.pfx* file and access the alias name, enter the following commands as root:

```
# keytool -list -v -keystore nms_cert.pfx -srcstoretype pkcs12
Enter keystore password: keystore
Keystore type: PKCS12
Keystone provider: SunJSSE
Your keystore contains 1 entry
Alias name: le-cgnms-75edd1e3-7e65-41b4-97f1-a913ebf21c8b
Creation date: March 29.2018
Entry type: PrivateKey Entry
Certificate chain length: 3
Certificate[1]:
Owner: CN=nms.sgbu.cisco.com
Issuer: CN=cisco-RSA-SUBCA-CA, DC=cisco, DC=com
...
```

Note
This example diplays the steps for the *nms_cert.pfx*. To view the details on the *tps_cert.pfx* and import the certificates to the TPS proxy, use the same commands but replace the references to *nms_cert.pfx* with *tps_cert.pfx*, and use the alias name from the *tps_cert.pfx* file.

Example 2:

To import the certificates to the **cgms_keystore** file on Cisco IoT FND, enter the following commands as root:

```
# keytool -importkeystore -v
-srckeystore nms_cert.pfx -srcstoretype pkcs12
-destkeystore cgms_keystore -deststoretype jks -srcalias
le-cgnms-75edd1e3-7e65-41b4-97f1-a913ebf21c8b -destalias cgms
-destkeypass
'keystore_password'

Enter destination keystore password: keystore_password
Re-enter new password: keystore_password
Enter source keystore password: keystore
...Storing cgms_keystore
```

Note
The **storing** *cgms* **_keystore** text indicates successful completion.

Properties Used in Cisco IoT FND and TPS Configuration

The Cisco Gateway Management System (CGMS) and TPSPROXY properties that are available for configuration in Cisco IoT FND and TPS are as given:

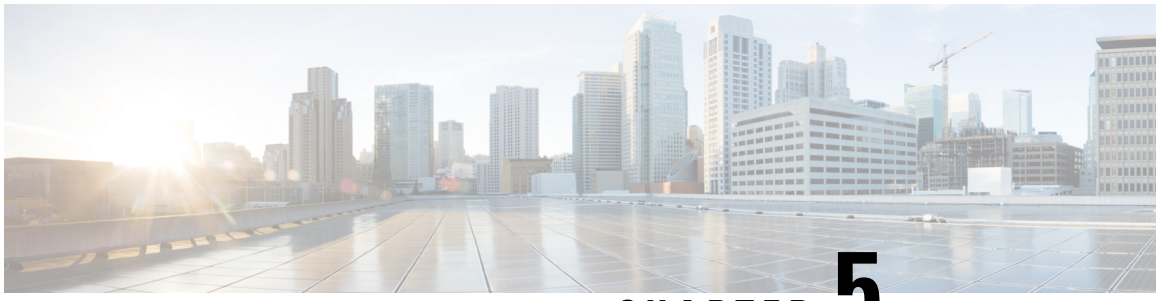
CGMS Properties

Property Name	Example Value	Description
cgms-keystore-password-hidden=	< encrypted >	Encrypted password for the cgms keystore. Encrypt or decrypt with encryption_util.sh.
hsm-keystore-name=	testGroup1	HSM partition name.
hsm-keystore-password=	< encrypted >	Encrypted HSM partition password.
security-module=	ssm/hsm	Type of security module being used.
ssm-host=	<ipv4 address >	IP Address of SSM server.
ssm-port=	8445	Port of SSM server.
ssm-keystore-alias=	ssm_csmp	Alias name for SSM certificate in keystore.
ssm-keystore-password=	< encrypted >	Encrypted password for the SSM keystore.
ssm-key-password=	< encrypted >	Encrypted key for the SSM key.
multicast-interface-address=	< ipv6 address >	Cisco IoT FND IPv6 source address for multicast traffic.
dhcpV4ClientListenAddresses=	<ipv4 address >	IPv4 address on your Cisco IoT FND server used to exchange DHCPv4 messages.
dhcpV6ClientListenAddresses=	< ipv6 address >	IPv6 address on your Cisco IoT FND server used to exchange DHCPv6 messages.
optimizeTunnelProv=	true/false	Indicates whether or not to lock the HER during tunnel provisioning.
allowed-outage-skew=	5000	Allow outage skew in seconds, for outage or restoration events.
rf.validate-firmware-tlvs=	true/false	Skips CG-Mesh device firmware validation.
googleMapsClientId=	< Client ID >	Google maps client ID.
googleMapsApiKey=	< API key >	Google maps API key.
enable-bootstrap-service=	true/false	Used to enable PNP bootstrapping service.

Property Name	Example Value	Description
scep-url=	http(s) :// < url of SCEP server >	URL of SCEP server.
ca-fingerprint=	< fingerprint of CA certificate >	Fingerprint of CA certificate.
proxy-bootstrap-ip=	<ipv4/v6 address or FQDN >	PNP server identity sent by Cisco IoT FND to the PNP agent.
bootstrap-fnd-alias=	subca	Alias name assigned to the CA certificate from the issuer in the Cisco IoT FND keystore.
pnp-server-port=	9125	PNP server port, default is 9125.
pnp-install-trustpool=	true/false	Send the CA bundle file which includes well known public CA certificates.
reload-during-bootstrap=	true/false	Indicates whether or not to reload a device after PNP boostrapping.
router-file-upload-retries	0	Number of retries for router file upload job
router-firmware-upload-retries	0	Number of retries for the firmware upload job.
router-firmware-install-retries	0	Number of retries for the firmware install job.
collect-cellular-link-metrics	true/false	Indicates whether or not to collect cellular metrics.
collect-cellular-link-metrics-interval	30	Interval for cellular metrics.
router-firmware-upload-timeout-minutes=	30	Firmware upload job timeout duration in minutes.
router-firmware-install-timeout-minutes=	60	Firmware install job timeout duration in minutes.
cgr-ha-fetch-mesh-key-attempts	3	Number of attempts to fetch the mesh keys.
cgr-ha-fetch-mesh-key-delay-mins	1	Number of minutes or interval between mesh-key-attempts.

TPSPROXY Properties

Property Name	Example Value	Description
cgdm-tpsproxy-addr=	<ipv4/v6 address or FQDN >	Source IP address of messages coming from the TPSProxy.
cgdm-tpsproxy-subject=	CN="common_name", OU="organizational_unit", O="organization", L="location", ST="state", C="country"	The exact certificate subject contained in the TPSPROXY's certificate.
bootstrap-proxy-listen-port=	9125	Port on which TPS is listening for HTTP traffic.
inbound-bsproxy-destination=	<ipv4/v6 address or FQDN >	IP address and port to forward info received from the router over HTTP.
outbound-proxy-allowed-addresses=	<ipv4/v6 address or FQDN >	Comma separated list of FQDN/IP addresses, the proxy allows outbound messages to originate from it.



CHAPTER 5

Configuring IoT FND for IPv6 Tunnel Provisioning and Registration

IoT FND OVA supports only IPv4 tunnels and Registration out of the box.

To setup an IPv6 network for tunnel provisioning and registration, follow these steps:

Procedure

Step 1 Ensure you have one interface with a valid IPv6 network which has a IPv6 prefix length less than125.

See the following example of the ens224 interface:

```
[root@iot-fnd ~]# ifconfig ens224
ens224: flags=4163[UP,BROADCAST,RUNNING,MULTICAST] mtu 1500
inet 2.2.56.117 netmask 255.255.0.0 broadcast 2.2.255.255
inet6 fe80::54f0:5d24:d320:8e38 prefixlen 64 scopeid 0x20[ink]
inet6 2001:420:7bf:5f::1522 prefixlen 64 scopeid 0x0[global]
ether 00:0c:29:18:1b:3a txqueuelen 1000 (Ethernet)
RX packets 97618 bytes 12391774 (11.8 MiB)
RX errors 1001 dropped 1011 overruns 0 frame 0
TX packets 3004 bytes 568097 (554.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[root@iot-fnd ~]#
```

Step 2 Run the `./setup-IPv6-network.sh` script in the `/opt/fnd/scripts` directory to obtain the FND IPv6 address on the router for tunnel provisioning and registration.

Note: While specifying the IPv6 address for the network-mgmt-bridge, provide an Interface Name and a valid IPv6 address (and IP address prefix length) that is in the subnet of the provided host interface. If IPv6 address is in a different subnet, the IPv6 tunnel provisioning and registration will not be successful.

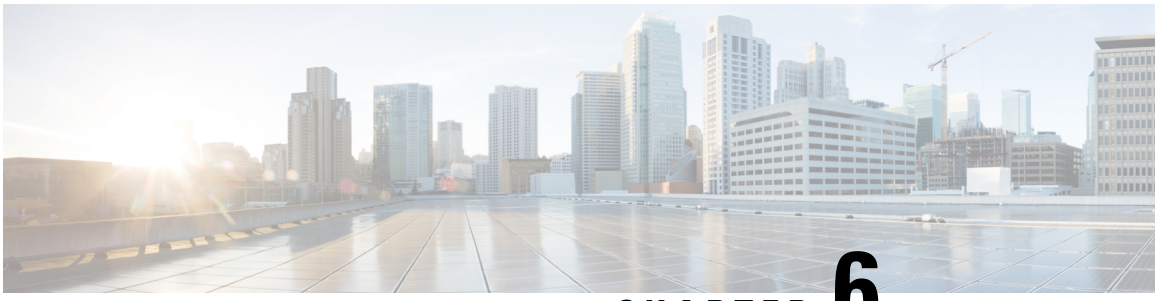
```
[root@iot-fnd scripts]# ./setup-IPv6-network.sh

Setup IPv6 Network For Containers
IPv6 Network setup process will require an active interface with a Global IPv6 Address.
IPv6 prefix length must be less than 125.

Enter Interface Name: ens32
Enter IPv6 Address: 2001:1111:2222:0:20c:29ff:fe44:ea4d
Enter IPv6 Prefix Length: 64

One of the IPv6 networks in /125 subnet from 2001:1111:2222:0:20c:29ff:fe44:ea4d/64 will be required to setup container network.
Enter IPv6 Address for network-mgmt-bridge from /125 subnet: 2001:1111:2222:0:20c:29ff:fe44:1515

Preparing Network Configuration...
Stopping Watchdog...
Stopping FND container...
Stopping FogD container...
Removing FND container...
Removing FogD container...
Prune Docker container...
Removing Docker network...
Configure Docker network for v6...
e6de98f5f67eea1c77491500e19c897eeac35b96cf718f0ac3f9bf2fb59b3836
Starting FND container...
6664d4178b244043a18aa2bfb1014a8cc2ce9faa7aa86ac1d9aa89f01e7df7d3
Starting Fog Director container...
fe93771cd31c731276376a47a5ed34d86a6a8b70c4064d9923d7076170193d9b
Configure containers for v6...
Starting Watchdog...
Configured IPv6 network on the containers
Please use following FND IPv6 address with prefix length 2001:1111:2222:0:20c:29ff:fe44:1511/125 on the router for IPv6 Tunnel Provisioning and Registration
```



CHAPTER 6

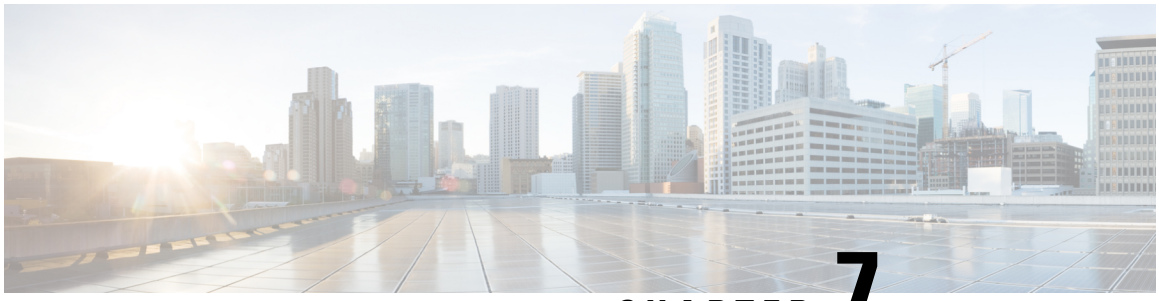
Starting and Stopping FND

Use the **fnd-container.sh {start|stop|status|restart}** script in the following directory to start, stop, obtain status, and restart FND:

cd /opt/fnd/scripts/

```
[root@iot-fnd scripts]# ./fnd-container.sh status
fnd-container is running, pid=22745
CONTAINER ID        NAME                CPU %               MEM USAGE / LIMIT     MEM %               NET I/O             BLOCK I/O           PIDS
4bc00c18b2c8        fnd-container       1.99%               1.064GiB / 23.38GiB   4.55%               8.63MB / 8.07MB     0B / 1.76MB         272
[root@iot-fnd scripts]# ./fnd-container.sh stop
Stopping FND container...
fnd-container
[root@iot-fnd scripts]# ./fnd-container.sh start
[root@iot-fnd scripts]# Starting FND container...
fnd-container

[root@iot-fnd scripts]# ./fnd-container.sh restart
Stopping FND container...
fnd-container
[root@iot-fnd scripts]# Starting FND container...
fnd-container
```



CHAPTER 7

Starting and Stopping Fog Director

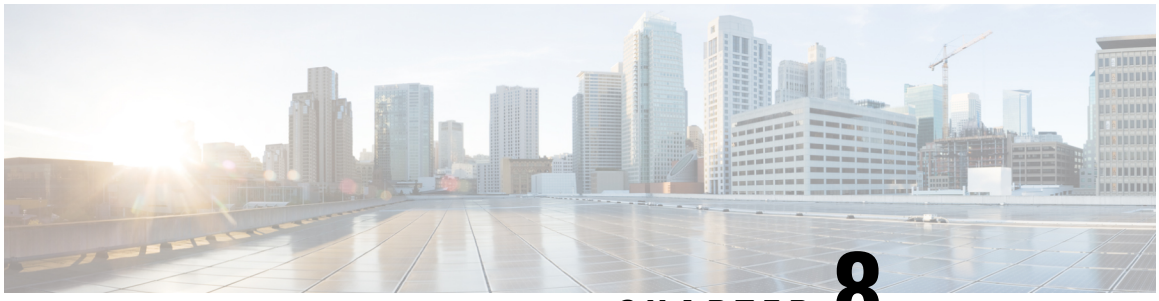
Use the **fogd-container.sh {start|stop|status|restart}** script in the following directory to start, stop, obtain status, and restart Fog Director:

```
cd /opt/fogd/scripts
```

```
[root@iot-fnd scripts]# ./fogd-container.sh stop
Stopping Fog Director container...
fogd-container
[root@iot-fnd scripts]# ./fogd-container.sh start
[root@iot-fnd scripts]# Starting Fog Director container...
fogd-container

[root@iot-fnd scripts]# ./fogd-container.sh status
fogd-container is running, pid=10759
CONTAINER ID        NAME                CPU %               MEM USAGE / LIMIT     MEM %               NET I/O             BLOCK I/O           PIDS
f2bc75fa77c2        fogd-container      2.00%               764.6MiB / 23.38GiB   3.19%               849kB / 1.5MB       0B / 41kB           119
[root@iot-fnd scripts]# ./fogd-container.sh restart
Stopping Fog Director container...
fogd-container
[root@iot-fnd scripts]# Starting Fog Director container...
fogd-container

[root@iot-fnd scripts]#
```



CHAPTER 8

Upgrade Cisco IoT FND on OVA

- Device compatibility check, on page 43
- Check the Postgres DB status, on page 43
- Cisco IoT FND on OVA upgrade matrix, on page 46
- Verify and reset the expired root password , on page 47
- Upgrade the database and docker server image, on page 48
- Upgrade Cisco IoT FND container images, on page 51
- Check DB and status post upgrade, on page 53
- Upgrade RHEL version, on page 55

Device compatibility check

Use the following to check for the validated device versions that are compatible with Cisco IoT FND Release 5.0. The release versions mentioned in this topic are only the list of validated versions by Cisco IoT FND and is not exhaustive. We recommend you to upgrade your devices to these validated versions, and it is not a mandate.

- FAR compatibility: See supported device types and versions on Cisco IoT FND Release Notes 5.0
- HER compatibility: See supported device types and versions on Cisco IoT FND Release Notes 5.0
- HSM compatibility: See upgrade hardware security module compatibility on Cisco IoT FND Release Notes 5.0
- TPS compatibility: The TPS server version must match the Cisco IoT FND release version. For example, If you're upgrading to Cisco IoT FND Release 5.0 from Cisco IoT FND Release 4.12.1, your TPS server should be upgraded to Cisco IoT FND Release 5.0.
- Cisco IoT FND compatibility: On initial installation, upgrade the OpenSSH package in the Cisco IoT FND server to RHEL version 8.8 and later versions.

Check the Postgres DB status

Performing this task helps you verify the system and database status before upgrading Cisco IoT FND on OVA.

Before you begin

- Take a snapshot of the existing VM before you upgrade.
- Perform a backup of **cgms.properties** file and **cgms_keystore** file in the location, /opt/fnd/data/. You can either SCP these files to another server for backup or you can copy in the same or different folder. Here's an example:

```
root@iot-fnd:~[root@iot-fnd ~]#
              root@iot-fnd:~[root@iot-fnd ~]# cd /opt/fnd/data
              root@iot-fnd:/opt/fnd/data[root@iot-fnd data]#
              root@iot-fnd:/opt/fnd/data[root@iot-fnd data]#ls
              cgms_keystore  cgms.properties  cisco-sudi-ca.pem  userPropertyTypes.xml

              root@iot-fnd:/opt/fnd/data[root@iot-fnd data]#
              root@iot-fnd:/opt/fnd/data[root@iot-fnd data]# cp cgms.properties
cgms.properties_backup_09May2025
              [root@iot-fnd data]# keytool -importkeystore -srckeystore cgms_keystore
-destkeystore cgms_keystore_backup_9May2022 -deststoretype PKCS12
              Importing keystore cgms_keystore to cgms_keystore_backup_9May2022...
              Enter destination keystore password:
              Re-enter new password:
              Enter source keystore password:
              Entry for alias cgms successfully imported.
              Entry for alias cisco_sudi successfully imported.
              Entry for alias jmarconi successfully imported.
              Import command completed:  3 entries successfully imported, 0 entries
failed or cancelled
              [root@iot-fnd data]#
              [root@iot-fnd data]# ls
              cgms_keystore                 cgms_keystore.selfsigned
cgms.properties_backup_09May2022  fnd_psk.keystore
             cgms_keystore_backup_9May2025  cgms.properties          cisco-sudi-ca.pem
                 userPropertyTypes.xml
              [root@iot-fnd data]#
```

- Ensure that the Postgres services are running before perfomring an upgrade.

Procedure

Step 1 Using the SSH terminal and navigate to the root directory.

Step 2 Run the following command:

Example:

```
/opt/scripts/status.sh
```

```
[root@iot-fnd ~]# /opt/scripts/status.sh
            --------------------
            ● postgresql-12.service - PostgreSQL 12 database server
            Loaded: loaded (/usr/lib/systemd/system/postgresql-12.service; enabled; vendor preset:
disabled)
            Active: active (running) since Mon 2022-05-09 02:01:29 PDT; 2h 6min ago
            Docs: https://www.postgresql.org/docs/12/static/
            Main PID: 27638 (postmaster)
            Tasks: 26
            Memory: 250.5M
            CGroup: /system.slice/postgresql-12.service
            --------------------
            ● influxdb.service - InfluxDB is an open-source, distributed, time series database
          Loaded: loaded (/usr/lib/systemd/system/influxdb.service; enabled; vendor preset: disabled)
```

```
             Active: active (running) since Mon 2022-05-09 02:02:39 PDT; 2h 5min ago
             Docs: https://docs.influxdata.com/influxdb/
             Main PID: 27892 (influxd)
             Tasks: 21
             Memory: 219.0M
             --------------------
             ● kapacitor.service - Time series data processing engine.
             Loaded: loaded (/usr/lib/systemd/system/kapacitor.service; enabled; vendor preset:
disabled)
             Active: active (running) since Mon 2022-05-09 02:02:06 PDT; 2h 5min ago
             Docs: https://github.com/influxdb/kapacitor
             Main PID: 27805 (kapacitord)
             Tasks: 14
             Memory: 21.0M
             --------------------
             fnd-container is running, pid=61255
             CONTAINER ID        NAME                CPU %               MEM USAGE / LIMIT     MEM %
                NET I/O             BLOCK I/O           PIDS
             a02e6388607d        fnd-container       6.44%               2.612GiB / 23.38GiB   11.17%
               17MB / 13.7MB       20.3MB / 2.64MB     580
             --------------------
             fogd-container is running, pid=63469
             CONTAINER ID        NAME                CPU %               MEM USAGE / LIMIT     MEM %
               NET I/O             BLOCK I/O           PIDS
             a40aa29e2392        fogd-container      6.38%               2.18GiB / 23.38GiB    9.32%
               434kB / 135kB       8.19kB / 145kB      99
             --------------------
             [root@iot-fnd ~]#
             docker version
             [root@iot-fnd ~]# docker version
             Client: Docker Engine - Community
             Version:           19.03.15
             API version:       1.40
             Go version:        go1.13.15
             Git commit:        99e3ed8919
             Built:             Sat Jan 30 03:17:57 2021
             OS/Arch:           linux/amd64
             Experimental:      false
             Server: Docker Engine - Community
             Engine:
             Version:          19.03.15
             API version:      1.40 (minimum version 1.12)
             Go version:       go1.13.15
             Git commit:       99e3ed8919
             Built:            Sat Jan 30 03:16:33 2021
             OS/Arch:          linux/amd64
             Experimental:     false
             containerd:
             Version:          1.4.4
             GitCommit:        05f951a3781f4f2c1911b05e61c160e9c30eaa8e
             runc:
             Version:          1.0.0-rc93
             GitCommit:        12644e614e25b05da6fd08a38ffa0cfe1903fdec
             docker-init:
             Version:          0.18.0
             GitCommit:        fec3683
             You have new mail in /var/spool/mail/root
             [root@iot-fnd ~]#
             /opt/fnd/scripts/fnd-container.sh status
             [root@iot-fnd ~]# /opt/fnd/scripts/fnd-container.sh status
             fnd-container is running, pid=61255
             CONTAINER ID        NAME                CPU %               MEM USAGE / LIMIT     MEM %
                NET I/O             BLOCK I/O           PIDS
             a02e6388607d        fnd-container       6.47%               2.613GiB / 23.38GiB   11.18%
```

```
  17MB / 13.8MB       20.3MB / 2.64MB     592
[root@iot-fnd ~]#
You have new mail in /var/spool/mail/root
[root@iot-fnd ~]#
docker exec -it fnd-container /etc/init.d/cgms status
[root@iot-fnd ~]# docker exec -it fnd-container /etc/init.d/cgms status
IoT-FND Version 4.7.2-8
05-09-2022 04:09:46 PDT: INFO: IoT-FND database server: 192.68.5.1
05-09-2022 04:09:47 PDT: INFO: IoT-FND database connection verified.
05-09-2022 04:09:47 PDT: INFO: IoT FND timeseries database server: 192.68.5.1
05-09-2022 04:09:47 PDT: INFO: IoT FND kapacitor server: 192.68.5.1
05-09-2022 04:09:47 PDT: INFO: IoT-FND timeseries database/kapacitor connection verified.

05-09-2022 04:09:49 PDT: INFO: IoT-FND application server is up and running.
05-09-2022 04:09:50 PDT: INFO: IoT-FND is up and running.
[root@iot-fnd ~]#
rpm -qa | grep -i postgres
root@iot-fnd:/opt/fnd/data[root@iot-fnd data]# rpm -qa | grep -i postgres
postgresql96-devel-9.6.15-1PGDG.rhel7.x86_64
postgresql96-libs-9.6.15-1PGDG.rhel7.x86_64
postgresql96-server-9.6.15-1PGDG.rhel7.x86_64
postgresql96-9.6.15-1PGDG.rhel7.x86_64
cgms-postgres-4.5.1-11.x86_64
postgresql96-contrib-9.6.15-1PGDG.rhel7.x86_64
root@iot-fnd:/opt/fnd/data[root@iot-fnd data]#
```

You can view all the statuses of your Cisco IoT FND on OVA before proceeding with an upgrade.

Cisco IoT FND on OVA upgrade matrix

The following table provides a detailed overview of the versions of different software components bundled with each Cisco IoT FND release.

Cisco IoT FND version	Postgres version	Docker server version	RHEL OS version
5.0.0	12.12	19.03.15	8.10
4.12.0	12.12	19.03.15	8.8
4.11.0	12.12	19.03.15	8.8
4.10.0	12.12	19.03.15	8.7
4.9.1	12.12	19.03.15	8.6
4.9.0	12.9	19.03.15	8.6

Verify and reset the expired root password

The root password must be valid and active before running the Cisco IoT FND upgrade. During the upgrade, scripts invoke sudo to execute multiple commands. If the root password has expired or is not set, sudo authentication fails. As a result, the upgrade stops..

Before you begin

Use these steps to verify the status of the root password and reset it if it has expired:

Procedure

Step 1 Enter the ESXi server's Internet Protocol (IP) address in a web browser and log in with your ESXi credentials.

Step 2 From the left pane, select the Cisco IoT FND VM.

Step 3 Click **Console** and select **Open Console in new tab**.

The RHEL server launches.

Step 4 Log in with your Cisco IoT FND server user credentials.

Step 5 Access the Cisco IoT FND Shell terminal.

Step 6 Enter the following command to verify the root password status:

Example:

```
[fnduser@iot-fnd ~]$ sudo -i
[root@iot-fnd ~]# sudo test
```

Table 2: Root password status

If the root password is	Then
active `[root@iot-fnd ~]#`	you can run the upgrade script. For upgrade instructions, refer to the next topics in this chapter.

expired and the sudo authentication fails with the following error:
`sudo: Account or password is expired, reset your password and try again`
`Current password:`
`sudo: unable to change expired password: Authentication token manipulation error`
	you must reset the root password. For instructions, go to step 7

Step 7 Run the following command to reset the root password:

Example:

```
[root@iot-fnd ~]# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Step 8 Run the following command to verify the sudo command.

Example:

```
[root@iot-fnd ~]# sudo test
[root@iot-fnd ~]#
```

After the root password is active, sudo commands will run successfully without authentication errors during the upgrade.

Upgrade the database and docker server image

To ensure compatibility and security, upgrade the database and docker server image for Cisco IoT FND.

To upgrade the database and the docker server image, run the rpm scripts and auto-integrate the DB with Cisco IoT FND scripts.

Before you begin

- Cisco IoT FND OVA upgrade will not upgrade the RHEL OS version. The RHEL version differs for different versions of Cisco IoT FND. After upgrading the OVA, we recommend you to upgrade the OS sooner than later. Although Cisco IoT FND is a secure application, OS security and patches must be regularly updated in accordance to guidance from Cisco.
- Ensure that you use the following procedure to upgrade from Cisco IoT FND Release 4.9.x, 4.10.x, 4.11.x, and 4.12.x versions to Cisco IoT FND Release 5.0.x

Procedure

Step 1 Obtain the Cisco IoT FND upgrade scripts from Cisco.

Step 2 Check the RHEL OS version before upgrading Cisco IoT FND OVA to Cisco IoT FND Release 5.0 or higher.

Example:

```
[root@fnd451testupgrade ~]# hostnamectl
            Static hostname: fnd451testupgrade
            Icon name: computer-vm
            Chassis: vm
            Machine ID: 58eb8d728d834d28ad426eca3c9b9c4e
            Boot ID: 40511dab9f4b4beaa8de82fb105423c9
            Virtualization: vmware
            Operating System: Red Hat Enterprise Linux
            CPE OS Name: cpe:/o:redhat:enterprise_linux:7.5:GA:server
            Kernel: Linux 3.10.0-862.el7.x86_64
            Architecture: x86-64
            [root@fnd451testupgrade ~]#r
```

Step 3 Extract the cgms rpms files to the Cisco IoT FND server.

Example:

If you are upgrading the DB and the docker server image for Cisco IoT FND release 5.0:

a. Download the following upgrade script from Cisco.

CISCO-IOTFND-VPI-K9-UPGRADE-SCRIPTS-5.0-101.zip

b. Extract the file to get the rpm:

upgrade-ova-5.0-101.rpm

c. Transfer the extracted rpm file to the Cisco IoT FND server.

Step 4 Navigate to the directory where the rpm file is located.

Example:

cd /opt or any directory where the *upgrade-ova-5.0-101.rpm file* is copied.

Step 5 Run the following upgrade script:

Example:

```
rpm -Uvh upgrade-ova-<release>-<build number>.rpm
```

```
root@iot-fnd:/opt[root@iot-fnd opt]# rpm -Uvh upgrade-ova-5-0-2-8.rpm
            Preparing...
            (1%)###############(100%)

            Updating / installing...
            1:upgrade-ova-5-0-2-8
            (1%)###############(100%)
            Started installer in background. Please check ~/rpm.log in few minutes for details.
            root@iot-fnd:/optYou have new mail in /var/spool/mail/root
            [root@iot-fnd opt]#
            Mon May  9 01:59:29 PDT 2022 Background installer started
            Mon May  9 01:59:29 PDT 2022 Please wait until the 'RPM installation completed' message
 is logged
            Mon May  9 01:59:29 PDT 2022 Upgrading cgms-postgres-5.0.2-8.x86_64.rpm
            Preparing...                          ########################################
            Updating / installing...
            cgms-postgres-5.0.2-8                 ########################################
            Cleaning up / removing...
            cgms-postgres-5.0-101                ########################################
            Mon May  9 01:59:47 PDT 2022 Upgrading cgms-influx-4.7.2-8.x86_64.rpm
            Preparing...                          ########################################
            Updating / installing...
            cgms-influx-5.0.2-8                   ########################################
            Cleaning up / removing...
            cgms-influx-5.0-101                  ########################################
            Mon May  9 02:00:04 PDT 2022 Upgrading monit-5.25.3-1.el7.x86_64.rpm
            warning: monit-5.25.3-1.el7.x86_64.rpm: Header V4 RSA/SHA1 Signature, key ID 222b0e83:
NOKEY
            Preparing...                          ########################################
            package monit-5.25.3-1.el7.x86_64 is already installed
            Mon May  9 02:00:18 PDT 2022 Stopping services
            Mon May  9 02:00:58 PDT 2022 Upgrading Postgresql to 12.5
            Preparing...                          ########################################
            Updating / installing...
            postgresql12-libs-12.5-1PGDG.rhel7    ########################################
            postgresql12-12.5-1PGDG.rhel7         ########################################
            postgresql12-server-12.5-1PGDG.rhel7  ########################################
            postgresql12-contrib-12.5-1PGDG.rhel7 ########################################
            Cleaning up / removing...
            postgresql12-contrib-12.4-1PGDG.rhel7 ########################################
            postgresql12-server-12.4-1PGDG.rhel7  ########################################
            postgresql12-12.4-1PGDG.rhel7         ########################################
            postgresql12-libs-12.4-1PGDG.rhel7    ########################################
            Mon May  9 02:01:27 PDT 2022 Restarting Postgresql
            Mon May  9 02:01:40 PDT 2022 Stopping InfluxDB and Kapacitor
            Mon May  9 02:01:50 PDT 2022 Upgrading influxdb-1.8.3.x86_64.rpm
```

```
            Preparing...                          ########################################
            Updating / installing...
            influxdb-1.8.3-1                      warning: /etc/influxdb/influxdb.conf created as
/etc/influxdb/influxdb.conf.rpmnew
            ########################################
            Cleaning up / removing...
            influxdb-1.5.3-1                      ########################################
            Mon May  9 02:02:02 PDT 2022 Upgrading kapacitor-1.5.7-1.x86_64.rpm
            Preparing...                          ########################################
            Updating / installing...
            kapacitor-1.5.7-1                     warning: /etc/kapacitor/kapacitor.conf created as
 /etc/kapacitor/kapacitor.conf.rpmnew
            ########################################
            Cleaning up / removing...
            kapacitor-1.5.0-1                     ########################################
            Mon May  9 02:02:06 PDT 2022 Restarting InfluxDB and Kapacitor
            Mon May  9 02:02:20 PDT 2022 Stopping Docker
            Mon May  9 02:02:26 PDT 2022 Upgrading Docker to 19.03.15
            warning: container-selinux-2.119.2-1.911c772.el7_8.noarch.rpm: Header V3 RSA/SHA256
Signature, key ID f4a80eb5: NOKEY
            Preparing...
            (1%)###############(100%)
            Updating / installing...
            1:container-selinux-2:2.119.2-1.911
            (1%)###############(100%)
            Cleaning up / removing...
            2:container-selinux-2:2.42-1.gitad8
            (1%)###############(100%)
            Preparing...
            (1%)###############(100%)

            Updating / installing...
            1:docker-ce-cli-1:19.03.15-3.el7
            (1%)###############(100%)
            2:containerd.io-1.4.4-3.1.el7
            (1%)###############(100%)
            3:docker-ce-3:19.03.15-3.el7
            (1%)###############(100%)
            /usr/bin/dockerd has not been configured as an alternative for dockerd
            Cleaning up / removing...
            4:docker-ce-3:18.09.6-3.el7
            (1%)###############(100%)
            5:containerd.io-1.2.5-3.1.el7
            (1%)###############(100%)
            6:docker-ce-cli-1:18.09.6-3.el7
            (1%)###############(100%)
            Mon May  9 02:04:11 PDT 2022 Restarting Docker
            Mon May  9 02:04:29 PDT 2022 Restarting services
            Mon May  9 02:04:59 PDT 2022 RPM installation completed
```

Your Cisco IoT FND on OVA upgrade is complete.

Upgrade Cisco IoT FND container images

Procedure

Step 1 Open the SSH terminal and log in to Cisco IoT server as a root user.

Step 2 Run the following script:

Example:

```
/opt/fnd/scripts/upgrade.sh
```

```
[root@iot-fnd ~]# /opt/fnd/scripts/upgrade.sh
            This script must be run with root privileges.
            Usage: Load container images: No resource required
            For container reload: No resource required
            1) Load container images
            2) Container reload
            3) Quit
            Enter your choice: 1
            Do you want to download docker image from registry (y/n)?y
            Enter docker registry [devhub-docker.cisco.com]: dockerhub.cisco.com
            Enter docker image tag: 5.0.2-8
            Downloading FND docker image...
            5.0.2-8: Pull complete
            ea3c714182eb: Pull complete
            177abefb5b93: Pull complete
            e696bdc28724: Pull complete
            89dd87262f50: Pull complete
            ff6164c0609f: Pull complete
            89a0b2205b62: Pull complete
            4dbd23bb6e45: Pull complete
            Digest: sha256:2ae8a3cba38ea28156a2c3db55cd8cea0448888a7704479cac33b665d8b2a132
            Status: Downloaded newer image for
dockerhub.cisco.com/field-network-director-dev-docker/fnd-image:5.0.2-8
            dockerhub.cisco.com/field-network-director-dev-docker/fnd-image:5.0.2-8
            Downloading Fog Director docker image...
            5.0.2-8: Pulling from fog-director-dev-docker/fogd-image
            5e9a6732a7a3: Pull complete
            55a104320bff: Pull complete
            506e5a93cf62: Pull complete
            9b2523a38071: Pull complete
            8e8389537d47: Pull complete
            e6fcef979884: Pull complete
            e2e278b80221: Pull complete
            63bc79650477: Pull complete
            Digest: sha256:16f3227fbac74804f1e2a77aa57ebeeb5b9f05eb4efb0ddccf242865fe673634
            Status: Downloaded newer image for
dockerhub.cisco.com/fog-director-dev-docker/fogd-image:5.0.2-8
            dockerhub.cisco.com/fog-director-dev-docker/fogd-image:5.0.2-8
            1) Load container images
            2) Container reload
            3) Quit
            Enter your choice: 2
            Stopping FND container...
            fnd-container
            Remove FND container...
            fnd-container
            Prune Docker container...
            Starting FND container...
```

```
            a02e6388607d79504f082dccf179514e5dc2d6bcd34021beac21baf1a555c266
            Stopping Fog Director container...
            fogd-container
            Remove Fog Director container...
            fogd-container
            Prune Docker container...
            Starting Fog Director container...
            a40aa29e2392e1e99a5f024d3d5838712d66ef638f0c6b0bf209b1932076611c
            1) Load container images
            2) Container reload
            3) Quit
            Enter your choice: 3
            You have new mail in /var/spool/mail/root
            [root@iot-fnd ~]#
```

Step 3 Enter **1** to load the container images.

Example:

```
[root@iot-fnd ~]# /opt/fnd/scripts/upgrade.sh
            This script must be run with root privileges.
            Usage: Load container images: No resource required
            For container reload: No resource required
            1) Load container images
            2) Container reload
            3) Quit
            Enter your choice: 1
            Do you want to download docker image from registry (y/n)? y
            Enter docker registry [devhub-docker.cisco.com]: dockerhub.example.com
            Enter docker image tag: 5.0-1
            Downloading FND docker image...
            5.0.2-8: Pulling from example-docker-repo/fnd-image
            a3ed95caeb02: Pull complete
            4e9f1a5e87b7: Pull complete
            bcd8f8dc5c34: Pull complete
            c5e155d5a1d1: Pull complete
            5b8c6e5e9b45: Pull complete
            b5e3b5c3f5b2: Pull complete
            f5b3c27c7f9f: Pull complete
            Digest: sha256:8d3d7b5e8d3f1c2b1e8b2f1b7c9a1234567890abcdef1234567890abcdef1234
            Status: Downloaded newer image for
dockerhub.example.com/example-docker-repo/fnd-image:5.0.2-8
            dockerhub.example.com/example-docker-repo/fnd-image:5.0-1
            Downloading Fog Director docker image...
            5.0-1: Pulling from example-docker-repo/fogd-image
            9f9a1c3f5f12: Pull complete
            6c5a9f7e9b34: Pull complete
            8d5e3b3c5f6b: Pull complete
            b5f1c9e7d1b2: Pull complete
            a5c2b6e4f8e7: Pull complete
            d1e3f5b4c6d3: Pull complete
            Digest: sha256:5e8d3f1a2b3c4d5e6f7a8b9c0d1e2f3a4b5c6d7e8f9a0b1c2d3e4f5g6h7i8j9k
            Status: Downloaded newer image for
dockerhub.example.com/example-docker-repo/fogd-image:5.0.2-8
            dockerhub.example.com/example-docker-repo/fogd-image:5.0.2-8
            1) Load container images
            2) Container reload
            3) Quit
            Enter your choice: 3
            [root@iot-fnd ~]#
```

Step 4 Download the latest container image for Cisco IoT FND from devhub-docker.cisco.com.

Step 5 After the images are downloaded successfully, enter **2** to reload container.

Example:

```
[root@iot-fnd ~]# /opt/fnd/scripts/upgrade.sh
            This script must be run with root privileges.
            Usage: Load container images: No resource required
            For container reload: No resource required
            1) Load container images
            2) Container reload
            3) Quit
            Enter your choice: 2
            Stopping FND container...
            fnd-container
            Remove FND container...
            fnd-container
            Prune Docker containers...
            Deleted Containers:
            fnd-container
            Starting FND container...
            c8e1f9a8d7c2b3a4e5f6d7c8b9a0b1c2d3e4f5g6h7i8j9k0l1m2n3o4p5q6r7s8
            Stopping Fog Director container...
            fogd-container
            Remove Fog Director container...
            fogd-container
            Prune Docker containers...
            Deleted Containers:
            fogd-container
            Starting Fog Director container...
            b7c6d5e4f3g2h1i0j9k8l7m6n5o4p3q2r1s0t9u8v7w6x5y4z3a2b1c0d9e8f7g6
            1) Load container images
            2) Container reload
            3) Quit
            Enter your choice: 3
            [root@iot-fnd ~]#
```

Step 6 Enter **3** to quit the menu.

You've upgraded the Cisco IoT FND containers.

Check DB and status post upgrade

Use the following steps to check the DB and Cisco IoT FND status to ensure that your upgrade is successful:

Before you begin

Use the following credentials for SSH access after upgrading OVA:

- Username: fnduser
- Password: C!sco123

  See Guidelines for resetting password.

Procedure

Step 1 Log in to the server or machine using SSH.

Step 2 Execute the `/opt/scripts/status.sh` command:

Example:

```
/opt/scripts/status.sh
```

```
Checking system status...
            Service: Database
            Status: Running
            Uptime: 24 hours
            Service: IoT FND
            Status: Running
            Uptime: 12 hours
            Service: Web Server
            Status: Stopped
            Action Required: Restart service
            Disk Usage:
            Filesystem      Size  Used Avail Use% Mounted on
            /dev/sda1        50G   30G   18G  63% /
            Memory Usage:
            Total: 8GB
            Used:  4GB
            Free:  4GB
            Network Status:
            eth0: Connected
            IP Address: 192.168.1.10
            All critical services are operational except the Web Server. Please address the issues
noted above.
```

Step 3 Execute the `docker version` command:

Example:

```
docker version
```

```
Client: Docker Engine - Community
            Version:           20.10.14
            API version:       1.41
            Go version:        go1.16.15
            Git commit:        a224086
            Built:             Thu Mar 24 01:50:09 2022
            OS/Arch:           linux/amd64
            Context:           default
            Experimental:      true
            Server: Docker Engine - Community
            Engine:
            Version:          20.10.14
            API version:      1.41 (minimum version 1.12)
            Go version:       go1.16.15
            Git commit:       87a90dc
            Built:            Thu Mar 24 01:48:43 2022
            OS/Arch:          linux/amd64
            Experimental:     false
            containerd:
            Version:          1.5.11
            GitCommit:        3df54a852345ae127d1fa3092b95168e4a88e2f8
            runc:
            Version:          1.0.3
            GitCommit:        f46b6ba2c9314cfc8caae24a32ec5fe9ef1059fe
            docker-init:
            Version:          0.19.0
            GitCommit:        de40ad0
```

Step 4 Execture the `/opt/fnd/scripts/fnd-container.sh status` command to check the status of the Cisco IoT FND container:

Example:

```
/opt/fnd/scripts/fnd-container.sh status
```

```
Checking IoT FND container status...
            Container Name: fnd-container
            Status: Running
            Uptime: 36 hours
            CPU Usage: 15%
            Memory Usage: 512MB / 2GB
            Network: Active
            IP Address: 172.17.0.2
            Port Mappings: 8080:80, 8443:443
            Last Health Check: Passed
            Health Check Interval: 5 minutes
            All monitored services within the container are operational.
```

Step 5 Execute the `docker exec -it fnd-container /etc/init.d/cgms status` command to check the status of the cgms service inside the Cisco IoT FND container.

Example:

```
docker exec -it fnd-container /etc/init.d/cgms status
```

```
Checking status of cgms service...
            cgms service is running
            PID: 1234
            Uptime: 24 hours
            Listening on Port: 9090
            No issues detected with the cgms service.
```

You've checked the Cisco IoT FND status to ensure that the upgrade has been successful.

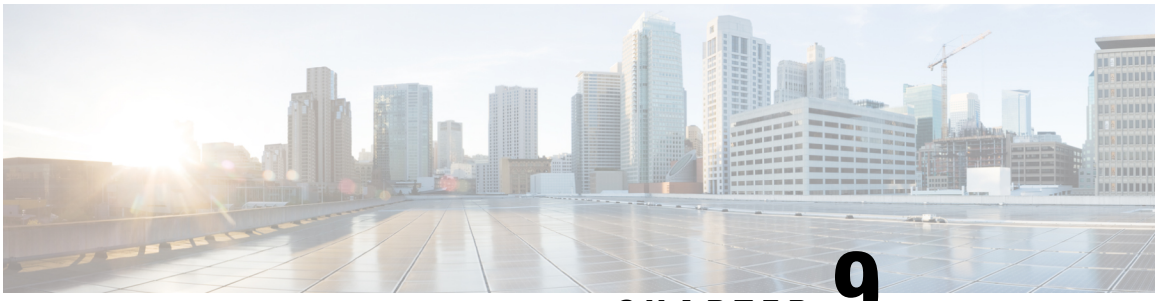
What to do next

Log into Cisco IoT FND to check if the services are working fine. For example, you can refresh the metrics for a couple of devices or add/delete devices using CSV.

Upgrade RHEL version

This section provides references to read about how to perform an in-place upgrade from Red Hat Enterprise Linux 7 (RHEL) to Red Hat Enterprise Linux 8 using the Leapp utility.

Follow the instructions provided in the Red Hat documentation about Upgrading from RHEL 7 to RHEL 8 .



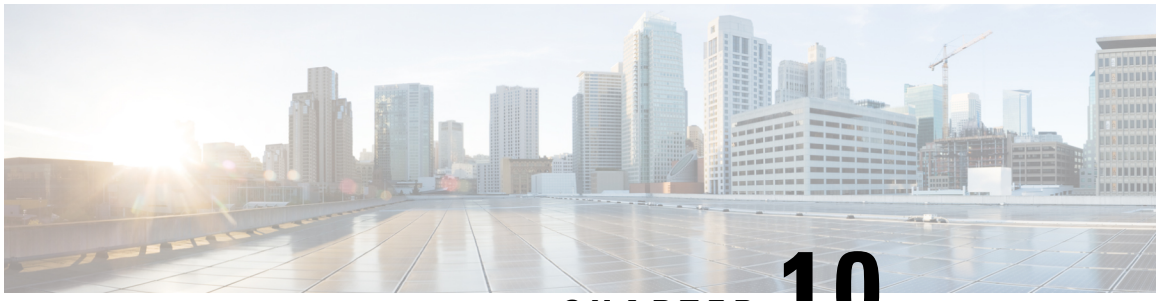
CHAPTER 9

Obtaining Status of All Services Running on the Host

Use the **status.sh** script in the following directory to show the status of all services running on the host.

```
cd /opt/scripts
```

```
[root@iot-fnd ~]# cd /opt/scripts/
[root@iot-fnd scripts]# ./status.sh
--------------------
● postgresql-9.6.service - PostgreSQL 9.6 database server
   Loaded: loaded (/usr/lib/systemd/system/postgresql-9.6.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2018-06-15 17:02:07 PDT; 13min ago
     Docs: https://www.postgresql.org/docs/9.6/static/
  Process: 1016 ExecStartPre=/usr/pgsql-9.6/bin/postgresql96-check-db-dir ${PGDATA} (code=exited, status=0/SUCCESS)
 Main PID: 1070 (postmaster)
    Tasks: 24
   Memory: 166.2M
--------------------
● influxdb.service - InfluxDB is an open-source, distributed, time series database
   Loaded: loaded (/usr/lib/systemd/system/influxdb.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2018-06-15 17:02:03 PDT; 13min ago
     Docs: https://docs.influxdata.com/influxdb/
 Main PID: 1024 (influxd)
    Tasks: 11
   Memory: 47.4M
--------------------
fnd-container is running, pid=2064
CONTAINER ID        NAME                CPU %               MEM USAGE / LIMIT     MEM %               NET I/O             BLOCK I/O           PIDS
a67827470562        fnd-container       1.04%               1.064GiB / 23.38GiB   4.55%               6.69MB / 8.19MB     581MB / 2.22MB      275
--------------------
fogd-container is running, pid=5192
CONTAINER ID        NAME                CPU %               MEM USAGE / LIMIT     MEM %               NET I/O             BLOCK I/O           PIDS
f6c0c5c313cb        fogd-container      1.64%               762.3MiB / 23.38GiB   3.18%               1.84MB / 3.45MB     106kB / 184kB       117
--------------------
[root@iot-fnd scripts]#
```



CHAPTER 10

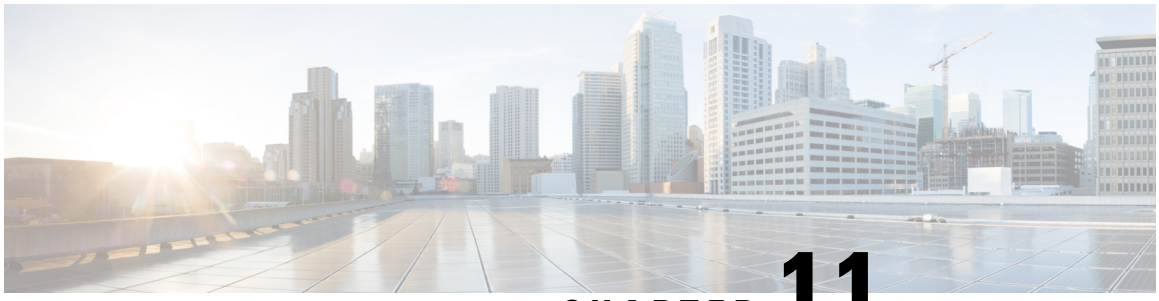
Backup and Restore

You can export the entire OVA image file as backup, port it to different deployment or restore from an older image file.

Procedure

Step 1 Power down the OVA in vSphere Client.

Step 2 Select **OVA**, and then select **File** > **Export** > **Export OVF Template**.



CHAPTER 11

Setting the Time and Timezone Using NTP Service

Use the **timedatectl** command on the Host VM to perform following operations to sync the time between the host and the docker:

- Displaying the Current Date and Time: **timedatectl**
- Changing the Current Time: **timedatectl set-time** HH:MM:SS
- Changing the Current Date: **timedatectl set-time** YYYY-MM-DD
- Listing the Time Zone: **timedatectl list-timezones**
- Changing the Time Zone: **timedatectl set-timezone** time_zone
- Enabling NTP Service: **timedatectl set-ntp** yes

```
[root@iot-fnd ~]# timedatectl
      Local time: Tue 2018-08-28 07:18:37 PDT
  Universal time: Tue 2018-08-28 14:18:37 UTC
        RTC time: Tue 2018-08-28 14:18:37
       Time zone: America/Los_Angeles (PDT, -0700)
     NTP enabled: yes
NTP synchronized: yes
 RTC in local TZ: no
      DST active: yes
 Last DST change: DST began at
                  Sun 2018-03-11 01:59:59 PST
                  Sun 2018-03-11 03:00:00 PDT
 Next DST change: DST ends (the clock jumps one hour backwards) at
                  Sun 2018-11-04 01:59:59 PDT
                  Sun 2018-11-04 01:00:00 PST
[root@iot-fnd ~]#
```

- Configuring NTP Server, on page 62

Configuring NTP Server

To configure the NTP server on Cisco IoT FND and TPS servers, follow the steps given.

Procedure

Step 1 Run the command to edit the chrony.conf file.

Example:

```
[root@iot-fnd ~]# nano /etc/chrony.conf
```

This will display the current chrony.conf file details.

Step 2 Enter the IP address of the server that you want to use as the NTP server.

Example:

```
server 209.165.200.225
```

Step 3 Save the changes by selecting **Y** and exit.

Step 4 Restart the chrony service using the command given in the example.

Example:

```
[root@iot-fnd ~]# systemctl restart chronyd
```

Step 5 To view the NTP server you configured, use the command given in the example.

Example:

```
[root@iot-fnd ~]# chronyc sources
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^* 209.165.200.225               2  10   377   915    +17us[  +19us] +/-   21ms
```

The newly configured NTP server details are displayed.