Managing Firmware Upgrades

This section describes managing firmware upgrade settings in IoT FND, and includes the following sections:

Use IoT FND to upgrade the firmware running on routers (CGR1000s, C800s, IR800s), AP800s and Cisco Resilient Mesh Endpoints (RMEs) such as meters and range extenders. IoT FND stores the firmware binaries in its database for later transfer to routers in a firmware group through an IoT FND and IoT-DM file transfer, and to RMEs using IoT FND.

Cisco provides the firmware bundles as a zip file. For Cisco IOS, software bundles include hypervisor, system image and IOx images (for example, Guest-OS, Host-OS).

For Cisco CG-OS, IoT FND automatically unzips the kickstart and system images included in the bundle. Firmware system images are large (approximately 130 MB); kickstart images are approximately 30 MB. Every firmware bundle includes a manifest file with metadata about the images in the bundle. You can pause, stop, or resume the upload process.

Router Firmware Updates

IoT FND updates router firmware in two steps:

1. Uploads the firmware image from IoT FND to the router. Firmware images upload to the flash:/managed/images directory on the router. **Note:** In some cases the router might be in a Firmware Group. Refer to Configuring Firmware Group Settings

   Because of their large size, firmware-image uploads to routers take approximately 30 minutes, depending on interface speeds.

2. Installs the firmware on the device and reloads it.

   During the firmware install the boot parameters on the routers are updated according to the new image file and the router is reloaded after enabling the *cg-nms-register* cgna profile.

Note: You **must** initiate the firmware installation process. IoT FND **does not** automatically start the upload after the image upload.

When a router contacts IoT FND for the first time to register and request tunnel provisioning, IoT FND rolls the router back to the default factory configuration (ps-start-config) before uploading and installing the new firmware image.

Note: This rollback requires a second reload to update the boot parameters in ps-start-config and apply the latest configuration. This second reload adds an additional 10–15 minutes to the installation and reloading operation.

Upgrading Guest OS Images

Depending on CGR factory configuration, a Guest OS (GOS) may be present in the VM instance. You can install or upgrade Cisco IOS on the **CONFIG > Firmware Update** page (see Router Firmware Updates). The GOS, hypervisor, and Cisco IOS all upgrade when you perform a Cisco IOS image bundle installation or update.

After after any Cisco IOS install or upgrade, when IoT FND discovers a GOS, it checks if the initial communications setup is complete before it performs the required setup. The CGR must have a DHCP pool and GigabitEthernet 0/1 interface configured to provide an IP address and act as the gateway for the GOS. The new GOS image overwrites existing configurations. IoT FND has an internal backup and restore mechanism that ports existing apps to the upgraded Guest OS (see Monitoring a Guest OS).

See the *Cisco 1000 Series Connected Grid Routers Configuration Guides* documentation page for information on configuring the CGR.

Note: If IoT FND detects a non-Cisco OS installed on the VM, the firmware bundle will not upload and the Cisco reference GOS will not install.

Upgrading WPAN Images

At the **CONFIG > Firmware Update** page, you can upload the independent WPAN images (IOS-WPAN-RF, IOS-WPAN-PLC, IOS-WPAN-OFDM, IOS-WPAN-IXM) to IoT FND using the **Images** sub-tab (left-hand side) and **Upload Image** button like other image upgrades. This process is known as a non-integrated WPAN firmware upgrade.

Note: The WPAN firmware image integrated with the IOS CGR image option is still supported.

Also, if only the WPAN firmware upgrade from the image bundled with IOS image is desired (for example, when the WPAN firmware upgrade option was not checked during IOS upgrade), the “Install from Router” option is also provided under respective WPAN image types (IOS-WPAN-RF or IOS-WPAN-PLC).

For detailed steps, go to Working with Router Firmware Images, page 219.

Changing Action Expiration Timer

You can use the cgnms_preferences.sh script to set or retrieve the action expiration timer value in the IoT FND database:

```
/opt/cgms
/bin/cgnms_preferences setCgrActionExpirationTimeout 50
```

Valid options are:

- set*<pkg>actionExpirationTimeoutMins<value>*

  where,

  - *<pkg>* is the preference package (required for *set* and *get* operations).
  - *actionExpirationTimeoutMins* is the preference key (required for *set* and *get* operations).
  - *<value>* is the preferred value, in minutes (required for *set* and *setCgrActionExpirationTimeout* operations).

- setCgrActionExpirationTimeout *<value>*
- get*<pkg>actionExpirationTimeoutMins*
- *getCgrActionExpirationTimeout*

Example

In the following example, the action timer value is retrieved, set, the current value retrieved again, the value removed, and a null value retrieved:

```
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh getCgrActionExpirationTimeout
2013-08-12 22:38:42,004:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
5
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh setCgrActionExpirationTimeout 50
2013-08-12 22:38:51,907:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
Successfully set the preferences.
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh getCgrActionExpirationTimeout
2013-08-12 22:38:58,591:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
50
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh get com.cisco.cgms.elements.ciscocgr
actionExpirationTimeoutMins
2013-08-12 22:39:12,921:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
50
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh set com.cisco.cgms.elements.ciscocgr
actionExpirationTimeoutMins 15
2013-08-12 22:39:23,594:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
Successfully set the preferences.
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh get com.cisco.cgms.elements.ciscocgr
actionExpirationTimeoutMins
2013-08-12 22:39:29,231:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
15
```

Working with Resilient Mesh Endpoint Firmware Images

This section describes how to add Resilient Mesh Endpoint (RME) firmware images to IoT FND, and how to upload and install the images on routers and addresses the following topics:

- Overview
- Uploading a Firmware Image to FND
- Uploading a Firmware Image to a Resilient Mesh Endpoint (RME) Group
- Firmware Update Transmission Settings
- Setting the Installation Schedule
- Set a Firmware Backup Image
- Viewing Mesh Device Firmware Image Upload Logs
- Modify Display of Firmware Management Page
- Viewing Mesh Device Firmware Image Upload Logs

Overview

When you instruct IoT FND to upload a firmware image to the members of an RME firmware group or subnet, IoT FND pushes the image to the group members in the background and tracks the upload progress to ensure that the devices receive the image.

A Resilient Mesh Endpoint (RME) stores three firmware images:

- Uploaded image: Image most recently uploaded.

- Running image: Image that is currently operational.
- Backup image: It serves as a golden (fallback) image for the RME if there is an issue with the running image.

Note: You can initiate up to 3 firmware downloads simultaneously.

Note: IR500s and other RME devices can coexist on a network; however, for firmware management they **cannot** belong to the same group.

Note: RME devices can report BL/Boot Loader image types to IoT FND, but IoT FND **cannot** upload boot loader images to devices.

Uploading a Firmware Image to FND

To upload a firmware image to mesh endpoint group members:

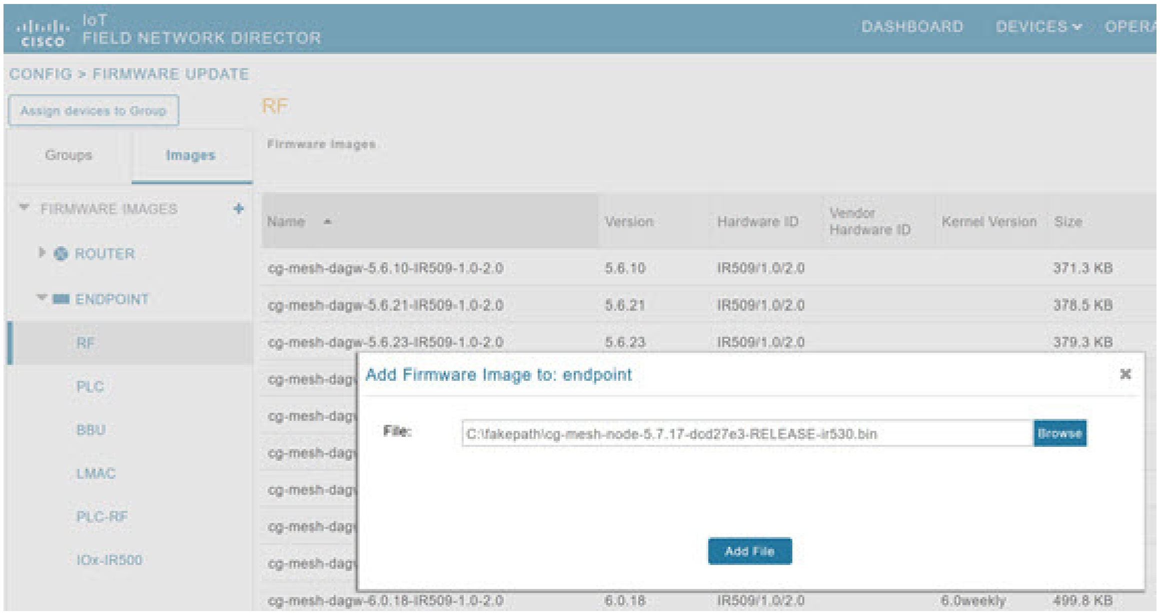
1. Choose CONFIG > FIRMWARE UPDATE.
2. Select the Images tab (left-pane).
3. Select the Endpoint Image type (such as BBU, IOx-IR500 LMAC) to be uploaded.
4. Click on **+** (plus icon) next to the FIRMWARE IMAGES heading to browse the firmware from your local system.
5. Browse and click on **Add file**.

IoT FND can upload the following image types to ENDPOINT devices (Table 1.)

Table 1 Firmware Images for Endpoints

Image Type	Description
BBU	For Battery back up (BBU) units.
IOx-IR500	For IR500 devices running Cisco IOx software.
LMAC	For Local MAC connected devices.
PLC	For endpoints with Power line communication (PLC) radio only.
PLC-RF	For endpoints with Dual PHY support.
RF	For endpoints with RF radio only.

Figure 1 Using IoT FND to Upload Images to an Endpoint



Name	Version	Hardware ID	Vendor Hardware ID	Kernel Version	Size
cg-mesh-dagw-5.6.10-IR509-1.0-2.0	5.6.10	IR509/1.0/2.0			371.3 KB
cg-mesh-dagw-5.6.21-IR509-1.0-2.0	5.6.21	IR509/1.0/2.0			378.5 KB
cg-mesh-dagw-5.6.23-IR509-1.0-2.0	5.6.23	IR509/1.0/2.0			379.3 KB
cg-mesh-dag					
cg-mesh-dag					
cg-mesh-dag					
cg-mesh-dag					
cg-mesh-dag					
cg-mesh-dag					
cg-mesh-dagw-6.0.18-IR509-1.0-2.0	6.0.18	IR509/1.0/2.0		6.0weekly	499.8 KB

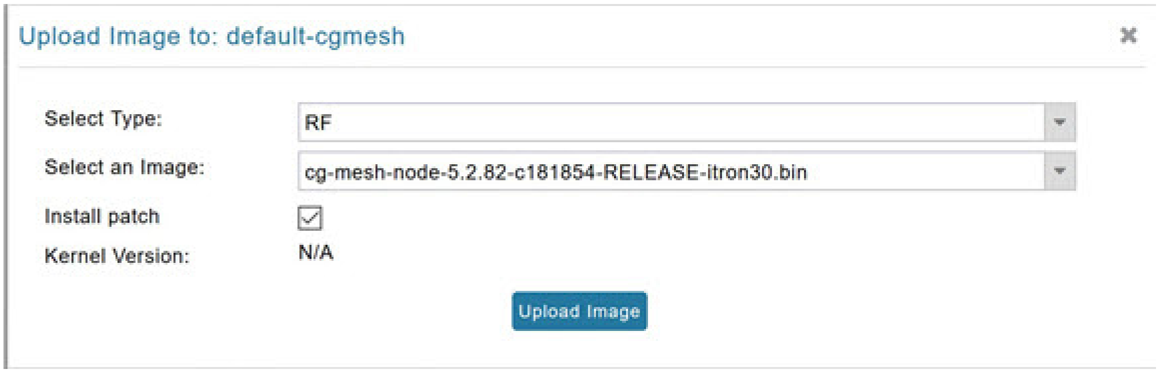
File: C:\fakepath\cg-mesh-node-5.7.17-dcd27e3-RELEASE-ir530.bin

Uploading a Firmware Image to a Resilient Mesh Endpoint (RME) Group

To upload a firmware image to mesh endpoint group members:

1. Choose CONFIG > FIRMWARE UPDATE.
2. Click the **Groups** tab (left-pane)
3. Select the Endpoint firmware group to update.
4. In the right panel, select Firmware Management and then click the **Upload Image** button. In the entry panel that appears, do the following:
    a. From the Select Type drop-down menu, choose the firmware type for your device.
    b. From the Select an Image drop-down menu, choose the firmware bundle to upload.
    c. Click **Upload Image**.
    d. (Optional) Check the **Install patch** box, if you choose *to install only the patch* of the new image (Figure 2)

Figure 2 Check Install Patch Item to ONLY Install the Patch Rather than the Full Image



Upload Image to: default-cgmesh

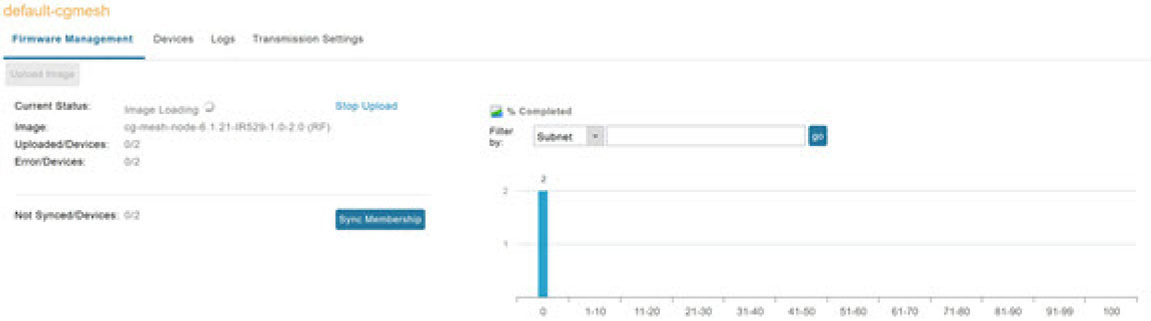
Select Type:	RF
Select an Image:	cg-mesh-node-5.2.82-c181854-RELEASE-itron30.bin
Install patch	☑
Kernel Version:	N/A

e. Click **OK**.

IoT FND adds the image to the list of images in the Firmware Management pane and starts the upload process in the background. A bar chart displays the upload progress (percentage complete). See Figure 3 and Figure 4.

Note: Click the **Sync Membership** button (Figure 3) to ensure that FND and the member endpoint firmware group information is the same.

Figure 3 Firmware Update - Percentage Complete (top-portion of screen)



default-cgmesh

Current Status: Image Loading

Image: cg-mesh-node-6.1.21-IR529-1.0-2.0 (RF)

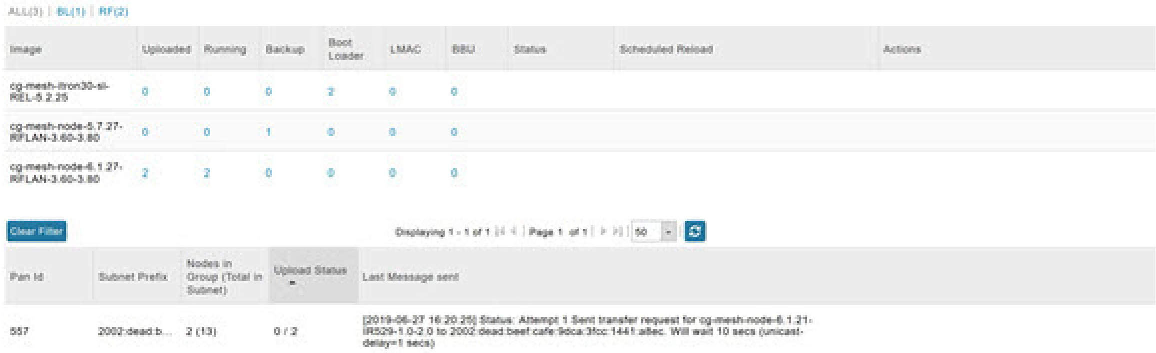
Uploaded/Devices: 0/2

Error/Devices: 0/2

Not Synced/Devices: 0/2

Filter by: Subnet

Figure 4 Firmware Update - Upload Summary (bottom-portion of screen)



ALL(3) | BL(1) | RF(2)

Image	Uploaded	Running	Backup	Boot Loader	LMAC	BBU	Status	Scheduled Reload	Actions
cg-mesh-itron30-sl-REL-5.2.25	0	0	0	2	0	0			
cg-mesh-node-5.7.27-RFLAN-3.60-3.80	0	0	1	0	0	0			
cg-mesh-node-6.1.27-RFLAN-3.60-3.80	2	2	0	0	0	0			

Displaying 1 - 1 of 1 | Page 1 of 1 | 50

Pan Id	Subnet Prefix	Nodes in Group (Total in Subnet)	Upload Status	Last Message sent
557	2002:dead:b...	2 (13)	0 / 2	[2019-06-27 16:20:25] Status: Attempt 1 Sent transfer request for cg-mesh-node-6.1.21-IR529-1.0-2.0 to 2002:dead:beef:cafe:9dca:3fcc:1441:a8ec. Will wait 10 secs (unicast-delay=1 secs)

Actions Supported and Information Displayed at the Firmware Management Pane

At the Firmware Management pane, you can filter the display by Subnet, PanID or Group when you are in the **Devices** tab.

For every image in the list, IoT FND displays the information noted in Table 2.

Table 2 Image Information Displayed by IoT FND

Item	Description
Image	Image name.
Uploaded	Specifies the number of devices that uploaded the image. Click the number to display a list of these devices.
Running	Specifies the number of devices running this image. Click the number to display a list of these devices.
Backup	Specifies the number of devices using this image as a backup. Click the number to display a list of these devices.
Boot Loader	Specifies the boot loader image version.
LMAC	Specifies the LMAC image version.
BBU	Specifies the BBU image version.
Status	Specifies the status of the upload process.
Scheduled Reload	Specifies the scheduled reload time.
Actions	Provides two actions: Schedule Install and Reload –Schedule the installation date and time of the loaded image and the reboot of the endpoint by selecting the Calendar icon . 📅 Set as Backup –Set the firmware backup image by selecting the clock icon with reverse arrow ⟲ See Setting the Installation Schedule for complete steps.

Firmware Update Transmission Settings

You can configure the Transmission Speed for pacing mesh firmware downloads at the Transmission Settings tab (CONFIG > FIMRWARE UPDATE page). See Figure 5.

1. Select the Transmission Speed. Options are Slow (default), Medium, Fast or Custom.

   Note: The Slow setting is recommended as the initial setting. You can increase the Slow setting to Medium (or even Fast) if the following conditions exist:

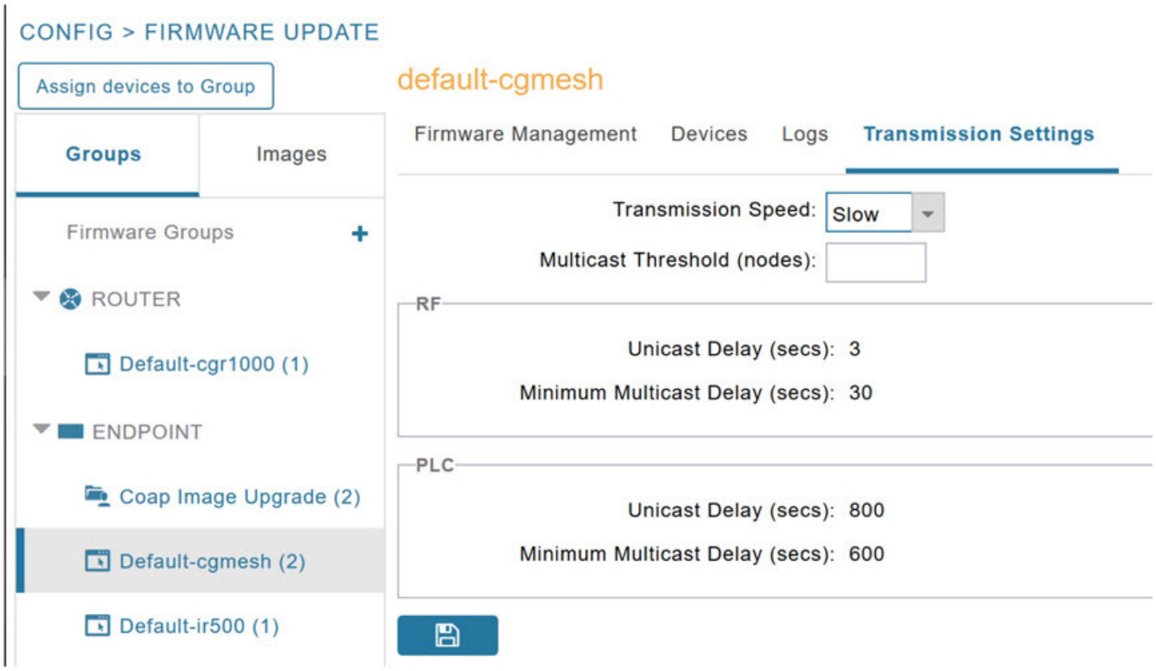
   – The slow setting does not cause any issues in the database and it is able to handle the workload presented without raising any alarms.

   – There is a need to improve on the time taken to do the firmware download.

2. Configure the minimum number of nodes necessary to enable the Multicast firmware upload.

Note: For Custom Transmission Speed, you will have to specify Multicast Threshold, Unicast Delay and Minimum Multicast Delay values. See Table 3 for definitions for terms on the CONFIG > FIRMWARE UPDATE > Transmissions Settings page.

Figure 5 CONFIG > FIRMWARE UPDATE



Transmission Speed: Slow

Multicast Threshold (nodes):

RF

Unicast Delay (secs): 3

Minimum Multicast Delay (secs): 30

PLC

Unicast Delay (secs): 800

Minimum Multicast Delay (secs): 600

Table 3 Definitions of variables seen on the CONFIG > FIRMWARE UPDATE > Transmissions Settings page

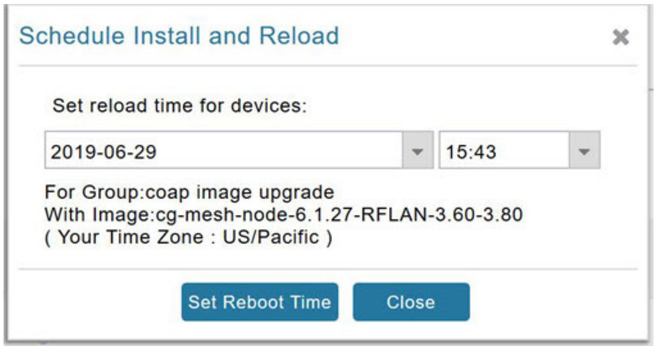
Item	Description
Minimum Multicast Delay (seconds)	Time between subsequent blocks when sending multi-cast messages/blocks/packets to a node.
Multicast Threshold (nodes)	Minimum number of nodes needed to ensure that a multicast transmission can happen in a subnet, if the number of elements requiring a specific image block is greater than or equal to the multicast-threshold value.
Transmission Speed	Options are Slow (default), Medium, Fast or Custom.
Unicast Delay (seconds)	Time between subsequent blocks when sending unicast messages, blocks or packets to a node.

Setting the Installation Schedule

To set the installation schedule for an image:

1. Click the **Schedule install and Reload** button (Calendar icon), See Actions summary in Table 2.
2. In the page that appears (Figure 6), specify the date and time for the installation of the image and rebooting of device.

Figure 6 Schedule and Install and Reload Page



Schedule Install and Reload

Set reload time for devices:

2019-06-29 15:43

For Group:coap image upgrade
With Image:cg-mesh-node-6.1.27-RFLAN-3.60-3.80
(Your Time Zone : US/Pacific)

3. Click **Set Reboot Time button**.

Set a Firmware Backup Image

To set an image as a firmware image backup:

1. Click the **Set as Backup** button. (See the icon in the Actions summary in Table 2).
2. Click **Yes** to confirm backup.

Viewing Mesh Device Firmware Image Upload Logs

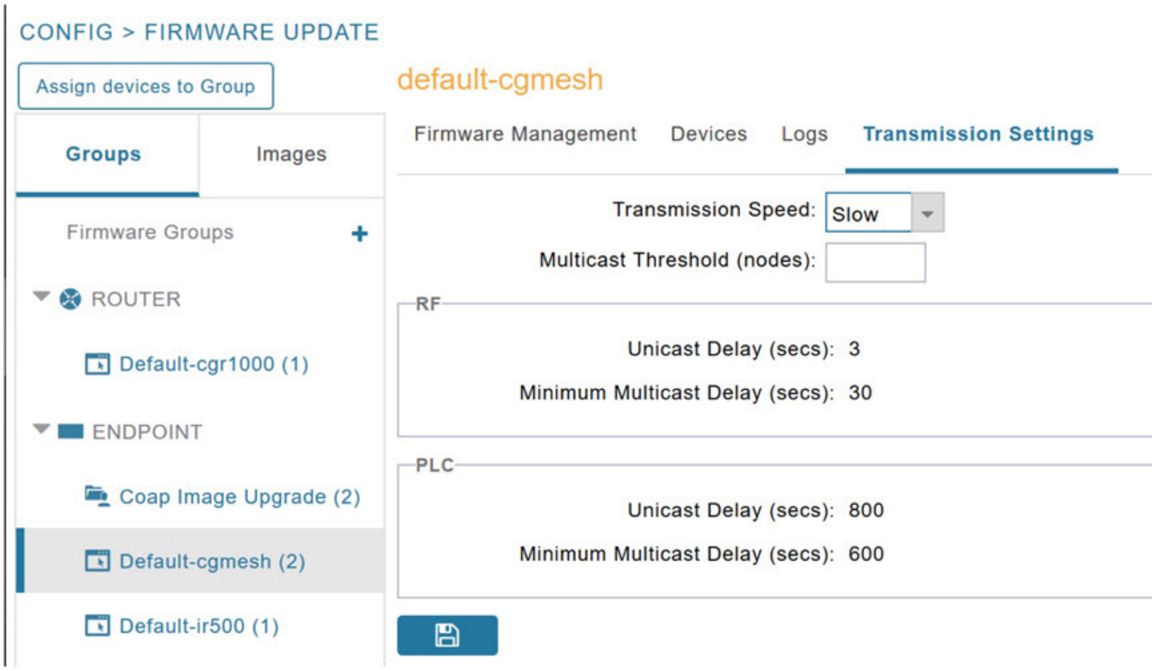
- To sync the group members in the same firmware group, click **Sync Membership** button (Figure 3).
- To view members devices, click the Devices tab. (Figure 3)
- To view log files for the group, click the Logs tab. (Figure 3)

Modify Display of Firmware Management Page

You can filter the Firmware Management page display by Subnet, PanId or Group in the **Devices** tab.

Click the **Sync Membership** button to ensure that the information for FND and the member endpoint firmware group is the same.

Figure 7 CONFIG > FIRMWARE UPDATE



Transmission Speed: Slow

Multicast Threshold (nodes):

RF

Unicast Delay (secs): 3

Minimum Multicast Delay (secs): 30

PLC

Unicast Delay (secs): 800

Minimum Multicast Delay (secs): 600

AP800 Firmware Upgrade During Zero Touch Deployment

During the PnP bootstrapping, whenever an access point (AP) or router sends the firmware request, FND will need to make the choice as to whether Unified Firmware or Autonomous Firmware is updated on the AP to make it accessible to the Cisco Wireless LAN Controller (WLC) after a firmware upgrade.

Note: Once you set up the DHCP server on a Cisco IOS router, WLC generally handles the software updates for the AP.

Allows you to set the desired firmware that will update an IR829 or C800 router during ZTD.

There are two possible firmware options:

- Option 1: Set the ‘unified’ version (k9w8: the factory-shipped version) as the desired firmware.
- Option 2: Set the autonomous firmware as the desired firmware version.

During the ZTD process, the firmware upgrade of an access point (AP) or embedded AP on an IR829 or C800 router will upgrade using the firmware version you define as the autonomous firmware.

To define the Autonomous Firmware for an IR829 or C800 router:

1. Choose CONFIG > DEVICE CONFIGURATION.
2. Select the desired router: Default-ir800 or C800 (left-pane).
3. Check the installed firmware version, BEFORE upload. if equal to the latest version, skip firmware upgrade.
4. Before you upload the software to the router, check the image and version:

   a) If the router image version is equal to the latest version, skip upgrade.

   b) If router image, has the latest

5. Select **Edit AP Configuration Template** tab (right-pane).
6. Enter the following text in the right-pane:

```
ip dhcp pool embedded-ap-pool
network <router_ip> 255.255.255.0
dns-server <dns_ip>
default-router <router_ip>
option 43 hex  f104.0a0a.0a0f      (Note: Enter a single WLC IP address(10.10.10.15) in hex format)
ip address <router_ip> 255.255.255.0
!                                {Note the symbol in this line is an exclamation point}
service-module wlan-ap 0 bootimage unified
```

7. Click **disk** icon (bottom of page) to save the commands in the configuration template.
8. Once you set up the DHCP server on a Cisco IOS router,

Mesh Firmware Migration (CG-OS CG4 platforms only)

Note: Mesh Firmware Migration to Cisco Resilient Mesh is not supported for CGRs running CG-OS version CG4(4).

IoT FND allows you to update earlier versions of CGR firmware to allow Cisco Resilient Mesh networking using the following IoT FND North Bound APIs:

- findEidByIpAddress
- startReprovisionByEidList
- startReprovisionByEidListAbridged
- startReprovisionByGroup
- startReprovisionByGroupAbridged

See the North Bound API User Guide for the Cisco IoT Field Network Director, Releases 3.x and 4.x for usage information.

Image Diff Files for IR809 and IR829

To reduce file size that transfers across network for IR809 and IR829, you can send a partial image.

At the Upload Image page, select type: IOS-IR800

Check box for option: “install patch for IOS and hypervisor from this bundle.”

Gateway Firmware Updates

IC3000 Firmware Updates

At the CONFIG > FIRMWARE UPDATE page, you can add or delete the IC3000 firmware image.

At the Images tab on that page, expand the Gateway icon and click on IC3000 to see a list of available IC3000 images.

Configuring Firmware Group Settings

This section describes how to add, delete, and configure firmware groups, and includes the following topics:

- Adding Firmware Groups

- Assigning Devices to a Firmware Group
- Renaming a Firmware Group
- Deleting Firmware Groups

Note: Upload operations only begin when you click the Resume button.

When you add routers or RMEs to IoT FND, the application sorts the devices into the corresponding default firmware group: default-*<router>* or default-cgmesh. Use these groups to upload and install firmware images on member devices. Add firmware groups to manage custom sets of devices. You can assign devices to firmware groups manually or in bulk. Before deleting a firmware group, you must move all devices in the group to another group. You cannot delete non-empty groups.

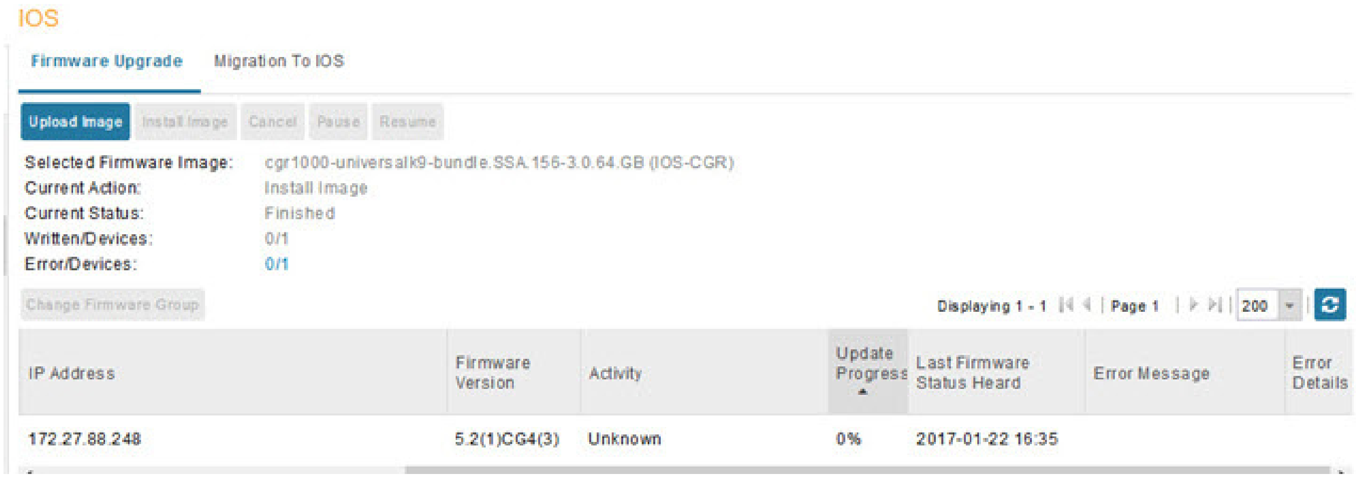
Note: When creating firmware groups note the guidelines:

- CGRs, IR800s, and C800s can coexist on a network; however, for firmware management, they cannot belong to the same firmware group.
- IR500s and other RMEs devices can coexist on a network; however, for firmware management, they cannot belong to the same group.

The Groups tab on the **CONFIG > Firmware Update** page displays various device metrics.

Tip: At the Firmware Update page, click the Error/Devices link (not shown) in Figure 8 to apply a filter. Click the **Clear Filter** to revert to an unfiltered view of the selected device group.

Figure 8 Firmware Update Page – Viewing Errored Devices



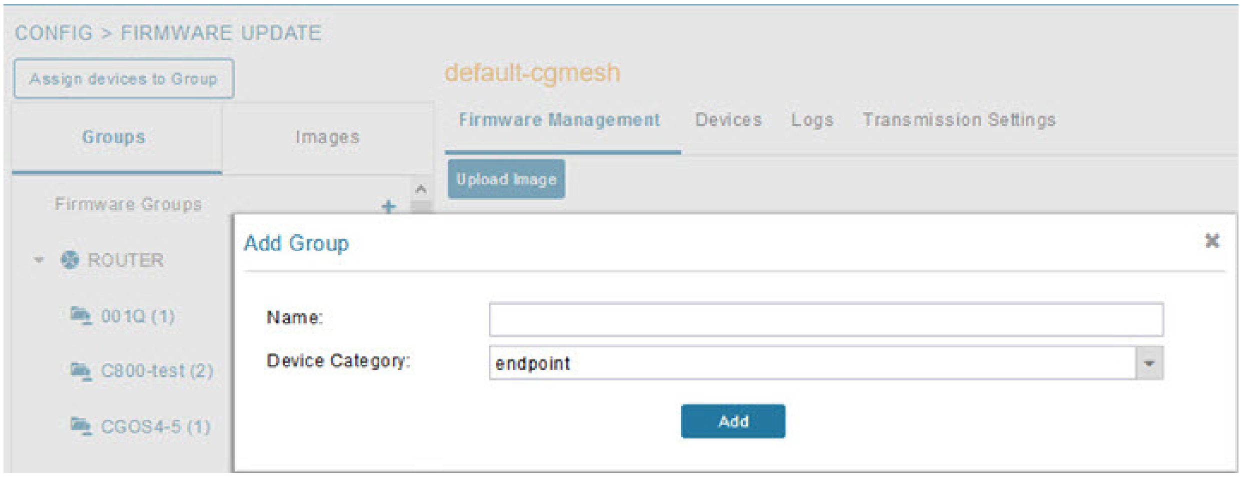
Selected Firmware Image: cgr1000-universalk9-bundle.SSA.156-3.0.64.GB (IOS-CGR)
Current Action: Install Image
Current Status: Finished
Written/Devices: 0/1
Error/Devices: 0/1

IP Address	Firmware Version	Activity	Update Progress	Last Firmware Status Heard	Error Message	Error Details
172.27.88.248	5.2(1)CG4(3)	Unknown	0%	2017-01-22 16:35		

Adding Firmware Groups

To add a firmware group:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.



3. In the **Groups** pane, select one of the following: **Default-cgr1000**, **Default-c800**, **Default-ir500**, **Default-ir800**, **Default-cgmesh** or **Default-sbr**.

4. Click **+** next to Firmware Groups heading in the Groups pane to Add Group.

5. In the **Add Group** dialog box, enter the name of the firmware group. Device Category options depend on the device type you select in step 3.

6. Click **Add**.

   The new group label appears under the corresponding device type in the Firmware Groups pane.

To assign devices to the new group, see Assigning Devices to a Firmware Group.

Assigning Devices to a Firmware Group

This section describes moving devices, and includes the following topics:

- Moving Devices to Another Group Manually
- Moving Devices to Another Group In Bulk

Moving Devices to Another Group Manually

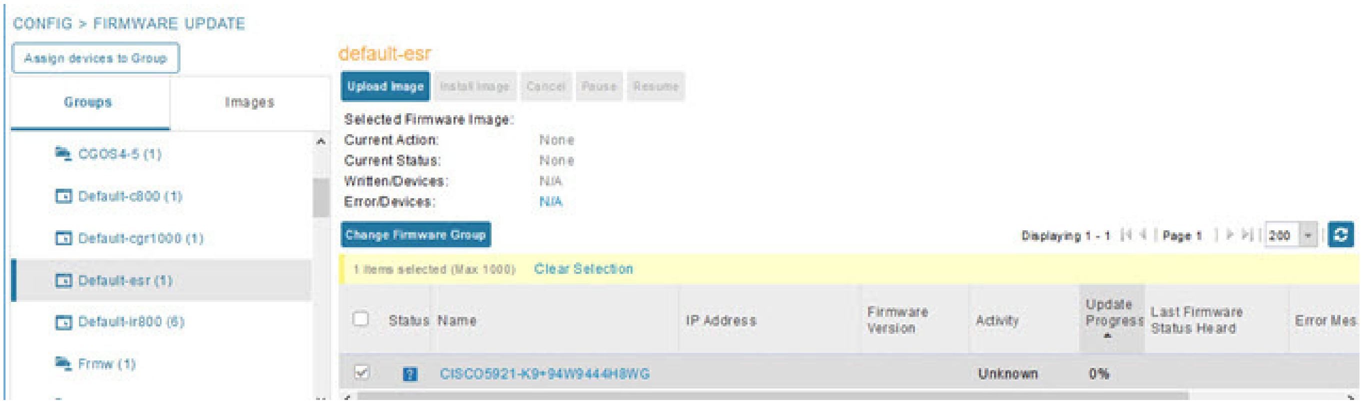
To manually move devices to a group:

1. Choose **CONFIG > Firmware Update**.

2. Click the **Groups** tab.

3. In the Firmware Groups pane, select the desired firmware group based on device type.

   Note: If this is an ENDPOINT firmware group, click the **Devices** tab above the main pane.



Selected Firmware Image:
Current Action: None
Current Status: None
Written/Devices: N/A
Error/Devices: N/A

1 items selected (Max 1000)

☐	Status	Name	IP Address	Firmware Version	Activity	Update Progress	Last Firmware Status Heard	Error Mes
☑	?	CISCO5921-K9+94W9444H8WG			Unknown	0%		

4. Check the check boxes of the devices that you want to move.
5. Click **Change Firmware Group**. to open a pop up window.
6. From the **Firmware Group** drop-down menu, choose the firmware group to which you want to move the devices or enter a new group name.
7. Click **Change Firmware Group**.
8. Click **Close**.

Moving Devices to Another Group In Bulk

To move devices from one group to another in bulk:

1. Create a CSV or XML file listing devices that you want to move using the format shown in the following examples:

   ***DeviceType/EID* for CGRs:**

   ```
   eid
   CGR1120/k9+JS1
   CGR1120/k9+JS2
   CGR1120/k9+JS3
   ```

   ***EID* only for mesh endpoints:**

   ```
   eid
   00078108003c1e07
   00078108003C210b
   ```

   ***EID* only for IR800s**

   ```
   eid
   ir800
   ```

   ***EID* only for ISR 800s:**

   ```
   eid
   C819HGW-S-A-K9+FTX174685V0
   C819HGW-S-A-K9+FTX174686V0
   C819HGW-S-A-K9+FTX174687V0
   ```

   ***EID* only for IR500s:**

   ```
   eid
   da1
   da2
   da3
   ```

   EID only for IC3000

   ```
   eid
   IC3000+FOC2219Y47Z
   ```

   Note: Each file can only list one device type.

2. Choose **CONFIG > Firmware Update**.
3. Click the **Groups** tab.
4. Click **Assign devices to Firmware Group** button (found above Groups tab).
5. In the window that appears, click **Browse** and locate the device list CSV or XML file.
6. From the **Group** drop-down menu, choose the destination group.
7. Click **Assign to Group**.

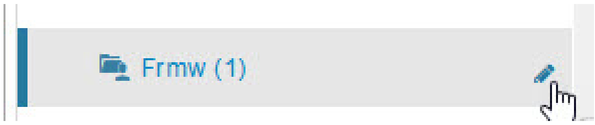
   IoT FND moves the devices listed in the file from their current group to the destination group.

8. Click **Close**.

Renaming a Firmware Group

To rename a firmware group:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.
3. In the Firmware Groups pane, select the firmware group to rename.
4. Move the cursor over the group and click the **Edit Group Name** pencil icon.



5. In the **Rename Group** window, enter the new name and then click **OK**.

   Note: When you enter an invalid character entry (such as, @, #, !, or +) within the Rename Group field, IoT FND displays a red alert icon, highlights the field in red, and disables the **OK** button.

Deleting Firmware Groups

Note: Before deleting a firmware group, you must move all devices in the group to another group. You cannot delete non-empty groups.

To delete a firmware group:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.
3. In the Firmware Groups pane, select a firmware group to display a list of all possible firmware images for that group in the right pane.
4. Check the box next to the firmware group that you want to delete.
5. Click **Clear Selection** that appears above the entry (yellow bar).
6. To confirm deletion, click **Yes**.
7. Click **OK**.

Working with Router Firmware Images

This section describes how to add router firmware images to IoT FND and how to upload and install the images on routers, and includes the following topics:

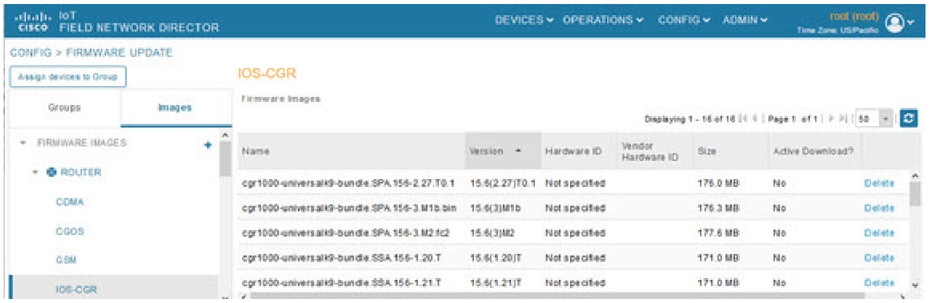
- Viewing Firmware Image Files in IoT FND
- Adding a Firmware Image to IoT FND
- Uploading a Firmware Image to a Router Group
- Canceling Router Firmware Image Upload
- Pausing and Resuming Router Firmware Image Uploads

- Installing a Firmware Image
- Stopping Firmware Image Installation
- Pausing and Resuming Router Firmware Image Installation

Viewing Firmware Image Files in IoT FND

You can display firmware image information from the **Images** pane in the **CONFIG > Firmware Update** page. Select ROUTER or ENDPOINT to display all firmware images for those devices in the IoT FND database. Select the firmware image type to refine the display (see Figure 9).

Figure 9 CONFIG > Firmware Update Images Pane



Name	Version	Hardware ID	Vendor Hardware ID	Size	Active Download?	
cgr1000-universalk9-bundle.SPA.156-2.27.T0.1	15.6(2.27)T0.1	Not specified		176.0 MB	No	Delete
cgr1000-universalk9-bundle.SPA.156-3.M1b.bin	15.6(3)M1b	Not specified		176.3 MB	No	Delete
cgr1000-universalk9-bundle.SPA.156-3.M2.fc2	15.6(3)M2	Not specified		177.6 MB	No	Delete
cgr1000-universalk9-bundle.SSA.156-1.20.T	15.6(1.20)T	Not specified		171.0 MB	No	Delete
cgr1000-universalk9-bundle.SSA.156-1.21.T	15.6(1.21)T	Not specified		171.0 MB	No	Delete

For every image in the list, IoT FND provides this information:

Field	Description
Name	The filename of the firmware image bundle.
Version	The version of the firmware bundle. Click the arrowhead icon to switch between ascending and descending listing of the firmware version.
Hardware ID	The hardware family to which you can download this image.
Size	The size of the firmware bundle.
Active Download?	The active firmware using the firmware image.

Adding a Firmware Image to IoT FND

Before you can upload and install a firmware image on a device, add the image file (as a zip archive) to IoT FND. IoT FND stores the image in its database.

Note: Do not unzip the image file. IoT FND unzips the file.

To add a firmware image to IoT FND:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Images** tab (Figure 9).
3. In the Images pane, select **ROUTER**, **ENDPOINT** or **GATEWAY**, and the type of device group.
4. Click the **+** icon to select an image found to the right of the Firmware Images heading.
5. Click **Browse** to locate the firmware image. Select the image, then click **Add File.**
6. Click **Upload**.

   The image appears in the Firmware Images panel (Figure 9).

- To delete an image, click **Delete** link shown at far-right of entry. Click **Yes** to confirm.

  Firmware images with a download in progress (with Yes in the Active Download? column) cannot be deleted.
- To upload the firmware image to devices in a group, select the group (from Groups listing on CONFIG > FIRMWARE UPDATE page) and then click **Upload Image.** See Uploading a Firmware Image to a Router Group.

Uploading a Firmware Image to a Router Group

When you upload a firmware image to router firmware group members, IoT FND pushes the image to the group members in the background and tracks the upload progress to ensure that the devices receive the image.

On routers, firmware image upload and installation requires 200 MB of free disk space. IoT FND stores image files in the .../managed/images directory on the router.

Note: If there is not enough disk space on the router for the firmware image, the IoT FND initiates disk cleanup process on the router and removes the following files, sequentially, until there is enough disk space to upload the new image:

- Unused files in the .../managed/images directory that are not currently running or referenced in the before-tunnel-config, before-registration-config, express-setup-config, and factory-config files for IOS CGRs; golden-config, ps-start-config, express-setup-config, or factory-config for CG-OS CGRs
- Unused .gbin and .bin files from the bootflash directory in CG-OS CGRs

If there is still not enough space, you must manually delete unused files on the router.

To upload a firmware image to router group members:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.
3. In the Groups pane, select the router firmware group that you want to update.

   Note: CGR groups can include devices running Cisco IOS and CG-OS. Therefore, Cisco IOS software images only upload to devices running Cisco IOS (C5921s, IR800s, ISR800s, CGR1000s); only CGRs accept CG-OS images.

   IoT FND displays the firmware image type applicable to the router:

Image	Type	Applicable Device
ACTD-CGR	cgr1000	Cisco IOS CGRs running Guest OS
CDMA	all	Cisco IOS CGRs, IR800s, and ISR800s
CGOS	cgr1000	Cisco IOS CGRs running Guest OS
ENDPOINT	IR500	Cisco IR500
GSM	all	Cisco IOS CGRs, IR800s, and ISR800s
IOS-CGR	cgr1000	Cisco IOS CGRs (CGR 1240 and CGR 1120)
IOS-ESR	c5921	Cisco 5921 ESR (C5921)
IOS-IOx	cgr1000	Cisco IOS CGRs (CGR 1240 and CGR 1120) universal image
IOS-C800	c800	Cisco 800 Series ISR connected devices.
IOS-AP800	ap800	Cisco 800 Series Access Points.
IOS-IR800	ir800	Cisco 800 Series ISRs.
IOS-IR807	ir800	Image (Cisco IOS only) loads to IR807 within the IR800 firmware group.
IOS-WPAN-IXM	ir800	LoRaWAN IXM module when operating as an interface for Cisco IR809.

Image	Type	Applicable Device
IOS-WPAN-RF	cgr1000	Cisco IOS-CGR
IOS-WPAN-PLC	cgr1000	Cisco IOS-CGR
IOT-FND-IC3000	ic3000	Cisco IC3000 Gateway
IOx-CGR	cgr1000-ioxvm	Cisco IOS-CGR
IOx-IR800	ir800	Cisco 800 Series ISRs.
LMAC	lmac	Local MAC connected devices.
LORAWAN	lorawan	Cisco IR829-GW

4. Click **Upload Image** to open the entry panel.
5. From the **Select Type:** drop-down menu, choose the firmware type for your device.
6. From the **Select an Image:** drop-down menu, choose the firmware bundle to upload.

   For some software bundles, you also have the option to select one or more of the following options (as noted in parenthesis next to the options listed below):

   – Install Guest OS from this bundle (IOS-CGR, IOS-IR800)

   – Clean LoRaWAN application data on the install (LORAWAN)

   – Install WPAN firmware from this bundle (IOS-CGR)
7. Click **Upload Image**.
8. Click **OK**.

IoT FND starts the upload process. After the image uploads, install the image as described in Installing a Firmware Image.

Canceling Router Firmware Image Upload

You can stop the image upload process to firmware router groups at any time. Stopping the upload can take a few minutes. When you cancel the image upload, the image upload process immediately stops currently running tasks, and blocks all queued tasks.

Note: Running tasks do not complete, leaving partial files on the disk and sets the firmware group status to CANCELING until you complete the upload operation.

To stop firmware image uploading to a group:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.
3. In the Groups pane, select the firmware group.
4. Click **Cancel**.
5. Click **Yes**.

Pausing and Resuming Router Firmware Image Uploads

You can pause the image upload process to router firmware groups at any time, and resume it later.

Note: The image upload process does not immediately pause; all queued (but not running) operations pause, but currently running tasks complete. The status changes to PAUSING until the active operations complete.

To pause firmware image upload:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.
3. In the Groups pane, select the firmware group.
4. Click **Pause**.

   The Status column displays PAUSING until the active upload operations complete. No new upload operations start until you click the Resume button.
5. Click **Yes**.

To resume the upload process, click **Resume**.

Note: If a IoT FND server goes down while the firmware image is being uploaded to devices, the server resumes the upload process for the scheduled devices after the server comes up. For IoT FND server clusters, if one server goes down during the upload process, another server in the cluster resumes the process.

Installing a Firmware Image

To install an image on devices in a router firmware group:

1. Choose **CONFIG > Firmware Update**.
2. Click the **Groups** tab.
3. In the Groups pane, select the firmware group.

   Note: IoT FND recognizes devices as firmware-specific, and uploads the proper image to selected devices.
4. In the Images pane, select a device subgroup (such as IOS-CGR, IOS-WPAN-RF, CDMA) to refine the display to those device types.

   This step above is necessary because IoT FND recognizes devices as firmware-specific and ensures the system uploads the proper image to selected devices.
5. At the **CONFIG > Firmware Update** page, click the Groups tab; and, then **Install Image** on the Firmware Upgrade tab.

   IoT FND sends commands to install the uploaded image and make it operational.
6. Click **Yes**.

   IoT FND starts the installation or reloading process.

Note: If you restart IoT FND during the image installation process, IoT FND restarts the firmware installation operations that were running prior to IoT FND going offline.

You can pause or stop the installation operation as described in:

- Stopping Firmware Image Installation
- Pausing and Resuming Router Firmware Image Installation

Note: The firmware installation operation can time out on some routers. If routers are not heard from for more than an hour, IoT FND logs error messages.

Stopping Firmware Image Installation

You can stop firmware image installation at any time. When you stop image installation, the running version of the firmware remains in place.

Note: Stopping the installation cancels all queued tasks. Currently running tasks complete.

To stop firmware image installation to devices in a firmware group:

1. Choose **CONFIG > Firmware Update**.
2. Click **Groups**.
3. In the Groups pane, select the firmware group.
4. In the Firmware Upgrade window, click **Cancel** button.
5. Click **Yes** to confirm action.

Pausing and Resuming Router Firmware Image Installation

You can pause the firmware image installation process at any time.

Note: Pausing the installation pauses all queued tasks. Currently running tasks complete.

To pause firmware image installation to devices in a firmware group:

1. Choose **CONFIG > Firmware Update**.
2. In the Groups pane, select the firmware group.
3. In the Firmware Upgrade window, click **Pause** button.
4. Click **Yes** to confirm action.

You can resume the installation process by clicking **Resume**.

Performing CG-OS to Cisco IOS Migrations

You can upgrade CGRs from CG-OS to IOS in bulk or by device. The migration package is in the IoT Field Network Director installation package, and is available in the **Select IOS Image** menu.

Note: The **Migration to IOS** button is disabled if all CGRs in the group are IOS.

BEFORE YOU BEGIN

For CG-OS CGRs that you are migrating, modify the device configuration properties CSV or XML file to include the following IOS properties (see Changing Device Configuration Properties, page 112):

EXAMPLE BOOTSTRAP PROPERTIES

This example preserves tunnels during migration:

```
enable
!
configure terminal
!
!
!
interface GigabitEthernet2/2
    no switchport
    ip address 66.66.0.75 255.255.0.0
    duplex auto
    speed auto
    no shut
!
crypto key generate rsa label LDevID modulus 2048
!
hostname IOS-IOT1
!
enable password cisco
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
!
aaa session-id common
clock timezone PDT -8 0
!
!
no ip domain lookup
ip domain name ios.com
ip host nms.sgbu.cisco.com 55.55.0.5
ip host ps.sgbu.cisco.com 55.55.0.8
ip cef
ipv6 unicast-routing
ipv6 cef
!
!
!
crypto pki profile enrollment NMS
enrollment url  http://55.55.0.17/certsrv/mscep/mscep.dll
!
crypto pki trustpoint LDevID
    enrollment mode ra
    enrollment profile NMS
    serial-number none
    ip-address none
    password
    fingerprint 1D33B1A88574F11E50F5B758EF217D1D51A7C83F
    subject-name CN=mig.ios.com/serialNumber=PID:CGR1240/K9 SN:JAF1712BCAP
    revocation-check none
    rsakeypair LDevID 2048
!
!
!
license accept end user agreement
license boot module cgr1000 technology-package securityk9
license boot module cgr1000 technology-package datak9
!
!
!
username admin password 0 cisco
username cg-nms-administrator privilege 15 secret Sgbu123!
!
!
do mkdir flash:archive
#await Create directory filename
#send_CR
!
!
archive
```

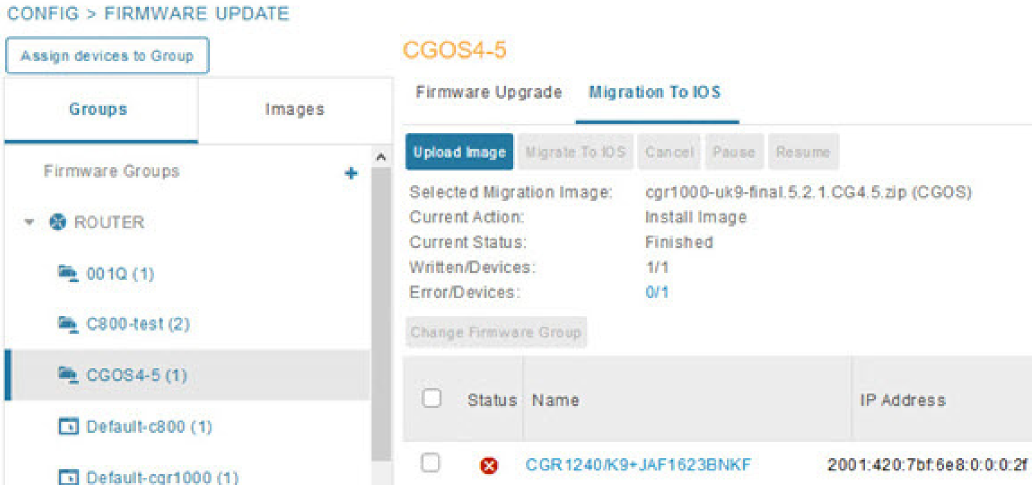
```
    path flash:archive/
    maximum 8
!
!
!
no ip http server
ip http authentication local
ip http secure-server
ip http secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha dhe-aes-256-cbc-sha
ip http secure-client-auth
ip http secure-port 8443
ip http secure-trustpoint LDevID
ip http max-connections 2
ip http timeout-policy idle 600 life 86400 requests 3
ip http client connection timeout 5
ip http client connection retry 5
ip http client source-interface GigabitEthernet2/2
ip http client secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha dhe-aes-256-cbc-sha
!
ip route 0.0.0.0 0.0.0.0 66.66.0.8
!
!
privilege exec level 2 dir /recursive
privilege exec level 2 dir
privilege exec level 2 show memory statistics
privilege exec level 2 show memory
privilege exec level 2 show inventory
privilege exec level 2 show platform hypervisor
privilege exec level 2 show platform led summary
privilege exec level 2 show platform led
privilege exec level 2 show processes cpu
privilege exec level 2 show processes
privilege exec level 2 show environment temperature
privilege exec level 2 show environment
privilege exec level 2 show module
privilege exec level 2 show version
privilege exec level 2 show logging
privilege exec level 2 show platform
privilege exec level 2 show
!
!
wsma agent exec
    profile exec
!
wsma agent config
    profile config
!
!
wsma profile listener exec
    transport https path /wsma/exec
!
wsma profile listener config
    transport https path /wsma/config
!
cgna profile cg-nms-tunnel
    add-command show hosts | format flash:/managed/odm/cg-nms.odm
    add-command show interfaces | format flash:/managed/odm/cg-nms.odm
    add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
    add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
    add-command show version | format flash:/managed/odm/cg-nms.odm
    interval 10
    url https://ps.sgbu.cisco.com:9120/cgna/ios/tunnel
    active
!
!
```

```
cgna exec-profile CGNA-default-exec-profile
    add-command event manager run no_config_replace.tcl flash:/before-tunnel-config cg-nms-tunnel 1 0
    interval 1
    exec-count 1
!
event manager environment ZTD_SCEP_CGNA_Profile cg-nms-tunnel
event manager environment ZTD_SCEP_LDevID_trustpoint_name LDevID
event manager directory user policy "flash:/managed/scripts"
event manager policy tm_ztd_scep.tcl type system authorization bypass
event manager policy no_config_replace.tcl type system authorization bypass
event manager environment ZTD_SCEP_Enabled TRUE
!
!
do write memory
!
do reload in 005
#await Proceed with reload?
#send_CR
!
crypto pki authenticate LDevID
!
end
```

Note: You can only migrate from CG4(3) to the minimum IOS image for that device. Refer to Table 4 on page 228 for minimum IOS image requirements.

To add CGR IOS images to IoT Field Network Director and upload and install the migration image on CGRs:

1. Select **CONFIG > Firmware Update**, and click the **Migration to IOS** tab.



Selected Migration Image: cgr1000-uk9-final.5.2.1.CG4.5.zip (CGOS)
Current Action: Install Image
Current Status: Finished
Written/Devices: 1/1
Error/Devices: 0/1

☐	Status	Name	IP Address
☐	☒	CGR1240/K9+JAF1623BNKF	2001:420:7bf:6e8:0:0:0:2f

2. In the Groups pane, select a CGR (or a group of CGRs) running CGOS4(5) software.
3. Select the Cisco IOS software image to upload to the CGR(s), and click **Upload Image** (right-pane).
4. Click **OK** to begin the upload.

   Upload progress appears in the device list.
5. Upload the following properties files (see Installing Cisco IoT FND in the appropriate Cisco IoT FND 4.3 installation guide):

- Cisco IoT Field Network Director Installation Guide-Oracle Deployment, Release 4.3.x
- Cisco IoT Field Network Director Post-Installation Guide - Release 4.3.x (Tunnel Provisioning and High Availability)

:

- config
- bootstrap
- tunnel provisioning
- runtime configuration

6. Click the **Migrate To IOS** button.
7. Click **Yes** to confirm and begin the migration process.

   The Update Progress displays as a percentage during the software image upload. If an upload fails, error messages and error details also appear for the software image. You can cancel, pause, or resume the migration process.

   Tip: If any routers fail to upgrade, restart migration on the group. IoT Field Network Director skips routers that were successfully upgraded.

Interface Names After Migration

IoT Field Network Director preserves metrics for the various interfaces and associated properties during migration. Table 4 maps CG-OS interfaces to the corresponding IOS interfaces to preserve metrics.

Table 4 CG-OS-to-IOS Interface Migration Map

CG-OS Interface	Corresponding IOS Interface
Wifi2/1	Dot11Radio2/1
Ethernet2/1	GigabitEthernet2/1
Ethernet2/2	GigabitEthernet2/2
Ethernet2/3	FastEthernet2/3
Ethernet2/4	FastEthernet2/4
Ethernet2/5	FastEthernet2/5
Ethernet2/6	FastEthernet2/6
Wpan4/1	Wpan4/1
Serial1/1	Async1/1
Serial1/2	Async1/2
Cellular3/1	Cellular3/1
N/A	GigabitEthernet0/1