



# Managing Firmware Upgrades

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

- [FAR Firmware Updates](#)
- [Configuring Firmware Group Settings](#)
- [Working with FAR Firmware Images](#)
- [Performing OS Migrations](#)
- [Working with Mesh Endpoint Firmware Images](#)

Use IoT FND to upgrade the firmware running on FARs (CGR1000s, C800s, IR800s), AP800s and Mesh Endpoints (CGEs and range extenders). IoT FND stores the firmware binaries in its database for later transfer to FARs in a firmware group through an IoT FND and IoT-DM file transfer, and to MEs 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.

## FAR Firmware Updates

IoT FND updates FAR firmware in two steps:

1. Uploads the firmware image from IoT FND to the devices.

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

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

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

When a FAR contacts IoT FND for the first time to register and request tunnel provisioning, IoT FND rolls the FAR 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 [FAR Firmware Updates](#)). The GOS, hypervisor, and Cisco IOS all upgrade when you perform a Cisco IOS image bundle installation or update.

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 [Managing 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 or IOS-WPAN-PLC) 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.

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 FAR Firmware Images, page 268](#).

## Changing Action Expiration Timer

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

```
/opt/cgms
/bin/cgms_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/cgms_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/cgms_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/cgms_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/cgms_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
```

## Mesh Endpoint Firmware Updates

When you instruct IoT FND to upload a firmware image to the members of an ME 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 mesh endpoint 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 endpoint if there is an issue with the running image.

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

## Mesh Firmware Migration (CG-OS CG4 platforms only)

**Note:** Mesh Firmware Migration to Cisco 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 mesh networking using the following IoT FND North Bound APIs:

- findEidByIpAddress
- startReprovisionByEidList
- startReprovisionByEidListAbridged
- startReprovisionByGroup
- startReprovisionByGroupAbridged

See the *Cisco Connected Grid NMS North Bound API Programming Guide* for usage information.

## 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 FARs or MEs 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 following caveats:

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

IoT FND displays this information about the image on the FARs in the selected firmware group:

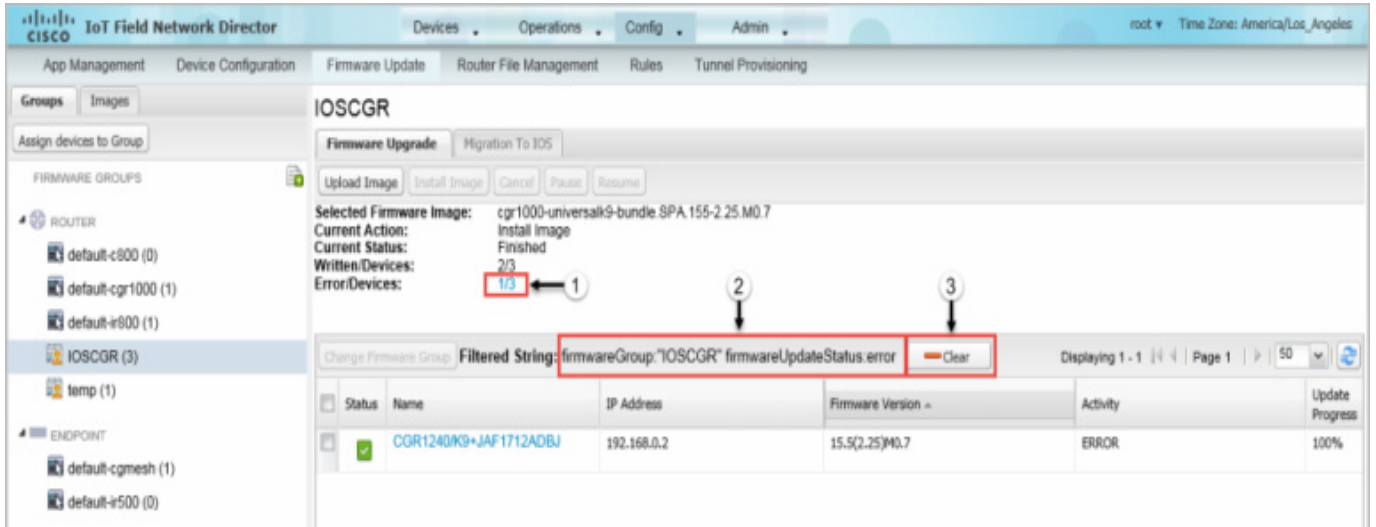
| Field                   | Description  |
|-------------------------|--|
| Selected Firmware Image | The name of the current image zip archive or the image being uploaded to group members.  |
| Current Action          | The name of the firmware action being performed.   |
| Current Status          | The status of the image uploading. Possible statuses are: <ul style="list-style-type: none"> <li>■ Image Loading, Upload Paused, Upload Stopped, Upload Finished, Upload Stopping, Upload Pausing</li> <li>■ Scheduling Reload, Reload Paused, Reload Stopped, Reload Scheduling Finished, Reload Stopping, Reload Pausing</li> <li>■ Setting Backup, Backup Paused, Backup Stopped, Backup Finished, Backup Stopping, Backup Pausing</li> </ul> |
| Written/Devices         | Specifies how many devices received or installed the image out of the total number of devices in the group.<br><br>For example, 1/3 means that one device received the firmware image out of 3 devices in the group.   |
| Error/Devices           | Specifies how many devices failed to receive or install the image out of the total number of devices in the group. For example, 2/3 means that two out of the three devices in the group failed to install the image.<br><br><b>Tip:</b> Click the Error/Devices link (1 in <a href="#">Figure 1</a> ) to view the devices that are in the errored state.  |

For every FAR in the group, IoT FND displays this information:

| Field                      | Description  |
|----------------------------|--|
| Status                     | Device status of the (for example, Up, Down, or Unheard).  |
| Name                       | EID of the device.   |
| IP Address                 | IP address of the device.  |
| Firmware Version           | Version of the firmware image installed on the device.   |
| Activity                   | Device activity.   |
| Update Progress            | Firmware image updating progress. A progress of 100% indicates that the image uploading is complete. |
| Last Firmware Status Heard | The last time the firmware status was heard.   |
| Error Message              | Error message if image upload failed.  |
| Error Details              | Displays error details for the selected device.  |

**Tip:** Click the Error/Devices link (1 in Figure 1) to apply a filter (3). Click the Clear (2) button to revert to an unfiltered view of the selected device group.

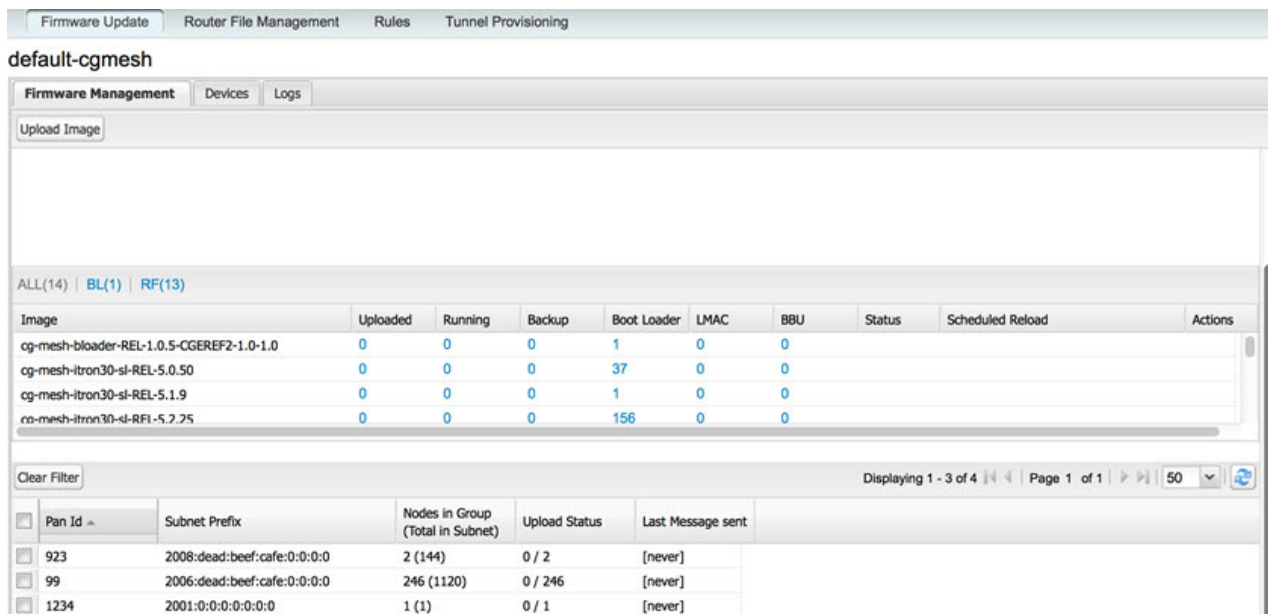
**Figure 1** Firmware Update Page – Errored Devices




## Adding Firmware Groups

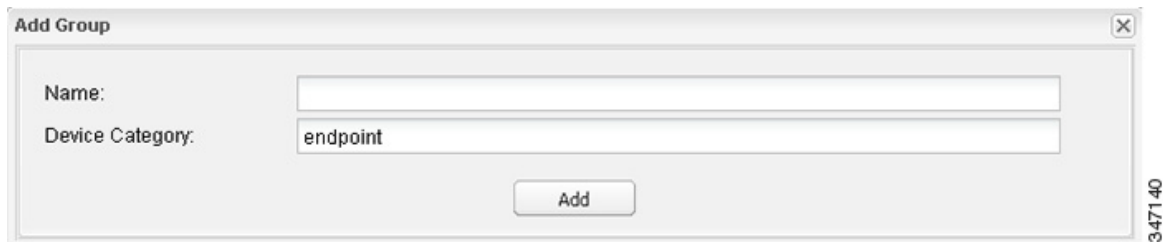
To add a firmware group:

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



3. In the FIRMWARE GROUPS pane, select **default-cgr1000**, **default-c800**, **default-ir500**, **default-ir800**, or **default-cgmesh**.

4. Click **Add Group** (  ) at the top-right of the FIRMWARE GROUPS pane.
5. In the **Add Group** dialog box, enter the name of the firmware group. Device Category is dependent on the device type you select in 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:

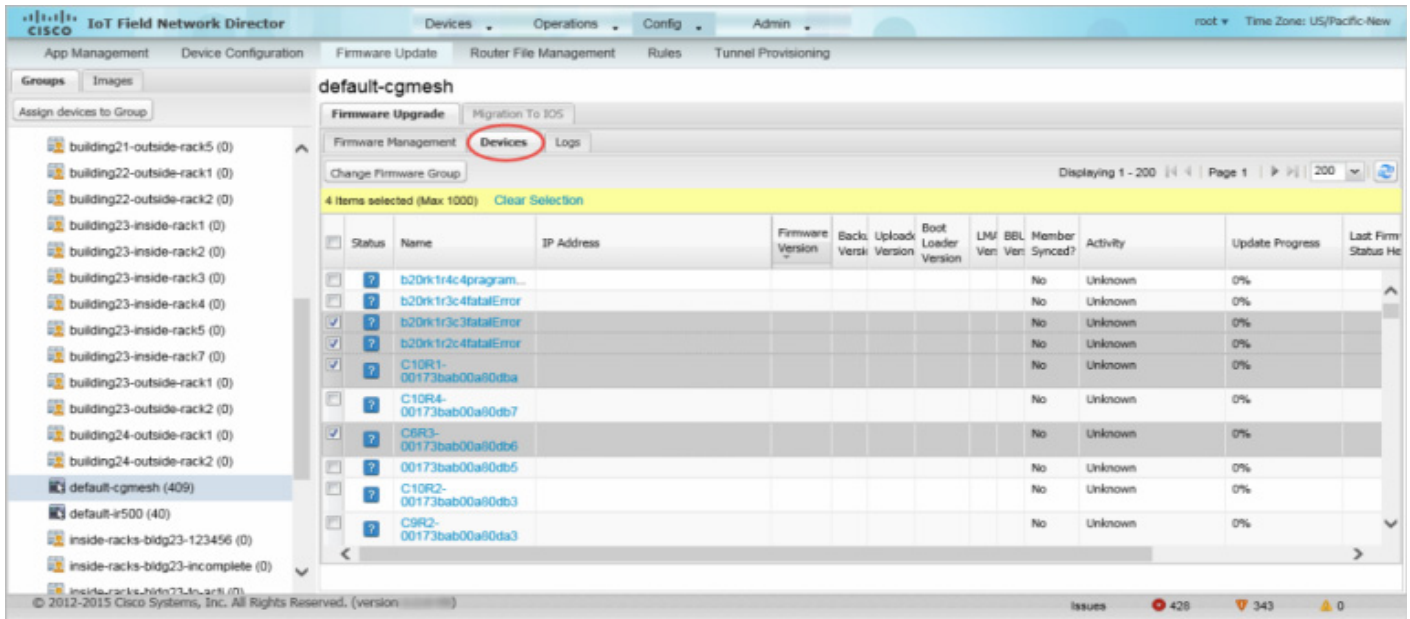
- [Moving Devices to Another Group Manually](#)
- [Moving Devices to Another Group In Bulk](#)

### 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.



4. Check the check boxes of the devices that you want to move.
5. Click **Change Firmware Group**.



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 MEs:**

eid  
 00078108003c1e07  
 00078108003C210b

**EID only for IR800s**

eid  
 ir800

**EID only for ISR 800s:**

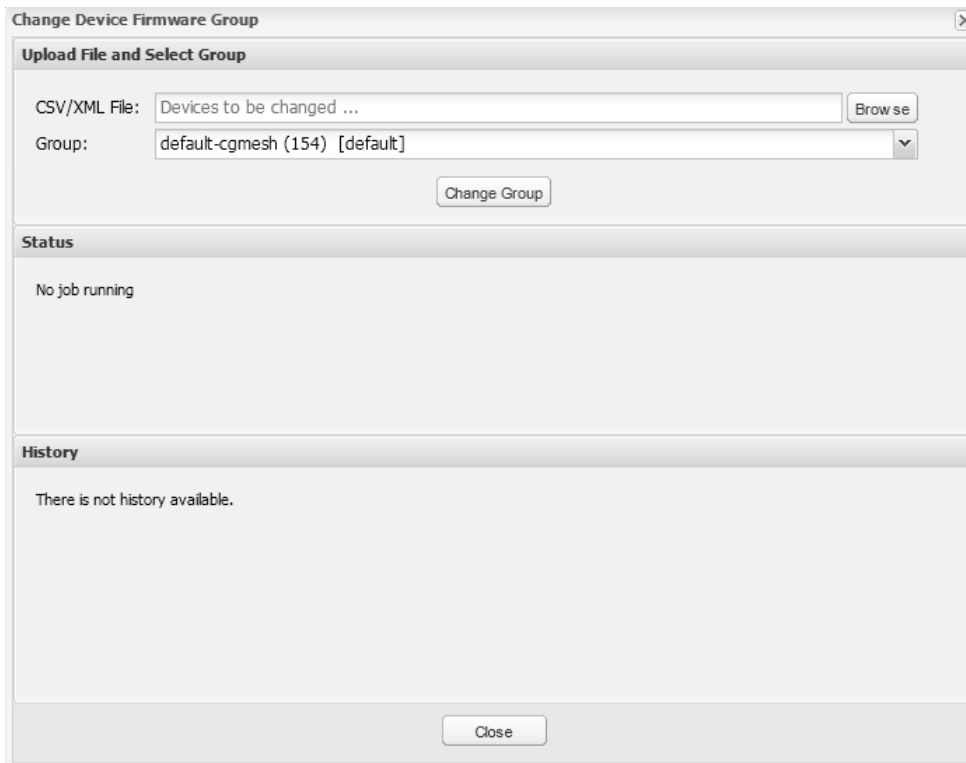
eid  
 C819HGW-S-A-K9+FTX174685V0  
 C819HGW-S-A-K9+FTX174686V0  
 C819HGW-S-A-K9+FTX174687V0

**EID only for IR500s:**

eid  
 da1  
 da2  
 da3

**Note:** Each file can only list one device type.

2. Choose **Config > Firmware Update**.
3. Click the **Groups** tab.
4. Click **Assign Devices to Group**.



5. Click **Browse** and locate the device list CSV or XML file.
6. From the **Group** drop-down menu, choose the destination group.
7. Click **Change Group**.

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

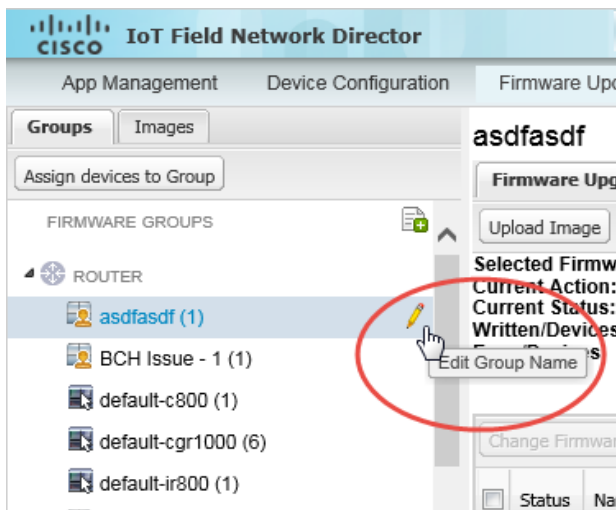


8. Click **Close**.

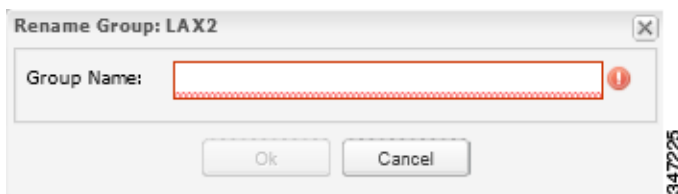
## Renaming a Firmware Group

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:** As shown above, when you enter an invalid character entry (such as, @, #, !, or +) within a 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 the firmware group to delete.
4. Move the cursor over the group and click **Delete Group** (🗑️).



5. To confirm deletion, click **Yes**.

6. Click **OK**.

## Working with FAR Firmware Images

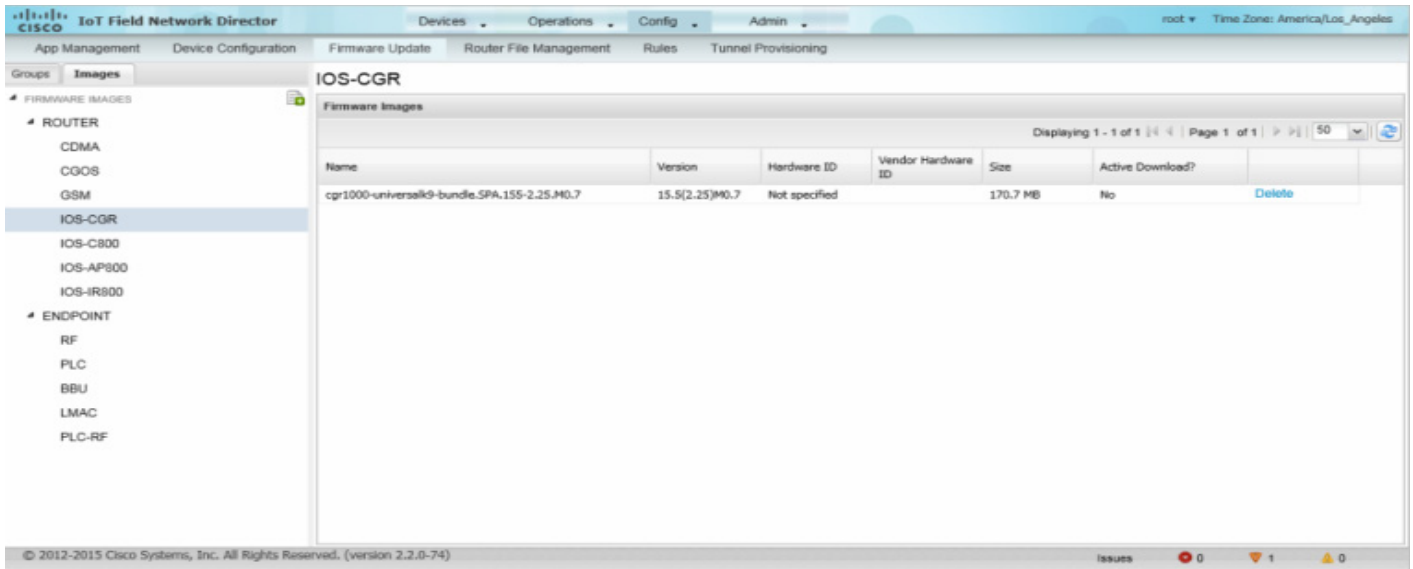
This section describes how to add FAR firmware images to IoT FND and how to upload and install the images on FARs, and includes the following topics:

- [Viewing Firmware Image Files in IoT FND](#)
- [Adding a Firmware Image to IoT FND](#)
- [Uploading a Firmware Image to a FAR Group](#)
- [Canceling FAR Firmware Image Upload](#)
- [Pausing and Resuming FAR Firmware Image Uploads](#)
- [Installing a Firmware Image](#)
- [Stopping Firmware Image Installation](#)
- [Pausing and Resuming FAR Firmware Image Installation](#)
- [Excluding Subnets from Firmware Image Installation and Other Actions](#)

## 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. For example, [Figure 2](#) shows that selecting **ENDPOINT > BBU** displays the available BBU firmware image file name and version, and supported Hardware ID.

Figure 2 Config > Firmware Update Images Pane



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.                       |
| 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 2).
3. In the Firmware Images pane, select **ROUTER** or **ENDPOINT**, and the type of device group.
4. Click **Add Image** (📎).
5. Click **Browse** to locate the firmware image. Select the image, then click **Choose**.
6. Click **Upload**.

The image appears in the Firmware Images pane.

## ENDPOINT

| Firmware Images                         |         |                    |
|---|---------|--------------------|
| Name                                    | Version | Hardware ID        |
| BBUFW-0.0.0-BBUFW-1.0-1.0               | 0.0.0   | BBUFW/1.0/1.0      |
| cg-mesh-node-5.5.23-CGEREF1-1.0-1.0     | 5.5.23  | CGEREF1/1.0/1.0    |
| cg-mesh-node-55.0.94-RFLAN-3.60-3.80    | 55.0.94 | RFLAN/3.60/3.80    |
| cg-mesh-node-55.1.1-RFLAN-3.60-3.80     | 55.1.1  | RFLAN/3.60/3.80    |
| cg-mesh-node-55.5.23-CGEPLCREF2-0.1-0.1 | 55.5.23 | CGEPLCREF2/0.1/0.1 |
| lmac-updater-1.1.260-ALAMO-0.1-0.1      | 1.1.260 | ALAMO/0.1/0.1      |

347190

- To delete an image, click its **Delete** link. 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 and then click **Upload Image**. See [Uploading a Firmware Image to a FAR Group](#).

## Uploading a Firmware Image to a FAR Group

When you upload a firmware image to FAR 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 FARs, firmware image upload and installation requires 200 MB of free disk space. IoT FND stores image files in the `.../managed/images` directory on the FAR.

**Note:** If there is not enough disk space on the FAR for the firmware image, the IoT FND initiates disk cleanup process on the FAR 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 FAR.

To upload a firmware image to FAR group members:

1. Choose **Config > Firmware Update**.
2. Click the **Groups** tab.
3. In the FIRMWARE GROUPS pane, select the firmware group 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 (IR800s, ISR800s, CGRs); only CGRs accept CG-OS images.

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

| Image   | Type    | Applicable Device                      |
|---------|---------|--|
| CDMA    | all     | Cisco IOS CGRs, IR800s, and ISR800s    |
| CGOS    | cgr1000 | Cisco IOS CGRs running Guest OS        |
| GSM     | all     | Cisco IOS CGRs, IR800s, and ISR800s    |
| IOS-CGR | cgr1000 | Cisco IOS CGRs (CGR 1240 and CGR 1120) |

| Image        | Type    | Applicable Device                       |
|--------------|---------|---|
| 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-WPAN-RF  | cgr1000 | Cisco IOS-CGR                           |
| IOS-WPAN-PLC | cgr1000 | Cisco IOS-CGR                           |
| 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 IOS-CGR software bundles, you might have the option to select one of the following options:

- Install Guest OS from this bundle
- Install WPAN firmware from this bundle

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 FAR 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 FIRMWARE GROUPS pane, select the firmware group.
4. Click **Cancel**.
5. Click **Yes**.

## Pausing and Resuming FAR Firmware Image Uploads

You can pause the image upload process to FAR 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 FIRMWARE 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 FIRMWARE 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 FIRMWARE 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 FAR Firmware Image Installation](#)
- [Excluding Subnets from Firmware Image Installation and Other Actions](#)

**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 FIRMWARE GROUPS pane, select the firmware group.
4. Click **Cancel**.
5. Click **Yes**.

## Pausing and Resuming FAR 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 FIRMWARE GROUPS pane, select the firmware group.
3. Click **Pause**.
4. Click **Yes**.

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

## Excluding Subnets from Firmware Image Installation and Other Actions

At the **Config > Firmware Update** page (bottom of page), you can sort entries (ascending/descending).

You can define filters for the Pan Id and Subnet Prefix by hovering over the column name to expose an arrow, which allows you define the action; and, view details of a subnet such as Pan Id, Subnet Prefix, Nodes in group, Total in subnet, Upload Status and Last Message sent.

You can exclude a subnet from a firmware upgrade installation or other action by selecting the Pan Id for that subnet.

When you select a check box for a Pan Id, that subnet will be excluded from the firmware action.

| default-cgmesh                            |          |         |        |             |      |     |        |                  |         |
|---|----------|---------|--------|-------------|------|-----|--------|------------------|---------|
| Firmware Management                       |          |         |        |             |      |     |        |                  |         |
| Upload Image                              |          |         |        |             |      |     |        |                  |         |
| ALL(14)   BL(1)   RF(13)                  |          |         |        |             |      |     |        |                  |         |
| Image                                     | Uploaded | Running | Backup | Boot Loader | LMAC | BBU | Status | Scheduled Reload | Actions |
| cg-mesh-bloader-REL-1.0.5-CGEREF2-1.0-1.0 | 0        | 0       | 0      | 1           | 0    | 0   |        |                  |         |
| cg-mesh-iron30-si-REL-5.0.50              | 0        | 0       | 0      | 37          | 0    | 0   |        |                  |         |
| cg-mesh-iron30-si-REL-5.1.9               | 0        | 0       | 0      | 1           | 0    | 0   |        |                  |         |
| cn-mesh-iron30-si-RFI-5.2.25              | 0        | 0       | 0      | 156         | 0    | 0   |        |                  |         |

| Pan Id | Subnet Prefix               | Nodes in Group (Total in Subnet) | Upload Status | Last Message sent |
|--------|-----------------------------|----------------------------------|---------------|-------------------|
| 923    | 2008:dead:beef:cafe:0:0:0:0 | 2 (144)                          | 0 / 2         | [never]           |
| 99     | 2006:dead:beef:cafe:0:0:0:0 | 246 (1120)                       | 0 / 246       | [never]           |
| 1234   | 2001:0:0:0:0:0:0:0          | 1 (1)                            | 0 / 1         | [never]           |

## Performing OS 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 204](#)):

### 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

```

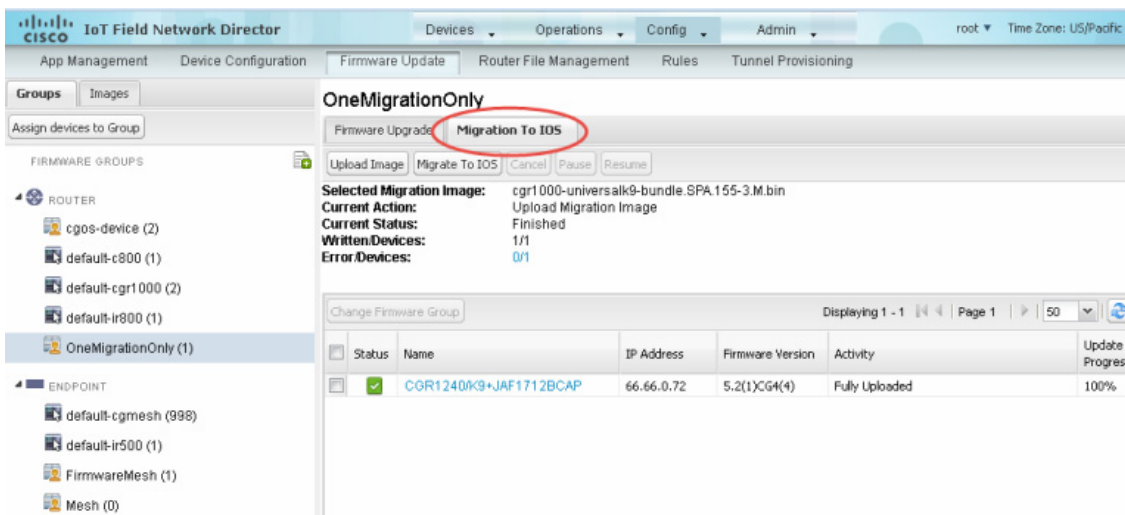
```
ip http client source-interface GigabitEthernet2/2
ip http client secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha
dhe-aes-256-cbc-sha
!
ip route 0.0.0.0 0.0.0.0 66.66.0.8
!
!
privilege exec level 2 dir /recursive
privilege exec level 2 dir
privilege exec level 2 show memory 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
```

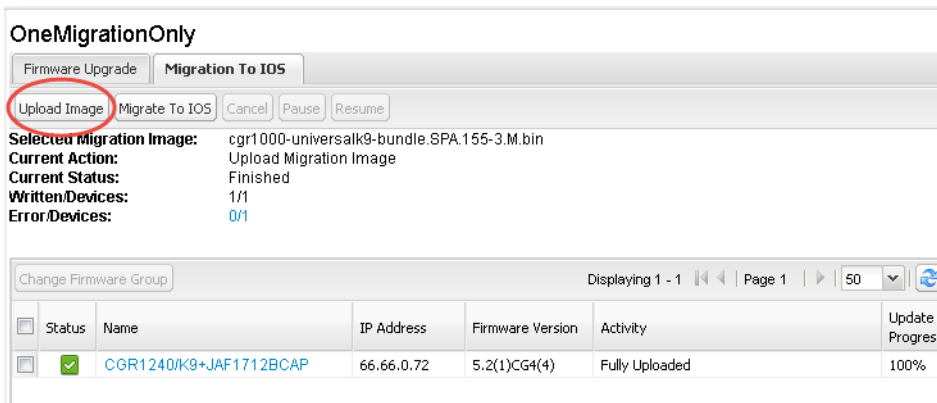
**Note:** You can only migrate from CG4(3) to the minimum IOS image for that device. Refer to [Table 1 on page 22](#) for minimum IOS image requirements.

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

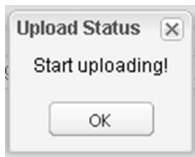
1. Select **Config > Firmware Update**, and click the **Migration to IOS** tab.



2. In the ROUTERS pane, select a CGR group.
3. Select the check box at the top of the devices list for group migration or individual CGRs, and click **Upload Image**.
4. From the **Select IOS Image** drop-down menu, choose the desired image, and click **Upload Image**.



5. Click **OK** to begin the upload.

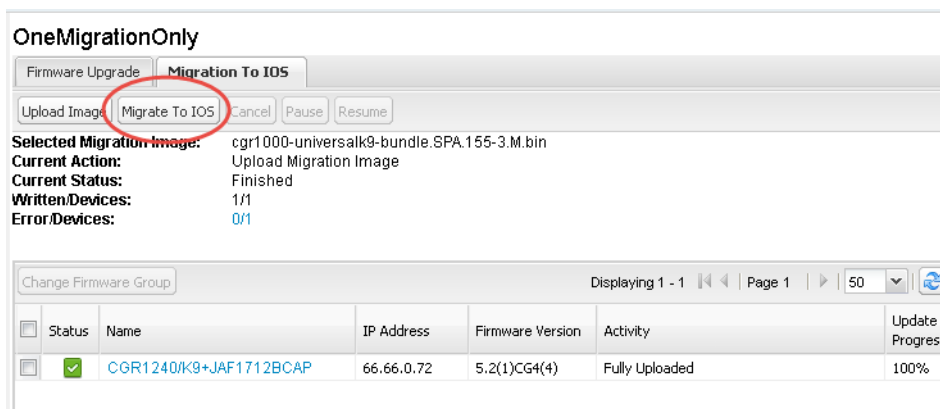


Upload progress appears in the device list.

6. Upload the following properties files (see [Installing Cisco IoT FND, page 21](#)):

- config
- tunnel provisioning
- bootstrap
- runtime configuration

7. Click the **Migrate To IOS** button.



8. Click **Yes** to confirm and begin the migration process.

You can follow the update progress in the devices list. Error messages also appear in the devices list. You can cancel, pause, and resume the migration process.

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

## Interface Names After Migration

IoT Field Network Director preserves metrics for the various interfaces and associated properties during migration. [Table 1](#) maps CG-OS interfaces to the corresponding IOS interfaces to preserve metrics.

**Table 1 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             |

**Table 1 CG-OS-to-IOS Interface Migration Map**

| CG-OS Interface | Corresponding IOS Interface |
|-----------------|-----------------------------|
| Ethernet2/6     | FastEthernet2/6             |
| Wpan4/1         | Wpan4/1                     |
| Serial1/1       | Async1/1                    |
| Serial1/2       | Async1/2                    |
| Cellular3/1     | Cellular3/1                 |
| N/A             | GigabitEthernet0/1          |

## Working with Mesh Endpoint Firmware Images

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

- [Uploading a Firmware Image to a Mesh Endpoint Group](#)
- [Viewing Mesh Device Firmware Image Upload Logs](#)
- [Viewing Mesh Endpoint Firmware Update Information](#)
- [Excluding Subnets from Firmware Image Installation and Other Actions](#)

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

**Note:** ENDPOINT 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 a Mesh Endpoint Group

To upload a firmware image to ME group members:

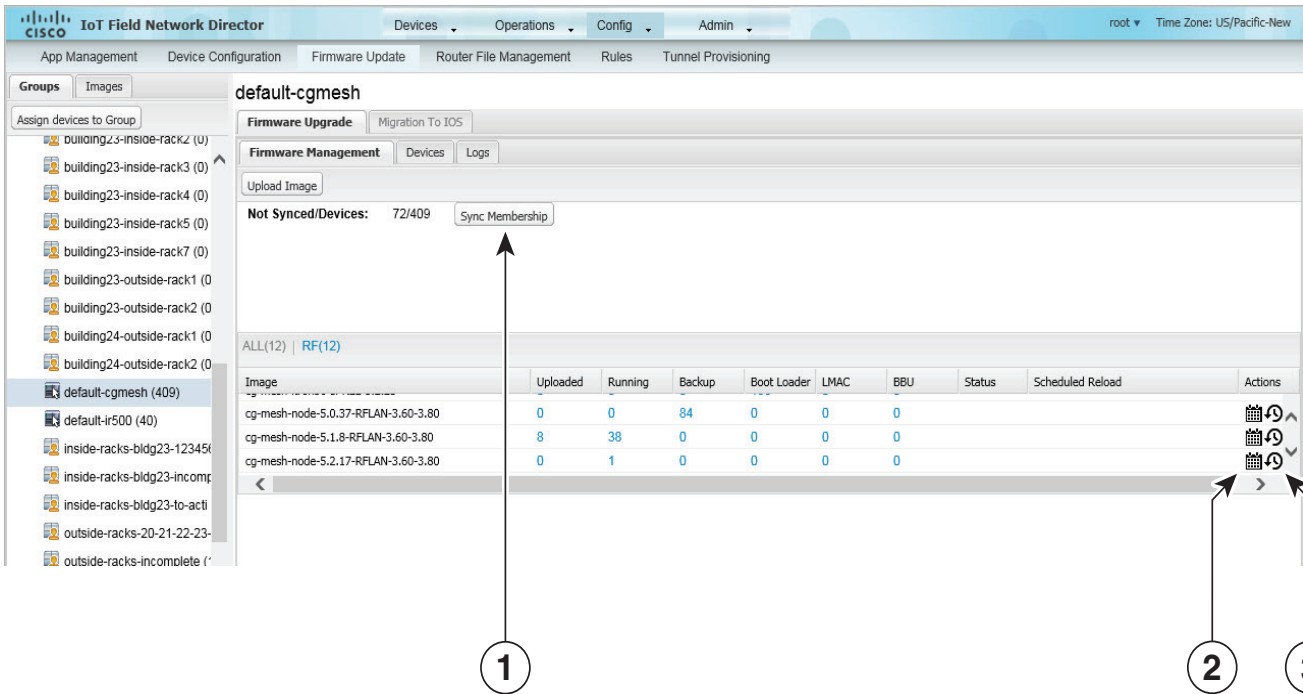
1. Choose **Config > Firmware Update**.
2. Click the **Groups** tab.
3. In the FIRMWARE GROUPS pane, select the firmware group to update.
4. Click **Firmware Management**.
5. Click **Upload Image**.
6. From the **Select Type:** drop-down menu, choose the firmware type for your device.

IoT FND can upload these image types to ENDPOINT devices.

| Image Type | Description                       |
|------------|-----------------------------------|
| RF         | RFLAN connected devices.          |
| PLC        | Power line communication devices. |
| BBU        | Devices with battery back up.     |
| LMAC       | Local MAC connected devices.      |
| PLC-RF     | PLC-Radio Frequency devices.      |

7. From the **Select an Image:** drop-down menu, choose the firmware bundle to upload.
8. Click **Upload Image**.
9. 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.



- 1 Sync membership button
- 2 Schedule Install and Reload button
- 3 Set as Backup button

For every image in the list, IoT FND displays the following information:

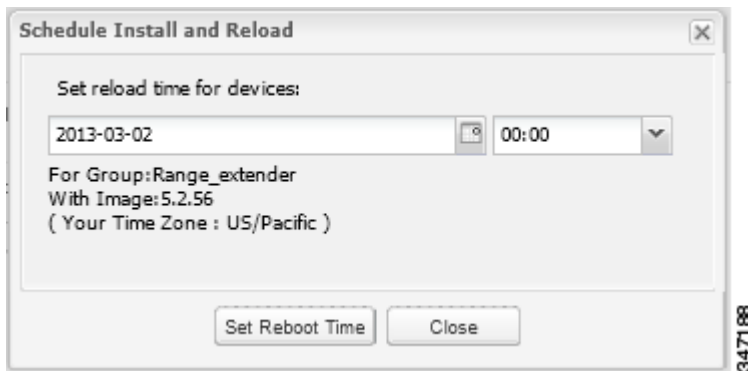
| Column      | Description  |
|-------------|--|
| Image       | Image name.  |
| Uploaded    | Specifies the number of devices that uploaded the image. Click the number to display a list of these devices.      |
| Running     | Specifies the number of devices running this image. Click the number to 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.  |

| Column           | Description  |
|------------------|--|
| Scheduled Reload | Specifies the scheduled reload time.   |
| Actions          | Provides two actions: <ul style="list-style-type: none"> <li>■ Schedule Install and Reload—Schedule the installation of the loaded image and the rebooting of the ME.</li> <li>■ Set as Backup—Set the image as the backup image.</li> </ul> |

## Setting the Installation Schedule

To set the installation schedule:

1. Click the **Schedule Install and Reload** button (2).
2. Specify the date and time for the installation of the image and the rebooting of the device.



3. Click **Set Reboot Time**.
  - To set the selected image as the firmware image backup, click the **Set as Backup** button (3).
4. Click **Yes**.
  - To sync the group members in the same firmware group, click **Sync Membership** (1).
  - To view member devices, click the **Devices** tab.
  - To view log files for the group, click the **Logs** tab.

## Viewing Mesh Device Firmware Image Upload Logs

To view the firmware image upload logs for mesh devices:

1. Choose **Config > Firmware Update**.
2. Click the **Groups** tab.
3. In the FIRMWARE GROUPS pane, select the mesh device firmware group.
4. Click the **Logs** tab.

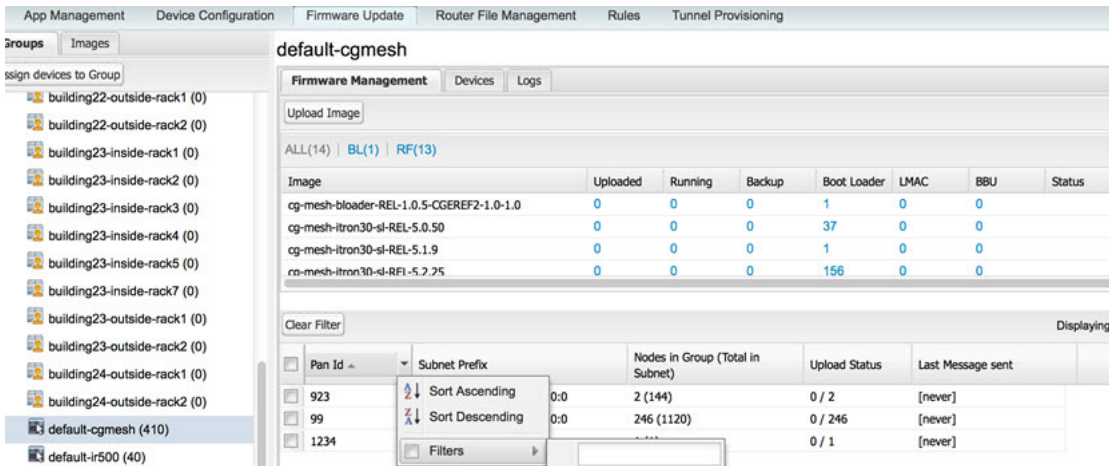
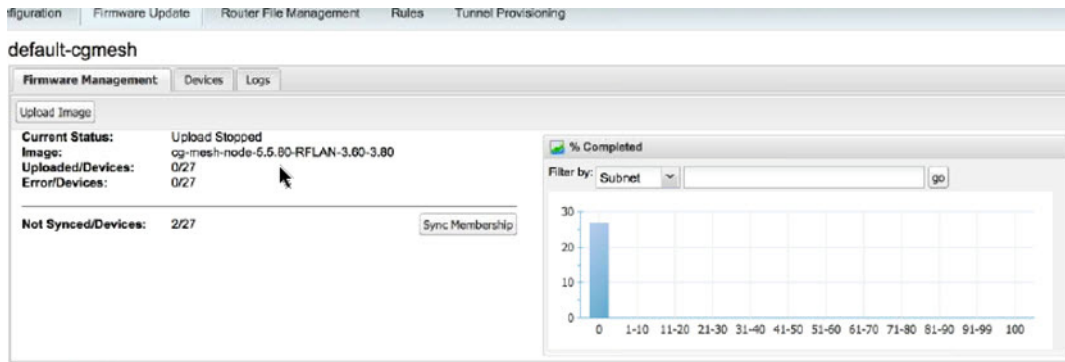
## Viewing Mesh Endpoint Firmware Update Information

You can view the endpoint firmware update process down to the subnet level for greater visibility. To view details of firmware updates for mesh endpoint devices (by subnet, Pan Id or Group) in a table or histogram, during the upgrade process or after the firmware upgrade completes, follow these steps:

**Note:** For Subnet and Pan Ids, you must enter the value in the text box provided:

1. Choose **Config > Firmware Update**.
2. Click the **Groups** tab.
3. In the FIRMWARE GROUPS pane, select a MESH DEVICES group.
4. Click the **Firmware Management** tab.





| Field                     | Description  |
|---------------------------|--|
| <b>(Top, Left Panel)</b>  |  |
| Upload Image radio button | Click radio button to begin the firmware upload.<br><b>Note:</b> By default, all subnets listed at the bottom of the screen will receive the image upload.<br><br><b>To exclude a subnet</b> from the firmware upload, check the box (such as 1 or 2) next to that subnet. For more details, see PAN ID definition below.  |
| Current Status            | Status of the firmware upload (for example, Image Loading or Upload Finished).<br><br><ul style="list-style-type: none"> <li>■ Image Loading, Upload Paused, Upload Stopped, Upload Finished, Upload Stopping, Upload Pausing</li> <li>■ Scheduling Reload, Reload Paused, Reload Stopped, Reload Scheduling Finished, Reload Stopping, Reload Pausing</li> <li>■ Setting Backup, Backup Paused, Backup Stopped, Backup Finished, Backup Stopping, Backup Pausing</li> </ul> |
| Image                     | Firmware image name.   |
| Uploaded/Devices          | Number of completed, successful firmware updates against the total devices that will receive the updates.  |
| Error/Devices             | Number of devices the operation failed (error) against the total devices in the group.   |

| Field                          | Description  |
|--------------------------------|--|
| Not Synced/Devices             | Number of firmware group membership non-synchronized devices against the total number of devices in the group.   |
| <b>(Right Panel) Histogram</b> |  |
| % Completed                    | Visual status of upload percentage completed.  |
| Filter by                      | Filter and display results by: Subnet, Pan ID, Group   |
| <b>(Bottom Panel)</b>          |  |
| All or RF                      | <p><b>All</b> displays information about all images in the Running, uploaded and backup slot as well as the BBU and PLC information for all device images (RF mesh, IR500 WPAN Range Extender and WPAN Range Extender with BBU and PLC) in the group; and the schedule reload and status information.</p> <p><b>RF</b> displays information regarding RF mesh images in the Running, uploaded and backup slots as well as the schedule reload and status information.</p>  |
| Image                          | <p>Displays image file name and provides the completion percentage of the firmware upload (0 to 100) with respect to the following states:</p> <ul style="list-style-type: none"> <li>■ Uploaded, Running, Backup, Bootloader, LMAC, BBU, Status, Sched Reload</li> </ul>  |
| Clear filter                   | Click radio button to clear selected firmware image update results.  |
| PAN ID                         | <p>Identifies the Personal Area Network Identifier for a group of endpoints (nodes).</p> <p>To <b>exclude</b> a group of nodes from a new firmware upload, you must select the Pan ID check box next to that group of nodes before selecting the <b>Upload Image</b> radio button in the Firmware Management pane.</p> <p><b>Note:</b> The check boxes next to the PAN IDs are not visible during a firmware upload.</p> <p><b>Note:</b> You can sort PAN IDs in an ascending or descending manner or filter by PAN ID to define which PAN ID displays in the window by selecting the downward arrow to the right of the column. Select <b>Clear Filter</b> to leave that view.</p> <p><b>Note:</b> To see a listing of all nodes within a subnet, select the <b>Device</b> tab.</p> |
| Subnet Prefix                  | <p>Identifies the IPv6 subnet prefix for the endpoint. To view all of the nodes within a given subnet, select the Devices tab.</p> <p><b>Note:</b> You can filter by Subnet by entering a portion of the subnet (for example, 200b:0:0) by selecting the downward arrow to the right of the column. Select <b>Clear Filter</b> to leave that view.</p>   |
| Nodes in Group                 | Number of nodes within the group. In the screen shot above, there are a total of 25 nodes within the group, which are split across two different subnets (8 nodes in 200b:0:0:0:0:0:0 and 17 nodes in 200c:0:0:0:0:0:0).   |
| Total in Subnet                | Number of nodes with the subnet. In the screen shot above, there are 19 nodes in the subnet.   |
| Upload status                  | Number of nodes out of the total nodes that have been successfully upgraded with the new firmware.   |
| Last message sent              | Display of latest message relevant to the current firmware update process within the given PAN.  |

## Viewing Mesh Device Firmware Information

To view the firmware information for mesh devices:

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

3. In the FIRMWARE GROUPS pane, select a MESH DEVICES group.
4. Click the **Devices** tab.

The screenshot shows the 'Firmware Management' interface with the 'Devices' tab selected. The interface includes a 'Change Firmware Group' dropdown, a pagination bar showing 'Displaying 1 - 50' on 'Page 1', and a table of device information. The table has columns for Status, Name, IP Address, Firmware Version, Backup Version, and Uploaded Version. Three devices are listed, each with a question mark icon in the Status column.

| Status | Name               | IP Address                                | Firmware Version | Backup Version | Uplo Vers |
|--------|--------------------|---|------------------|----------------|-----------|
| ?      | sgbuB1_cgmesh100   | 2004:0ba0:6f0a:0000:0000:0e01:0f01:00101  |                  |                |           |
| ?      | sgbuB1_cgmesh1000  | 2004:0ba0:6f0a:0000:0000:0e01:0f05:00105  |                  |                |           |
| ?      | sgbuB1_cgmesh10000 | 2004:0ba0:6f0a:0000:0000:0e01:0f045:00145 |                  |                |           |

For every device in the group, IoT FND displays this information:

| Field                      | Description   |
|----------------------------|---|
| Status                     | Status of the device (for example, Up, Down, or Unheard).   |
| Name                       | EID of the device.  |
| IP Address                 | IP address of the device.   |
| Firmware Version           | Version of the firmware image running on the device.  |
| Backup Version             | Version of the firmware image used as a backup.   |
| Uploaded Version           | Version of the firmware image loaded on the device.   |
| Member Synced?             | Whether the device is in sync with the rest of the group.   |
| Activity                   | Firmware image upload activity.   |
| Update Progress            | Firmware image upload progress. An update progress of 100% indicates that the upload is complete. |
| Last Firmware Status Heard | Last time the firmware status was heard.  |
| Scheduled Reload Time      | The time set for upload image reloads.  |
| Error Message              | Error message if image upload failed.   |

