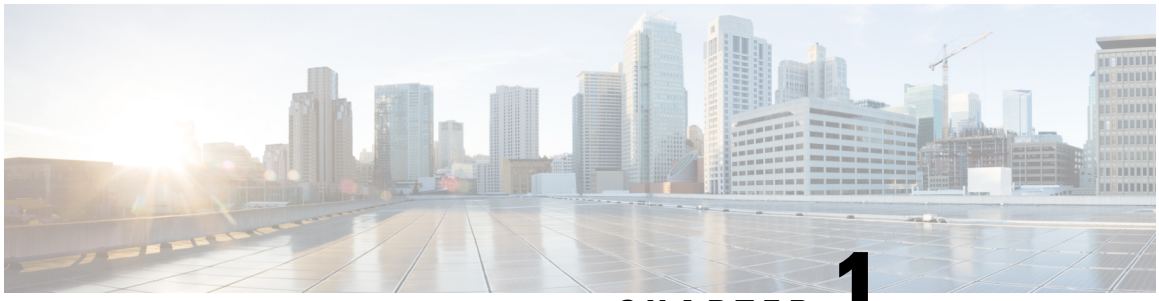
Cisco IC3000 Industrial Compute Gateway Deployment Guide

First Published: 2021-02-28

Last Modified: 2021-02-16

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



CHAPTER 1

Unboxing, Installing, and Connecting the IC3000

This section contains the following topics:

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.

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

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.

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

Procedure

Step 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

Step 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.

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.

Step 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.

What to do next

There is a new banner during boot starting with release 1.3.1, informing the user to use Local Manager or FND for configuring the networking and device. For example:

```
Press RETURN to get started


********************************************************************************

                      *
*     CLI is for viewing configuration, settings and device information       *
*
                                  *
*     Use Field Network Detector/Local Manager for configuring IC3000         *
********************************************************************************
```

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.

Table 1: show commands

Show Command	Description
show version	shows the version information
show dns	shows the domain name service information
show ida status	shows the device management tool connection information
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
show operating-mode	shows operating mode information
show ntp manual config	shows the ntp configuration pushed from FND or LM
show ntp association	shows the ntp association information
show ntp status	shows whether the device has been synced with ntp server
show ntp mode	shows whether ntp config mode is in auto or manual mode
show dns manual config	shows the dns configuration pushed from FND or LM
show dns mode	shows whether dns config mode is in auto or manual mode
show clock	shows the time on the device
help standalone-mode	shows instructions for configuring standalone-mode
help managed-mode	shows instructions for configuring managed-mode

Show Command	Description
show sfp information port3/port4	Shows the Fiber/Copper SFP details.
show golden image	Shows the golden image and golden application image (If the device is shipped with application).
show tech support usb2/sdcard	Show tech support no longer prints on console. Support has been added for downloading logs to usb2.

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

Related Documentation

All of the IC3000 documentation is found here:

https://www.cisco.com/c/en/us/support/routers/3000-series-industrial-compute-gateways/tsd-products-support-series-home.html

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/support/cloud-systems-management/iox/products-technical-reference-list.html

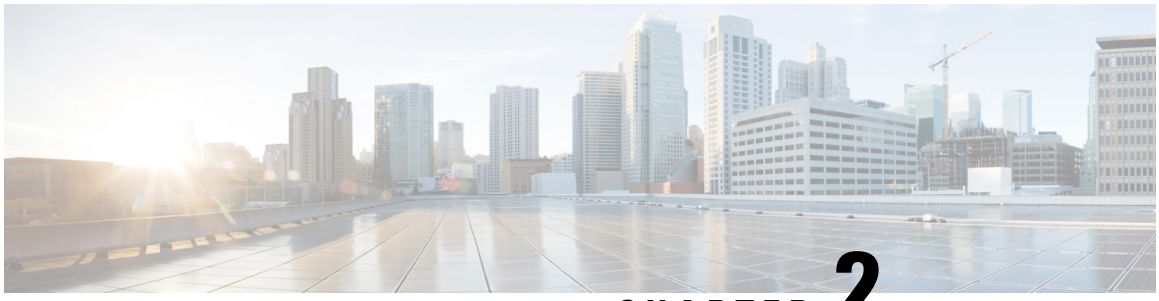
For additional information about Cisco IOx, go to the following:

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



CHAPTER 2

Managing the IC3000 with Field Network Director (FND)

The following steps show how to install and manage your device with FND.

Step 1: Installing FND

If this is your first time setting up the FND OVA infrastructure, go to Appendix for complete information.

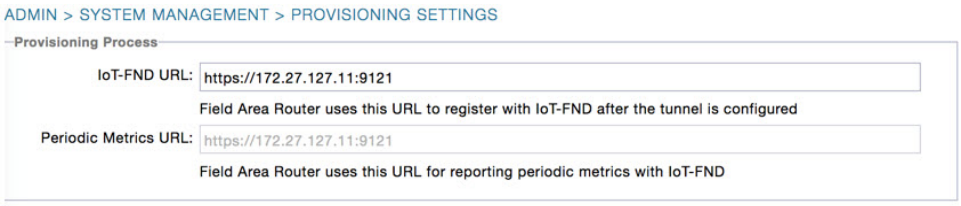
Download the IoT Field Network Director software from this location:

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 below. Otherwise, registration may fail.

Figure 1: Provisioning Settings



Step 2: DHCP Options

If the IC3000 gateway gets an IP address from the DHCP server, Option 43 is used to advertise the FND IP address and Option 42 is used to advertise the NTP server IP address via DHCP.

The management interface sends a DHCP option 60, also known as vendor-class-identifier, in its request. The device identification is sent as the string cisco-ic3000. Upon receiving the vendor-class-identifier, the DHCP server can take actions as required.

Example of DHCP Option 42 and 43

Configure the following on an IR8x9:

```
ip dhcp pool ic3000_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";
}
```

In the above example for option 43, the following describes the options:

- 5A;K4;B2;I172.27.88.63;J9125
  - 5 – DHCP type code 5
  - A – Active feature operation code
  - ; - Delimiter
  - K4 – HTTP transport protocol
  - B2 – PnP server /FND IP address type is IPv4
  - J9125 - port number

Option 42 Usage

The system time may not be synchronized when receiving the device from the factory. It is important to provide ntp server information to get the device clock to current time. This will avoid any issues when establishing a connection to FND and make sure the timestamp on data packets from apps are up to date.

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

```
cat /etc/ntp.conf
subnet 10.10.100.0 netmask 255.255.255.0 {
max-lease-time 604800;
default-lease-time 86400;
option ntp-servers 10.10.100.112;
}
```

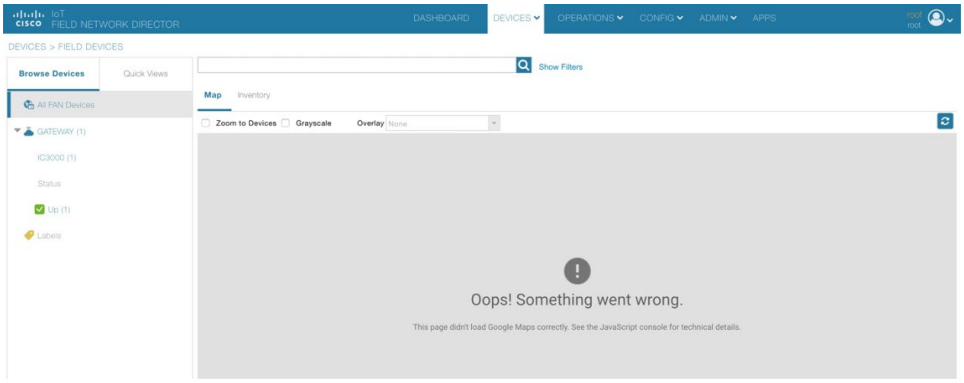
Step 3: Understanding the Device Configuration Template

There is a default template within the FND for IC3000. It is located under **CONFIG >Device Configuration tab > default-IC3000 > Edit Configuration template**. See Step 6: Adding the IC3000 Gateway(s) to FND, on page 10.

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 the following image. This error does not impact the operation of the device, you can still continue.

Figure 2: Map Error



Step 4: NTP Configuration

To push the NTP configuration via FND, perform the following:

Procedure

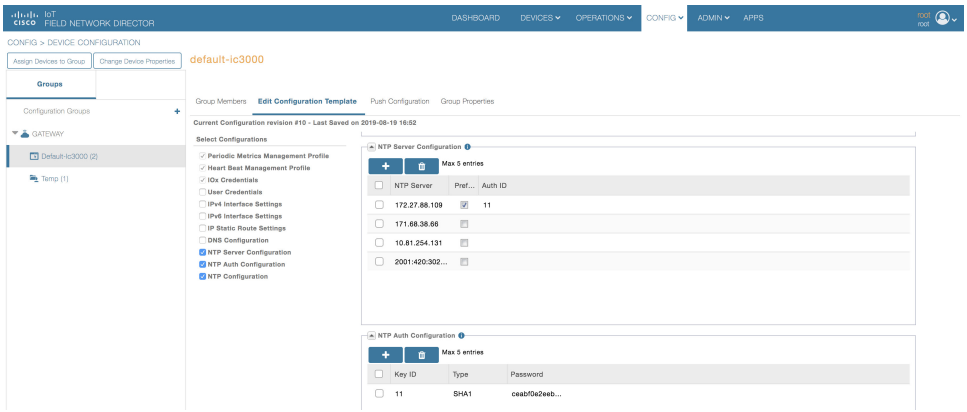
Step 1 Go to **FND GUI > Config > Device Configuration > Edit Configuration Template**.

Step 2 Select **both** the NTP Server Configuration and the NTP Configuration checkbox.

a) Optional: Select the **NTP Auth Configuration** checkbox if the NTP server has been configured with authentication. Add the Key ID and corresponding SHA1 key as the password. Refer to Figure 3: Add NTP Authentication, on page 8. **Note**: NTP Authentication is only offered for NTP servers that support SHA1.

b) Optional: Select the **Auto Get** checkbox under NTP Configuration to delete the NTP configuration that has been manually pushed onto the device from FND

Figure 3: Add NTP Authentication

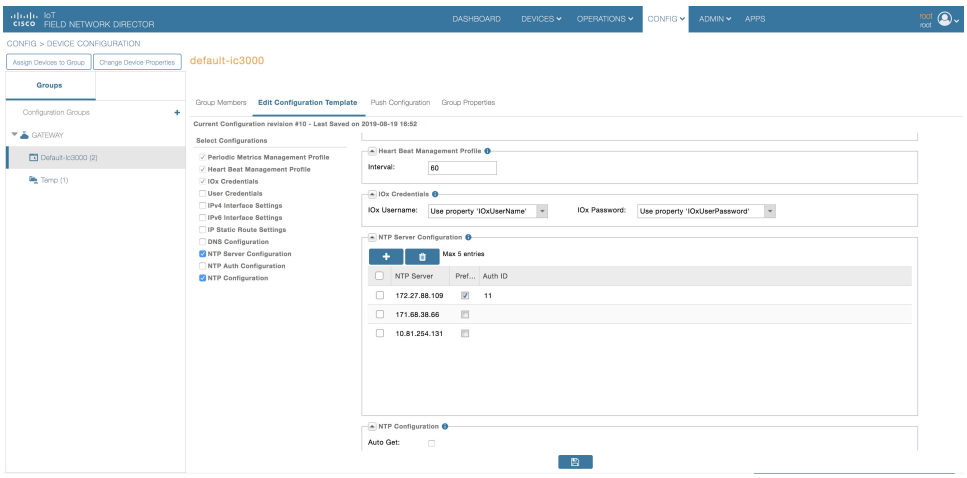


Step 3 Add the NTP server entry. Click the **+** symbol under NTP Server Configuration. Refer to Figure 4: Add NTP Configuration, on page 9.

a) To prioritize a certain NTP server for clock synchronization, click the **Preferred** checkbox

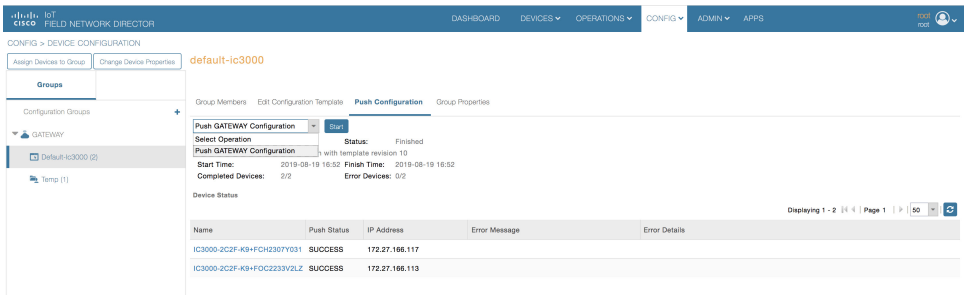
b) If NTP authentication is to be configured, add the Key ID set in the NTP Auth Configuration as the Auth ID.

Figure 4: Add NTP Configuration



Step 4 Push NTP configuration by going to **Push Configuration > Select Operation Scroll down > Push GATEWAY Configuration > Start**. Refer to Figure 5: Push NTP Configuration, on page 9.

Figure 5: Push NTP Configuration



Step 5 The NTP Configuration is now complete.

Step 5: DNS Configuration

To push DNS configuration via FND perform the following steps, referring to Figure 6: Add DNS Configuration, on page 10 for guidance.

Procedure

Step 1 Go to **FND GUI > Config > Device Configuration > Edit Configuration Template**.

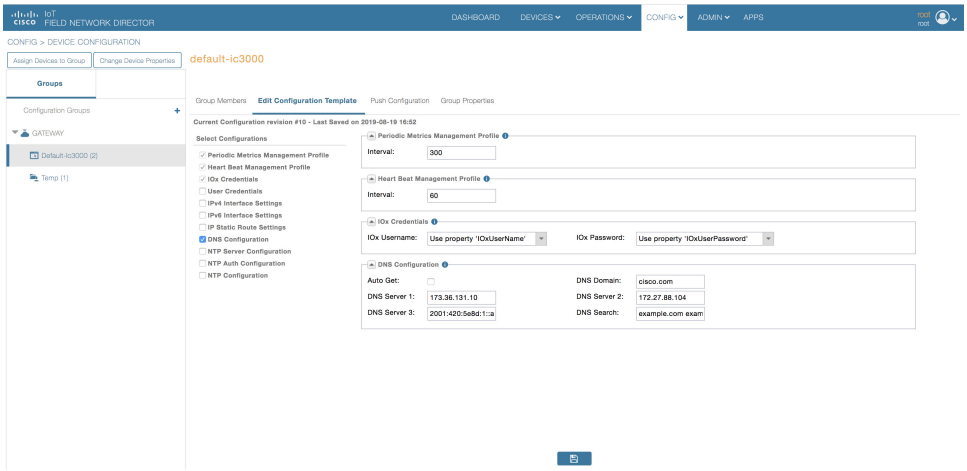
Step 2 Select the DNS configuration checkbox.

Step 3 Add DNS search, domain, or server entries.

a) Optional: Select the Auto Get checkbox within the DNS Configuration tab to delete the DNS configuration that has been manually pushed onto the device from FND.

Step 4 Push the DNS configuration by navigating to **Push Configuration > Select Operation Scroll down > Push GATEWAY Configuration > Start**.

Figure 6: Add DNS Configuration



Step 6: Adding the IC3000 Gateway(s) to FND

Follow these steps to add your device to FND.

Procedure

Step 1 Prepare a spreadsheet with the list of devices to add. This must be completed **before** adding devices to avoid additional steps. The default template is in .csv format, and can be downloaded from the **FND - import Inventory -> Add device** tab.

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

Example:

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

Note The following password rules for the IOxUserPassword 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

To download a sample spreadsheet go to **FND -> Inventory -> Add devices.** Then click **IC3000.**

Step 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:

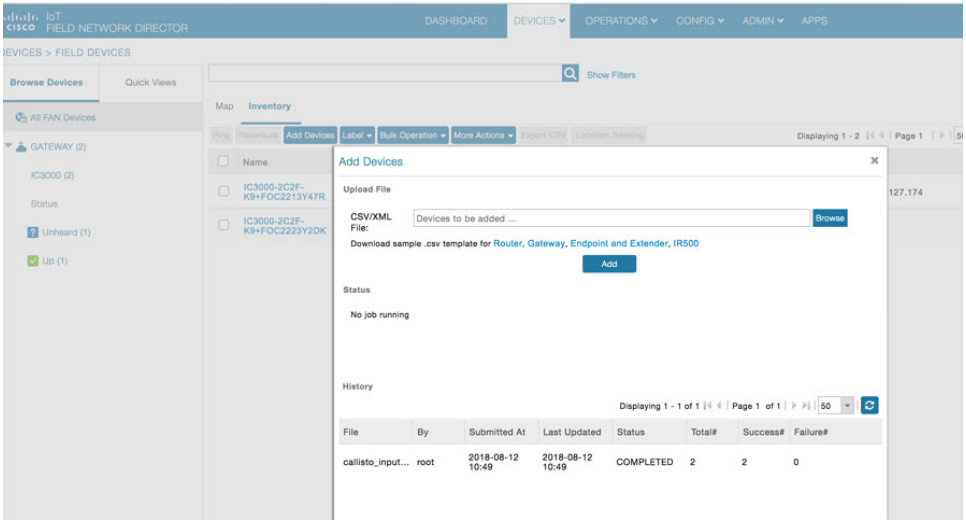
Example:

```
ic3k>show version

Version: 1.2.1
Platform ID: IC3000-2C2F-K9
Hardware ID: FOC2227Y304
ic3k>
```

Step 3 Click **DEVICES > FIELD DEVICES > Inventory > Add Devices**. Browse to the location of your excel spreadsheet and click **Add**. See Figure 7: Add Devices, on page 11.

Figure 7: Add Devices



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

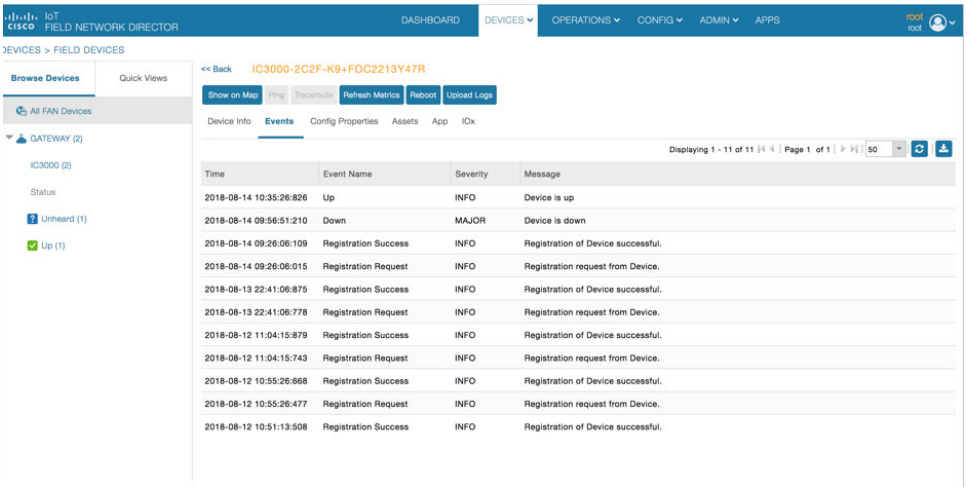
Step 7: IC3000 Registration

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 8: Device Registration, on page 12.

Figure 8: Device Registration



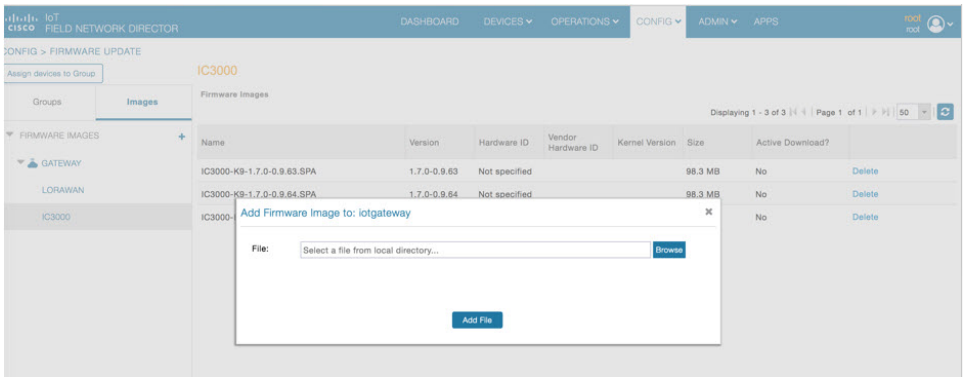
The refresh metric should work and should be able to refresh the device related details.

Step 8: 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 9: Firmware Upload, on page 13.

Figure 9: Firmware Upload



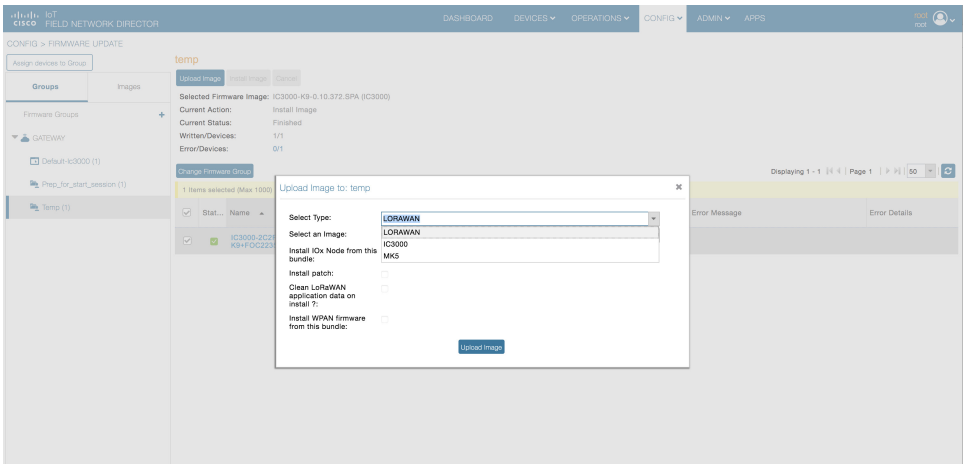
Step 9: Upgrading Firmware with FND

Once Step 5: DNS Configuration, on page 9 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 10: Firmware Update



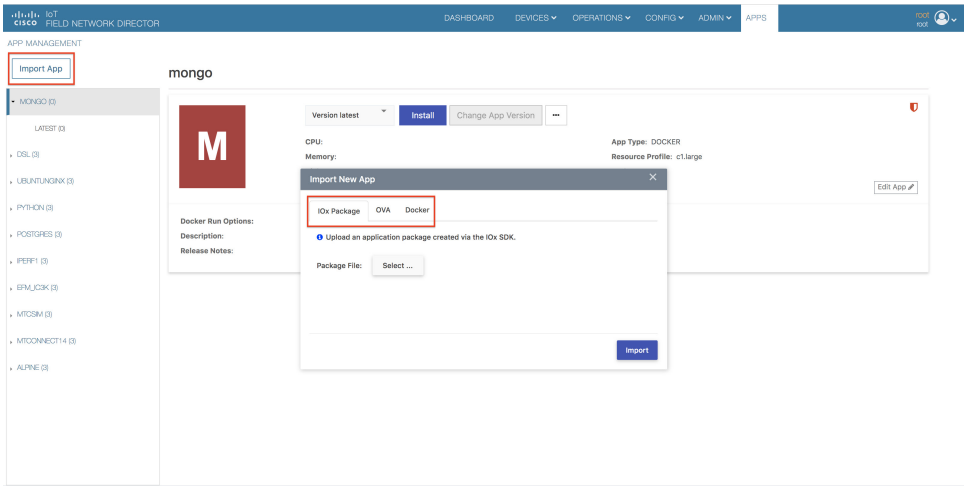
Step 10: Deploying IOx Applications via FND

To deploy an IOx application perform the following:

Procedure

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

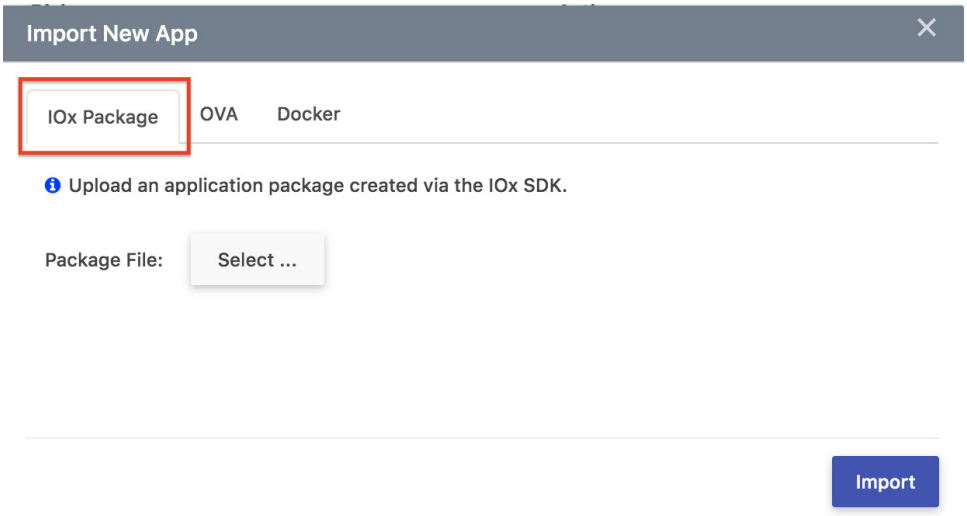
Figure 11: Application Upload



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

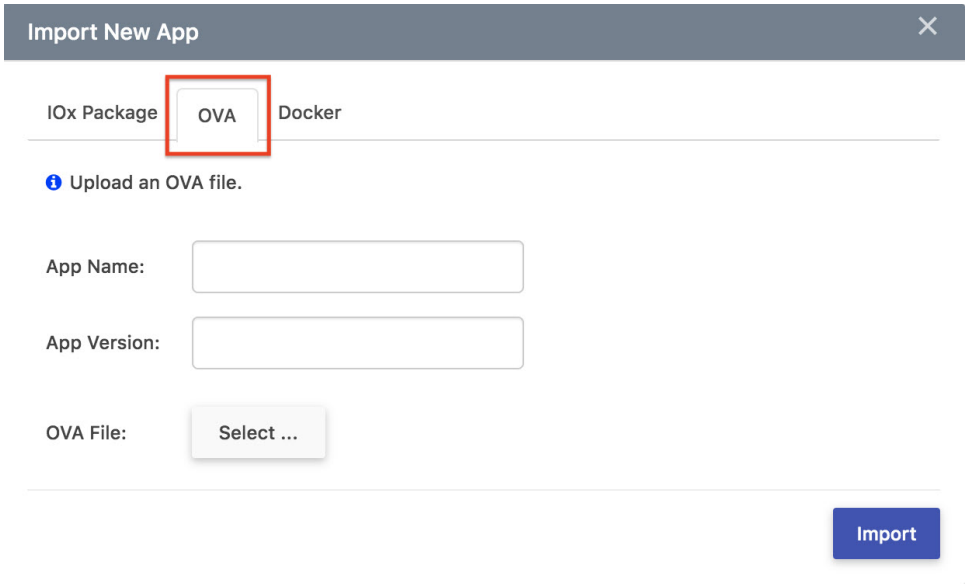
a) To upload an application from your local machine that has been packaged using IOx client, use the IOx Package option as shown in Figure 12: Import New App (IOx Package Option), on page 14

Figure 12: Import New App (IOx Package Option)



b) To upload an OVA VM application use the OVA option as shown in Figure 13: Import New App (OVA Option), on page 15.

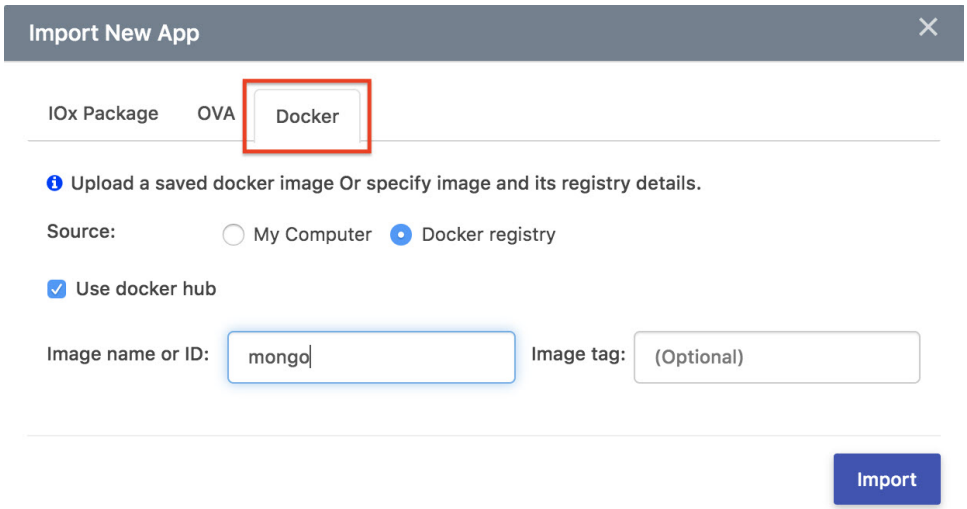
Figure 13: Import New App (OVA Option)



c) To upload a native docker app from the docker hub/registry or from your local machine use the Docker option as shown in Figure 14: Import New App (Docker Option), on page 15.

Note To upload a native docker application using the docker hub option just pass the docker image name exactly as shown from the docker hub.

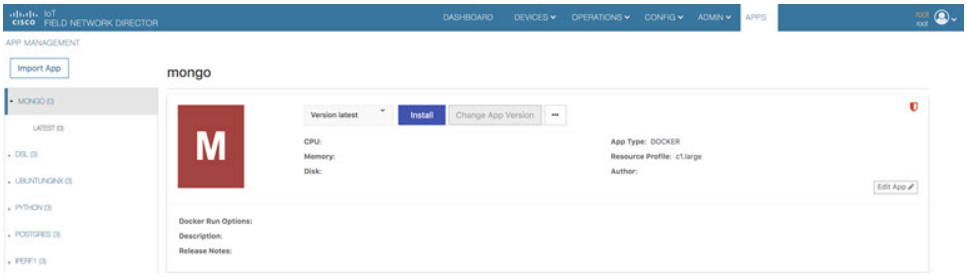
Figure 14: Import New App (Docker Option)



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

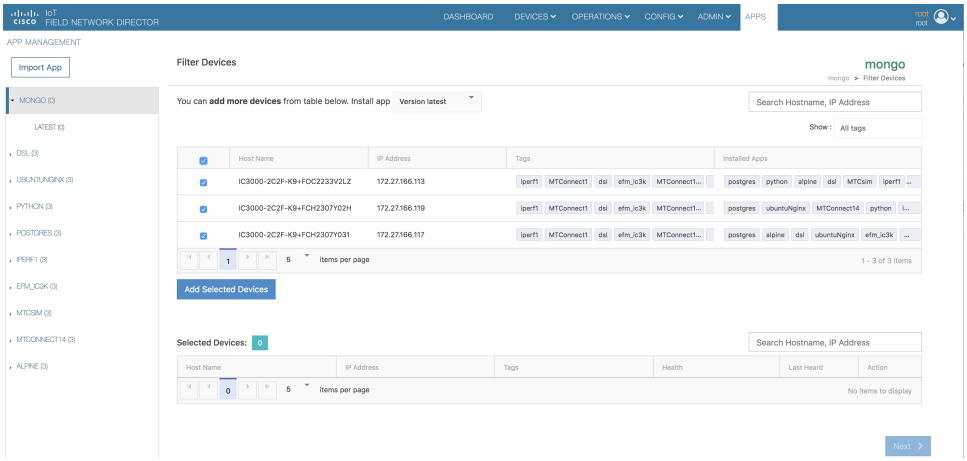
Note You can now import multiple versions of the same application (IoT FND 4.5 and greater).

Figure 15: Application Install



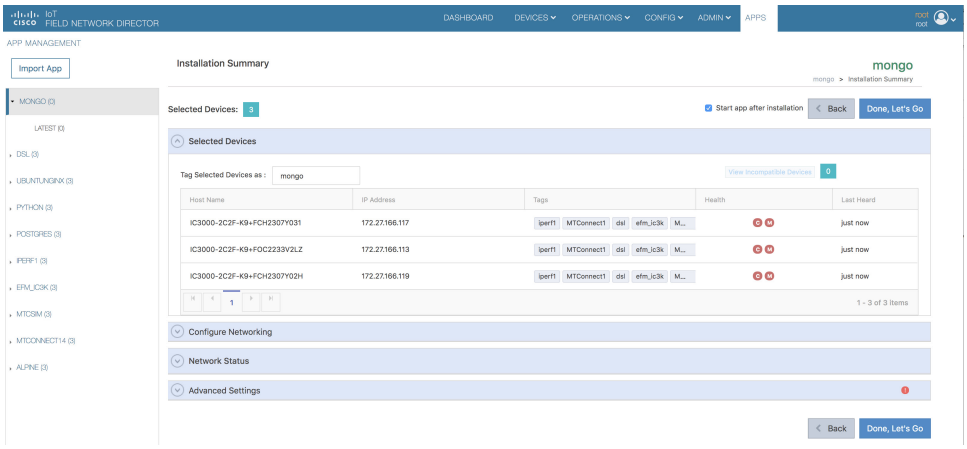
Step 3 Select the **Devices** > **Add Selected Devices**. With your device present, click **Next**

Figure 16: Add Devices



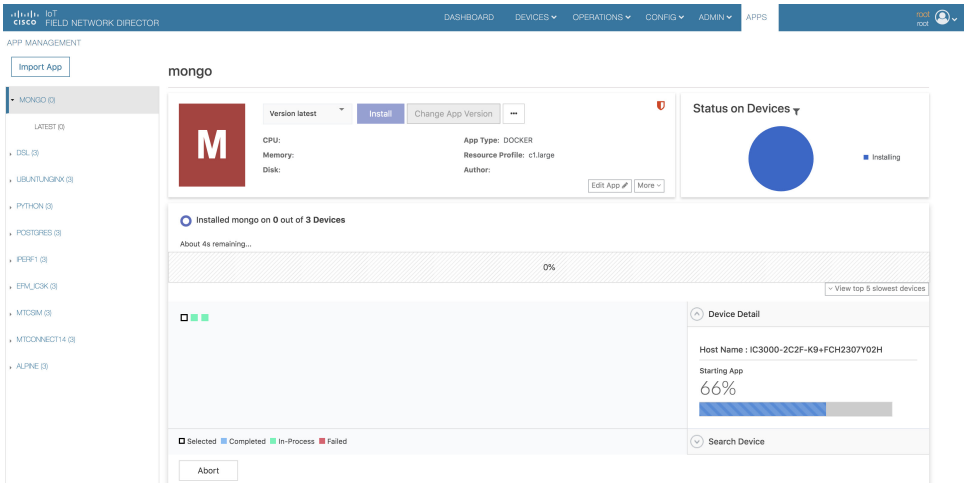
Select the appropriate actions and tabs and provide details as required. See Figure 17: Selected Device Action Tabs, on page 16

Figure 17: Selected Device Action Tabs



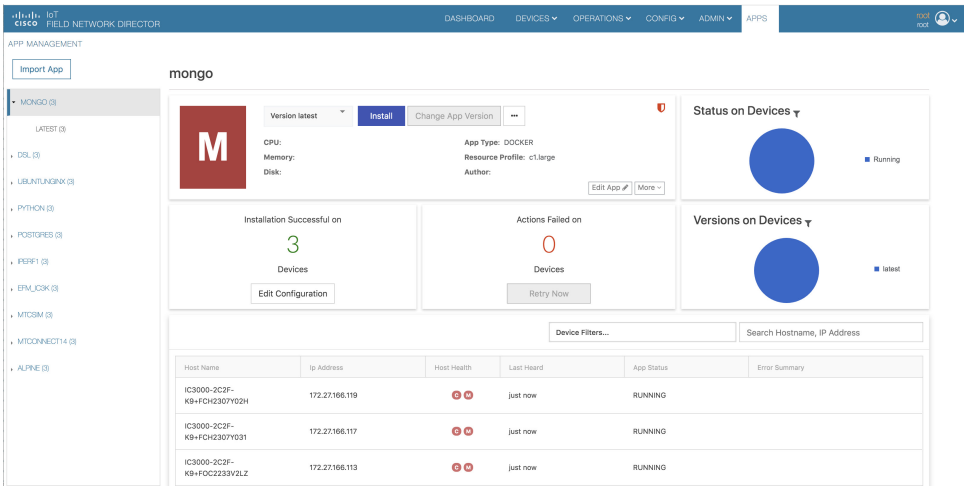
Step 4 Then click **Done, Let's Go**. The Installation progress window appears. See Figure 18: Installation Progress, on page 17.

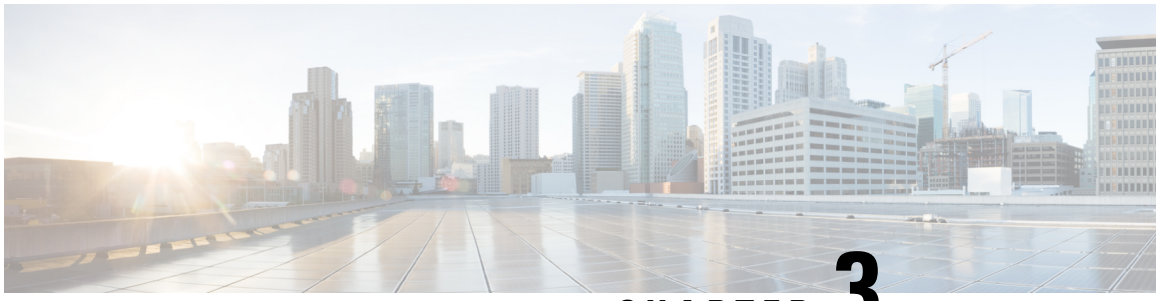
Figure 18: Installation Progress



If installation is successful, you should be able to see the installed count increasing. See Figure 19: Installation Successful, on page 17.

Figure 19: Installation Successful





CHAPTER 3

Standalone Mode: Testing IOx Applications Via Local Manager

This section contains the following topics:

Understanding Standalone Mode

Typically, when connected to the IC3000 through a laptop, you are in standalone 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.

For additional information, refer to Remote Device Management, on page 34. To see an example, go to Use Case Example: Installing a Prebuilt Application via Local Manager, on page 31.

Understanding Managed 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 to Step 7: IC3000 Registration, on page 12.

Standalone Mode Connectivity

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

- Brand new devices (fresh from Cisco factory) have the capability of determining the mode autonomously depending on the networking configurations.
- Standalone mode enables the Cisco IOx Local Manager interface which can be accessed via the browser on the computer connected to the gateway.

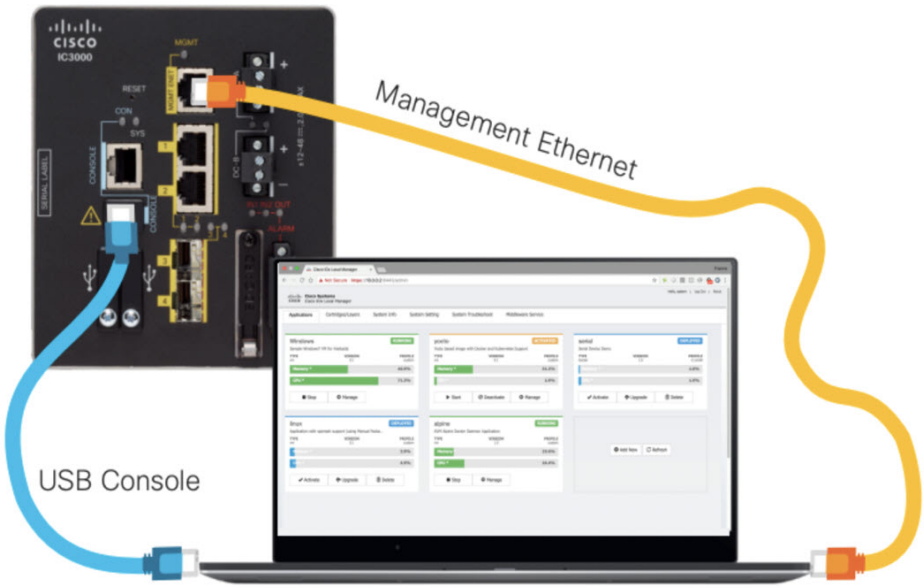
- Standalone mode is activated ONLY over the management Ethernet port of the device.
- Standalone mode CANNOT be turned ON via FND.
- An IC3000 deployed in managed mode can be re-configured to operate in standalone mode by pressing the "Config-Reset" button on the device. Refer to reset button options in IC3000 Related , on page 45 for details.

Standalone mode operates only over a predetermined IPv4 link local address for the first time. To extend the standalone mode to use a LAN/WAN address, please follow the steps in Remote Device Management, on page 34. The Remote management feature is turned on by default from release 1.2.1 and greater, so that the local manager access is available on all the time.

Steps to Connect to the Management Port:

The following graphic shows a laptop connected to the management interface via a standard Ethernet cable.

Figure 20: PC Connected to Management Interface



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

IDA maintains a service which monitors the management interface every 30 seconds. If IDA detects the IP address is not available, IDA will assign the link local IP address of 169.254.128.2 to the management interface.

If the device is in managed mode, IDA will enable the device configuration page as well. Once the WebSocket connection is established, IDA will disable the device configuration page.

Note This is new with release 1.3.1. This enhancement will only be effective when the management interface is using a DHCP configuration.

Procedure

Step 1 Follow steps 1-4 of Installing the IC3000, on page 2.

Step 2 Connect the Management interface on the IC3000 and your laptop with a console cable.

Step 3 Do not power on the IC3000 yet.

Step 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.

Step 5 Now, power-on the IC3000.

Step 6 The device will be in discovery state for the first 30 seconds to learn its dhcp address. After 30 seconds the device will assign an LLA address.

Step 7 The IC3000 will be ready to operate in standalone 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 standalone mode without delay).

Step 8 Open a browser on your laptop and enter https://169.254.128.2:8443 as a URL. The Local Manager opens. Enter **admin/cisco123** as your username/password, and then update the default password.

Note admin/cisco123 is the default account credentials from release 1.2.1 release and greater.

Password Rules:

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

Step 9 For devices running 1.2.1, use the default credentials (admin/cisco123) for logging in the first time. The user is required to change the password when logging in the first time. The IC3000 devices running 1.1.1 and 1.0.1 may need to create or use developer credentials to login via local manager.

Upgrading the IC3000 Firmware with Local Manager

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

Procedure

Step 1 Login to LM GUI using the LLA address

Step 2 Use the default or newly created password (default is admin/cisco123).

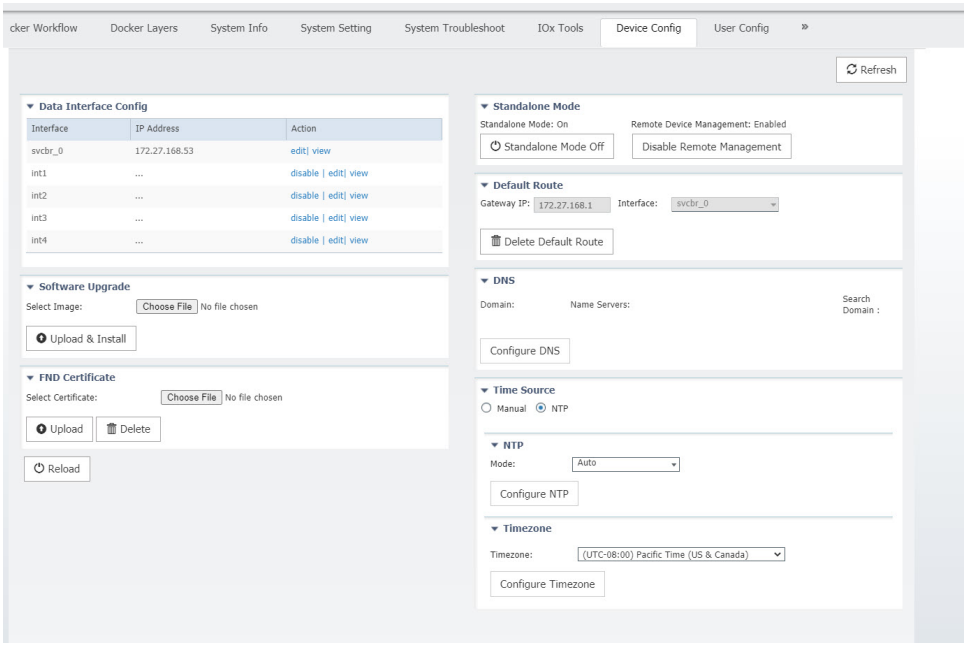
Step 3 Once you are logged into the GUI, click on the **Device Config** tab, then select the **Software Upgrade**. (See Figure 21: Device Config Tab, on page 22).

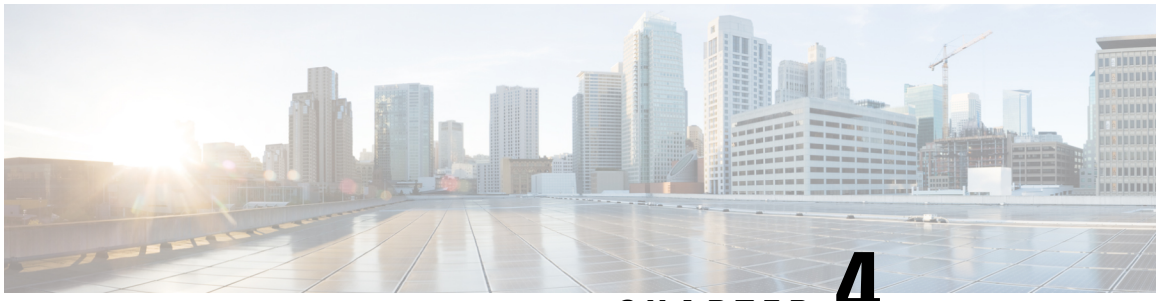
Step 4 Select the image file and then click **Upload & Install**.

Step 5 If you receive any pop-up messages click **OK**.

Step 6 The image is pushed to the IC3000 and it is rebooted with the new firmware.

Figure 21: Device Config Tab





CHAPTER 4

Connecting and Managing via Local Manager (LM)

This section contains the following topics:

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 managed mode, or standalone 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 standalone mode, you will be using an IPv4 LLA address of 169.254.128.x. The rest of the following work flow is the same.

Procedure

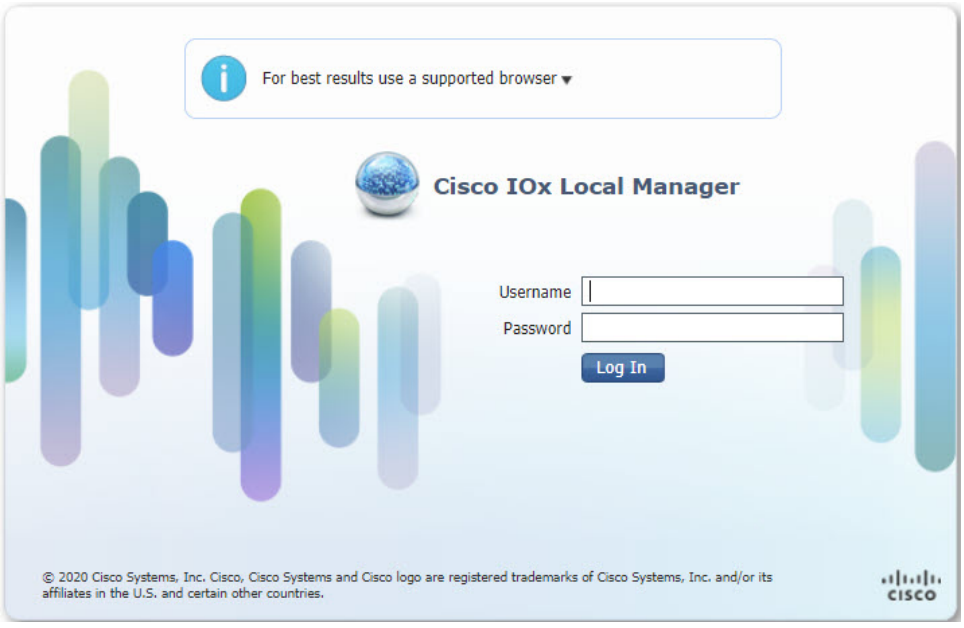
Step 1 Open a web browser and enter **https://169.254.128.2:8443** in the address bar.

Step 2 Login by using the default credentials **admin/cisco123** for the first time if you are running release 1.2.1. For older devices running 1.1.1 or 1.0.1, use **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 device via Local Manager. You should be familiar with the standalone 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 22: Supported Browsers, on page 24.

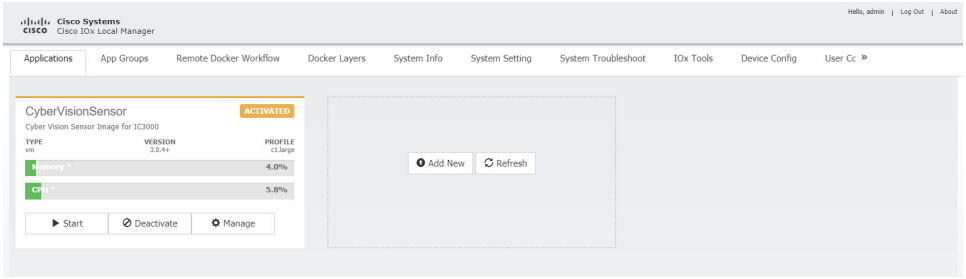
Figure 22: Supported Browsers



Step 3 Click **Log In**. The **Local Manager Applications Tab** appears. See Figure 23: Local Manager Applications Tab, on page 25.

What to do next

Figure 23: Local Manager Applications Tab



Setting the Date and Time

The time feature in Local Manager provides the user with the ability to change the system time, date and time zone on an IC3000. Although this feature is available, it is still recommended to provide access to an NTP server to avoid any issues.

Release 1.3.1 provides enhanced capabilities. The user can now select the time source between manual date and time or NTP. When using NTP, the user can provide information about NTP servers manually, or get that information from a DHCP Server.

The following are options that the user can select from the Device Configuration page of the User Interface (UI):

- Manual Date and Time (User provides the information)
- Network Time Protocol (NTP)
  - Auto (DHCP Server provides the information)
  - Manual (User provides the information)

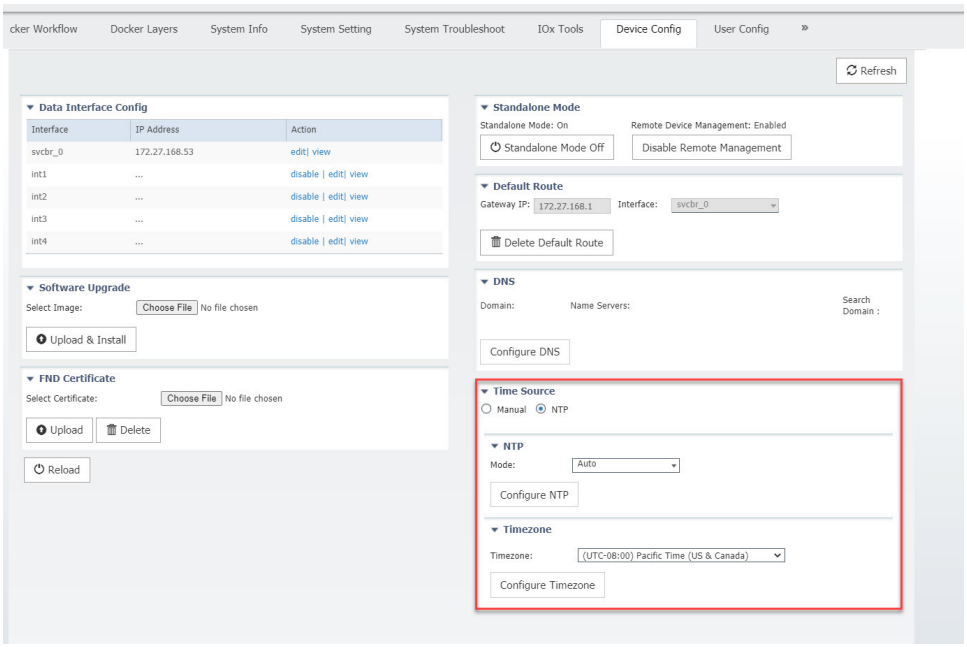
Note Either Manual or NTP date and time options can be selected.

Some of the feature caveats are:

- Time Zone can be individually selected by the customer regardless of the time source.
- Up to 5 NTP servers and 1 Preferred NTP server
- Polling interval includes max and min poll
- For NTP Authentication, the user provides the id, type, and value of the keys
- For NTP, either hostname or IP address can be used.

From the Local Manager GUI, click on the **Device Config** Tab. The following shows the Time Source section highlighted.

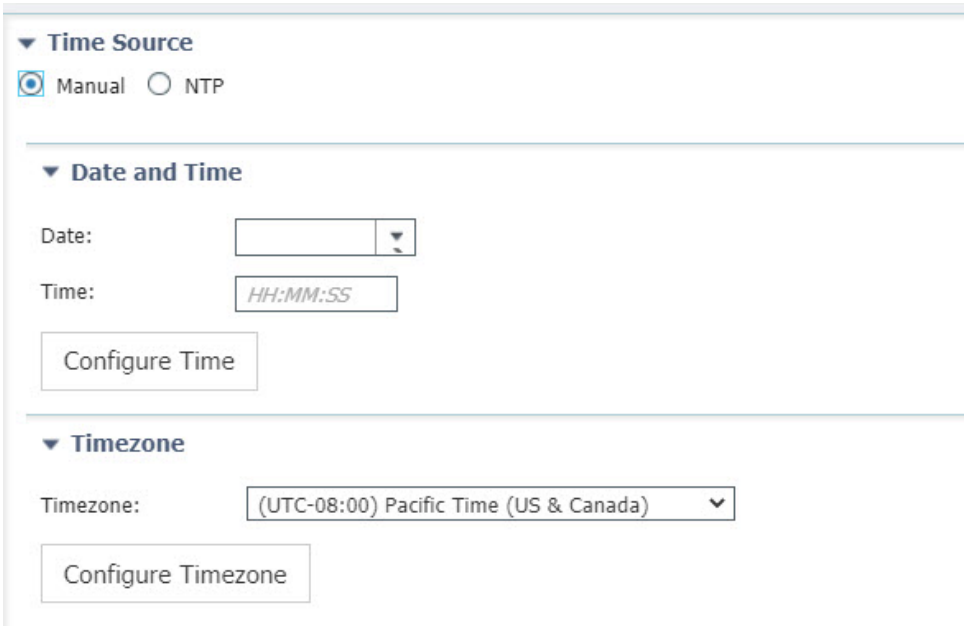
Figure 24: Local Manager Time Source



From this section, you can click on Manuel or NTP as your time source. Choosing NTP defaults to Auto. Click Configure NTP and the settings are updated.

To configure your Date and Time manually, select the Manual button. The Time Source window appears as the following:

Figure 25: Manual Date and Time



Fill in the date and time you wish and then click **Configure Time**.

To configure NTP manually, move on to the next section.

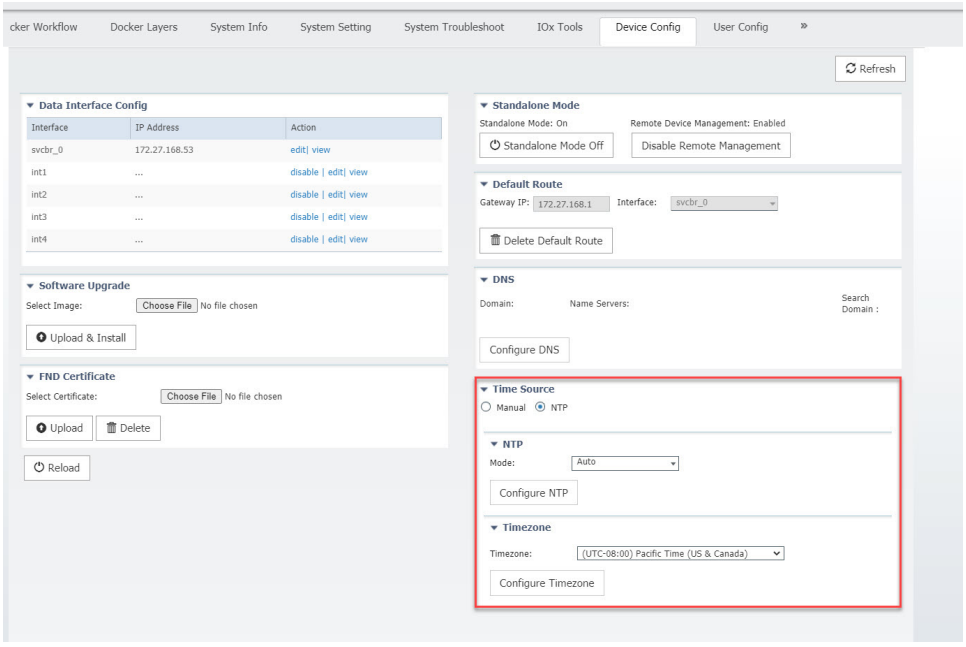
Setting NTP Manually

The NTP feature in Local Manager provides the user with the ability to set Network Time Protocol (NTP) manually on an IC3000.

Procedure

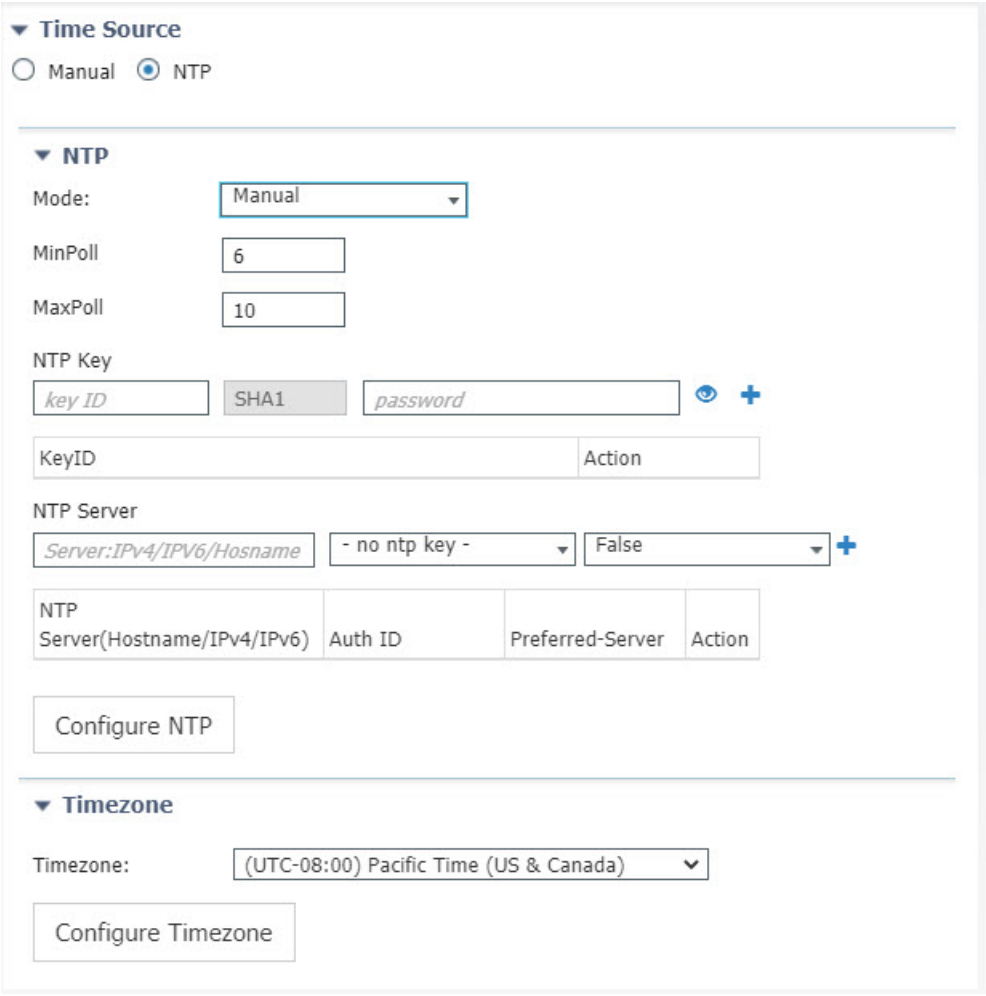
Step 1 From the Local Manager GUI, click on the **Device Config** Tab.

Step 2 Under the Time Source section, click on **NTP**. Refer to the following:



Step 3 Beside the Mode, select the pulldown and click **Manual**. Refer to the following graphic.

Figure 26: NTP Manual Configuration



Step 4 Fill out the NTP entries, then click the plus sign (+)

Note **Optional**: Add an **NTP Key** entry if the NTP server has been configured with authentication. Add the **Key ID** and corresponding **SHA1 key** as the password.

Note **Note**: Authentication is only offered for NTP servers that support SHA1.

Step 5 Click **Configure NTP**.

What to do next

Note To check if the device has synchronized to the NTP server, run the command **show ntp status** on the IC3000. If the NTP server is reachable, it will show a message stating the clock is synchronized:

```
IC3000> show ntp status
Clock is synchronized, stratum 3, reference is <your ip address>
```

Setting DNS Manually

The DNS feature in Local Manager provides the user with the ability to push a DNS configuration on an IC3000 device that's in standalone mode.

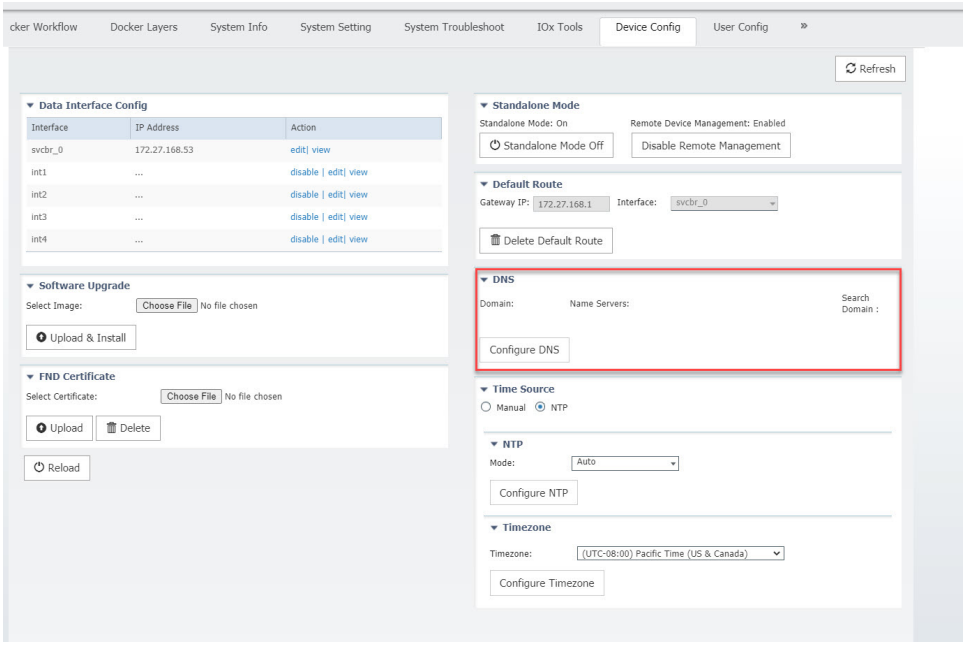
To push DNS configuration via LM perform the following:

Procedure

Step 1 From the Local Manager GUI, click on the **Device Config**Tab.

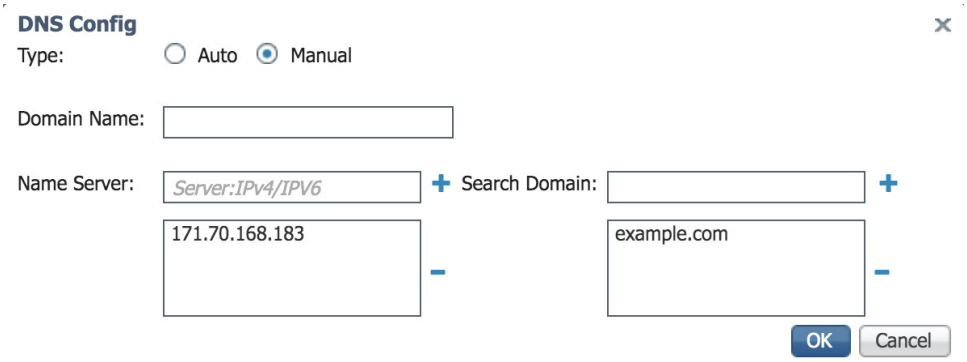
Step 2 Under the DNS section, click on **Configure DNS**. Refer to Figure 27: Configure DNS , on page 29.

Figure 27: Configure DNS



Step 3 After clicking on **Configure DNS**, the **DNS Config** window opens. Refer to Figure 28: DNS Config Window, on page 30.

Figure 28: DNS Config Window



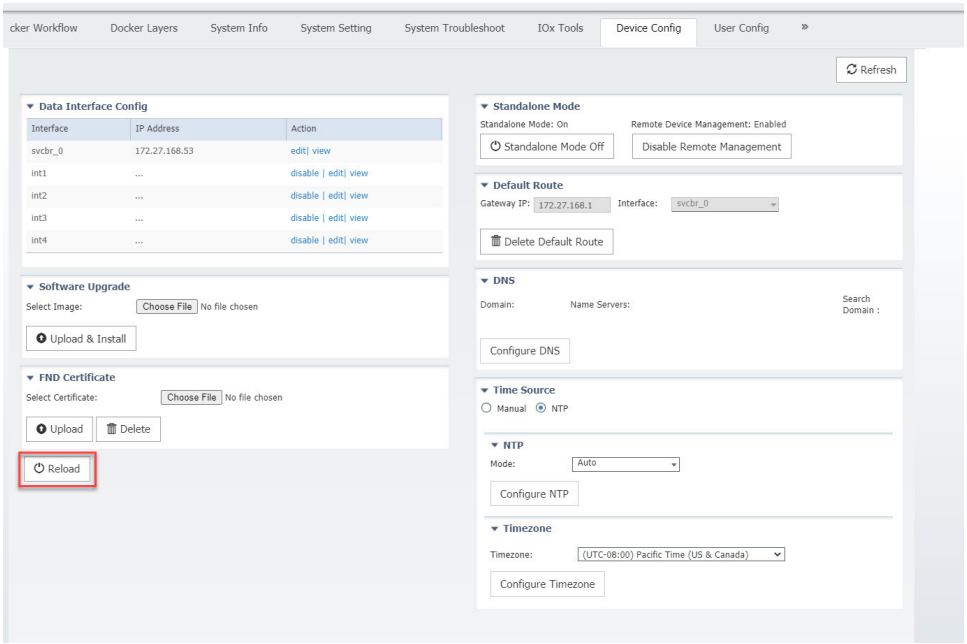
Step 4 Add a DNS entry or search domain, then click the plus sign (+)

Step 5 Click on **OK**.

Software Reboot Button

When managing the IC3000 in standalone mode, and the device is not functioning as expected, a software reboot button is provided under the Device Config tab. Refer to Figure 29: GUI Reload Button, on page 30.

Figure 29: GUI Reload Button



Note After pressing the **Reload** button, you will temporarily lose access to the LM GUI for approximately 2 to 3 minutes until the device comes back up.

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

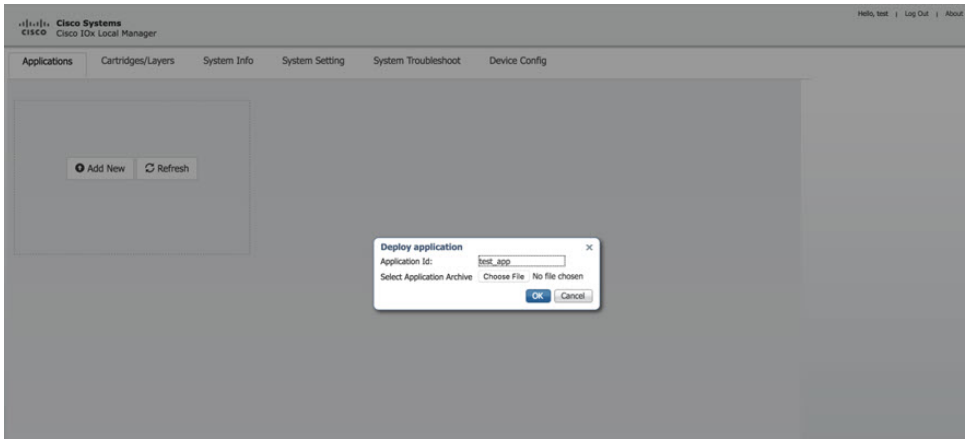
Procedure

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

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

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

Figure 30: Deploy application



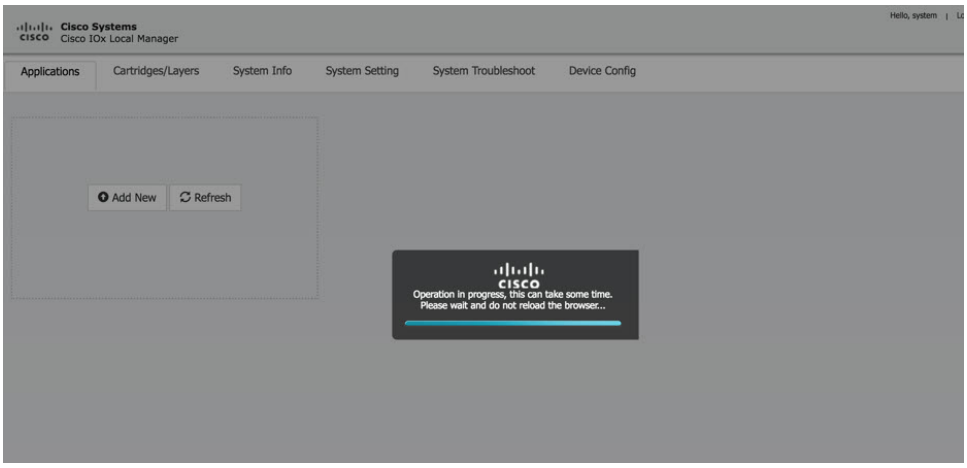
Step 3 In the Deploy Application dialog box, take these actions:

a) In the **Application ID** field, enter a name. The App ID requires more than one character and follows this regex syntax: [a-zA-Z0-9][a-zA-Z0-9_.-]

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**

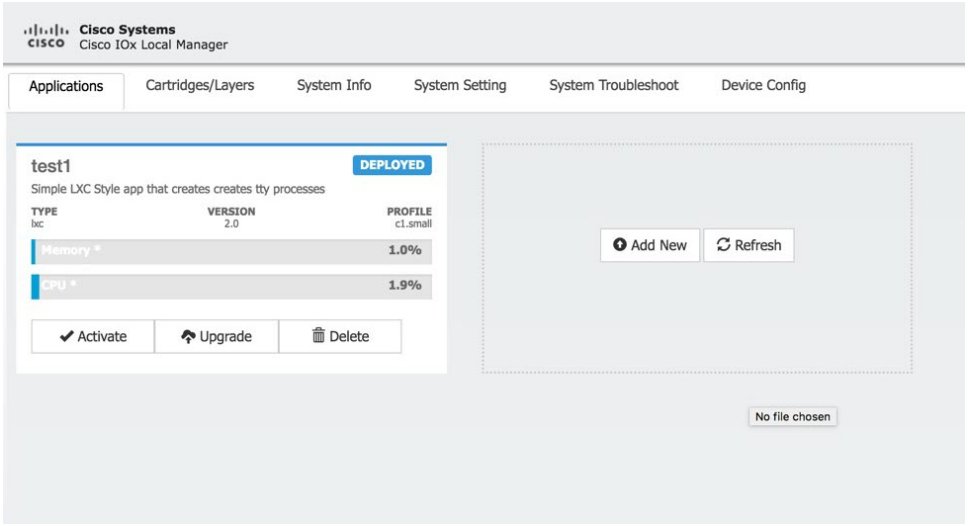
Step 4 The application file uploads to Cisco IOx.



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

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

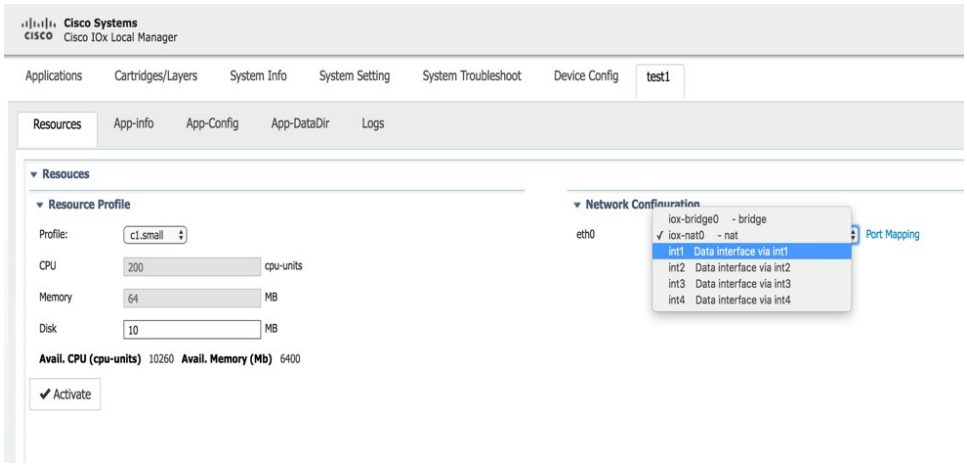
Figure 31: Application Successfully Deployed



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

Step 6 In the test1/APP area, click the **Activate** button. The **Applications > Resources** tab displays, see #unique_38 unique_38_Connect_42_fig_1060957.

Figure 32: Applications > Resources Tab



Step 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.

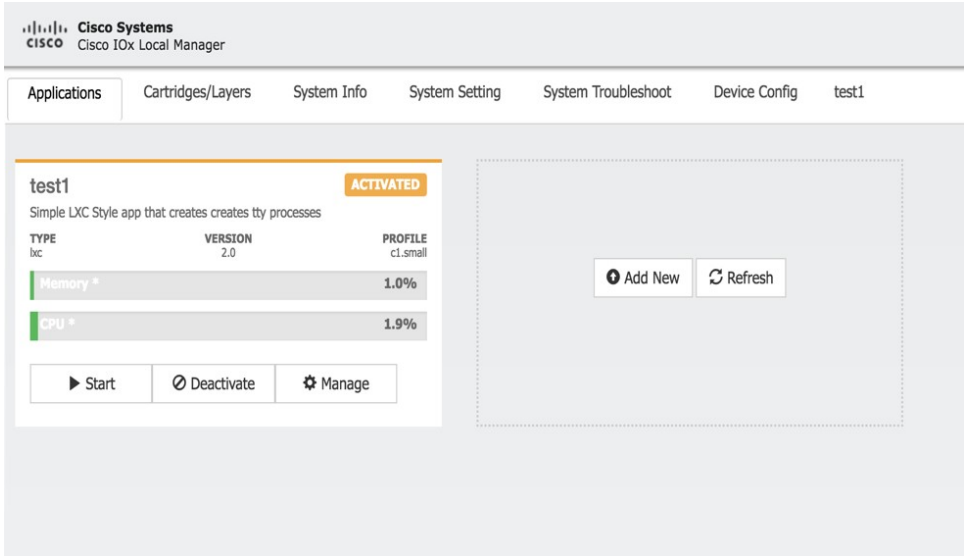
Step 8 While still in the **Applications** > **Resources** tab, click the **Activate** button to activate the application.

Step 9 Click the **Applications** tab.

Step 10 In the EFM area, click the **Start** button.

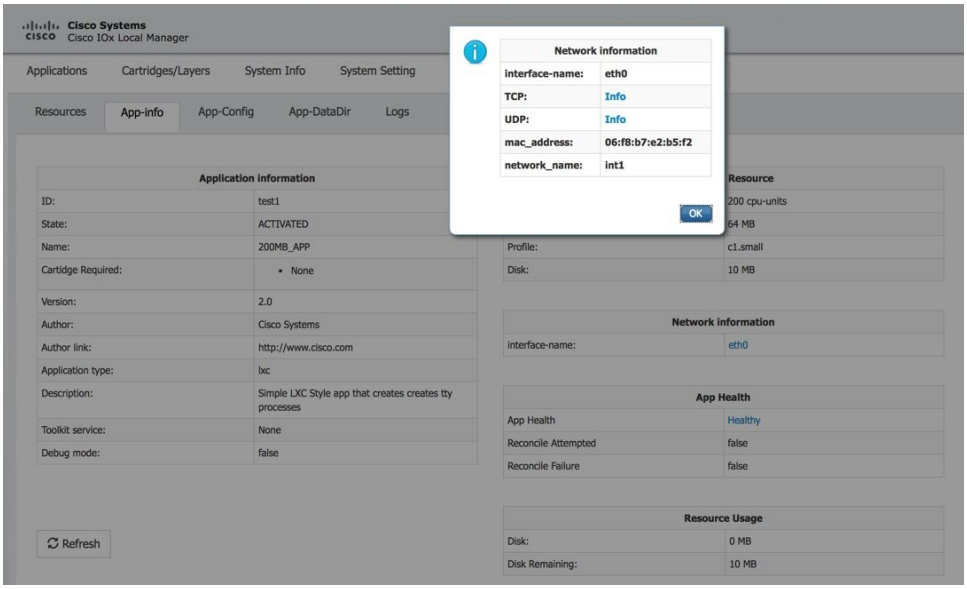
Note Make sure that activated the application before clicking **Start**.

Figure 33: Applications > Start



Step 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.

Figure 34: 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. This is turned ON or enabled by default thus allowing for local and remote access of the local manager GUI. The below steps are valid for older release, for example 1.1.1, where the user needs remote management.

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 Standalone Mode remains exactly same as previously described in Phase 3: Standalone Mode: Testing IOx Applications via Local Manager, page 1. Use the pre-defined link-local address169.254.128.2 to get the device up in standalone mode.

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

Procedure

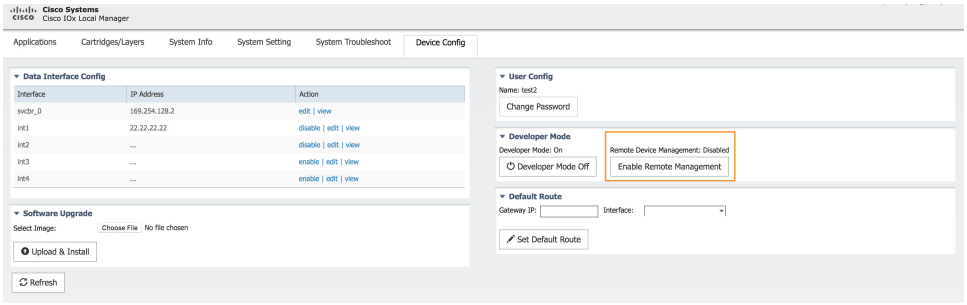
Step 1 If required, upload the new Image from the Device Config tab and it will reload the device with the latest image.

Step 2 Open a **NEW** browser and login again with the 169.254.128.2 address to the Local Manager using default credentials. (admin/cisco123) or the new password if the credentials are changed.

Note The old browser is now non-functional.

Step 3 In the Device Config tab there is a new section on the right side called “Remote Device Management”. See the highlighted area in the following graphic.

Figure 35: Remote Device Management



Step 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.

Step 5 Use the https://<*new address*> :8443 in a new browser window to login to Local Manager using developer credentials. See Figure 36: Remote Device Management (Enabled), on page 36 for guidance for these steps.

Step 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.

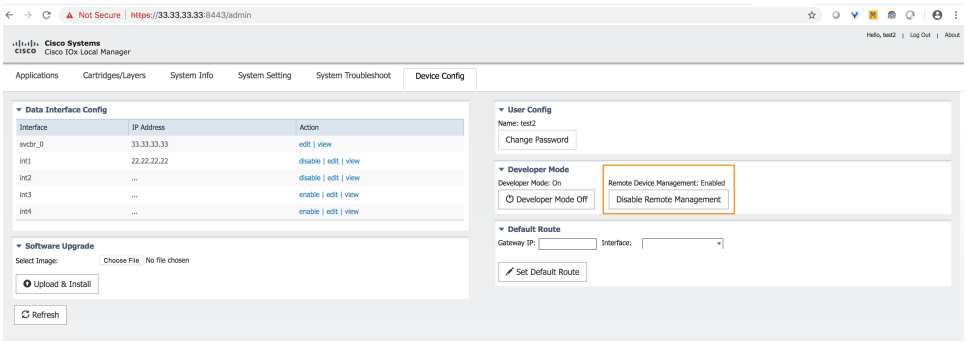
a) Disconnect IC3000 management port from laptop and connect to the network for active DHCP learning on svcbr_0.
b) Check the ip address learned via DHCP on the platform console using the CLI **show interfaces**.
c) Use the https://<*new address*> :8443 in a new browser window to login to LM using developer credentials.

Step 7 Obtain the default-route details and add the Gateway IP route details to the svcbr_0 interface below **Default Route**.

Step 8 On the left side of the Device Config screen, edit the svcbr_0 interface with chosen IP address and mask. Click **Ok**

Step 9 See Figure 36: Remote Device Management (Enabled), on page 36 for guidance for these steps.

Figure 36: Remote Device Management (Enabled)

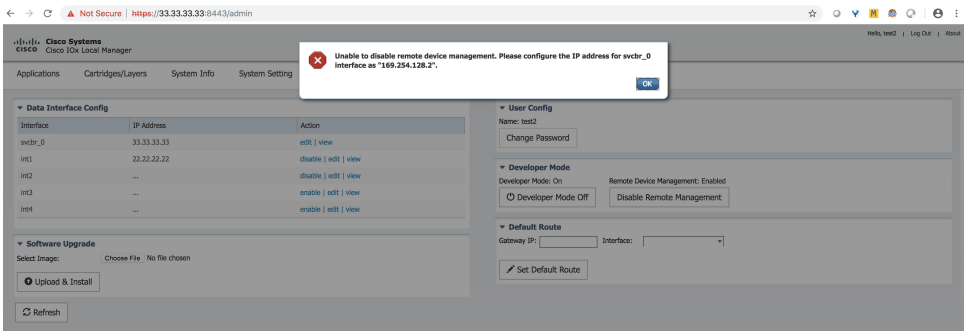


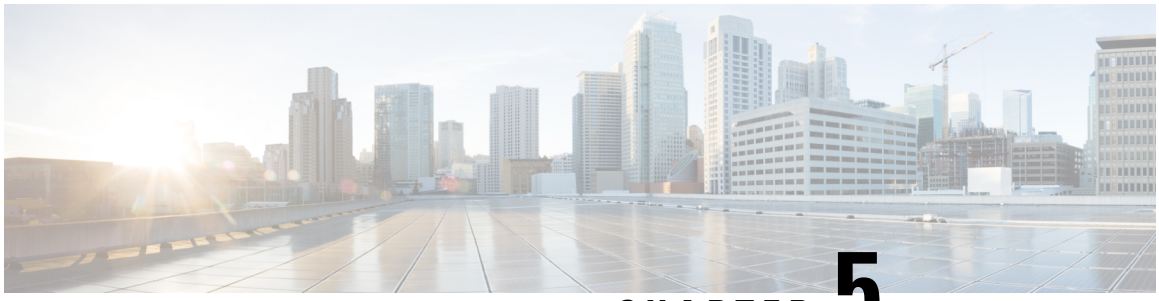
To disable remote device management

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 37: Disable Remote Device Management Warning





CHAPTER 5

Additional Administration

This section contains the following topics:

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.

For example:

```
ic3k>show version
Version: 1.2.1
Platform ID: IC3000-2C2F-K9
Hardware ID: FOC2235V0SW
ic3k>
```

The version string shown in the example is a representation of the CCO download image C3000-K9-1.2.1.SPA.

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.

Note As of release 1.3.1, the operating image is verified before flashing to the boot. The system will check the image, and if it is found corrupt, an error will be returned to the updater agent. This error will be propagated to the end user to inform them about the cause of the image update failure.

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:

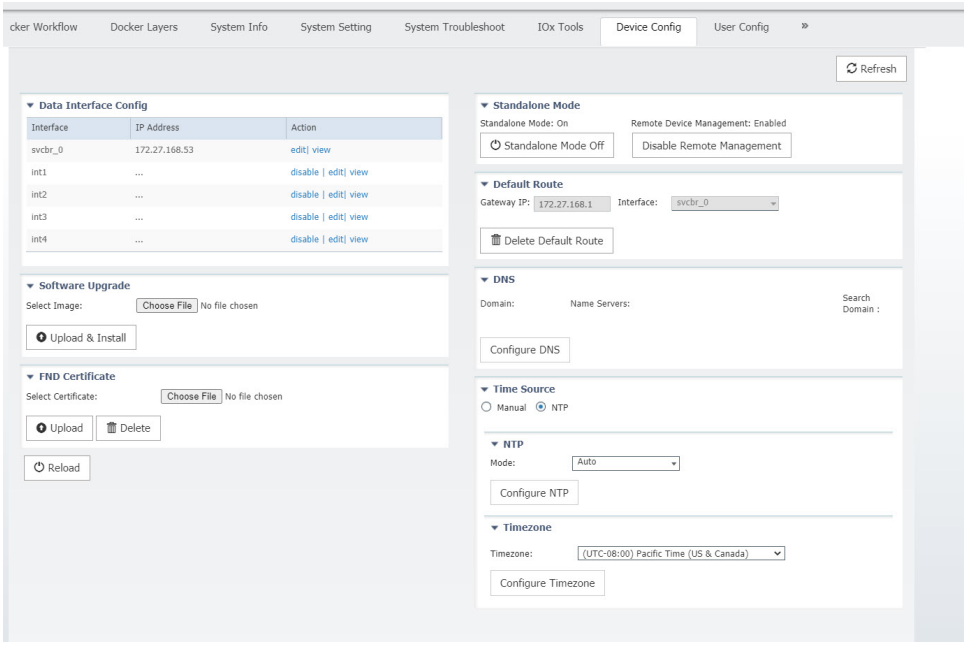
The LM work flow is as follows:

Procedure

Step 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

Step 2 Select the **Device Config** tab, then click the **Choose File** button in the Software Upgrade section to select the image file. See Figure 38: Device Config Tab, on page 38. 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 standalone mode to access the device configuration tab and this can be achieved by factory resetting the box. Refer to reset button options in IC3000 Related , on page 45 for details.

Figure 38: Device Config Tab



The FND work flow is as follows:

Please follow the Step 9: Upgrading Firmware with FND, page 8 procedure.

Note The reboot time is approximately 3 minutes and the size of the firmware is roughly 160MB. 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 standalone mode. The application console is enabled in standalone mode. If standalone mode is off, the application console access is disabled.

Connecting to the Console of a Running Application

Accessing the console of a running application while in standalone mode can be used to troubleshoot and debug a running or failing application. Connecting to the application console can be done using the address of the svcbr_0 interface of the IC3000. It can be a Link-Local Address of 169.254.128.2 or a dhcp address. For Cyber Vision cases, use the IP address configured via USB when filling out the Hosts Management IP address field.

Connecting to the Application Console using the Command Prompt/Terminal

Follow these steps:

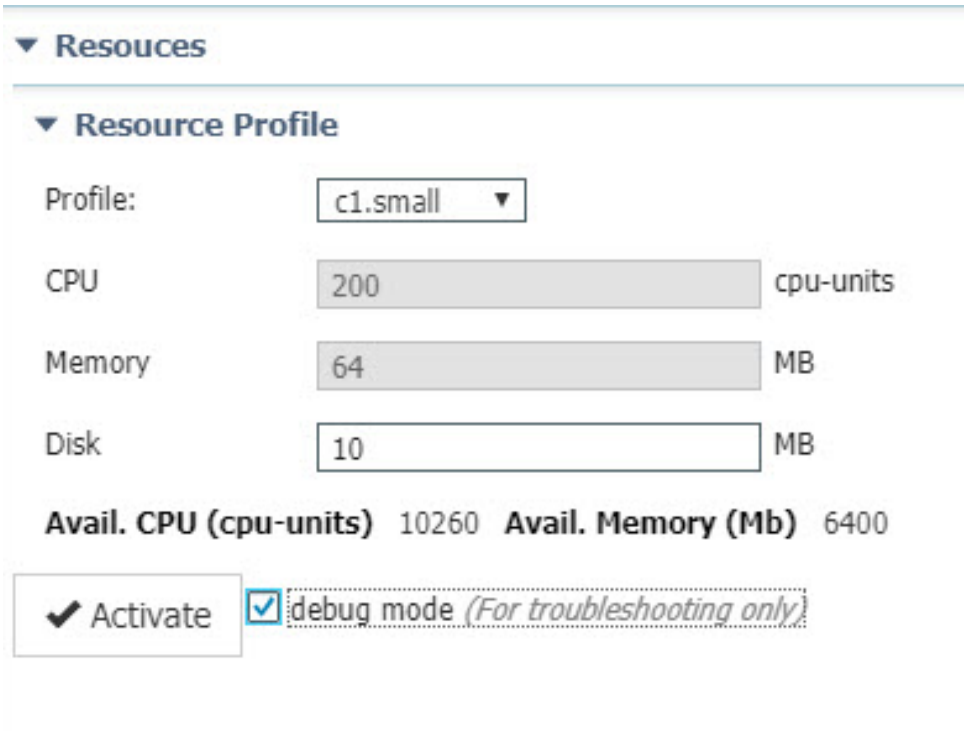
Procedure

Step 1 Deploy, Activate, and Start an IOx Application.

a) Access the Local Manager through your browser in order to deploy, activate and start your IOx application package.

b) Optionally, you can enable the debug option when you activate the application as shown in Figure 39: Resources, on page 39. This prevents the application container from stopping when your application terminates unexpectedly.

Figure 39: Resources



Step 2 Save the PEM certificate on your local machine.

a) Create the **.pem* file by going to the terminal and running **touch** <*pemFileName*>**.pem** in the directory you want to save the certificate. For example:

Example:

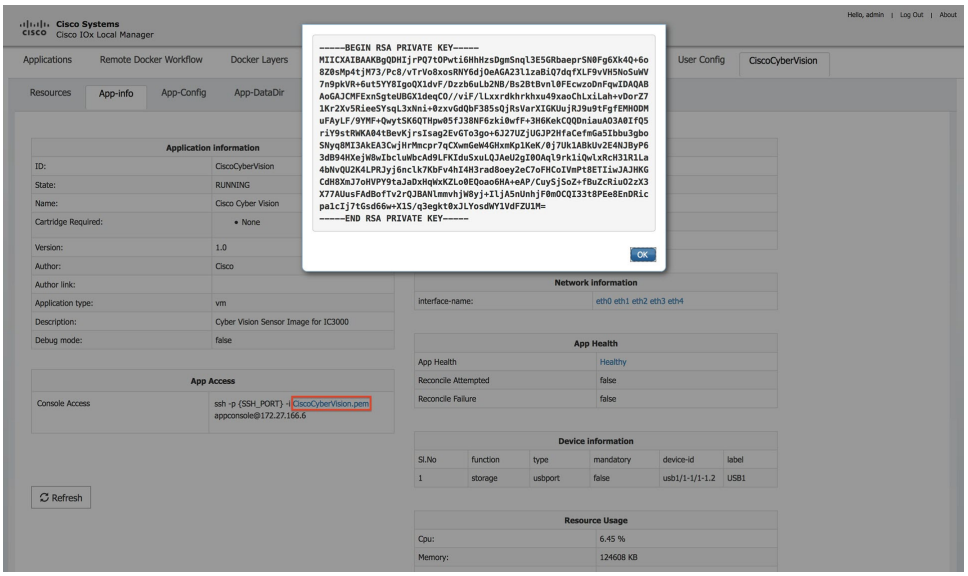
```
Device$ cd Desktop -
Change directory to your Desktop
Device$ mkdir pem_certificates -
Makes a directory called pem_certificates
Device$ cd pem_certificates/ -
Change directory to the pem_certificates directory
Device$ touch CiscoCyberVision.pem -
Creates a file named CiscoCyberVision.pem

Device$ ls -
Lists the contents of the directory
  CiscoCyberVision.pem
```

b) Get the private key of the container by going to **Local Manager -> Application ->** <*specific app*> **-> Manage -> App Info -> *.pem** file. Clicking on **CiscoCyberVision.pem** displays the contents of the private key. See Figure 40: Click to Display Key, on page 40 and Figure 41: App info Page, on page 40.

Figure 40: Click to Display Key

Figure 41: App info Page



c) Save the private key by copying the entire content into the <*pemFileName*>**.pem** file you created in Step 2a. Make sure to save the changes. For example:

Example:

```
Device$ vi CiscoCyberVision.pem  -
Opens the file in the vi editor
*cut and paste the contents of the file into the open file*
Device$ wq -
Writes the file and quits the vi editor
Device$ cat CiscoCyberVision.pem -
Displays the contents of the file
```

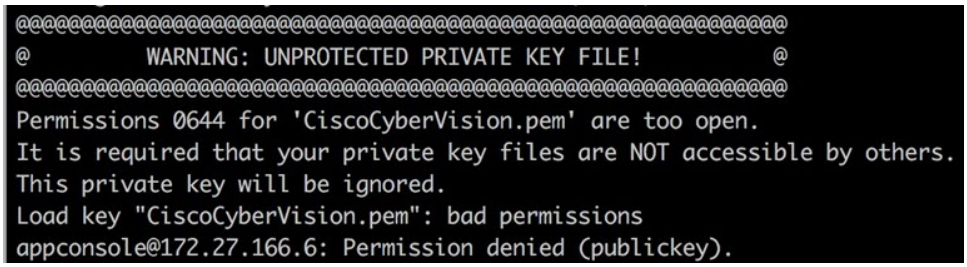
d) Add the necessary permissions for the file. Recommended using "chmod 600". For example:

Example:

```
Device$pwd -
Prints the working directory
Desktop/pem_certificates
Device$ls -
Displays the contents of the directory
  CiscoCyberVision.pem
Device$chmod 600 CiscoCyberVision.pem -
Changes the mode of the file to 600 which is more secure
```

e) If you see a warning as shown in Figure 42: Warning Message, on page 41 when trying to ssh to the application console, it is because the current file permissions are too open.

Figure 42: Warning Message



Step 3 SSH to the Application Console.

a) Run the command that is found under the App info tab in the directory you saved the pem certificate: **ssh -p {SSH_PORT} -i <pemFileName>.pem appconsole@169.254.128.2 {SSH_PORT} = 22**

Figure 43: App Access

Step 4 You should now be able to navigate the app logs to begin troubleshooting.

Connecting to the Application Console using PuTTY

PuTTY is an SSH and telnet client, developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is available with source code and is developed and supported by a group of volunteers.

Follow steps **1** and **2** under the Connecting to the Application Console using the Command Prompt/Terminal , on page 39 before starting a PuTTY session.

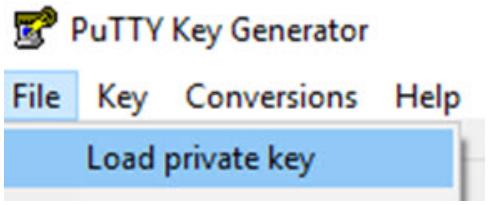
On Windows, when you use PuTTY, first convert the .pem file to a PuTTY-compatible .ppk with the use of PuTTygen.

Follow these steps:

Procedure

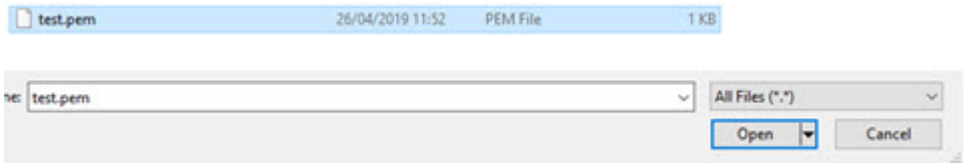
Step 1 Start PuTTygen by navigating to **File > Load private key** as shown in Figure 44: PuTTY Key Generator, on page 42.

Figure 44: PuTTY Key Generator



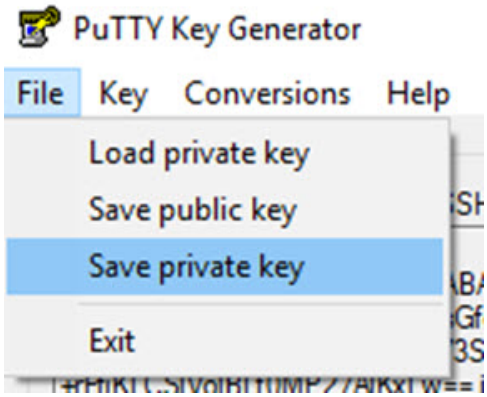
Step 2 **Set the file filter to** All Files and open the downloaded .pem as shown in the following graphic.

Figure 45: File Filter



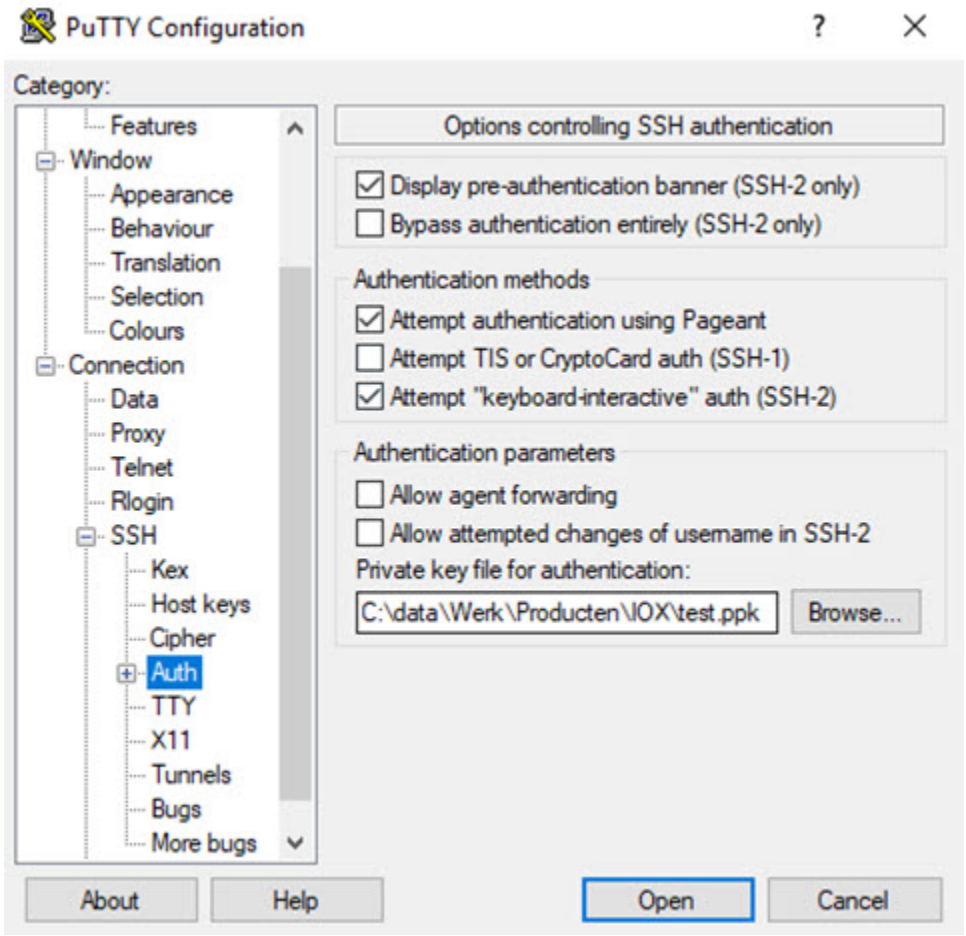
Step 3 Go to **File > Save private key** and save the .pem as .ppk as shown in Figure 46: Save Key, on page 43.

Figure 46: Save Key



Step 4 Once you have the .ppk, start PuTTY and enter 169.254.128.2, port 22 in the session dialog. Next, go to **Connection - SSH - Auth** and supply the private key file <*test*>**.ppk** file as shown in the following graphic.

Figure 47: PuTTY Configuration



Step 5 Click **Open** in order to start the session. Enter the username **appconsole** as shown in the following graphic.

Figure 48: PuTTY Session

Performing these steps should bring you to the application console of the running IOx container on the IC3000.

Audit Trail for Application Management Operations

Note This functionality is only supported in the IoT FND and Fog Director Integrated Solution.

The following two Application Management operations will generate an Audit Log:

- Install App
- Uninstall App

Note There is no audit trail to track when you import or delete an application to or from the IoT FND and Fog Director Integrated Solution.

To view the Audit Log details, choose **ADMIN > SYSTEM MANAGEMENT > AUDIT TRAIL**.

Figure 49: Audit Trail

Note You can now import multiple versions of the same application.

Troubleshooting

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

IC3000 Related

Reset Button Options

The device can be returned to the original factory configuration by using the reset button. The reset button is a small button accessed through a pinhole located on the front of the device. For the location, see the IC3000 Hardware Configuration Guide .

The reset button options have changed with release 1.3.1. The following table shows the timings before and after release 1.3.1:

Table 2: Reset Button Timings

	Prior to Release 1.3.1	Release 1.3.1 and Beyond
Action	**Time Pressed and Released in Seconds**	**Time Pressed and Released in Seconds**
Reload	10-15	10-20
Configuration Reset	30-35	30-50
Factory Reset	60-65	60-80

Note Release 1.3.1 provides an enhanced Factory Reset and Configuration Reset. Both are described here: Enhanced Reset Options for Release 1.3.1, on page 52

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 standalone mode or managed mode:

```
#show ida
```

- To view the status of IOx:

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

Note If an SD card is inserted into its slot, the **show tech support** command will copy tech support logs to the USB or SD card. The logs can be viewed later on a PC. The USB or SD card should be formatted as an ext2/ext4, ExFAT, or FAT32 filesystem.

Examples of Show Commands

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

ic3k>show clock
Tue Aug 13 22:22:12 UTC 2019
ic3k>

ic3k>show dns
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 172.27.88.104
nameserver 173.36.131.10
search cisco.com example.com example.edu example.org
ic3k

ic3k>show dns manual-config
Nameserver 1 : 172.27.88.104
Nameserver 2 : 173.36.131.10
Domain : cisco.com
Search 1 : example.com
Search 2 : example.edu
Search 3 : example.org
ic3k>

ic3k>show dns mode
DNS Mode : Manual
ic3k>

ic3k>show ida status
IDA Version: 2.2.0
Status: Running
> The ida is running
Operation Mode: Standalone
> The device is in standalone 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)
Remote Device Management: N/A

ic3k>show interfaces
 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: sit0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/sit 0.0.0.0 brd 0.0.0.0
3: int1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master dpbr_1 state UP group
default qlen 1000
    link/ether d0:ec:35:cb:5e:23 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::d2ec:35ff:fecb:5e23/64 scope link
       valid_lft forever preferred_lft forever
4: int2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master dpbr_2 state UP group
default qlen 1000
    link/ether d0:ec:35:cb:5e:24 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::d2ec:35ff:fecb:5e24/64 scope link
       valid_lft forever preferred_lft forever
5: int3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master dpbr_3 state UP group
default qlen 1000
    link/ether d0:ec:35:cb:5e:25 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::d2ec:35ff:fecb:5e25/64 scope link
       valid_lft forever preferred_lft forever
6: int4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master dpbr_4 state UP group
default qlen 1000
    link/ether d0:ec:35:cb:5e:26 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::d2ec:35ff:fecb:5e26/64 scope link
       valid_lft forever preferred_lft forever
7: mgmt0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master svcbr_0 state UP group
 default qlen 1000
    link/ether d0:ec:35:cb:5e:20 brd ff:ff:ff:ff:ff:ff
8: svcbr_0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
 qlen 1000
    link/ether d0:ec:35:cb:5e:20 brd ff:ff:ff:ff:ff:ff
    inet 172.27.168.53/25 brd 172.27.168.127 scope global svcbr_0
       valid_lft forever preferred_lft forever
    inet6 2001:face::d2ec:35ff:fecb:5e20/64 scope global dynamic mngtmpaddr
       valid_lft 2591980sec preferred_lft 604780sec
    inet6 fe80::d2ec:35ff:fecb:5e20/64 scope link
       valid_lft forever preferred_lft forever
9: dpbr_docker_n_0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
group default
    link/ether 02:42:00:9e:fa:8e brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.65/27 brd 192.168.10.95 scope global dpbr_docker_n_0
       valid_lft forever preferred_lft forever
10: dpbr_n_0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group
default qlen 1000
    link/ether 52:54:00:c7:5a:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.1/27 brd 192.168.10.31 scope global dpbr_n_0
       valid_lft forever preferred_lft forever
11: dpbr_n_0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master dpbr_n_0 state
DOWN group default qlen 1000
    link/ether 52:54:00:c7:5a:5d brd ff:ff:ff:ff:ff:ff
12: dpbr_0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
 qlen 1000
    link/ether 4a:0c:17:5b:48:e8 brd ff:ff:ff:ff:ff:ff
13: dpbr_0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master dpbr_0 state DOWN
```

```
group default qlen 1000
    link/ether 52:54:00:1e:5d:42 brd ff:ff:ff:ff:ff:ff
14: veth1_0@veth0_0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master dpbr_0
 state UP group default qlen
1000
    link/ether 4a:0c:17:5b:48:e8 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::480c:17ff:fe5b:48e8/64 scope link
       valid_lft forever preferred_lft forever
15: veth0_0@veth1_0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master svcbr_0
 state UP group default qlen
 1000
    link/ether fe:54:dd:a7:53:e1 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::fc54:ddff:fea7:53e1/64 scope link
       valid_lft forever preferred_lft forever
16: dpbr_1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
 qlen 1000
    link/ether 52:54:00:83:c0:e3 brd ff:ff:ff:ff:ff:ff
17: dpbr_1-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master dpbr_1 state DOWN
group default qlen 1000
    link/ether 52:54:00:83:c0:e3 brd ff:ff:ff:ff:ff:ff
18: dpbr_2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
 qlen 1000
    link/ether 52:54:00:a1:1f:99 brd ff:ff:ff:ff:ff:ff
19: dpbr_2-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master dpbr_2 state DOWN
group default qlen 1000
    link/ether 52:54:00:a1:1f:99 brd ff:ff:ff:ff:ff:ff
20: dpbr_3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
 qlen 1000
    link/ether 52:54:00:a2:67:10 brd ff:ff:ff:ff:ff:ff
21: dpbr_3-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master dpbr_3 state DOWN
group default qlen 1000
    link/ether 52:54:00:a2:67:10 brd ff:ff:ff:ff:ff:ff
22: dpbr_4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
 qlen 1000
    link/ether 52:54:00:6a:bb:22 brd ff:ff:ff:ff:ff:ff
23: dpbr_4-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master dpbr_4 state DOWN
group default qlen 1000
    link/ether 52:54:00:6a:bb:22 brd ff:ff:ff:ff:ff:ff
ic3k>

ic3k>show iox summary

IOx Infrastructure Summary:
---------------------------
eid: IC3000-2C2F-K9+FCH2307Y02C
pfm: IC3000-2C2F-K9
s/n: FCH2307Y02C
images: Lnx: 0.10.481., IOx: 1.10.0:r/1.10.0.0:530203c
boot: 2019-11-09 01:10:38
time: 2019-11-15 01:14:04
load: 01:14:04 up 6 days, 3 min, 0 users, load average: 0.05, 0.05, 0.06
memory: ok, used: 1691/7795 (21%)
disk: ok, used: /:491560/549348 (89%), /software:351932/87462892 (0%)
process: ok, running: 5/5
networking: warning, failed: gateway
logs: warning, errors: caf (1)
apps: ok, CyberVisionSensor (R)

ic3k>show iox detail

IOx Infrastructure Summary:
---------------------------
eid: IC3000-2C2F-K9+FCH2307Y02C
pfm: IC3000-2C2F-K9
```

```
s/n: FCH2307Y02C
images: Lnx: 0.10.481., IOx: 1.10.0:r/1.10.0.0:530203c
boot: 2019-11-09 01:10:38
time: 2019-11-15 01:14:54
load: 01:14:54 up 6 days, 4 min, 0 users, load average: 0.19, 0.09, 0.07
memory: ok, used: 1691/7795 (21%)
disk: ok, used: /:491560/549348 (89%), /software:351932/87462892 (0%)
process: ok, running: 5/5
networking: warning, failed: gateway
logs: warning, errors: caf (1)
apps: ok, CyberVisionSensor (R)
Application Information:
------------------------
--Virsh--
Containers:
 Id    Name                           State
----------------------------------------------------
Virtual Machines:
 Id    Name                           State
----------------------------------------------------
 1     CyberVisionSensor              running
Networking Information:
-----------------------
--Address--
svcbr_0 UP 172.27.166.6/25 7000::d2ec:35ff:feca:1de0/64 fe80::d2ec:35ff:feca:1de0/64
--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 1653011 0 13236 0 27045 0 0 0 BMRU
dpbr_0 1500 0 1888079 0 13236 0 0 0 0 0 BMRU
dpbr_n_0 1500 0 0 0 0 0 0 0 0 0 BMU
--Bridge Info--
bridge name     bridge id               STP enabled      interfaces
dpbr_0          8000.525400b0d5d7       no               dpbr_0-nic
       veth1_0
       vnet0
dpbr_1          8000.525400963909       no  d            pbr_1-nic
       int1
       vnet1
dpbr_2          8000.525400b2265b       no               dpbr_2-nic
       int2
       vnet2
dpbr_3          8000.5254002c5c97       no               dpbr_3-nic
       int3
       vnet3
dpbr_4          8000.5254005ddacd       no               dpbr_4-nic
       int4
       vnet4
dpbr_docker_n_0    8000.0242b1138a88   no              dpbr_n_0-nic
dpbr_n_0          8000.525400483753    no                mgmt0
svcbr_0          8000.d0ec35ca1de0     yes               veth0_0

--IP Routes--
Limit exceeded
Process Information:
--------------------
--Monit--
Process 'mhdserver'
 status Running
 pid 1707
 uptime 6d 0h 2m
 memory percent total 0.0%
 cpu percent total 0.0%
Process 'dockerd'
 status Running
```

```
 pid 1467
 uptime 6d 0h 2m
 memory percent total 1.0%
 cpu percent total 0.2%
Process 'igma'
 status Running
 pid 2109
 uptime 6d 0h 2m
 memory percent total 0.1%
 cpu percent total 0.0%
Process 'libvirtd'
 status Running
 pid 1638
 uptime 6d 0h 2m
 memory percent total 0.1%
 cpu percent total 0.0%
Process 'caf'
 status Running
 pid 2088
 uptime 6d 0h 2m
 memory percent total 0.7%
 cpu percent total 0.0%
--Process Info--
  PID STIME CMD
 1697 Nov09 /usr/bin/monit -s /var/run/monit.state
 2088 Nov09 python /home/root/iox/caf/scripts/startup.pyc
/home/root/iox/caf/config/system-config.ini /home/root/iox/caf/config/log-config.ini
 1638 Nov09 /usr/sbin/libvirtd --daemon --listen
 2458 Nov09 /usr/sbin/sshd
 2109 Nov09 /usr/bin/igma
--PID info--
monit:1697
caf:2088
libvirtd:1638
sshd:2458
igma:2109
Disk Usage Information:
-----------------------
--Free Disk--
Filesystem 1024-blocks Used Available Capacity Mounted on
/dev/root 595000 491560 57788 90% /
/dev/sda2 92167844 351932 87110960 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--
/*:
430M /usr
316M /boot
/software/*:
288M /software/caf
ic3k>

ic3k>show ntp

NTP Servers received from DHCP:
171.70.168.183
ic3k>
ic3k>show ntp manual-config
NTP-Server : 3.ntp.esl.cisco.com
NTP-Server : 10.81.254.202
```

```
NTP-Server : 10.81.254.131
NTP-Server : 7.ntp.esl.cisco.com
Preferred-Server : 172.27.88.109 Key : 11
Keys Configuration
Id Type Password
------------------
11  SHA1  pzybf0e2atybc612abb4b08d459f652acudad8eb9
ic3k>
ic3k>show ntp association
     remote           refid                     st   t   when poll reach   delay   offset
 jitter
==============================================================================
 127.127.1.0     .LOCL.                   14    l  27h   64    0        0.000    0.000
0.000
*172.27.88.109   171.68.38.65       2    u  167 1024  377    0.450   -0.012   0.228
+10.81.254.202   .GNSS.               1    u  902 1024  377   72.843    0.062   0.274
-10.81.254.131   .GNSS.               1    u  769 1024  377   72.367    0.385   0.217
+171.68.38.65    .GNSS.               1    u  708 1024  317    2.389   -0.085   0.279
+72.163.32.44    .GNSS.               1    u  909 1024  377   43.472    0.042   0.216
-144.254.15.78   .GNSS.               1    u  228 1024  377  164.244    4.440   0.440
ind assid status  conf reach  auth   condition  last_event         cnt
===========================================================
  1 37781  8013   yes    no   none     reject       unreachable       1
  2 37782  f61a   yes   yes     ok       sys.peer      sys_peer         1
  3 37783  9414   yes   yes   none   candidate   reachable         1
  4 37784  9314   yes   yes   none     outlier       reachable         1
  5 37785  9414   yes   yes   none   candidate   reachable         1
  6 37786  9414   yes   yes   none   candidate   reachable         1
  7 37787  9314   yes   yes   none     outlier       reachable         1
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
ic3k>

ic3k>show ntp status
Clock is synchronized, stratum 3,reference is 172.27.88.109
nominal freq is 100.0000HZ, precision is 2**21
reference time is E0FDB617.0D1C5651 (22:20:07.051000 Tue Aug 13 2019)
clock offset is -0.011554 msec, root delay is 2.861 msec
root dispersion is 60.971 msec, peer dispersion is 15.260 msec
ic3k>

ic3k>show ntp mode
NTP Mode : Manual
ic3k>

ic3k>show operating-mode

Operating-mode: Standalone
Remote Device Management: Enabled
ic3k>

ic3k>show version

Version: 1.2.1
Platform ID: IC3000-2C2F-K9
Hardware ID: FOC2227Y304
ic3k>

ic3k>help standalone-mode

In standalone mode, the IC3000 is an unmanaged device. It will be controlled via Local
Manager and ioxclient.
1. Connect the Management interface on the IC3000 to your Computer with a network cable.
2. Assign "169.254.x.x (netmask 255.255.0.0)" IP address to the network interface on your
computer. NOTE: Use any IP address other than 169.254.128.2 within 169.254.x.x subnet.
```

```
4. The IC3000 will be ready to operate in standalone 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 standalone mode without delay).
5. Access "https://169.254.128.2:8443" from your browser on the computer.
6. Login using the default user and password.
7. Change the default password; user will be logged out of the Local Manager.
8. Login using the default user and the password you set in the previous step.
ic3k>

ic3k>help managed-mode

In managed 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>
```

Enhanced Reset Options for Release 1.3.1

Release 1.3.1 has changed the way Factory reset and configuration reset work:

Enhanced Factory Reset

The factory reset behavior has changed with this release. Factory reset will restore applications if the device was ordered with the application. After factory reset is executed, the device will return with the application in a running state as it came from the factory, with the default configuration on the platform.

If there was not an application shipped from the factory, then the application will not be restored. User installed applications on the device will be erased from the device by this operation.

If the device was shipped prior to release 1.3, the factory reset cannot restore the APP, even if the current running image version is 1.3. This action will result in a loss of all user installed applications, and the device will not have any applications after the reload.

Enhanced Configuration Reset

The configuration reset behavior has changed with this release.

On the IC3000 Platform

When a configuration reset is executed, the system configuration and logs are erased. After the reload, the IC3000 will boot up into a default configuration with respect to the system configuration and logs.

IOx Applications

Previous behavior was to delete all the IOx applications during configuration reset. Release 1.3.1 changed this behavior to NOT delete all IOx applications. All pre-existing applications will come back to the same operational state after the configuration reset.

All activated and running applications will get notified of a platform configuration reset operation via a sentinel file at $CAF_APP_CONFIG_DIR/.iox_app_config_reset. Applications can make use of this sentinel file to reload the application configuration upon platform configuration reset operation. Then, the application is expected to delete this sentinel file.

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.

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

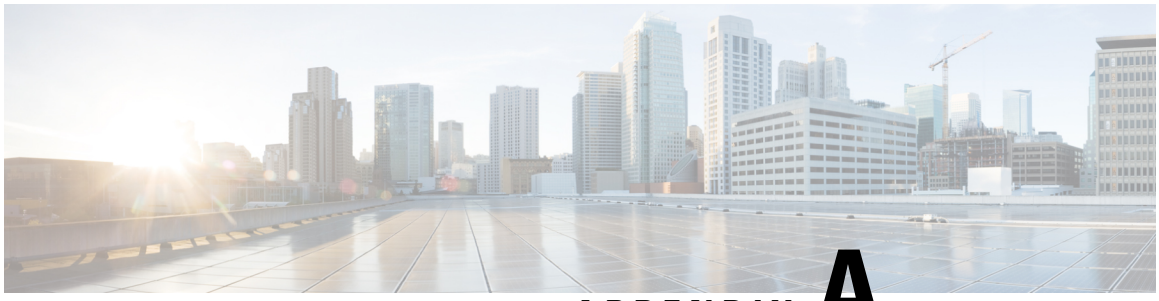
FND Logs

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 A

Appendix

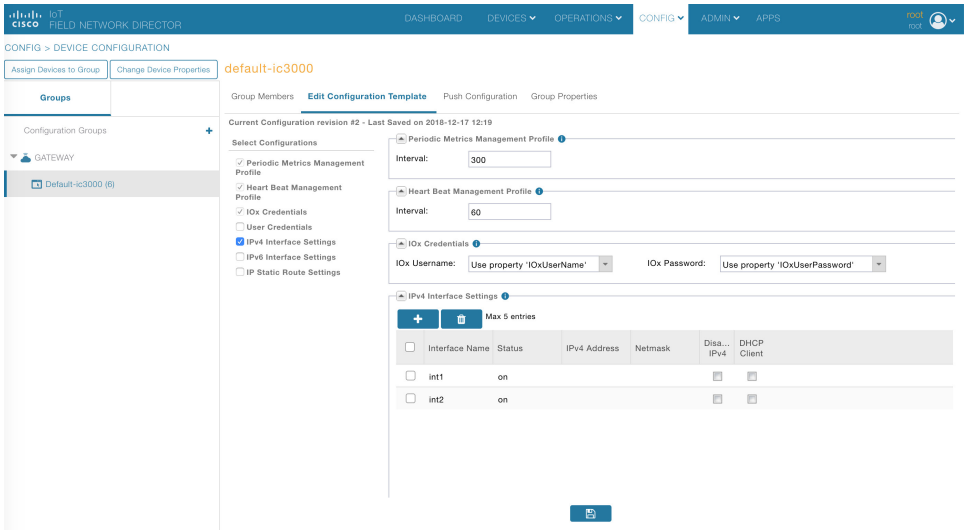
This section contains the following topics:

FND 4.3 device-configuration templates

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 50: Edit Configuration Template



For the FND 4.3.1 release and greater, 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 interfaces up on an 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
   }
  }
]
```

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 and greater 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 and greater, 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, Releases 4.3.x, 4.4.x and 4.5.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 for your current FND release.

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
-
  - 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

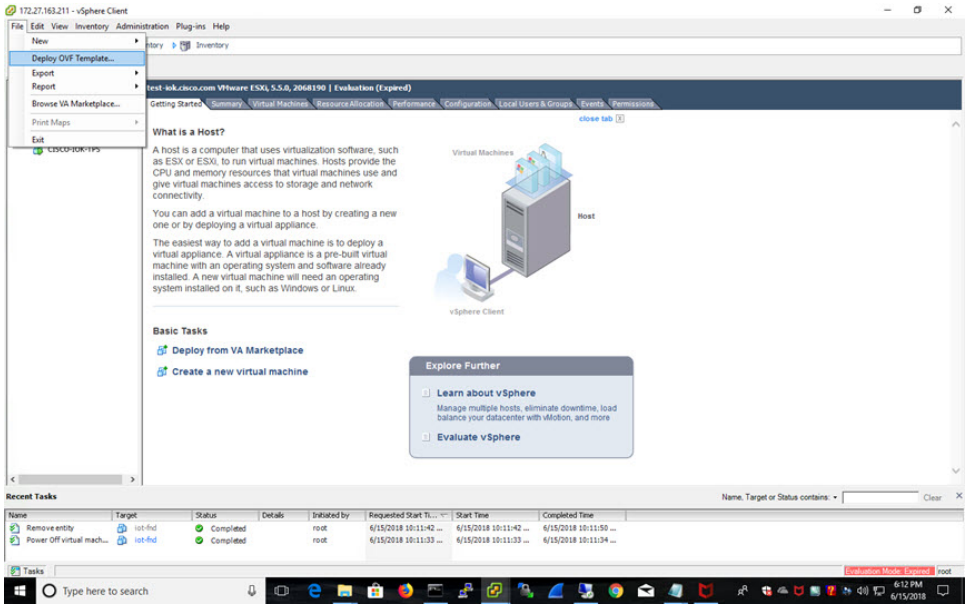
-
  - 16 GB memory
  - 1 core and 4 virtual sockets
  - 150 GB of virtual storage
- Download the OVA from Cisco.com.

Installing the OVA

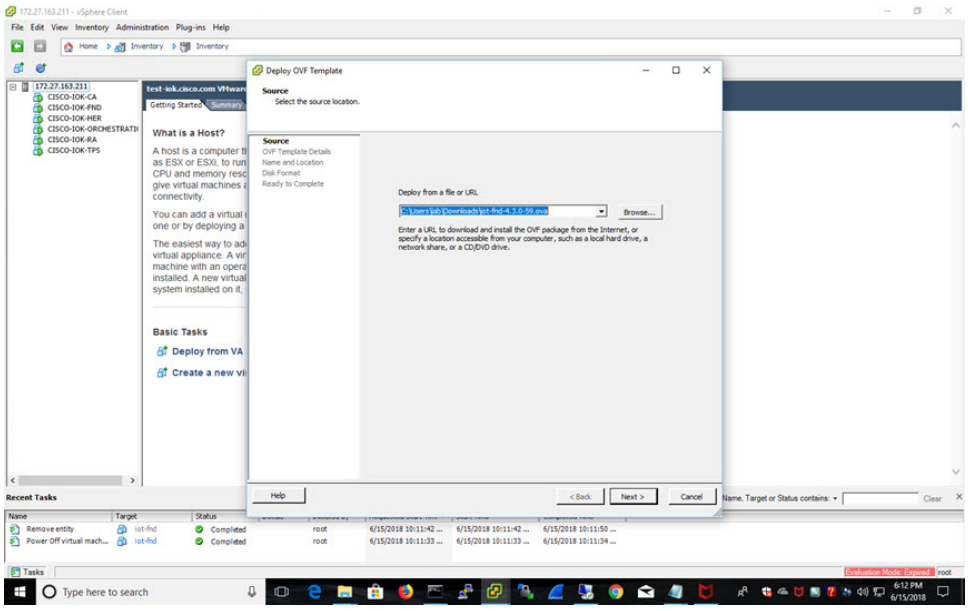
Procedure

Step 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**.

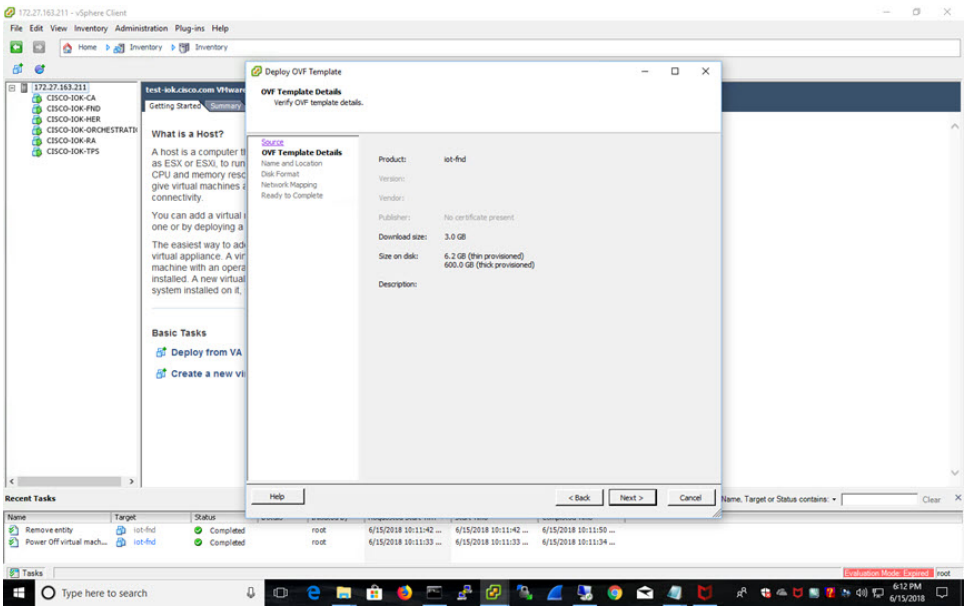


b) Keep the default location and click **Next**.

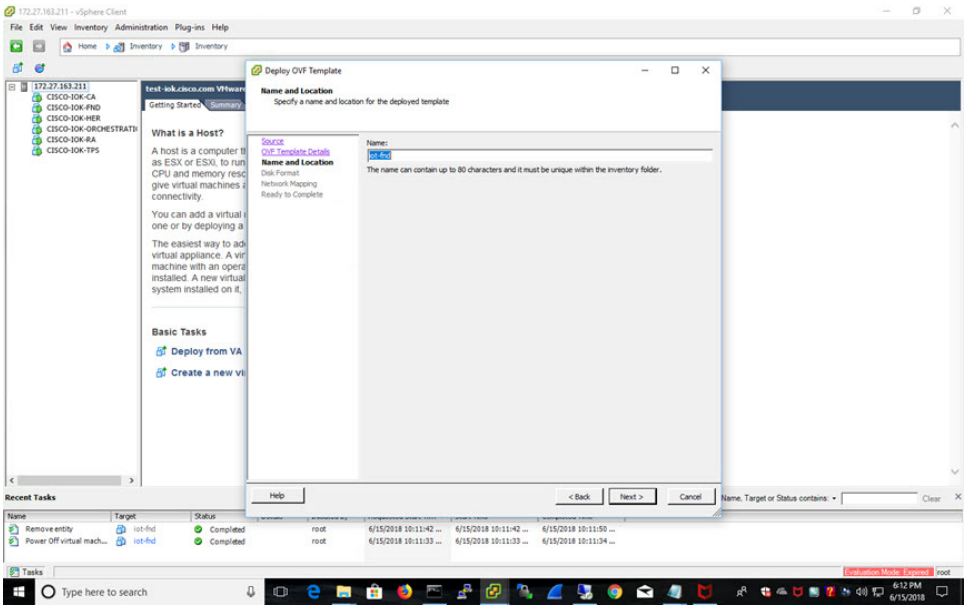


c) Click **Next**.

Appendix

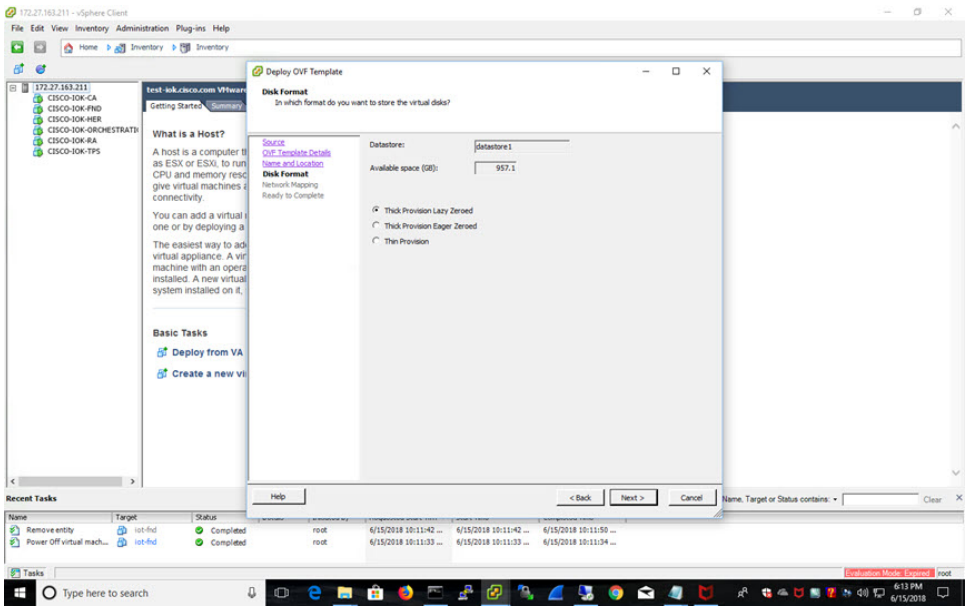


d) Enter a name of the deployed template.

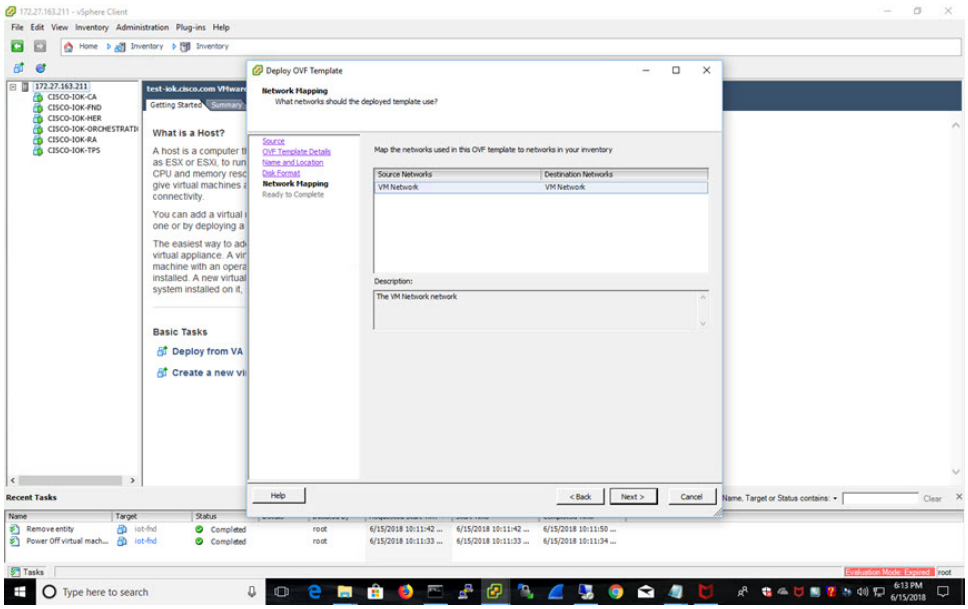


e) Choose the format that you want virtual disks to be stored.

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

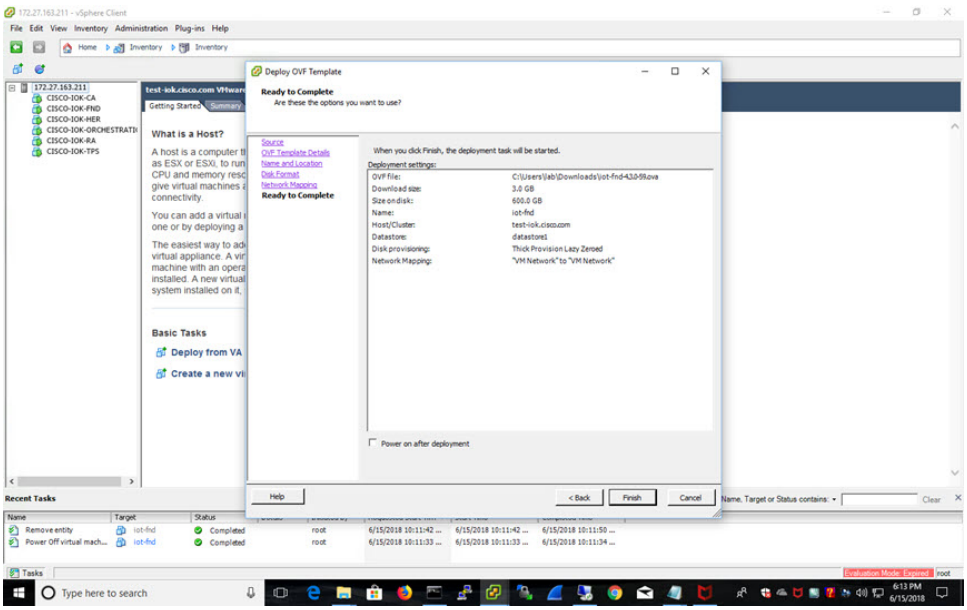


f) Click **Next**.

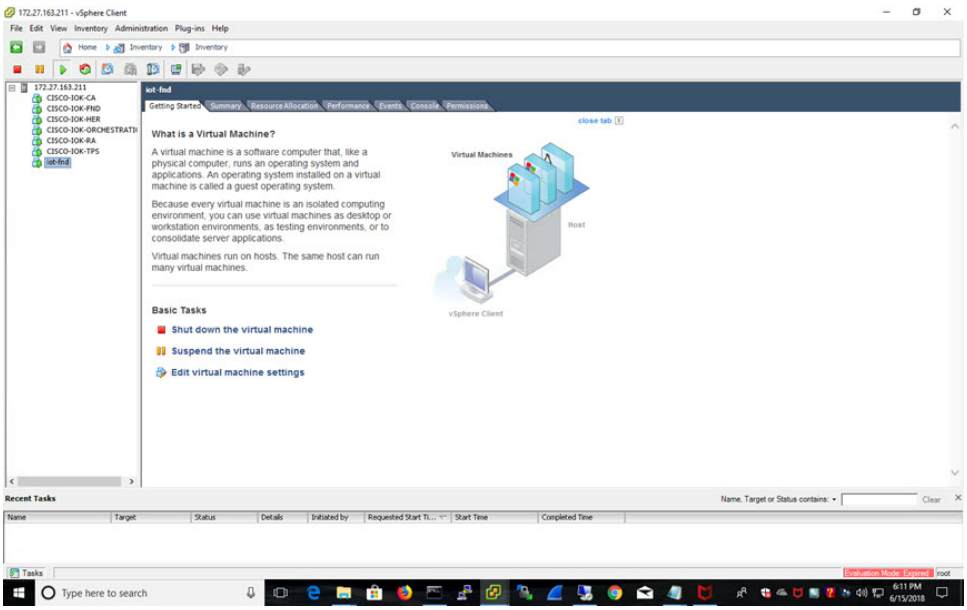


g) Review and click **Finish**.

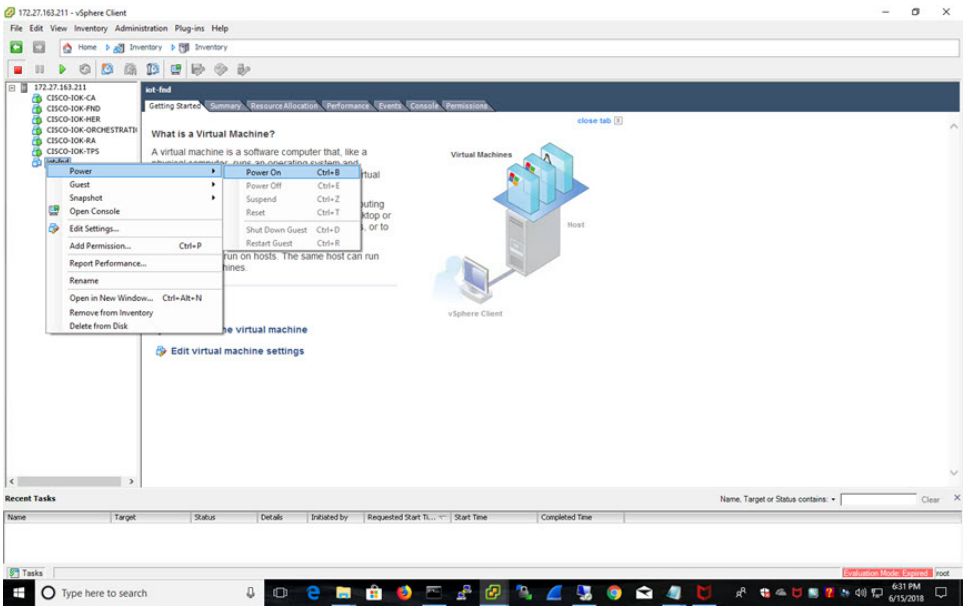
Appendix



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

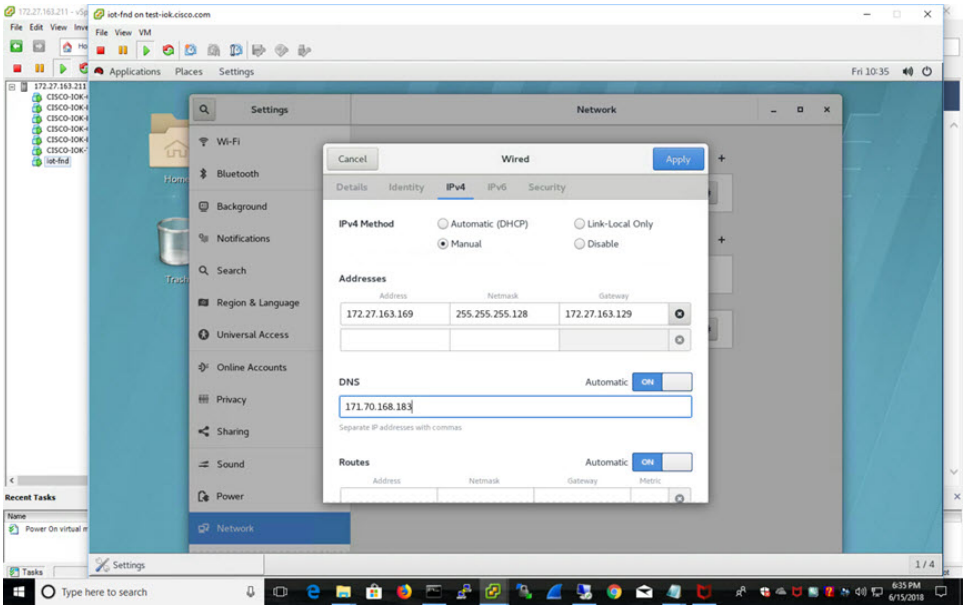


Step 2 Power on the VM. Right click on the iot-fnd template name. Select **Power** and **Power On**.



Step 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.

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

a) Once logged in, go to **Applications -> System Tools -> Settings -> Network**.

b) Click the plus sign (**+**).

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

Step 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==
```

1. 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 4.3.1 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:

Procedure

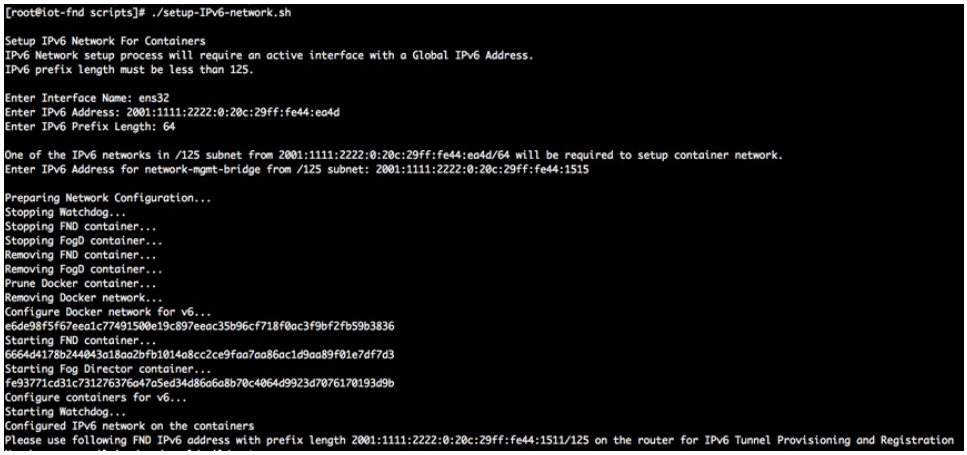
Step 1 Ensure you have one interface with a valid IPv6 network which has a IPv6 prefix length less than125.

See the following example of the ens32 interface:

Example:

```
[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.

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.

Procedure

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

/opt/fnd/data/

Step 2 Enter into FND container

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

Step 3 Change into the conf directory.

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

Step 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

Step 5 Restart FND.

/etc/init.d/cgms restart

Step 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:

cd /opt/fnd/scripts/

```
[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