Cisco IC3000 Industrial Compute Gateway Deployment Guide

The purpose of this document is to describe the procedures to successfully deploy the IC3000 by following these phases:

This guide also discusses:

Introduction

The IC3000 Industrial Compute Gateway (IC3000) is an edge computing platform which extends the cloud computing paradigm to the edge of the network. Instead of hosting applications in a remote data center, applications can now be hosted on the edge itself. Imagine, if we can host specific applications in the field close to the sensors, meters or the things. whatever may be the IOT use case, IC3000 serves the purpose by allowing us to deploy applications that need more cores and memory.

The Cisco IC3000 Industrial Compute Gateway is fully supported by Cisco IoT Field Network Director for zero-touch deployment, lifecycle management, application management, monitoring, and troubleshooting securely at scale from a single pane of glass.

The IC3000 is a mid-range, low-power, fanless, edge server ruggedized for Industrial Applications. It is powered by a 4 core 1.2GHz Intel Rangeley CPU with 8 GB of 1333MHz DDR3 memory, and a 100GB mSATA drive (internal). For connectivity it supports 2x1GbE SFP and 2x10/100/1000Base-T with a management port.

This next section describes the phases you will need to follow for a successful installation.

Note: Examples shown in this document use IP addresses that are from a lab environment and should not be used on a typical customer installation.

Phase 1: Unboxing, Installing and Connecting to the IC3000 Device

Unboxing the IC3000

Complete details for the hardware installation of the product are covered in the Cisco IC3000 Industrial Compute Gateway Hardware Installation Guide. The following steps are a high level overview.

Installing the IC3000

1. Review the general description of the unit in the Product Overview section of the hardware installation guide.
2. Check the Equipment, Tools, and Connections section of the hardware installation guide to ensure you have everything you need for the installation.
3. Review the procedures for Mounting, Grounding, Connecting to DC Power and Connecting to the IC3000 in the hardware installation guide.

4. If you are installing the device in a Hazloc location, follow the printed instructions that came inside the box with the device.
5. Power on the device.

Connecting the IC3000 to a PC

1. Connect a PC to the device. If your PC warns you that you do not have the proper drivers to communicate with the device, you can obtain them from your computers manufacturer or go to:

   https://software.cisco.com/download/home/282774227/type/282855122/release/3.1

2. Determine how your computer mapped the new COM port that was created when you installed the USB-to-serial port driver. You need this information to appropriately configure your serial communications program in the next step.
3. Start your serial communications program and connect to the router. The console port settings to use for the serial connection are:
   - 9600 baud
   - 8 data bits
   - 1 stop bit
   - no parity
   - no flow control

   If the device is properly connected and powered up, you should see the **ic3k>** prompt.
4. Verify that your computer is properly connected to the device by checking the LEDs on the unit as described in the Hardware Installation Guide.

IC3000 Show Commands

The following show commands are supported on the device via the console. Unlike other Cisco routers, the IC3000 only supports one user mode, which is user EXEC mode. The device prompt shows as **ic3k>**.

The CLI and prompt is a CLISH wrapper built on top of Linux OS for administrator usage.

Show Command	Description
show version	shows the version information
show dns	shows the domain name service information
show ida	shows whether the device is in production or developer mode.
show ntp	shows the network time protocol information
show techsupport	shows the technical support logs
show iox	shows the IOx application hosting information
show iox summary	shows the application hosting summary
show iox detail	shows the application hosting details
help developer-mode	shows instructions for configuring developer-mode
help production-mode	shows instructions for configuring production-mode

There are examples of command output to illustrate the show commands located in Troubleshooting, page 177. Your device may show different results depending on your configuration.

Phase 2: Managing the IC3000 with FND

There are seven steps involved in deployment:

Step 1: Installing FND

If this is your first time setting up the FND OVA infrastructure, go to Appendix: FND 4.3 device-configuration templates (Deprecated), page 184 for complete information.

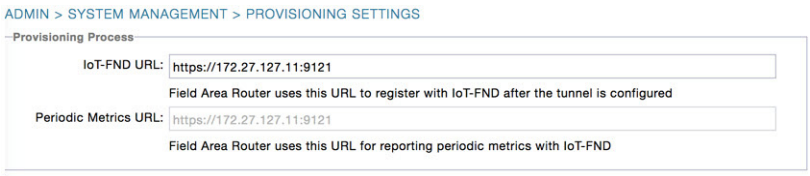
Download the IoT Field Network Director software from this location:

https://software.cisco.com/download/home/286287993/type

Visit FND URL https://<IP address from step 4>/ and change the password for root user. Default username/password is root/root123

Note: Change the **ADMIN > SYSTEM MANAGEMENT > PROVISIONING SETTINGS > IOT FND URL** with the FND IP address as shown in Figure 1. Otherwise, registration may fail.

Figure 1 Provisioning Settings



Step 2: DHCP Option 43 Settings

If the IC3000 gateway gets an IP address from the DHCP server, Option 43 is used to advertise the FND IP address via DHCP.

Example DHCP Option 43

Configure the following on an IR8x9:

```
ip dhcp pool callisto_pool2
network 172.27.88.0 255.255.255.128
dns-server 173.36.131.10
option 43 ascii 5A;K4;B2;I172.27.88.63;J9125
option 42 ip 171.70.168.183
default-router 172.27.88.1
lease 0 0 2
```

Please make note of Option 43 usage:

- If you have a DHCP server, use the “same” PNP discovery option string that we use for regular IOS routers Option 43 ascii “5A;K4;B2;I172.27.88.63;J9125" (IGMA will use port 9121 as default. IoT FND IP is 172.27.88.63)
- If you wish to use a different port provide the following configuration:

  option 43 ascii “5A;K4;B2;I192.168.10.6;J9125;W9128"

On a regular Linux server running DHCP, use the following instructions:

```
cat /etc/dhcp/dhcpd.conf
subnet 10.10.100.0 netmask 255.255.255.0 {

option routers 10.10.100.1;
range 10.10.10.100 10.10.10.199;
option domain-name-servers 10.10.100.1;
option domain-name "test1.dom";
option vendor-encapsulated-options "5A;K4;B2;I10.48.43.227;J9125";
}
```

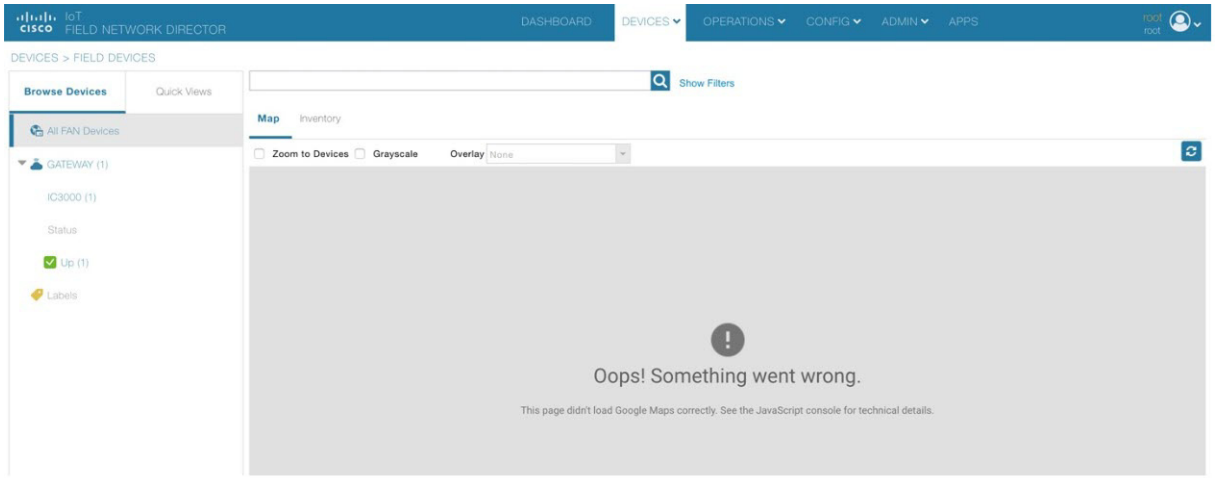
Step 3: Understanding the Device Configuration Template

There is a default template within the FND for IC3000. It is located under **CONFIG >Device Configuration tab > default-IC3000 > Edit Configuration template**. See Figure 2.

Edit the interface configuration or add interface settings as required by your use case. Once edited, use the Push Configuration tab to push the new configuration to the active or registered devices.

Note: It is important to make sure the map is correctly configured. If valid entries do not exist, you will get an error message like the on shown in Figure 2.

Figure 2 Map Error



Step 4: Adding the IC3000 Gateway(s) to FND

1. Prepare a spreadsheet with the list of devices to add. This must be completed **before** adding devices to avoid additional steps.

Your spreadsheet will need the fields as shown in the following example:

```
eid                          deviceType  lat          lng           IOxUserName  IOxUserPassword
IC3000-2C2F-K9+FOC2227Y2ZC   IC3000      37.414639  -121.936836   admin        IC3000password
```

Note: The eid is a combination of the PlatformID+HardwareID. The platform id for the IC3000 is always IC3000-2C2F-K9 and the HardwareID or Serial number is unique for each platform. The serial number can be read from the label on the box, or if you have access to the console of the device run the **show version** command and the hardware id /serial number will be displayed.

Note: The latitude (lat) and Longitude (lng) entries in the spreadsheet will need to represent actual values, complete with decimal notation. For latitude, a positive number represents North and a negative number represents South. For longitude, a positive number represents East and a negative number represents West. Failure to specify an actual value will result in an error being displayed from Google Maps.

To download a sample spreadsheet click on the following link:

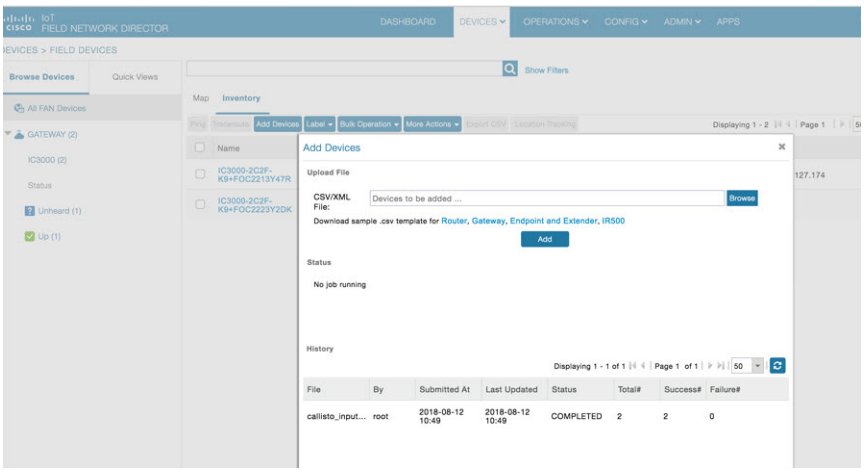
https://www.cisco.com/c/dam/en/us/td/docs/routers/ic3000/deployment/guide/IC3000-default-Input-template.csv

2. Get the Serial number and Model number and use system as the ioxusername and admin as the password. The serial number is located on the device label and is something like " FOC2227Y304" . The serial number can also be found through the show version command output:

```
c3k>show version
Version: 1.7.0-0.9.59
Platform ID: IC3000-2C2F-K9
Hardware ID: FOC2227Y304
ic3k>
```

3. Click **DEVICES > FIELD DEVICES > Inventory > Add Devices**. Browse to the location of your excel spreadsheet and click **Add**. See Figure 3.

Figure 3 Add Devices



Note: The IC3000 belongs under the gateway category when adding devices.

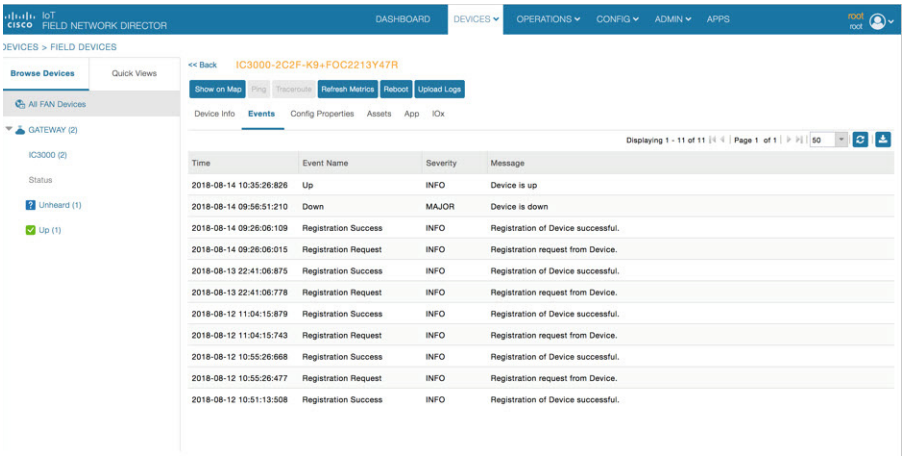
Step 5: IC3000 Registration

After you add devices to the IoT FND (FND) Network Management application, wait for a few minutes for the IC3000 devices to learn the option 43 settings from the DHCP server, and then register with FND. Once the IC3000 gets an ip address from DHCP server, the option 43 issues an FND IP address for the device to register to FND.

Note: Make sure the DHCP server settings are set properly with FND IP in option 43 string.

Once the device is registered you should see the registration events listed for each IC3000 unit as shown in the example on Figure 4.

Figure 4 Device Registration



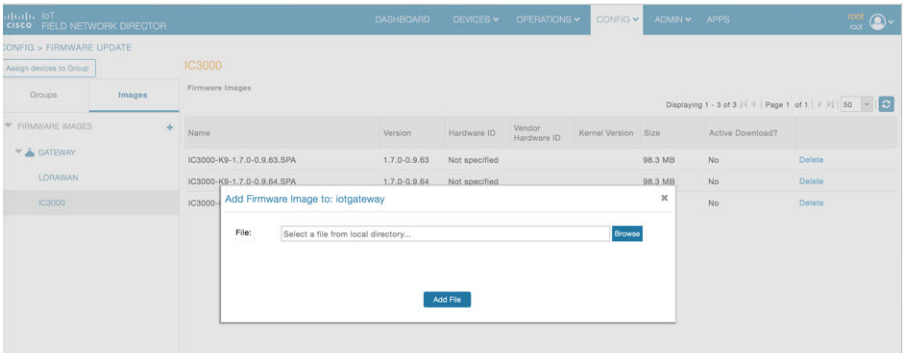
The refresh metric should work and should be able to refresh the device related details.

Step 6: Uploading the Firmware to FND

In order to upgrade the firmware of the IC3000, you must download the required firmware from Cisco.com to upload the firmware to FND.

Select **CONFIG > Firmware Update > Images**. A list of the IC3000 images is presented. Click **+** – and upload the required image. See Figure 5.

Figure 5 Firmware Upload



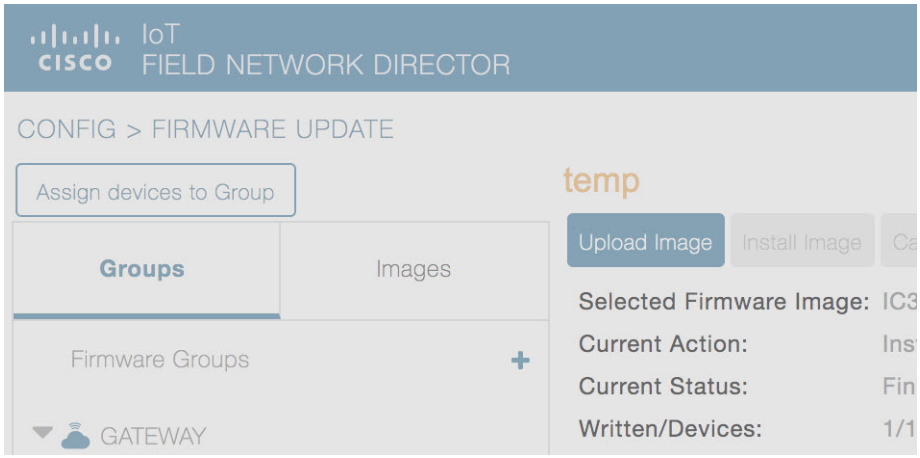
Step 7: Upgrading Firmware with FND

Once Step 5 is complete, you may now upgrade the firmware against the registered Units that require the update.

Select **CONFIG > Firmware update > Select the device group > Upload Image**

Once the Image upload is complete, select the **Install Image** tab and proceed with upgrading the firmware.

Figure 6 Firmware Update

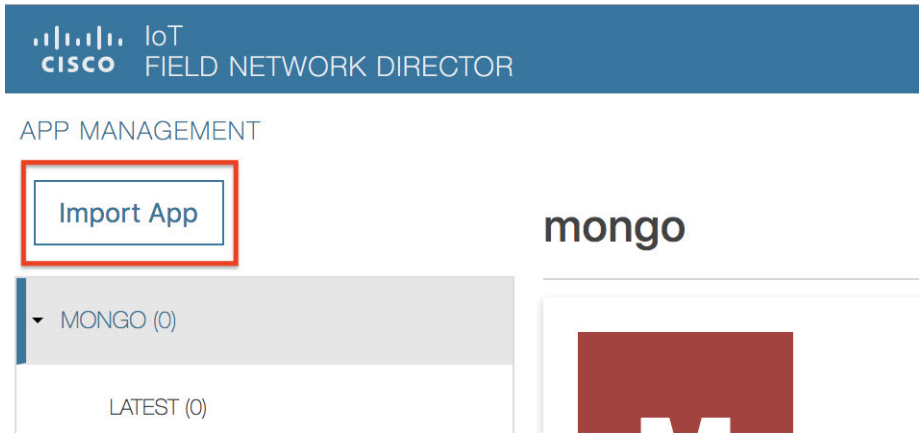


Step 8: Deploying the IOx Applications via FND

To deploy an IOx application perform the following:

1. From the Main page select **APP > Import Apps** and select the required application to install.

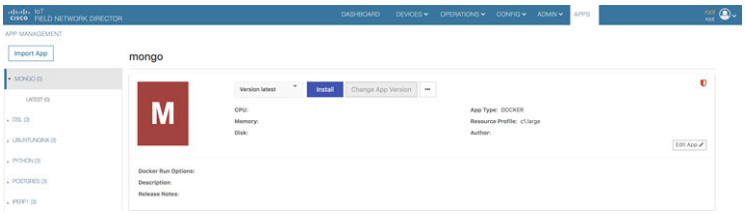
Figure 7 Application Upload



Once imported, you will find the list of applications imported in the right column.

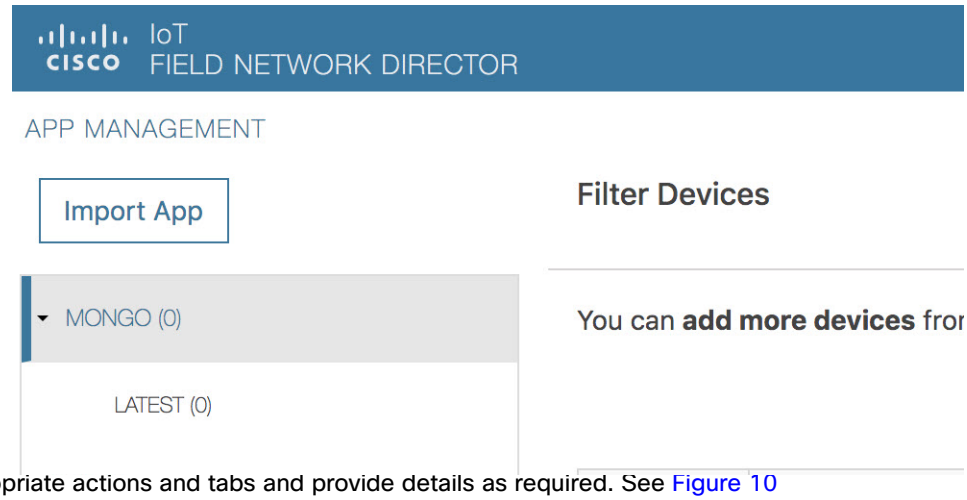
2. Select the application that needs to be installed and click **Install**.

Figure 8 Application Install



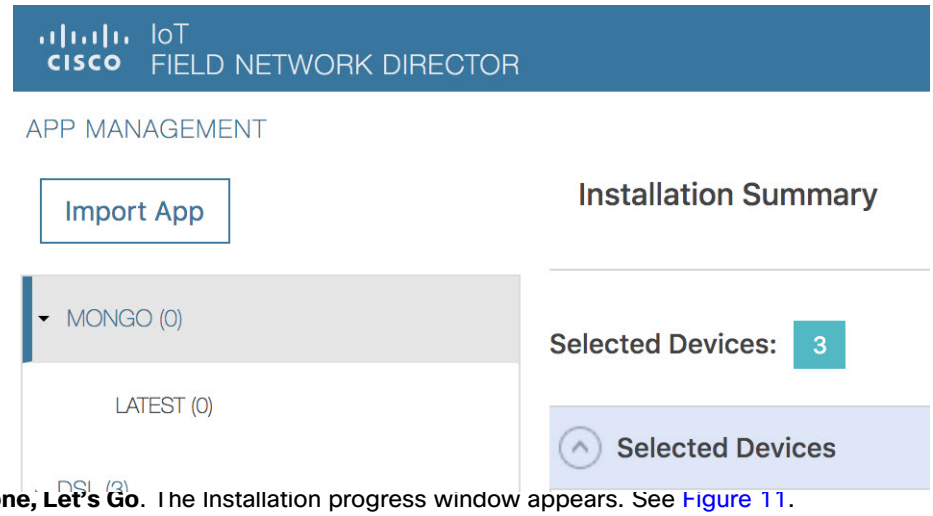
3. Select the **Devices > Add Selected Devices**. With your device present, click **Next**

Figure 9 Add Devices



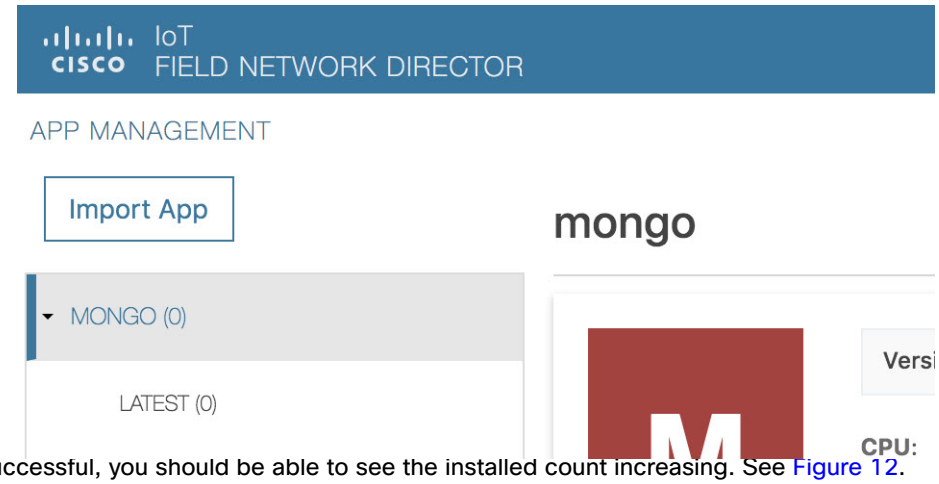
Select the appropriate actions and tabs and provide details as required. See Figure 10

Figure 10 Selected Device Action Tabs



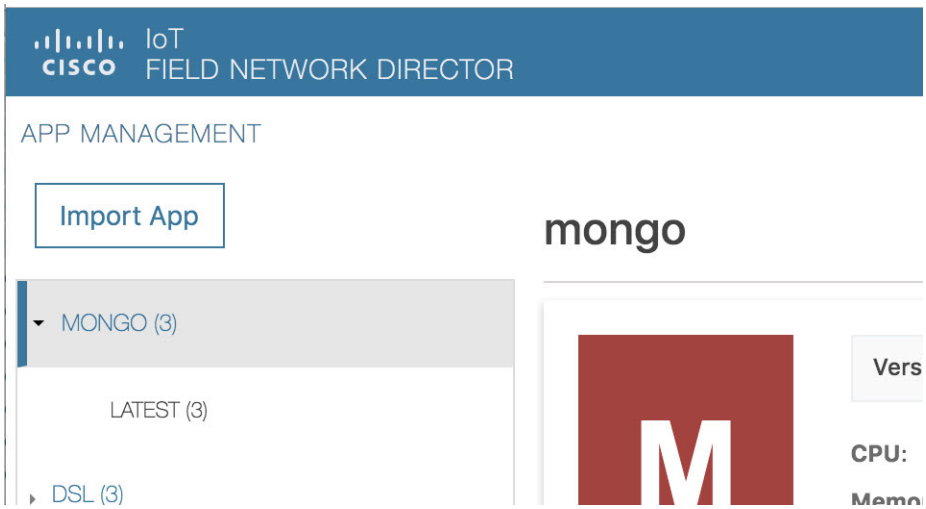
4. Then click **Done, Let's Go**. The Installation progress window appears. See Figure 11.

Figure 11 Installation Progress



If installation is successful, you should be able to see the installed count increasing. See Figure 12.

Figure 12 Installation Successful



Phase 3: Developer Mode: Testing IOX Applications via Local Manager

Understanding Developer Mode

Typically, when connected to the IC3000 through a laptop, you are in developer mode. This mode is suitable for developers, system integrators or engineers who want to test or build an application, which is specific to their choice of use case, before deploying in large scale via FND. It is assumed that the IOX client utility can be used to package the application as a container or Docker. VM based APP support will be included in later releases.

Understanding Production Mode

This mode is typically when the IC3000 has been deployed in field, and actively performing in the field hosting apps that were prebuilt and designed to run. This mode must be managed by FND. The device management ports learn the DHCP address and gradually registers with FND. Please refer the IC3000 device registration section.

Developer Mode Connectivity

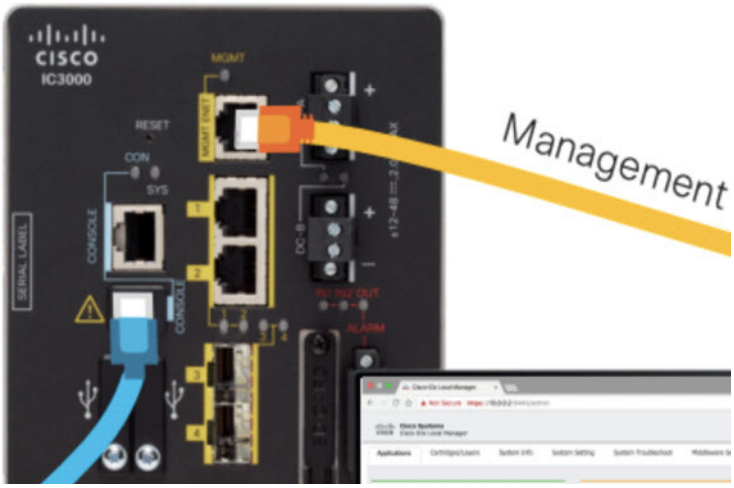
Consider the following points in order to connect to the IC3000 in developer mode:

- Brand new devices (fresh from Cisco factory) have the capability of determining the mode autonomously depending on the networking configurations.
- Developer mode enables the Cisco IOx Local Manager interface which can be accessed via the browser on the computer connected to the gateway.
- Developer mode is activated ONLY over the management Ethernet port of the device.
- Developer mode operates ONLY over a predetermined IPv4 Link-local addresses (169.254.x.x). You cannot use developer mode over a LAN/WAN.
- Developer mode CANNOT be turned ON via FND.
- An IC3000 deployed in production can be re-configured to operate in developer mode by pressing the "Reset" button on the device. All existing configuration information is removed on reset.

Steps to Connect to the Management Port

Figure 13 shows a laptop connected to the management interface via a standard Ethernet cable.

Figure 13 PC Connected to Management Interface



1 (Management Interface Configuration)	2 (Laptop Configuration)
IP address 169.254.128.2 Netmask 255.255.0.0	IP address 169.254.128.4 Netmask 255.255.0.0

1. Follow steps 1-4 of Phase 1: Unboxing, Installing and Connecting to the IC3000 Device, page 158.
2. Connect the Management interface on the IC3000 and your laptop with a console cable.
3. Do not power on the IC3000 yet.
4. Assign the IP address of 169.254.128.4 with a netmask of 255.255.0.0 to the network interface on your computer.

Note: It is critical you assign this specific IPv4 link-local address.

5. Now, power-on the IC3000.
6. The IC3000 will be ready to operate in developer mode in 30 seconds (The delay of 30 seconds only occurs the first time a device is booted up. All subsequent reloads will immediately take the device to developer mode without delay).
7. Open a browser on your laptop and enter https://169.254.128.2:8443 as a URL. The Local Manager opens. Enter **developer** as your username and then create a password. Use the following commands to establish a password.

   Note: The following password rules must be adhered to:

   - Minimum length = 6
   - Must not be based upon a dictionary word
   - Must not be a combination of dictionary words
   - Must not be composed of common string patterns like “qwerty”, “asdfgh” etc...
   - Must not be a combination of common string patterns and dictionary words
   - Currently not supporting Unicode

```
ic3k>developer set-password
Enter password: <your-password>
Re-enter password: <your-password>
Password set successfully!
```

8. You can change an existing password using the following commands:

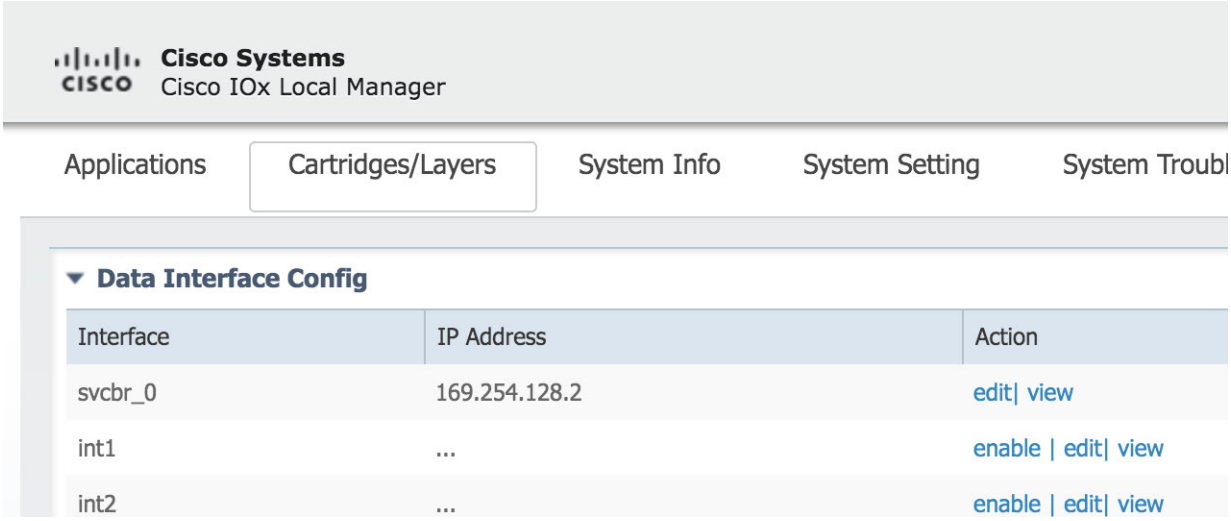
```
ic3k>developer change-password
Enter old password: <your-old-password>
Enter new password: <your-new-password>
Re-enter new password: <your-new-password>
Password changed!
```

Upgrading the IC3000 Firmware with Local Manager

The following steps are used to upgrade the device firmware through the Local Manager GUI in Developer Mode.

1. Login to LM GUI using the LLA address
2. Use the developer password previously created.
3. Once you are logged into the GUI, click on the **Device Config** tab, then select the **Software Upgrade**. (See Figure 14).
4. Select the image file and then click **Upload & Install**.
5. If you receive any pop-up messages click OK.
6. The image is pushed to the IC3000 and it is rebooted with the new firmware.

Figure 14 Device Config Tab



Phase 4: Connecting and Managing via Local Manager

About Local Manager

Cisco IOx Local Manager provides a web-based user interface that you can use to manage, administer, monitor, and troubleshoot applications on a device, and to perform a variety of related activities.

Accessing the IC3000 via Local Manager

Find the Management port address to access the IC3000 via a web browser. After connecting the IC3000 to a laptop, gather the svcbr_0 address whether you are in production mode, or developer mode. Use the **show interfaces** command to determine the IP address, or if you are managing the device via FND, get the device IP address. Use the ioxusername and ioxpassword to login via Local Manager, or you can create users on the IC3000 from the device configuration tab. Use the json commands to create users and passwords that Local Manger can use.

```
ic3k>show interfaces

svcbr_0   Link encap:Ethernet  HWaddr f8:b7:e2:b5:26:80
          inet addr:172.27.127.174  Bcast:172.27.127.255 Mask:255.255.255.0
          inet6 addr: fe80::fab7:e2ff:feb5:2680/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:396 errors:0 dropped:0 overruns:0 frame:0
          TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29614 (28.9 KiB)  TX bytes:3373 (3.2 KiB)
```

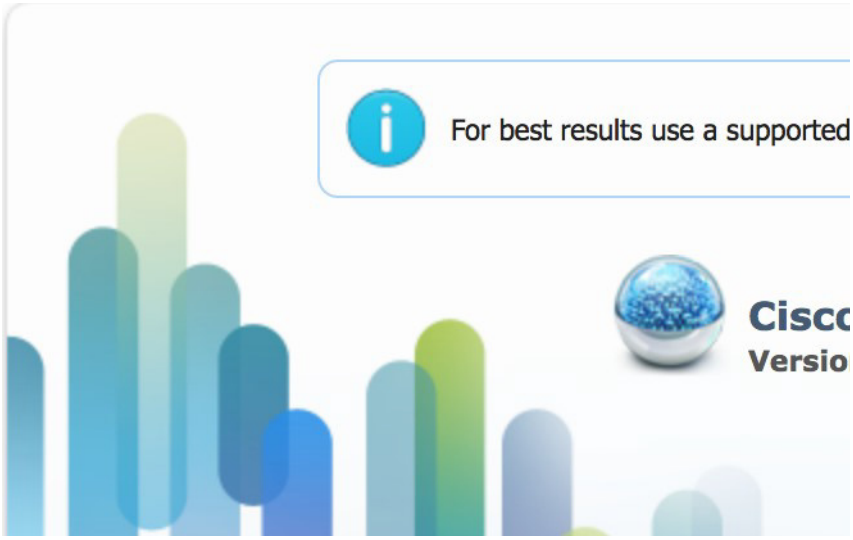
Note: If the IC3000 is in developer mode, you will be using an IPv4 LLA address of 169.254.128.x. The rest of the following work flow is the same.

1. Open a web browser and enter **https://169.254.128.2:8443** in the address bar.
2. Login by using the credentials **developer/<*your-password*>**. This is the password that was created by the **developer set-password** or **developer change-password** command. You should have various tabs that Local Manager supports, since you are accessing the unit via Local Manager. You should be familiar with the developer mode options like **Device Config** tab.

If a security exception message appears in your browser, confirm the exception to continue to the Cisco IOx Local Manager Login screen.

If you see the message "For best results use a supported browser" near the top of this screen, your browser may have compatibility issues with this version of Cisco IOx Local Manager. In this case, we recommend that you load a compatible browser. Hover your mouse pointer over the down-arrow next to this message to see a list of compatible browsers as shown in Figure 15.

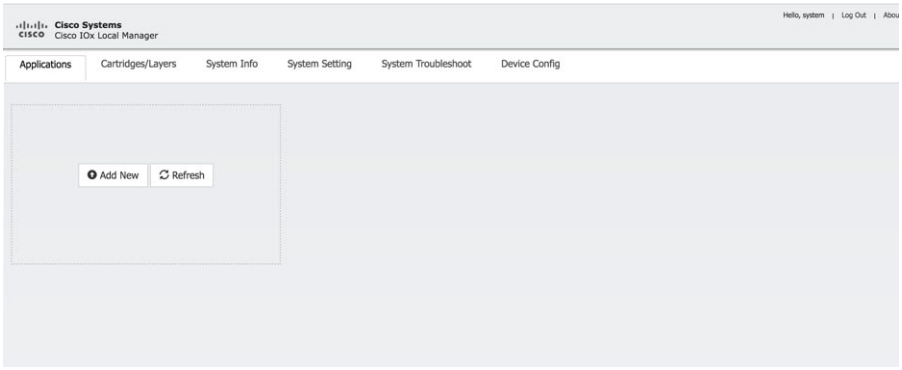
Figure 15 Supported Browsers



3. Click **Log In**.

   The **Local Manager Applications Tab** appears. See Figure 16.

Figure 16 Local Manager Applications Tab



4. Your IC3000 is now ready for Cisco IOx application development.

Use Case Example: Installing a Prebuilt Application via Local Manager

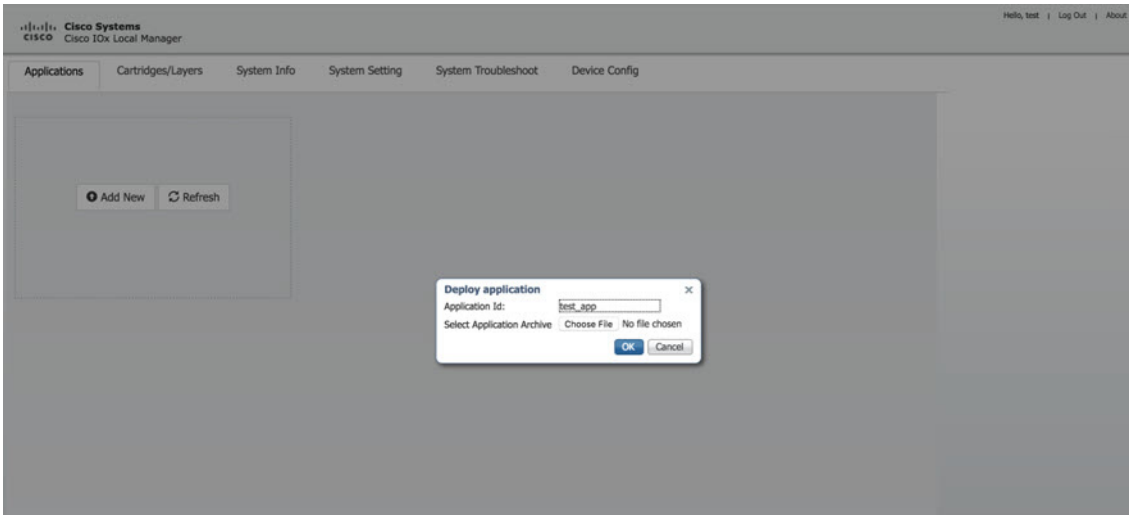
This section shows you how to use Cisco IOx Local Manager to load a sample EFM application and how to run the application.

1. Download the LXC or Docker application on to your desktop. Go to the following link:

   https://software.cisco.com/download/home/286316104/type/286312892/release/1.5.0

2. In the Cisco IOx Local Manager Applications Tab, click **Add New**. The **Deploy application** dialog box appears, see Figure 17.

Figure 17 Deploy application



3. In the Deploy Application dialog box, take these actions:

   a. In the **Application ID** field, enter a name.

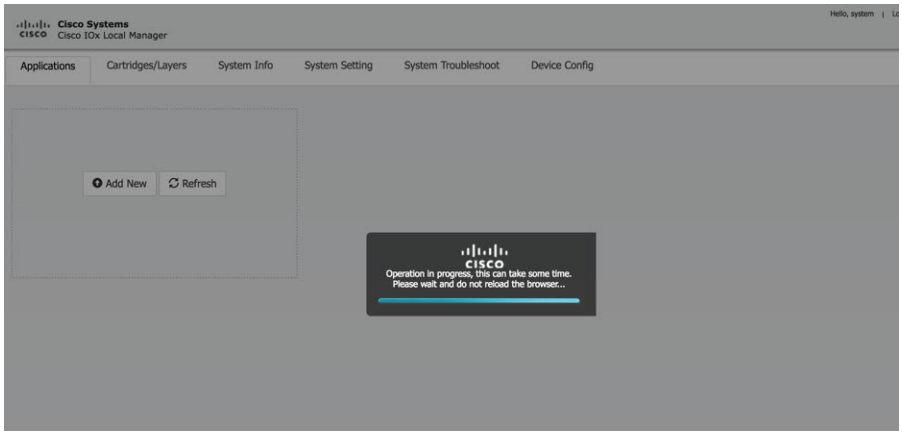
   b. In the **Select Application Archive** field, click **Choose File** and navigate to, then select the sample application file that you downloaded in Step 1.

   c. Click **OK**.

4. The application file uploads to Cisco IOx. See Figure 18

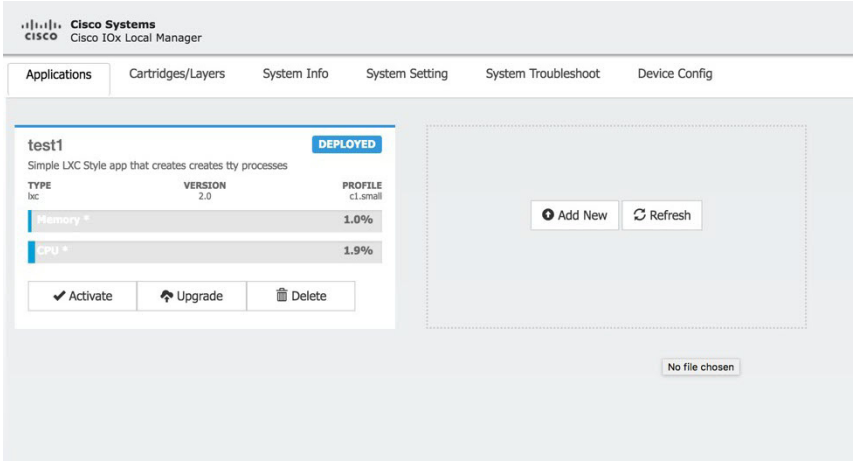
   Note: Do **NOT** refresh the browser during the upload.

Figure 18 Upload Operation Window



5. When you see the pop-up message " Successfully Deployed", click **OK**.

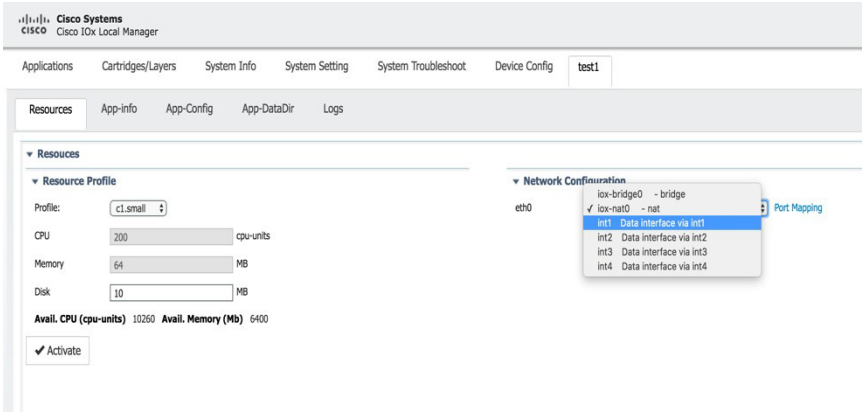
Figure 19 Application Successfully Deployed



The Cisco IOx Local Manager Applications tab updates to show the EFM application area.

6. In the test1/APP area, click the **Activate** button. The **Applications > Resources** tab displays, see Figure 20.

Figure 20 Applications > Resources Tab

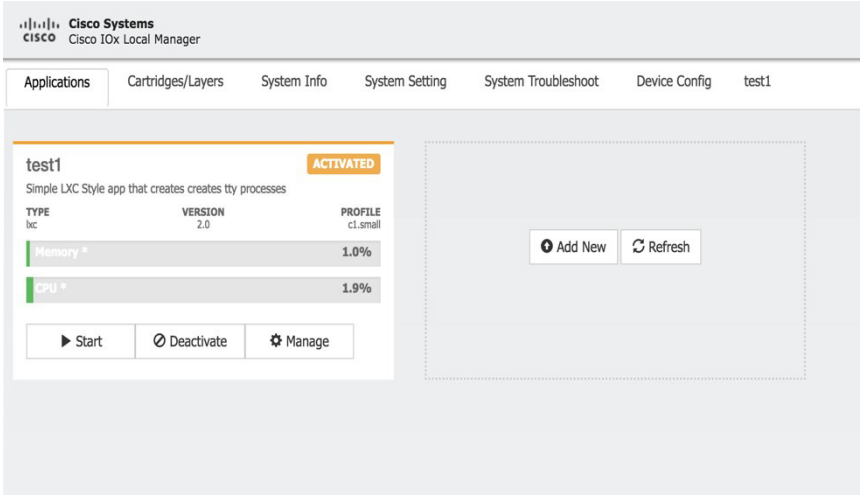


7. In the **Network Configuration** area of the **Applications > Resources** tab, perform the following:
   a. Choose **int1 Default Network** from the eth0 drop-down list.
   b. Choose **int2** from the eth1 drop down list.

      Note: Always use eth1 to connect your device to your local network.
8. While still in the **Applications > Resources** tab, click the **Activate** button to activate the application.
9. Click the **Applications** tab.
10. In the EFM area, click the **Start** button. See Figure 21.

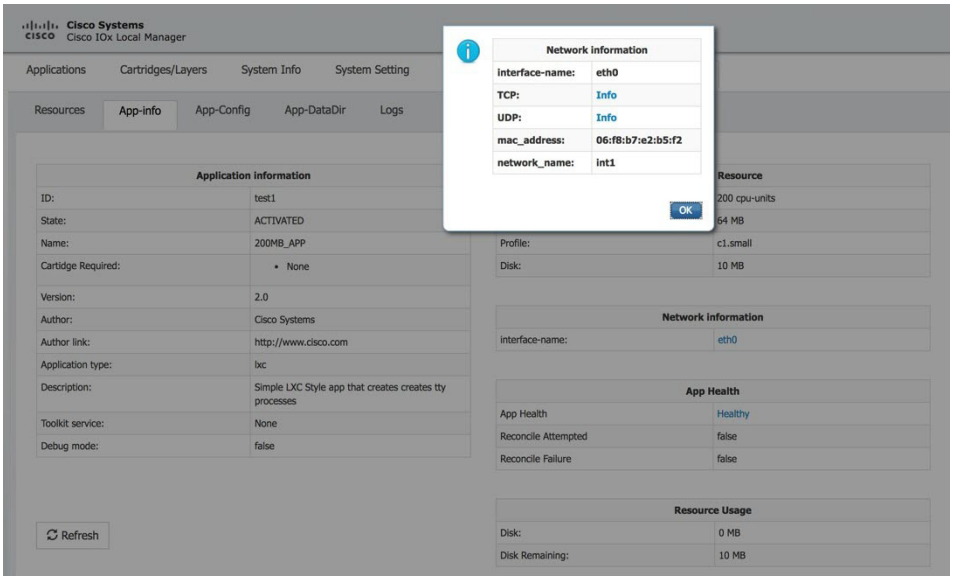
    Note: Make sure that activated the application before clicking **Start**.

Figure 21 Applications > Start



11. Click the **App-info** tab and make sure that data ports int1 and int2 are up. Then, once the application is started check the dhcp obtained address in the **App-info** tab. See Figure 22.

Figure 22 App-info Tab



Additional Examples

There are a number of applications that can be loaded onto the IC3000. Developers can package any application as long as it is in a container or VM. Additional information and examples are located on DevNet documentation on IOx. Provides an overview as well as details by scrolling down the left hand side:

https://developer.cisco.com/site/devnet/support/

Remote Device Management

The remote device management feature provides the user with the ability to enable or disable the remote access to the device configuration page from Cisco IOx Local Manager over a non-link local address.

Note: Remote Device Management is new with Local Manager version 1.8. If your device is still running version 1.7, you will need to upload the new image. See Step 1. below.

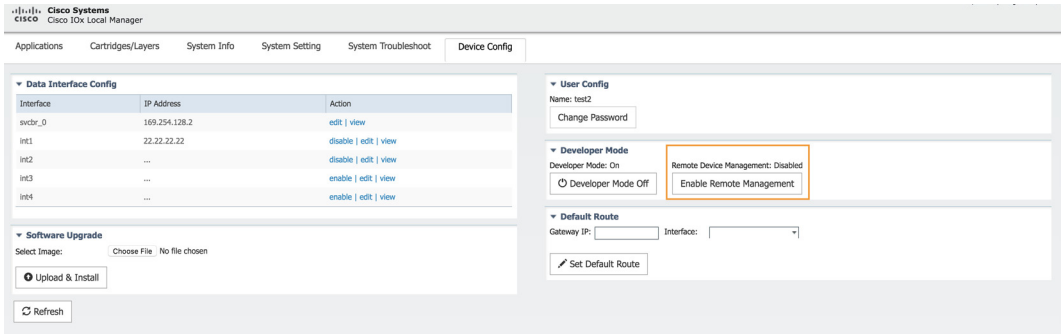
The procedure to bring the IC3000 up into Developer Mode remains exactly same as previously described in Phase 3: Developer Mode: Testing IOX Applications via Local Manager, page 166. Use the pre-defined link-local address169.254.128.2 to get the device up in developer mode.

Next, follow these additional steps to enable remote device management:

1. If required, upload the new Image from the Device Config tab and it will reload the device with the latest image.
2. Open a **NEW** browser and login again with the 169.254.128.2 address to the Local Manager using developer credentials.

   Note: The old browser is now non-functional.
3. In the Device Config tab there is a new section on the right side called “Remote Device Management”. See the highlighted area in Figure 23.

Figure 23 Remote Device Management



4. Click **Enable Remote Management**, and then respond with **Yes/Okay** for any pop-ups.

   After enabling remote device management, the user can access the device configuration page from any IP address other than the link local address.

   Note: Since the HTTP server is not only binding with the link local IP address, the user can access the device config page from the data port as long as it has routable IP address configured with an up state.
5. Use the https://*<new address>*:8443 in a new browser window to login to LM using developer credentials.

   See Figure 24 for guidance for these steps.
6. Make sure you are aware of your network topology (static ip address or DHCP) for the management interface svcbr_0.

If the address is non link local address other than 169.x.x.x:

a. Edit the svcbr_0 address to *<your ip address>* and make sure to add a network on the laptop to connect to the Local Manager.

b. Use the new address from the browser to login to the Local Manager with developer credentials.

If the address is a static routable address:

a. Obtain the default-route details and add the Gateway IP route details to the svcbr_0 interface below" Default Route" section below

b. On the left side of the Device Config screen, edit the svcbr_0 interface , static option ,with chosen IP address and set mask. Click **Ok**.

c. Attach the MGMT port to the network where the address is reachable.

Note: The Local Manager is not reachable anymore once the configuration is pushed, you have to connect the MGMT port of the IC3000 to a network where the address is reachable.

d. Use the new chosen address from a new browser window to login into Local Manager with the developer credentials.

If the MGMT/svcbr_0 is connected to a DHCP network, after enabling remote management edit the svcbr_0 interface to select the DHCP option.

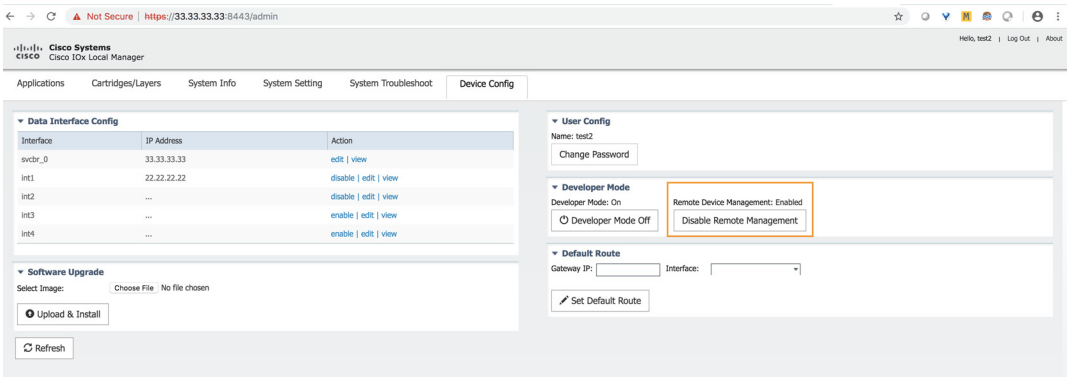
a. Disconnect IC3000 mgmt port from laptop and connect to the network for active DHCP learning on svcbr_0.

b. Check the ip address learned via DHCP on the platform console using the CLI **show interfaces.**

c. Use the https://*<new address>*:8443 in a new browser window to login to LM using developer credentials.

7. Obtain the default-route details and add the Gateway IP route details to the svcbr_0 interface below **Default Route**.
8. On the left side of the Device Config screen, edit the svcbr_0 interface with chosen IP address and mask. Click **Ok**
9. See Figure 24 for guidance for these steps.

Figure 24 Remote Device Management (Enabled)

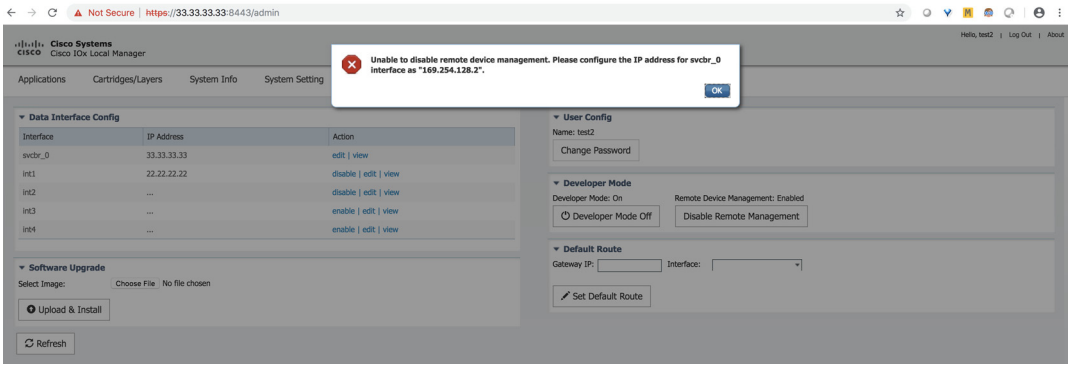


To disable remote device management

From the same Device Config tab window, you can see the Remote Device Management section status has toggled to “Enabled”. To disable the feature, click **Disable Remote Management.**

Disabling the remote device management feature will bind the server back to the 169.254.128.2 address of the link local manager. The user will not be allowed to disable the remote device management unless they change the IP address for " svcbr_0" back to 169.254.128.2.

Figure 25 Disable Remote Device Management Warning



Additional Administration

The following are some of the additional items to consider as an administrator:

- IC3000 Image Installation, page 176
- SSH Access, page 177

IC3000 Image Installation

The IC3000 is shipped with a factory installed image. Once the device is powered up the version installed can be verified by running the **show version** command via the console.

If the version is the latest CCO version, or a recommended version, you may continue with your next steps.

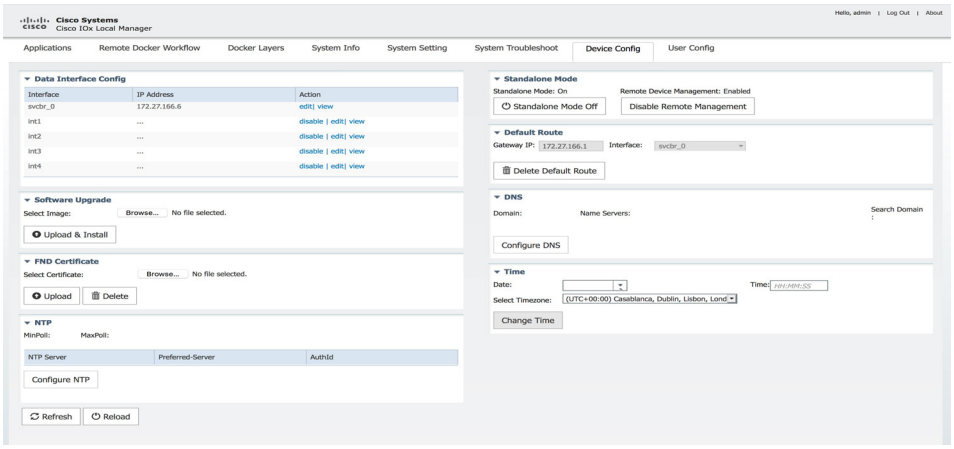
If the version is an older version and needs to be upgraded, then please download the latest version from CCO site and update the firmware using LM or FND.

Choose LM or FND as a preference of choice. For example, if you are accessing the device locally connected to a PC, then you may be able to use LM to upgrade the firmware. If you are managing a number of IC3000 devices via FND, then you should be able to use the firmware update tab in FND to upgrade the firmware.

The LM work flow is as follows:

1. Connect the IC3000 to a laptop or use the svcbr_0 interface address and access the LM via the following URL: https://*<ipaddress>*:8443
2. Select the **Device Config** tab, then click the **Choose File** button in the Software Upgrade section to select the image file. See Figure 26. Click the **Upload & Install** button to upload the image. Note that the device will be rebooted after the new image is installed.
   Note: the device configuration tab will not be enabled in standalone mode. You should be in developer mode to access the device configuration tab and this can be achieved by factory resetting the box.

Figure 26 Device Config Tab



The FND work flow is as follows:

Please follow the Step 7: Upgrading Firmware with FND, page 163 procedure.

Note: The reboot time is approximately 3 minutes and the size of the firmware is roughly 100MB. It could take 5 to 6 minutes for the IC3000 to upgrade the firmware. The CAF or IGMA will be upgraded as well, and will be automatically loaded and running once the device is up. There is no upgrade needed for CAF.

SSH Access

SSH access is disabled by default to prevent unauthorized access to the device. However, you can troubleshoot an application while you are in developer mode. The application console is enabled in developer mode. If developer mode is off, the application console access is disabled.

Troubleshooting

This section provides some tips for troubleshooting problems that may occur.

IC3000 Related

Use the following commands from the console to determine the status of running applications.

- To view which version of software the device is running:

  ```
  #show version
  ```

- To view whether the device is running developer mode or production mode:

  ```
  #show ida
  ```

- To view the status of IOx:

  ```
  #show iox summary
  #show iox details
  ```

- To display debugging information when working with support:

```
#show tech support
```

Examples of Show Commands

```
ic3k>show
dns
ida
interfaces
iox
ntp
operating-mode
tech-support
version

ic3k>show dns
search cisco.com
nameserver 171.70.168.183  > The DNS Server is obtained via DHCP

ic3k>show ida status
Status: Running                     > The ida is running
Operation Mode: Production          > The device is in production mode
FND Host: 172.27.88.60:9121         > The device is connected to an FND host IP address
FND Connection Status: Connected    > The device is connected to FND
Periodic Metrics Interval: 300      > The device will update its metrics every 300 seconds
Heartbeat Interval: 60              > What is the heartbeat for?
Is Registered: True                 > The device is registered with FND
HTTP Server Status: N/A (Stopped)

ic3k>show version
Version: 1.0.1
Platform ID: IC3000-2C2F-K9
Hardware ID: FOC2227Y304
ic3k>

ic3k>show interfaces
dpbr_0    Link encap:Ethernet  HWaddr 52:54:00:b2:0a:6f
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:157904 errors:0 dropped:556 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7520723 (7.1 MiB)  TX bytes:0 (0.0 B)

dpbr_0-nic Link encap:Ethernet  HWaddr 52:54:00:b2:0a:6f
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

dpbr_n_0  Link encap:Ethernet  HWaddr 52:54:00:a1:2b:7b
          inet addr:192.168.10.1  Bcast:0.0.0.0  Mask:255.255.255.224
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

dpbr_n_0-nic Link encap:Ethernet  HWaddr 52:54:00:a1:2b:7b
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

```
int1      Link encap:Ethernet  HWaddr f8:b7:e2:b5:ed:83
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Memory:809a0000-809bffff

int2      Link encap:Ethernet  HWaddr f8:b7:e2:b5:ed:84
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Memory:809c0000-809dffff

int3      Link encap:Ethernet  HWaddr f8:b7:e2:b5:ed:85
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Memory:809e0000-809fffff

int4      Link encap:Ethernet  HWaddr f8:b7:e2:b5:ed:86
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Memory:80a00000-80a1ffff

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:5038 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5038 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1047250 (1022.7 KiB)  TX bytes:1047250 (1022.7 KiB)

mgmt0     Link encap:Ethernet  HWaddr f8:b7:e2:b5:ed:80
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:173199 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6432 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11348931 (10.8 MiB)  TX bytes:1051377 (1.0 MiB)
          Memory:80000000-807fffff

sit0      Link encap:UNSPEC  HWaddr 00-00-00-00-30-30-30-00-00-00-00-00-00-00-00-00
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

svcbr_0   Link encap:Ethernet  HWaddr f8:b7:e2:b5:ed:80
          inet addr:172.27.88.6  Bcast:172.27.88.127  Mask:255.255.255.128  <<svcbr_0 address
          inet6 addr: fe80::fab7:e2ff:feb5:ed80/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:164135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6411 errors:0 dropped:0 overruns:0 carrier:0
```

```
          collisions:0 txqueuelen:1000
          RX bytes:8055206 (7.6 MiB)  TX bytes:1049871 (1.0 MiB)

veth0_0   Link encap:Ethernet  HWaddr 22:24:b5:97:78:88
          inet6 addr: fe80::2024:b5ff:fe97:7888/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:158137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:648 (648.0 B)  TX bytes:9751066 (9.2 MiB)

veth1_0   Link encap:Ethernet  HWaddr ea:75:6b:25:a2:3e
          inet6 addr: fe80::e875:6bff:fe25:a23e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:158137 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9751066 (9.2 MiB)  TX bytes:648 (648.0 B)



ic3k>

ic3k>show ntp
NTP Servers received from DHCP:
171.70.168.183
ic3k>

ic3k>show iox summary
IOx Infrastructure Summary:
---------------------------
eid: IC3000-2C2F-K9+FOC2227Y304
pfm: IC3000-2C2F-K9
s/n: FOC2227Y304
images: Lnx: 1.0.1., IOx: 1.7.0:r/1.7.0.0:fc6e9cf
boot: 2018-09-17 17:37:55
time: 2018-09-18 18:07:28
load: 18:07:28 up 1 day, 29 min, 0 users, load average: 0.32, 0.11, 0.02
memory: ok, used: 481/7854 (6%)
disk: ok, used: /:270305/338869 (79%), /software:57272/87462892 (0%)
process: warning, running: 4/5, failed: sshd
networking: ok
logs: ok, errors: caf (0)
apps: ok,


ic3k>show iox detail
IOx Infrastructure Summary:
---------------------------
eid: IC3000-2C2F-K9+FOC2227Y304
pfm: IC3000-2C2F-K9
s/n: FOC2227Y304
images: Lnx: 1.0.1., IOx: 1.7.0:r/1.7.0.0:fc6e9cf
boot: 2018-09-17 17:37:55
time: 2018-09-18 18:07:22
load: 18:07:22 up 1 day, 29 min, 0 users, load average: 0.03, 0.05, 0.00
memory: ok, used: 482/7854 (6%)
disk: ok, used: /:270305/338869 (79%), /software:57272/87462892 (0%)
process: warning, running: 4/5, failed: sshd
networking: ok
logs: ok, errors: caf (0)
apps: ok,

Application Information:
------------------------
```

```
--Virsh--

Containers:
 Id    Name                           State
----------------------------------------------------

Virtual Machines:
 Id    Name                           State
----------------------------------------------------

Networking Information:
-----------------------

--Address--
svcbr_0 UP 172.27.88.6/25 fe80::fab7:e2ff:feb5:ed80/64

--Interface Stats--
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
svcbr_0 1500 0 164167 0 0 0 6412 0 0 0 BMRU
dpbr_0 1500 0 157935 0 556 0 0 0 0 0 BMRU
dpbr_n_0 1500 0 0 0 0 0 0 0 0 0 BMU

--Bridge Info--
bridge namebridge idSTP enabledinterfaces
dpbr_0  8000.525400b20a6fnodpbr_0-nic
                           veth1_0
dpbr_n_08000.525400a12b7bnodpbr_n_0-nic
svcbr_0 8000.f8b7e2b5ed80nomgmt0
                           veth0_0

--IP Routes--
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 172.27.88.1 0.0.0.0 UG 0 0 0 svcbr_0
172.27.88.0 0.0.0.0 255.255.255.128 U 0 0 0 svcbr_0
192.168.10.0 0.0.0.0 255.255.255.224 U 0 0 0 dpbr_n_0

Process Information:
--------------------

--Monit--
Process 'igma'
 status Running
 pid 1147
 uptime 1d 0h 28m
 memory percent total 0.1%
 cpu percent total 0.0%
Process 'libvirtd'
 status Running
 pid 1015
 uptime 1d 0h 28m
 memory percent total 0.1%
 cpu percent total 0.0%
Process 'caf'
 status Running
 pid 1109
 uptime 1d 0h 28m
 memory percent total 0.6%
 cpu percent total 0.0%

--Process Info--
  PID STIME CMD
 1073 Sep17 /usr/bin/monit -s /var/run/monit.state
```

```
 1109 Sep17 python /home/root/iox/caf/scripts/startup.pyc /home/root/iox/caf/config/system-config.ini
/home/root/iox/caf/config/log-config.ini
 1015 Sep17 /usr/sbin/libvirtd --daemon --listen
Error: /usr/sbin/sshd not found
 1147 Sep17 /usr/bin/igma
--PID info--
monit:1073
caf:1109
libvirtd:1015
sshd:0
igma:1147

Disk Usage Information:
-----------------------

--Free Disk--
Filesystem 1024-blocks Used Available Capacity Mounted on
/dev/root 362084 270305 68564 80% /
/dev/sda2 92167844 57272 87405620 1% /software

--Mount--
/dev/ram on / type ext4 (rw,relatime,data=ordered)
/dev/sda2 on /software type ext4 (rw,relatime,data=ordered)
tmpfs on /run type tmpfs (rw,nosuid,nodev,mode=755)
tmpfs on /var/volatile type tmpfs (rw,relatime)
cgroup on /sys/fs/cgroup type tmpfs (rw,relatime,mode=755)

--Top Disk Usage--
/*:
233M/usr
99M /golden
/software/*:
208K/software/caf
28K /software/ssh
ic3k>

ic3k>help developer-mode

In developer mode, the IC3000 is an unmanaged development device. It will be controlled via Local
Manager and ioxclient.

1. Set the password for "developer" user (use command developer set-password).
2. Connect the Management interface on the IC3000 to your Computer with a network cable.
3. Assign "169.254.128.4 (netmask 255.255.0.0)" IP address to the network interface on your computer.
NOTE: It is critical you assign this specific IPv4 link-local address.
4. The IC3000 will be ready to operate in Developer mode in 30 seconds (The delay of 30 seconds only
occurs the first time the IC3000 is booted up. All subsequent reloads will immediately take the IC3000
to developer mode without delay).
5. Access "https://169.254.128.2:8443" from your browser on the computer.
6. Login using the "developer" user and password you set in step #1 above.

ic3k>help production-mode

In production mode, the IC3000 is managed by the IoT Field Network Director (FND).

1. Setup a DHCP server for assigning an IP address to the management interface.
2. DHCP server MUST provide "option 43" to the IC3000 for FND discovery.
         - Option 43 string must carry "I<fnd ip or host>". Example - "I172.27.133.25"
3. Connect the management interface to the DHCP server.
4. Claim the IC3000 on the FND setup suitable configurations. Follow FND User Guide from Cisco's
website.
5. The IC3000 will connect with FND after the DHCP discovery process is completed.

ic3k>
```

Local Manager Related

The Local Manager GUI provides some details on your device status.

- To debug Application status use the **APP Tab**
- To download APP logs go to the **APP Tab > Manage APP > APP-Dir** or **App-Logs** and download the logs.
- To view Application failure issues go to the **System Troubleshooting Tab** and look for events or errors.
- To turn off the Developer Mode, go to **Device-Config > Developer Mode Off.**

FND Related

If your device is not registering with FND, check the following:

- Check the option 43 address format, and validate if it is the correct ip address of FND
- Check the platform **show ida** status and **show interfaces** status to see which ip address the device has learned.
- Check the FND provisional setting URL to ensure FND IP address:9121
- Check whether the serial number in the FND input file is accurate

FND Logs

See the following table for details on the location and names of FND log files.

File Type	Host	Container	Files
FND-logs	/opt/fnd/logs/	/opt/cgms/server/cgms/log/	cgms_setup.log server.log access_log.<date> cgms_stacktrace.log cgms_db_connection_test.log cgms_status.log
FND-data	/opt/fnd/data/	/tmp/fnd-data/	cgms_keystore.selfsigned cgms.properties userPropertyTypes.xml
FND-scripts	/opt/fnd/scripts/	N/A	upgrade-fnd.sh (To upgrade FND docker image) **Note**: If required Postgres, Influx rpm has to be upgraded separately on the host.)
Docker environment	/opt/fnd/conf/	N/A	fnd-env.list

See the following table for details on the location and names of FD log files.

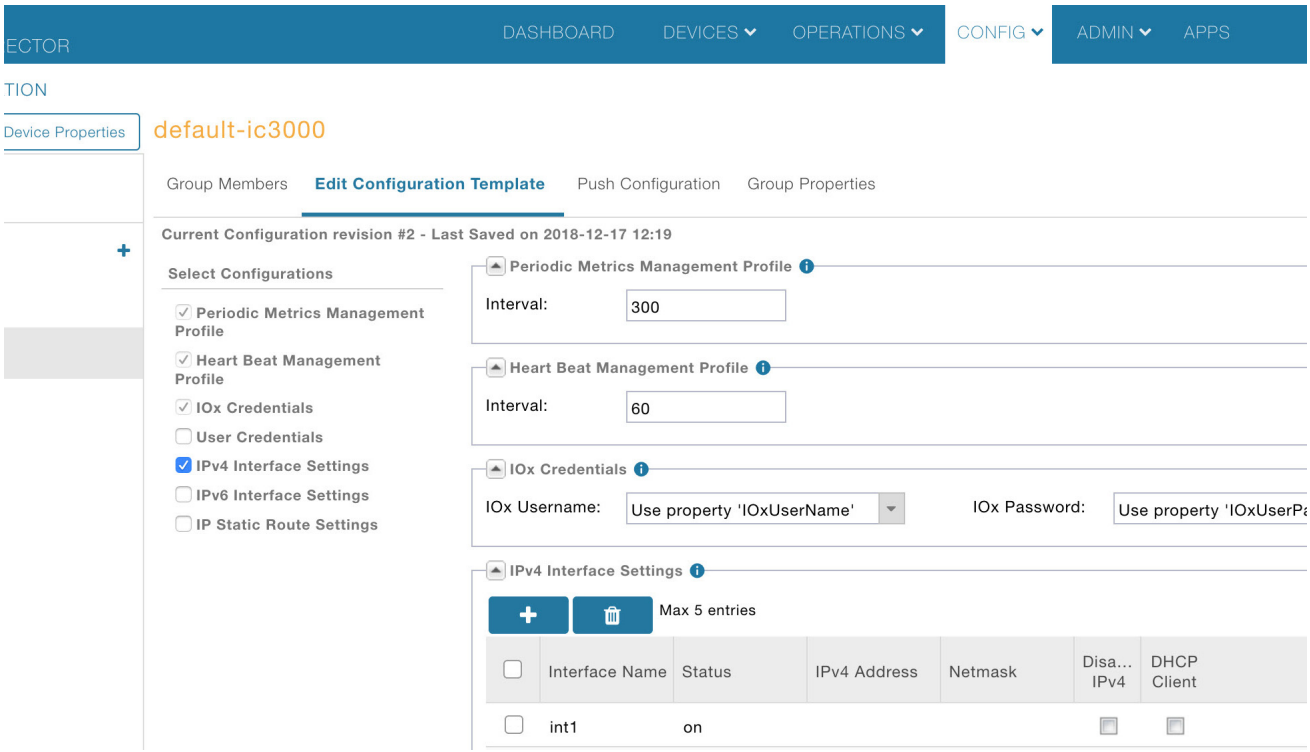
File Type	Host	Container	Files
FD-logs	/var/lib/docker/volumes /fd_logs/_data/	/var/log/fd	application.log appmgr-console.log catalina.out host-manager.<date>.log manager.<date>.log appmgr-backup-restore.log catalina.<date>.log hibernate localhost.<date>.log metrics usagestats
FD-data	/var/lib/docker/volumes /fogd_data/_data/	/var/cisco/appmgr	.bash_history .bashrc backup certificate extensions fog_director.properties .InstallAnywhere .java .keystore .profile .rnd
FD-scripts	/opt/fogd/scripts/		upgrade-fogd.sh (To upgrade FogD docker image)
Docker environment	/opt/fogd/conf/		fogd-env.list

Appendix: FND 4.3 device-configuration templates (Deprecated)

Understand the default values and select the other parameters as required and save the template. Use the (i) button to understand the optional and mandatory parameters.

Once complete, push the configurations to the devices using the **Push Configuration tab** on the top of the window.

Figure 27 Edit Configuration Template



For the FND 4.3.1 release, the JSON formats for editing a particular IC3000 device are as follows:

```
Bring up interface:
"{
"name": "InterfaceSettings",
"value": {
"ifName": "int1",
"status": 1
}
}

Bring down interface:
{
"name": "InterfaceSettings",
"value": {
"ifName": "int2",
"status": 0
}
}

Setting DHCP:
{
"name": "InterfaceSettings",
"value": {
"ifName": "int3",
"dhcpClient": 1
}
}

Setting static IP:
{
"name": "InterfaceSettings",
"value": {
```

```
"ifName": "int4",
"status": 1,
"ipv4": "12.23.34.45",
"netmask": "255.255.255.0"
}
}

Create user:
{
"name": "UserMgmt",
"value": {
"userName": "user1",
"newPassword": "passwd4user1!"
}
}

Delete user:
{
"name": "UserMgmt",
"value": {
"userName": "user1",
"delUser": "True"
}
}

Change user password:
{
"name": "UserMgmt",
"value": {
"userName": "user1",
"oldPassword": "passwd4user1!",
"newPassword": "user1passwd!"
}
}
```

To download a text file with clean JSON entries, go here:

https://www.cisco.com/c/dam/en/us/td/docs/routers/ic3000/deployment/guide/IC3000-JSON.txt

Note: Make sure your JSON is validated properly before pushing the configuration to device. It is highly recommended to use a JSON validator such as this one:

https://jsonlint.com/

Copy and paste your entire device configuration template and see if its set appropriately. Anything that's commented has to be removed before validation.

A typical comment section in json is between the following characters.

<#--

Comment text here

-->

As an example, a working JSON entry for bringing all the interface up on IC3000 is as follows.

```
[{
        "name": "MgmtProfile",
        "value": {
            "id": 2,
            "name": "PeriodicMetrics",
            "interval": 300,
            "dataIds": ["5", "18", "23", "24", "25"]
        }
```

```
    }, {
        "name": "UserMgmt",
        "value": {
            "userName": "${device.IOxUserName}",
            "newPassword": "${device.IOxUserPassword}"
        }
    },
    {
        "name": "MgmtProfile",
        "value": {
            "id": 1,
            "name": "Heartbeat",
            "interval": 60,
            "dataIds": ["4"]
        }
    }, {
        "name": "InterfaceSettings",
        "value": {
            "ifName": "int1",
            "status": 1
        }
    }, {
        "name": "InterfaceSettings",
        "value": {
            "ifName": "int2",
            "status": 1
        }
    }, {
        "name": "InterfaceSettings",
        "value": {
            "ifName": "int3",
            "status": 1
        }
    }, {
        "name": "InterfaceSettings",
        "value": {
            "ifName": "int4",
            "status": 1
        }
    }
]
```

Appendix: Installing Cisco IoT Field Network Director (Cisco IoT FND)

This section provides the steps required to install the Cisco IoT Field Network Director (Cisco IoT FND) Release 4.3.1 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 4.3 and Oracle on an OVA for Release 4.3, 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

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, Release 4.3.x.

Prerequisites

- Access to the VMware ESXi server.
  - Contact your IT administrator to obtain the IP address to the VMware ESXi server.

  or

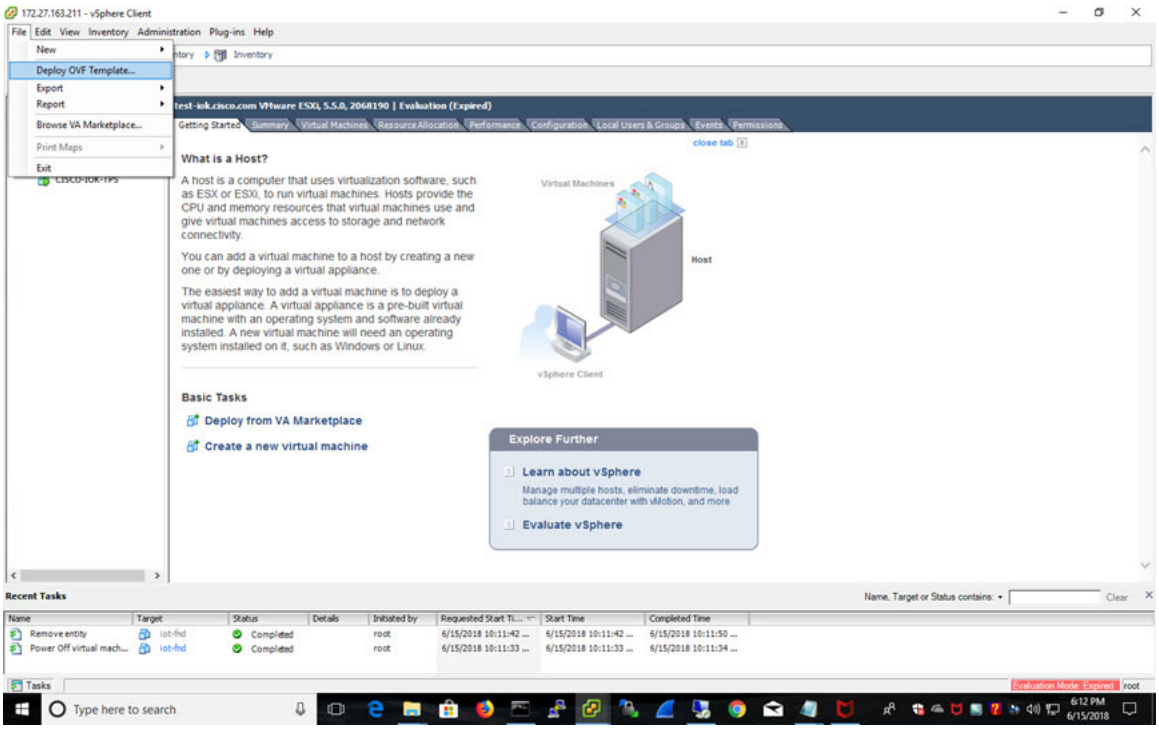
  - If you are installing the VMware ESXi server software yourself, go to the VMware ESXi site to download the software: https://www.vmware.com/products/esxi-and-esx.html
- Install the VMware vSphere Client for the ESXi 5.5 or 6.0 server.
- Locate the VMware credentials to create virtual machines in ESXi 5.5. or 6.0, respectively.
- Ensure that you meet the VMware server machine requirements. Listed below are the VM CPU and memory requirements for a small scale deployment:

  NMS OVA

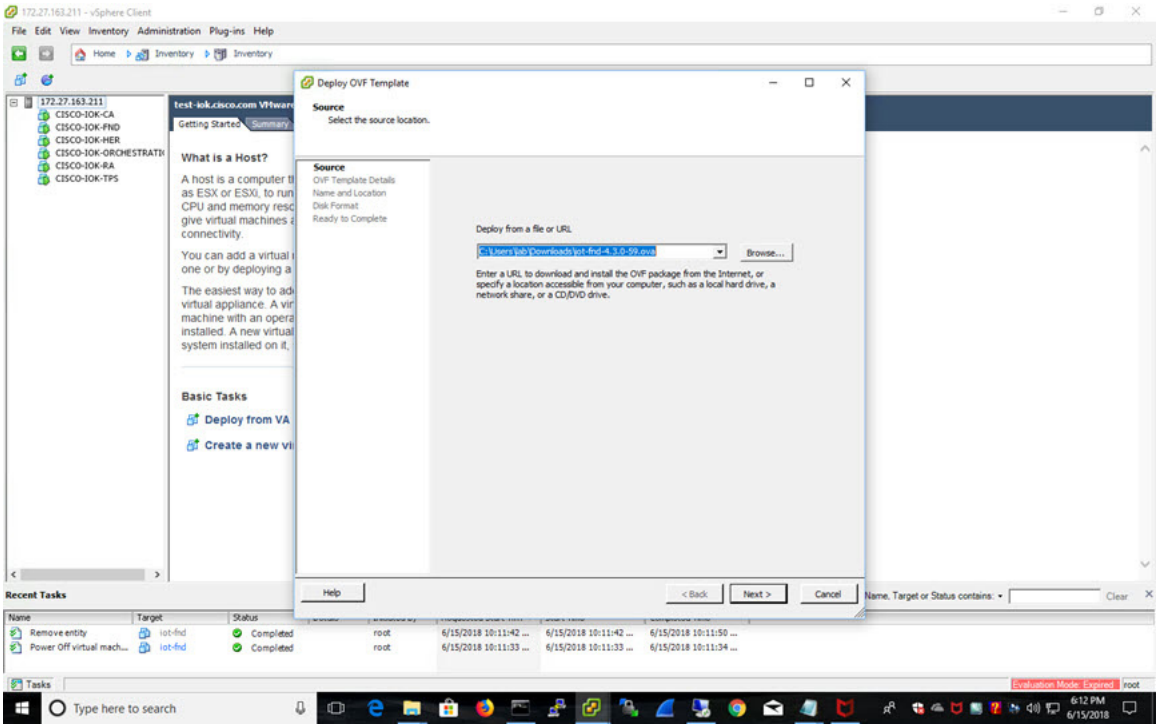
  - 16 GB memory
  - 1 core and 4 virtual sockets
  - 150 GB of virtual storage
- Download the OVA from Cisco.com.

Installing the OVA

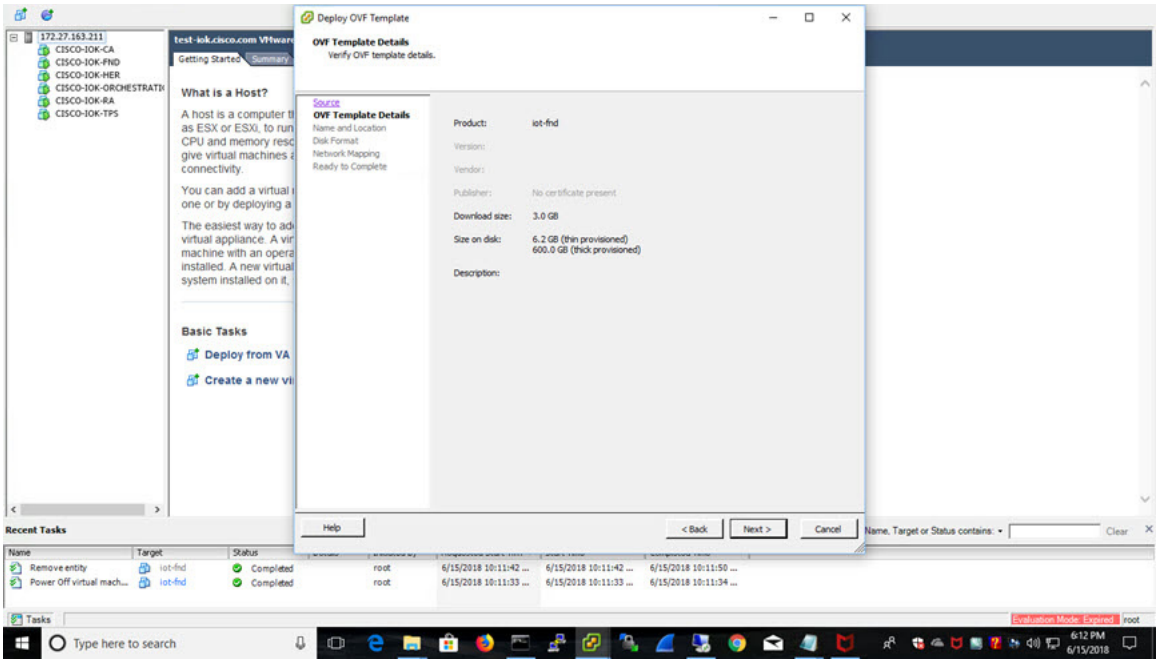
1. Use VMware Fusion or VMware vSphere client to deploy OVA on ESXi Server. Do not change the defaults for the installation.
   a. Under File, choose Deploy OVF template.



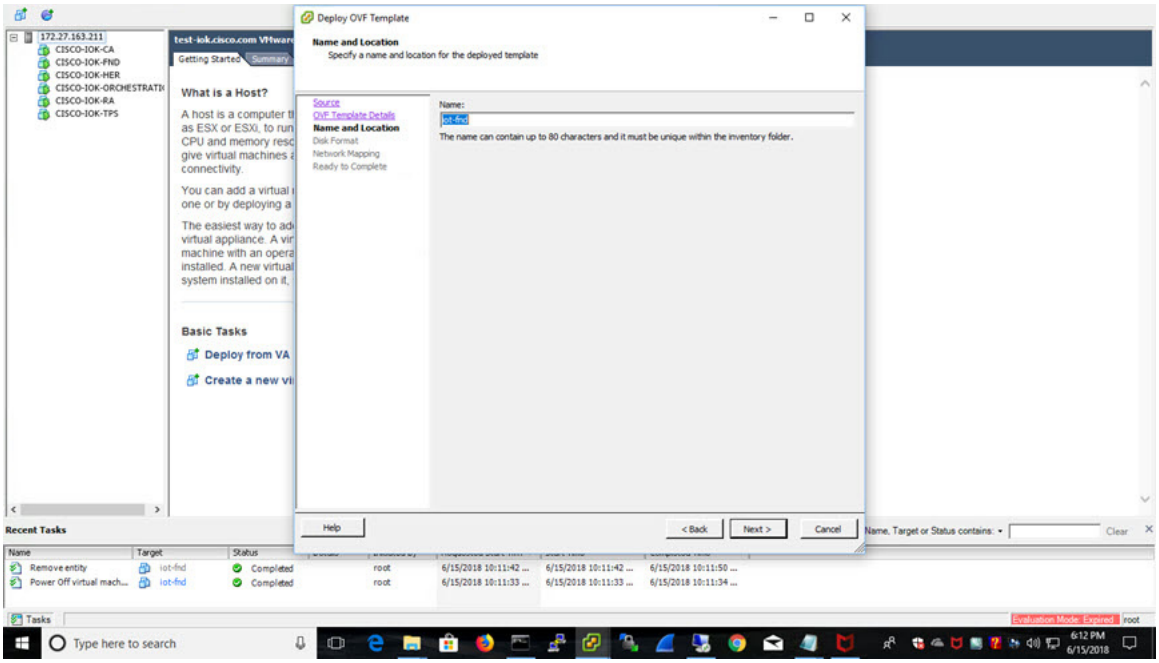
b. Keep the default location and click Next.



c. Click Next.

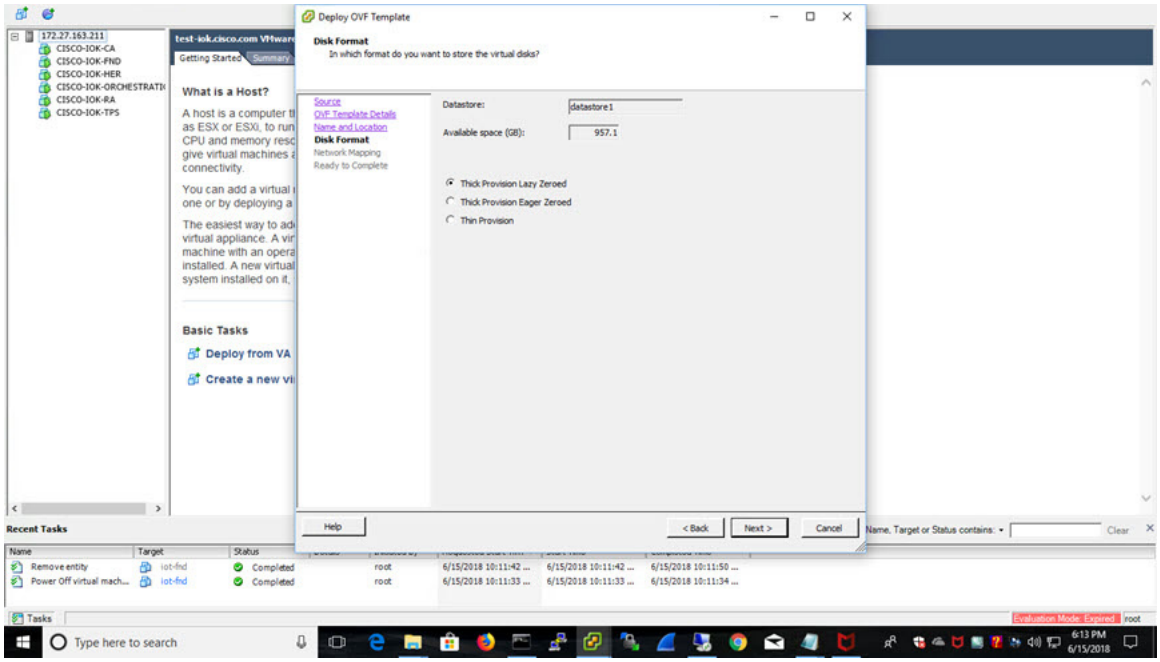


d. Enter a name of the deployed template.

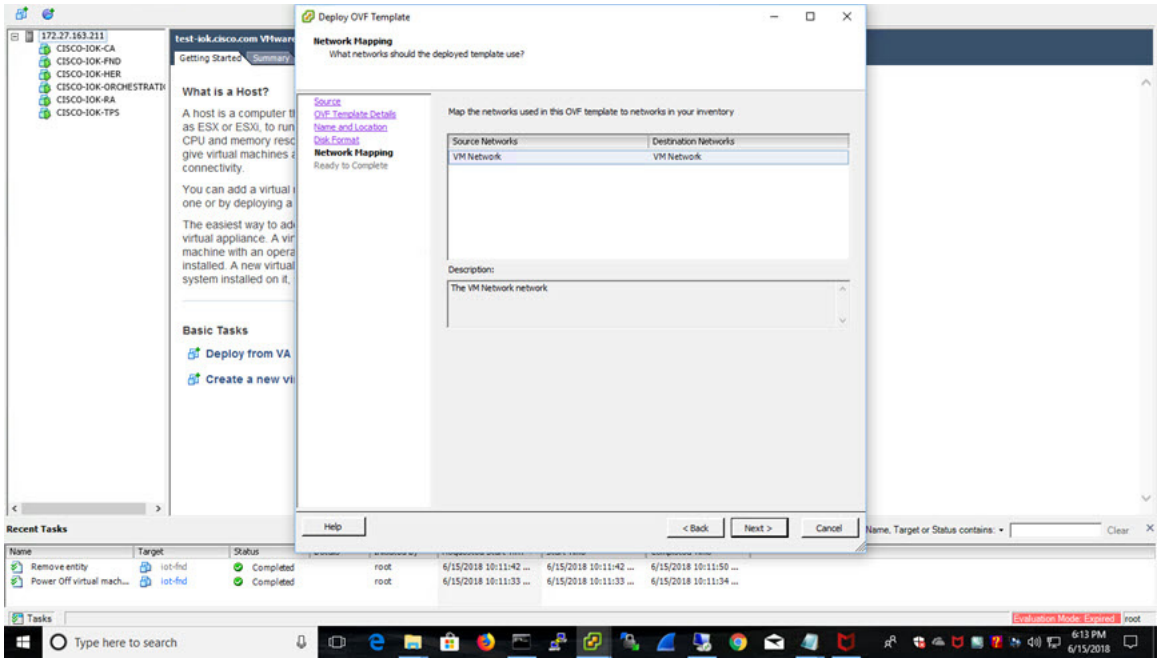


e. Choose the format that you want virtual disks to be stored.

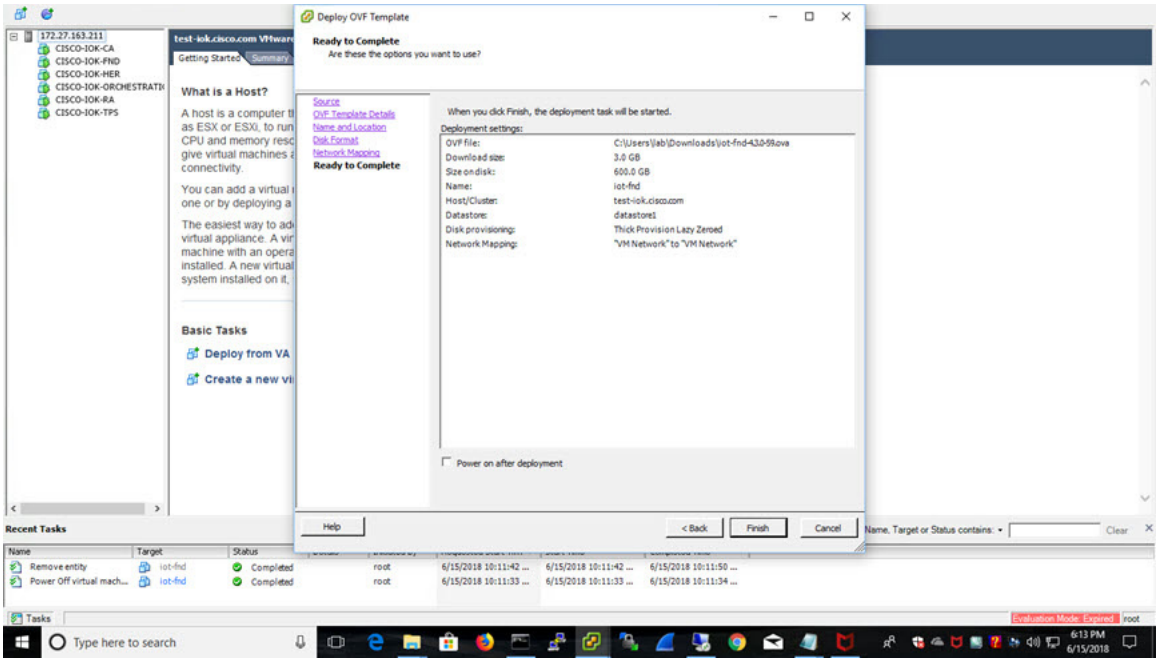
Note: Thick provisions require 600 GB of disk space on the ESXi server.



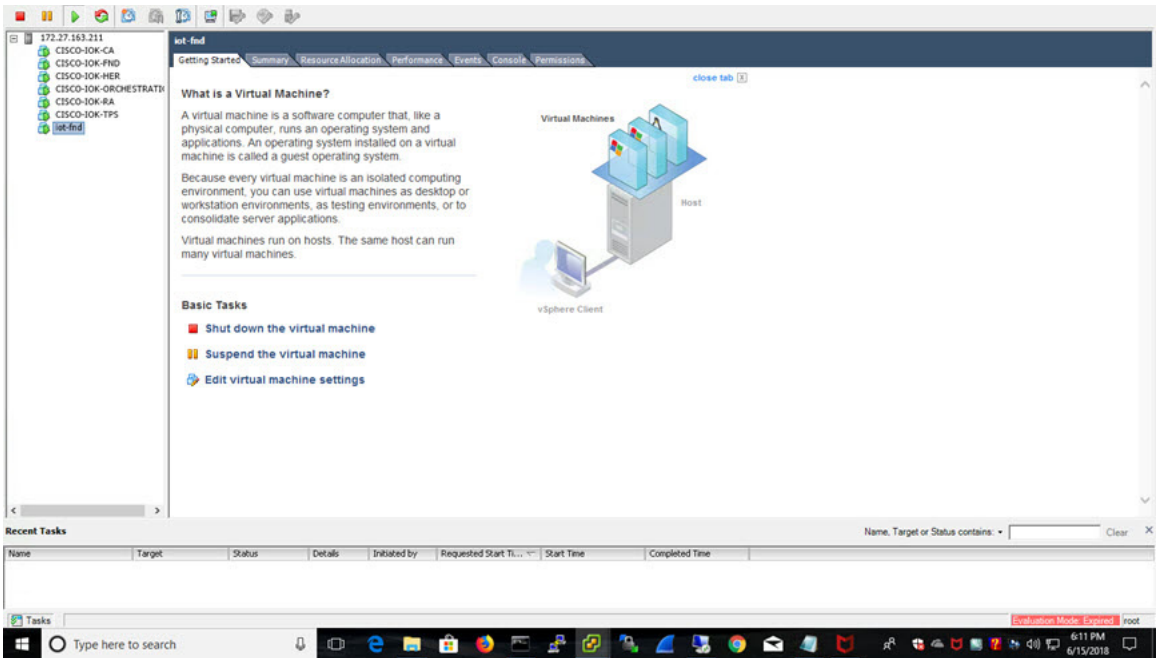
f. Click Next.



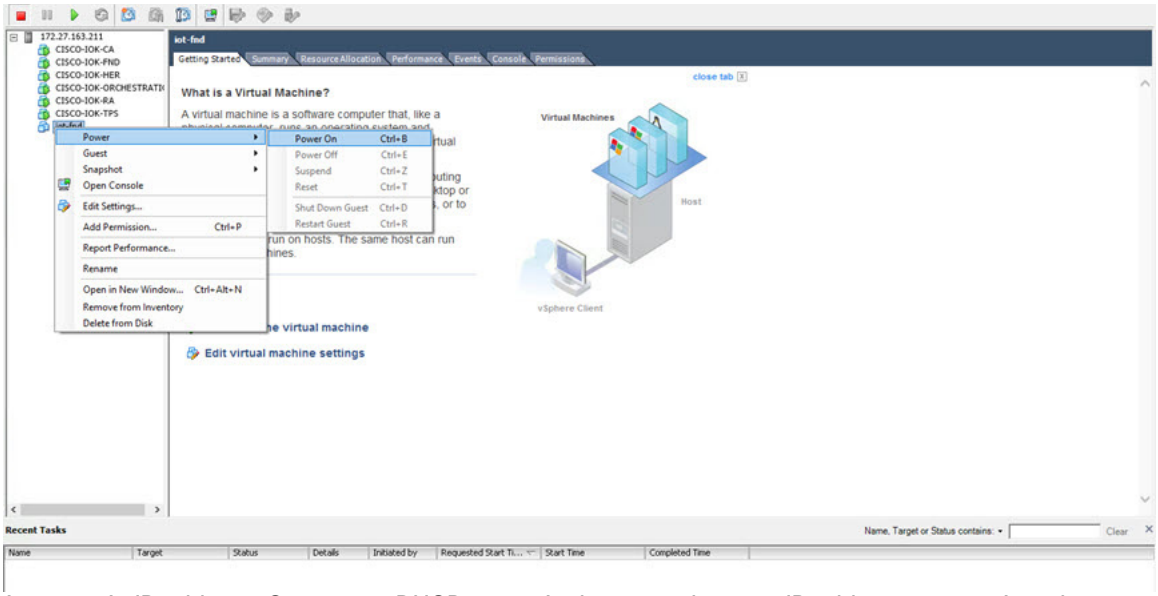
g. Review and click Finish.



The template starts downloading. When it is completed, the template is listed on the left pane.

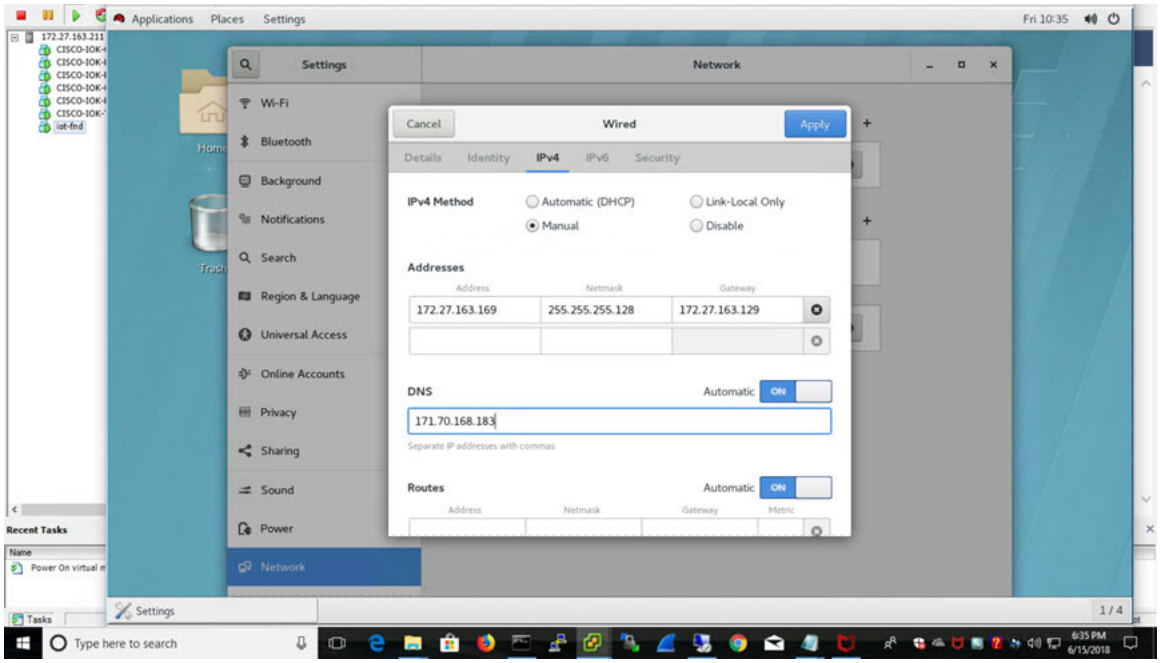


2. Power on the VM. Right click on the iot-fnd template name. Select Power and Power On.



3. Assign a static IP address. Or, setup a DHCP server in the network, so an IP address gets assigned.

   Setup a valid, reachable working DNS server on the Host VM. (mandatory)



   Use this IP address to access the FND GUI.

4. Click on Console and login with root/cisco123 once the OS is up.

   a. Once logged in, navigate to Applications -> System Tools ->Settings ->Network.

   b. Click the plus sign (+).

5. From a web browser, access FND URL and change the password for the root user. Default username/password is root/root123.

6. Open a terminal window, and setup 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, FND starts monitoring Fog Director container on the ADMIN → SERVERS page.

Using a Custom cgms_keystore in the FND Container

Enter the following information to provide a secure connection to devices within this OVA deployment.

Use these steps to have FND use your custom keystore.

1. Put your cgms_keystore file in /opt/fnd/data/ on the Host.
2. Run the following command to encrypt the password for the new cgms_keystore:

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

```
[root@iot-fnd ~]# docker exec -it fnd-container /opt/cgms/bin/encryption_util.sh encrypt cisco123
2bVvZsq+vsq94YxuAKdaag==
```

3. 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.

Configuring FND for IPv6 Tunnel Provisioning and Registration

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:

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 ens32 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 ~]#
```

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.

```
[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
```

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.

Installing Custom CA Certificates on FND

By default the FND container comes bundled with cgms_keystore.

- Keystore Location in the FND Container: /opt/cgms/server/cgms/conf/
- Keystore Name: cgms_keystore
- Default Password: Public123!
- Default Trusted Certification Entry in Keystore: cisco_sudi, jmarconi

To use a custom CA certificate on the router, add a CA certificate to the trusted certificate entries in the cgms_keystore.

1. Place the certificate file in the following location on the host machine.

   /opt/fnd/data/

2. Enter into FND container

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

3. Change into the conf directory.

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

4. Import a root or intermediate CA certificate to cgms_keystore.

/opt/cgms/jre/bin/keytool -import -trustcacerts -alias alias-name -file /tmp/fnd-data/ca.crt -keystore cgms_keystore

Use a preferred alias name

5. Restart FND.

   /etc/init.d/cgms restart

6. Verify that the certificate was added to the trusted entry.

   /opt/cgms/jre/bin/keytool -list -v -keystore cgms_keystore

   Enter keystore password.

Upgrading FND

To update FND, you must have access to dockerhub.cisco.com.

Run the upgrade-fnd.sh script from the following directory:

1. cd /opt/fnd/scripts/

The following examples show the upgrade process which includes upgrading cgms-postgres.rpm and cgms-influx.rpm.

```
[root@iot-fnd scripts]# ./upgrade-fnd.sh
This script must be run with root privileges.
Usage: All upgrade: Requires <path to cgms-postgres.rpm> and <path to cgms-influx.rpm>
       For FND container upgrade: No resource required
       For FND Postgres RPM upgrade: Requires <path to cgms-postgres.rpm>
       FND Influx RPM upgrade: Requires <path to cgms-influx.rpm>

1) Full upgrade              4) FND Influx RPM upgrade
2) FND container upgrade     5) Quit
3) FND Postgres RPM upgrade
Enter your choice: 3
Enter cgms-postgres rpm file path:
/root/cgms-postgres-4.3.0-48.x86_64.rpm
Stopping FND container...
fnd-container
Preparing...                          ################################# [100%]
Updating / installing...
   1:cgms-postgres-4.3.0-48           ################################# [ 50%]
Cleaning up / removing...
   2:cgms-postgres-4.3.0-47           ################################# [100%]
Starting FND container...
```

```
[root@iot-fnd scripts]# ./upgrade-fnd.sh
This script must be run with root privileges.
Usage: All upgrade: Requires <path to cgms-postgres.rpm> and <path to cgms-influx.rpm>
       For FND container upgrade: No resource required
       For FND Postgres RPM upgrade: Requires <path to cgms-postgres.rpm>
       FND Influx RPM upgrade: Requires <path to cgms-influx.rpm>

1) Full upgrade              4) FND Influx RPM upgrade
2) FND container upgrade     5) Quit
3) FND Postgres RPM upgrade
Enter your choice: 2
Stopping FND container...
fnd-container
Remove FND container...
fnd-container
Prune Docker container...
WARNING! This will remove all stopped containers.
Are you sure you want to continue? [y/N] Total reclaimed space: 0B
Downloading latest FND docker image...
latest: Pulling from field-network-director-dev-docker/fnd-image
469cfcc7a4b3: Already exists
78e1c8192d09: Already exists
24106544ca78: Already exists
7ad1c8dc78ad: Already exists
3ed6a9248eed: Already exists
ae1446b14021: Already exists
ba0a265aacaf: Already exists
Digest: sha256:4451daf1d8b0f0d7f370dda8c553a68807d545a881e059029f6f0b0a31cfd6b1
Status: Image is up to date for dockerhub.cisco.com/field-network-director-dev-docker/fnd-image:latest
Starting FND container...
4bc00c18b2c83f7f10215878c9552a17fecc9e852949ab80348e448ea25d6fb2
```

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
```

Upgrading Fog Director

To update Fog Director, you must have access to dockerhub.cisco.com.

Run the upgrade-fogd.sh script from the following directory:

cd /opt/fogd/scripts

```
[root@iot-fnd scripts]# ./upgrade-fogd.sh
Stopping Fog Director container...
fogd-container
Remove Fog Director container...
fogd-container
Prune Docker container...
WARNING! This will remove all stopped containers.
Are you sure you want to continue? [y/N] Total reclaimed space: 0B
Downloading latest Fog Director docker image...
latest: Pulling from fog-director-dev-docker/fogd-image
324d088ce065: Already exists
2ab951b6c615: Already exists
9b01635313e2: Already exists
04510b914a6c: Already exists
83ab617df7b4: Already exists
39460e334589: Already exists
c6dff050367e: Already exists
2b0b56e80504: Already exists
54614f34f9fa: Already exists
24f76a367fd4: Already exists
Digest: sha256:0a4d1ae165aa6be0de20c1196055ab5153b34f808bc08aaaf9087eb23bd805cf
Status: Image is up to date for dockerhub.cisco.com/fog-director-dev-docker/fogd-image:latest
Starting Fog Director container...
f2bc75fa77c29127f7cc7de7e9cba9011e7d09e8dbcf692729141b94e0815cf6
[root@iot-fnd scripts]#
```

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]#
```

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]#
```

Upgrading Both Fog Director and FND

Use the upgrade.sh script in the following directory to fully upgrade both Fog Director and FND.

opt/fnd/scripts/

Note: Since this performs a full FND upgrade, you must provide the paths to cgms-postgres.rpm and cgms-influx.rpm

```
[root@iot-fnd scripts]# ./upgrade-fnd.sh
This script must be run with root privileges.
Usage: All upgrade: Requires <path to cgms-postgres.rpm> and <path to cgms-influx.rpm>
       For FND container upgrade: No resource required
       For FND Postgres RPM upgrade: Requires <path to cgms-postgres.rpm>
       FND Influx RPM upgrade: Requires <path to cgms-influx.rpm>

1) Full upgrade              4) FND Influx RPM upgrade
2) FND container upgrade     5) Quit
3) FND Postgres RPM upgrade
Enter your choice: 2
Stopping FND container...
fnd-container
Remove FND container...
fnd-container
Prune Docker container...
WARNING! This will remove all stopped containers.
Are you sure you want to continue? [y/N] Total reclaimed space: 0B
Downloading latest FND docker image...
latest: Pulling from field-network-director-dev-docker/fnd-image
469cfcc7a4b3: Already exists
78e1c8192d09: Already exists
24106544ca78: Already exists
7ad1c8dc78ad: Already exists
3ed6a9248eed: Already exists
ae1446b14021: Already exists
ba0a265aacaf: Already exists
Digest: sha256:4451daf1d8b0f0d7f370dda8c553a68807d545a881e059029f6f0b0a31cfd6b1
Status: Image is up to date for dockerhub.cisco.com/field-network-director-dev-docker/fnd-image:latest
Starting FND container...
4bc00c18b2c83f7f10215878c9552a17fecc9e852949ab80348e448ea25d6fb2
```

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.

1. Power down the OVA in vSphere Client.
2. Select the OVA, and then select File -> Export -> Export OVF Template.

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 ~]#
```

Please refer to the following link for more info on usage of timedatectl command

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/chap-configuring_the_date_and_time

Related Documentation

For information about FND, go to the following:

https://www.cisco.com/c/en/us/support/cloud-systems-management/iot-field-network-director/tsd-products-support-series-home.html

Cisco Fog Director Reference Guide:

http://www.cisco.com/c/en/us/support/cloud-systems-management/fog-director/products-technical-reference-list.html

Cisco IOx Local Manager User Guide

https://www.cisco.com/c/en/us/td/docs/routers/access/800/software/guides/iox/lm/reference-guide/1-6/iox_local_manager_ref_guide.html

For additional information about Cisco IOx, go to the following:

DevNet documentation on IOx. Provides an overview as well as details by scrolling down the left hand side:

https://developer.cisco.com/site/devnet/support/

Cisco IOx:

https://www.cisco.com/c/en/us/support/cloud-systems-management/iox/tsd-products-support-series-home.html