

Manage 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, 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).

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, on page 1
- Manage Router Firmware Upgrades, on page 5
- Manage Firmware Upgrade Properties For A Router Group, on page 6
- Working with Resilient Mesh Endpoint Firmware Images, on page 8
- AP800 Firmware Upgrade During Zero Touch Deployment, on page 13
- Enhancement to Firmware Update Page for Device Status Types, on page 15
- Avoid Firmware Upgrade Overlap with Certificate Auto Renewal, on page 15
- Configuring Firmware Group Settings, on page 16
- Firmware images, on page 20
- Search Firmware Updates, on page 33
- Push StackMode, on page 35
- Upgrading Firmware Image during Bootstrapping, on page 44
- Skipping Firmware Upgrades during PNP, on page 45
- Update Target Firmware Versions For All Users, on page 46

Router Firmware Updates

IoT FND updates router firmware in two steps:

Procedure

Step 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, on page 16.

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

Note If you set the property, collect-cellular-link-metrics, to 'true' in cgms.properties, then the following Cellular link quality metrics are collected for CGR1000, IR800 and IR1100, each time you initiate a firmware upload from IoT FND:

- RSRP: Reference Signal Received Power which is the power of the reference signal
- RSRQ: Reference Signal Received Quality or the quality of the reference signal which is the a ratio of RSSI to RSRP
- SINR: Signal-to-Noise Ratio which compares the strength of the signal to the background noise.
- RSSI: Received Signal Strength Indicator or the strength of the reference signal

Additionally, the following cgna profile is created on the CGR1240 and activated when the firmware upload is triggered.

```
cgna profile cg-nms-cellularlinkmetrics
add-command show cellular 3/1 all | format
flash:/managed/odm/cg-nms.odm
interval 5
url https://<FND IP address>:9121/cgna/ios/metrics
gzip
active
```

Note On execution of the cgna profile above, the metrics data is persisted in the Metrics_History table in the database and can be collected by using the getMetricHistory NBAPI.

Step 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

Guest OS images can be installed or upgraded through the Cisco IoT FND Firmware Update page.

Guest OS Image Upgrade Details

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 are upgraded when you perform a Cisco IOS image bundle installation or update.

After any Cisco IOS installation or upgrade, when IoT FND discovers a GOS, it checks whether the initial communications setup is complete before performing the required setup. The CGR must have a DHCP pool and the 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 applications to the upgraded Guest OS. See Monitoring a Guest OS for more information.

See Cisco 1000 Series Connected Grid Routers Configuration Guides for information about 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 Firmware images, on page 20.

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:

Procedure

Step 1 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).

Step 2 setCgrActionExpirationTimeout <value>

Step 3 get <*pkg*>*actionExpirationTimeoutMins*

Step 4 *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
```

Manage Router Firmware Upgrades

Manage Router Firmware Upgrades

Table 1: Feature History

Feature Name	Release	Description
Manage Router Firmware Upgrades	Cisco IoT FND Release 5.0	Manage router firmware upgrade and install counts using Cisco IoT FND, eliminating the need to manually edit .jboss property files.

Information About Manage Router Firmware Upgrades

Manage router firmware upgrade and install counts directly using Cisco IoT FND. You no longer have to manually edit .jboss property files, simplifying the firmware management process. The router firmware management is now intuitive and accessible. Define the **Maximum Router Firmware Upload Count**, **Maximum Router Firmware Install Count**, and **Router Firmware Upload Retry Count** values globally on Cisco IoT FND. Apply the maximum parallel or concurrent firmware upgrade values to all the group of routers on Cisco IoT FND.

Restrictions For Manage Router Firmware Upgrades

Here are the default counts for the respective fields:

- **Router Firmware Upload Count**: 48
- **Router Fimware Install Count**: 48
- **Router Firmware Upload Retry Count**: 5

Here are some of the maximum counts for the respective fields:

- **Router Firmware Upload Count**: 48
- **Router Fimware Install Count**: 48
- **Router Firmware Upload Retry Count**: 100

Use Cases For Manage Router Firmware Upgrades

- Manage firmware upgrades and installations for a large fleet of routers across multiple locations, ensuring all devices are up to date.
- Minimize configuration errors that might occur with manual property file edits, ensuring smoother and more reliable firmware management.

Configure Router Firmware Upgrades Using Cisco IoT FND

Here are the instructions to configure the router firmware upgrades using Cisco IoT FND:

1. From the Cisco IoT FND Menubar, choose **ADMIN** > **Server Settings** > **Property Settings**.
2. Enter the number of routers in the **Router Firmware Upload Count** field on which a firmware file is uploaded to the device repository. For example, 48
3. Enter the number of routers in the **Router Firmware Install Count** field on which you want to apply the uploaded firmware to the routers for upgrading them. For example, 45
4. Enter the number of attempts that you want Cisco IoT FND to try when there's a failure of firmware uploads in the **Router Firmware Upload Retry Count** field. For example, 5

Manage Firmware Upgrade Properties For A Router Group

Manage Firmware Upgrade Properties For A Router Group

Feature Name	Release	Description
Manage Firmware Upgrade Properties For A Router Group	Cisco IoT FND Release 5.0	Cisco IoT FND includes a **Router Firmware Upload Retry Count** in the **Firmware Update** page. Customize the retry count at the router group level, allowing for tailored firmware update strategies for specific groups of routers.
Enable fimware upload progress percentage	Cisco IoT FND Release 5.1	Cisco IoT FND displays the firmware upload progress for Cisco IoT routers running Cisco IOS-XE namely: • Cisco Catalyst IR1100 • Cisco Catalyst IR8100 • Cisco Catalyst IR1800

Information About Manage Firmware Upgrade Properties For A Router Group

Cisco IoT FND introduces a **Router Firmware Upload Retry Count** field in the **Firmware Update** page. You can customize the retry count at the router group level, allowing you to implement tailored firmware upgrade strategies for specific groups of routers. The firmware upload retry count is not defined by default at the group level. In case you don't define the upload retry count, the global value in the **Property Settings** page is applied to the groups as well.

Benefits Of Manage Firmware Upgrade Properties For A Router Group

- You can customize the retry count for firmware uploads at both global and router group levels, providing greater control over the update process.
- You can enhance the reliability of firmware updates, reducing the likelihood of failed uploads due to network issues or other disruptions.
- Different groups of routers can have tailored firmware update strategies, allowing for more efficient management based on specific network conditions or requirements.

Restrictions For Manage Firmware Upgrade Properties For A Router Group

The default value of **Router Firmware Upload Retry Count** is 5 and the maximum value is 100.

Configure Firmware Upgrade Properties For A Router Group

Here are the steps to configure firmware upload retry count using Cisco IoT FND:

1. From the Cisco IoT FND menubar, choose **CONFIG** > **Firmware Update**.
2. Select a router group from the **Firmware Groups** list.
3. Click **Group Properties**.
4. Enter a value between 0 to 100 in the **Router Firmware Upload Retry Count**.

Enable firmware upload progress percentage

This task helps you enable the firmware upload progress percentage for Cisco IOS-XE routers using Cisco IoT FND.

Before you begin

You must enable the progress percentage for it to appear in the firmware image update page.

Here are the steps to enable the progress percentage:

Procedure

Step 1 From the Cisco IoT FND dashboard, choose **ADMIN** > **Server Settings**.

Step 2 Navigate to the **Property Settings** tab.

Step 3 Check the **Enable Fimrware upload progress % for IOS-XE devices** check box.

Step 4 Configure the **IOS-XE Firmware upload progress timer (seconds)** field based on which the the progress percentage is updated in Cisco IoT FND. The default value is 90 seconds and the range is between 30 seconds to 180 seconds.

You've enabled firmware upload progress percentage. This percentage progress will appear for Cisco IOS-XE routers in the **Firmware Upload** page.

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.

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.

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 as noted in the table:

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, on page 10 for complete steps.

Set a Firmware Backup Image

To set an image as a firmware image backup:

Procedure

Step 1 Click the Set as Backup button. (See the icon in the Actions summary in Table 2: Image Information Displayed by IoT FND, on page 9).

Step 2 Click **Yes** to confirm backup.

Setting the Installation Schedule

To set the installation schedule for an image:

Procedure

Step 1 Click the **Schedule Install and Reload** button (Calendar icon). For more information, see Table 2: Image Information Displayed by IoT FND, on page 9.

The following message appears if you try to schedule a reload operation for the node that is scheduled for stack switch operation.

Step 2 In the page that appears, specify the date and time for the installation of the image and rebooting of device.

Figure 1: Schedule and Install and Reload Page

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

Firmware Update Transmission Settings

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

Procedure

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

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.

Step 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. Refer to the table below for the definitions of the terms on the **CONFIG** > **FIRMWARE UPDATE** > **Transmissions Settings** page.

Figure 2: CONFIG > FIRMWARE UPDATE

Table 3: Definitions of variables seen on 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.

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

To upload a firmware image to mesh endpoint group members:

Procedure

Step 1 Choose **CONFIG** > **FIRMWARE UPDATE**.

Step 2 Click the **Groups** tab (left-pane).

Step 3 Select the Endpoint firmware group to update.

Step 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 (For more information, see Figure 3: Check Install Patch Item to ONLY Install the Patch Rather than the Full Image, on page 11).

Figure 3: Check Install Patch Item to ONLY Install the Patch Rather than the Full Image

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 4: Firmware Update - Percentage Complete (top-portion of screen), on page 12 and Figure 5: Firmware Update - Upload Summary (bottom-portion of screen), on page 12.

Note Click the Sync Membership button to ensure that FND and the member endpoint firmware group information are the same.

Figure 4: Firmware Update - Percentage Complete (top-portion of screen)

Figure 5: Firmware Update - Upload Summary (bottom-portion of screen)

Uploading a Firmware Image to FND

To upload a firmware image to mesh endpoint group members:

Procedure

Step 1 Choose **CONFIG** > **FIRMWARE UPDATE**.

Step 2 Select the **Images** tab (left-pane).

Step 3 Select the Endpoint Image type (such as BBU, IOx-IR500 LMAC) to be uploaded.

Step 4 Click on + (plus icon) next to the FIRMWARE IMAGES heading to browse the firmware from your local system.

Step 5 Browse and click on **Add file**.

IoT FND can upload the following image types to ENDPOINT devices as shown in the table below:

Table 4: Firmware Images for Endpoints

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

Figure 6: Using IoT FND to Upload Images to an Endpoint

Modifying Display of Firmware Management Page

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

To modify the display of firmware management page:

Procedure

Step 1 Choose **CONFIG** > **FIRMWARE UPDATE**.

Step 2 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

Viewing Mesh Device Firmware Image Upload Logs

To view the mesh device firmware image upload logs:

Procedure

Step 1 Click the **Sync Membership** button to sync the group members in the same firmware group.

Step 2 Click the **Devices** tab to view member's devices.

Step 3 Click the **Logs** tab to view log files for the group.

For more information, refer to Figure 4: Firmware Update - Percentage Complete (top-portion of screen), on page 12 .

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 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 router will upgrade using the firmware version you define as the autonomous firmware.

To define the Autonomous Firmware for an IR829 router:

Procedure

Step 1 Choose **CONFIG** > **DEVICE CONFIGURATION**.

Step 2 Select the desired router: Default-ir800 (left-pane).

Step 3 Check the installed firmware version, BEFORE upload. if equal to the latest version, skip firmware upgrade.

Step 4 Before you upload the software to the router, check the image and version:

- If the router image version is equal to the latest version, skip upgrade.
- If router image has the latest

Step 5 Select Edit AP Configuration Template tab (right-pane).

Step 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
```

Step 7 Click disk icon (bottom of page) to save the commands in the configuration template.

Image Diff Files for IR809 and IR829

To reduce the 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.

Note Firmware image upload depends on interface speeds. You can set the timeout duration (in minutes) for firmware upload in cgms.properties file using "igma-idle-timeout" key. If you don’t set this duration, then default timeout duration will be 15 minutes.

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

Enhancement to Firmware Update Page for Device Status Types

Table 5: Feature History

Feature Name	Release Information	Description
Enhancement to Firmware Update Page for Device Status Types	Cisco IoT FND Release 5.0	Cisco IoT FND includes two additional device statuses in the **Firmware Update** page: **Down Devices** and **All Devices**. Use the **Down Devices** link to filter the down devices search and **All Devices** displays the count of total devices in the firmware group of routers.

Enhancement to Firmware Update Page for Device Status Types

Starting from Cisco IoT FND 5.0 release, the **Firmware Update** page includes a new device status count link called **Down Devices** which is added for routers. The status field is used in identifying and calculating the count of **All Devices**, **Written Devices**, **Error Devices** and **Down Devices** within a given firmware group.

The **Down Devices** link is used to filter the search for all the down devices in the firmware group of routers. A device is considered down when the status appears with a red cross icon, indicating it is offline. The **All Devices** count displays the total number of devices in the firmware group of routers.



Note The **Down Devices**, **Error Devices** and **Written Devices** status counts are hyperlinked for filtering the search based to the device state.

Benefits of Using Device Status Count Links

Device status count links help in filtering the search for devices based on their status types. These links also help in determining the count of the devices in each state.

Accessing Device Status Links

In the **Firmware Update** page click the link for each device status count to view the devices based on their state.

Avoid Firmware Upgrade Overlap with Certificate Auto Renewal

Problem

As part of the reload process, the cellular modem is powered off during firmware upgrade. If there is an Embedded Event Manager (EEM) script which is in the running configuration, which executes the write

memory operation after getting a renewed certificate, then it saves the startup configuration with the cellular modem turned off. This results in an outage after router reload. Once the router reloads and comes up again, due to cellular modem which is in the powered off state, the router cannot register with Cisco IoT FND.

Solution

There are two steps for upgrade:

- Firmware upload.
- Firmware installation.

In case of an overlapping duration between certificate auto renewal and firmware installation, ensure that the firmware installation is initiated only after the certificates are successfully auto renewed for routers. Also, select only those routers which have already completed the certificate auto renewal for the firmware upgrade group.

Note This is applicable only for firmware installation as firmware upload has no such restriction.

Identifying and Avoiding Routers for Firmware Upgrade

To identify and avoid selecting the routers which have certificate expiration, follow the given step:

1. From the Cisco IoT FND menu bar, click **OPERATIONS** > **Issues**.

Note Avoid selecting any router which appears in the **Issues** table with certification expiry message.

Configuring Firmware Group Settings

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

- Adding Firmware Groups, on page 17
- Assigning Devices to a Firmware Group, on page 18
- Renaming a Firmware Group, on page 19
- Deleting Firmware Groups, on page 20

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.

When creating firmware groups note the guidelines:

- CGRs, IR800s 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.

Figure 8: CONFIG > FIRMWARE UPDATE

Tip At the Firmware Update page, click the Error/Devices link (not shown) in the **Firmware Update** page to apply a filter.

Click **Clear Filter** to revert to an unfiltered view of the selected device group.

Adding Firmware Groups

To add a firmware group:

Procedure

Step 1 Choose **CONFIG** > **FIRMWARE UPDATE**.

Step 2 Click the **Groups** tab.

Step 3 In the Groups pane, select one of the following:

- Default-cgr1000
- Default-ir500
- Default-ir800
- Default-cgmesh

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

Step 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.

Step 6 Click **Add**.

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

Note To assign devices to the new group, see Assigning Devices to a Firmware Group, on page 18.

Assigning Devices to a Firmware Group

This section explains moving devices to another firmware group in bulk or manually.

Moving Devices to Another Group In Bulk

To move devices from one group to another in bulk:

Procedure

Step 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* only for mesh endpoints:**	***EID* only for IR800s**

`eid`
`CGR1120/k9+JS1`
`CGR1120/k9+JS2`
`CGR1120/k9+JS3`
	`eid`
	`00078108003c1e07`
	`00078108003C210b`
		`eid`
		`ir800`

***EID* only for ISR 800s:**	***EID* only for IR500s:**	***EID* only for IC3000**

`eid`
`C819HGW-S-A-K9+FTX174685V0`
`C819HGW-S-A-K9+FTX174686V0`
`C819HGW-S-A-K9+FTX174687V0`
	`eid`
	`da1`
	`da2`
	da3
		`eidIC3000+FOC2219Y47Z`

Note Each file can only list one device type.

Step 2 Choose **CONFIG** > **FIRMWARE UPDATE**.

Step 3 Click the **Groups** tab.

Step 4 Click the **Assign devices to Firmware Group** button (found above the Groups tab).

Step 5 In the window that appears, click **Browse** and locate the device list CSV or XML file.

Step 6 From the **Group** drop-down menu, choose the destination group.

Step 7 Click **Assign to Group**.

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

Step 8 Click **Close**.

Moving Devices to Another Group Manually

To manually move devices to a group:

Procedure

Step 1 Choose **CONFIG** > **FIRMWARE UPDATE**.
Step 2 Click the **Groups** tab.
Step 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.

Step 4 Check the check boxes of the devices that you want to move.
Step 5 Click **Change Firmware Group** to open a pop up window.
Step 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.
Step 7 Click **Change Firmware Group**.
Step 8 Click **Close**.

Renaming a Firmware Group

In the **Firmware Update** page, there are two firmware groups available, namely user-created groups and default groups of router, endpoint, or gateway. IoT FND allows you to rename the user-created firmware groups only. You cannot rename the default firmware groups.

To rename a firmware group:

Procedure

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



Note Starting with IoT FND, you can only rename the user-created firmware groups and you cannot rename the default firmware groups. The pencil icon does not appear for the default firmware groups.

Step 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:

Procedure

Step 1 Choose **CONFIG** > **FIRMWARE UPDATE**.

Step 2 Click the **Groups** tab.

Step 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.

Step 4 Check the box next to the firmware group that you want to delete.

Step 5 Click Clear Selection that appears above the entry (yellow bar).

Step 6 To confirm deletion, click **Yes**.

Step 7 Click **OK**.

Firmware images

Firmware images in Cisco IoT FND are software files that you use to update and enhance the firmware of managed Cisco IoT devices.

A router group in Cisco IoT FND is a collection of routers that you can organize together to simplify managing, monitoring, and configuring tasks across multiple routers simultaneously.

Table 6: Feature history

Feature name	Release information	Description
Export firmware and configuration group data	Cisco IoT FND Release 5.1	Export the firmware group update information from the **Firmware Update** page, and export the configuration group update information from the **Device Configuration** page. The export option is available only for routers and endpoints.
Enable firmware upload progress percentage	Cisco IoT FND Release 5.1	Cisco IoT FND displays the firmware upload progress for Cisco IoT routers running Cisco IOS-XE namely: • Cisco Catalyst IR1100 • Cisco Catalyst IR8100 • Cisco Catalyst IR1800
Upgrade firmware of cellular modems	Cisco IoT FND Release 5.1	Upgrade firmware of the cellular modems based on cellular technologies like LTE and 5G for Cisco Catalyst IR1100, Cisco Catalyst IR8100, and Cisco Catalyst IR1800 using Cisco IoT FND.
Scheduled upload and install of firmware images	Cisco IoT FND Release 5.1	Schedule the uploading and installing firmware images to a router group.
Bundle Boot and Install Boot modes for Cisco Catalyst IR8100	Cisco IoT FND Release 5.1	You can select between Bundle Boot and Install Boot Modes in the router firmware upgrade process.

Feature name	Release information	Description
Automatic bootflash space cleanup for Cisco IOS XE Devices	Cisco IoT FND Release 5.1	Cisco IoT FND automatically removes unused firmware images from both `bootflash:` and `bootflash:/managed/images` directories during every firmware upload, install, and during registration post the reload, ensuring optimal use of storage space without any manual intervention. This proactive cleanup not only simplifies the upgrade process but also helps prevent storage-related issues, allowing upgrades to proceed smoothly.
Bootflash Space Cleanup	Cisco IoT FND Release 5.0	Check the **Remove unused firmware images from bootflash** check box to remove unused firmware bin files from the bootflash when Cisco IoT FND uploads the image to the router. The check box is enabled for the following devices running Cisco IOS-XE: • Cisco Catalyst IR1100 • Cisco Catalyst IR8100 • Cisco Catalyst IR1800 **Note** Starting from Cisco IoT FND Release 5.1, this button is disabled on Cisco IoT FND and works in the backend without you having to enable it.

Add firmware images

Import the firmware file into the Cisco IoT FND database so it can be managed and later deployed to Cisco IoT routers.

Here are the steps to add firmware images to Cisco IoT FND:

Procedure

Step 1 In the Cisco IoT FND menubar, choose **CONFIG** > **Firmware Update**.

Step 2 Click the **Images** tab.

Step 3 Select **ROUTER** or **ENDPOINT** or **GATEWAY** and then select a device group. For example, IOS-XE-IR1100.

Step 4 Click the **+** icon adjacent to **FIRMWARE IMAGES**.

Step 5 Click **Browse** to locate the firmware image. Select the image, then click **Add File**.
The image appears in the **Firmware Images** list.

What to do next

Upload firmware images

Upload firmware images

This task guides you to upload firmware images to a router group, Cisco IoT FND pushes the image to the router group in the background and tracks the upload progress to ensure that the devices receive the firmware image.

Here are the steps to upgrade firmware on a router group:

Before you begin

- Firmware image upload and installation require the following free disk space:
  - For bundle boot mode: 20 MB + uploaded file size
  - For install boot mode: 800 MB + uploaded file size
- Auto-cleanup is applicable to both Bundle and Install boot modes. Cisco IoT FND checks both `bootflash:` and `bootflash:/managed/images` during cleanup. In Install boot mode, cleanup removes unwanted package files, .conf files, and .bin files from both locations.
- If you find firmware files in `bootflash:` or `bootflash:/managed/images`, Cisco IoT FND cleans up all files except the currently running one. You must manually remove any other files that are not .bin, .pkg, or .conf.
- For Cisco IOS XE devices, Cisco IoT FND automatically performs bootflash space cleanup during every firmware upload, install, and post-reload registration. Any image not part of the active boot parameters or referenced in before-tunnel-config, before-registration-config, express-setup-config, or factory-config is proactively removed from `bootflash` and `bootflash:/managed/images`, regardless of whether a space issue is detected.

  If, after this proactive cleanup, a router group still does not have enough free space, Cisco IoT FND continues space-recovery cleanup by removing additional unused files until sufficient space is available to upload the new image. If there is still not enough space, you must manually delete unused files on the router.
- Starting from Cisco IoT FND Release 5.1, you'll see an auto-cleanup error when there is not enough space for the firmware upload to progress. Cleanup operations always examine both `bootflash:` and `bootflash:/managed/images`.
- In install boot mode, files in the bootflash directory are cleaned up. In a brownfield scenario, the installed images point to the `bootflash managedimages.bin` file directory, so cleanup occurs in both `bootflash` and `managedimages.bin`.

- If any devices in the router group encounter errors during firmware upload, Cisco IoT FND prevents firmware installation and you can see an error message indicating the presence of errored devices. For errored or cancelled devices, move them to a separate install group and repeat the upload and installation process.
- If you cancel the firmware upload for some devices, firmware installation proceeds only on devices that successfully completed the upload. For errored or cancelled devices, move them to a separate install group and repeat the upload and installation process.

Procedure

Step 1 In the Cisco IoT FND menubar, choose **CONFIG** > **Firmware Update**.

Step 2 Click the **Groups** tab.

Step 3 Select the router group that you want to upgrade.

Step 4 Click **Upload Image**.

Step 5 The **Select Type:** drop-down list is auto-selected based on the selected router group.

Step 6 For Cisco IOS XE devices, select between **Bundle Boot Mode** and **Install Boot Mode** from the **Mode of installation** drop-down list.



Note
- Bundle boot mode is a software loading method used in Cisco IOS XE devices, such as routers and switches, where the device boots and runs the operating system directly from a single consolidated image file (the “bundle” file, typically with a `.bin` extension) rather than from extracted individual package files.
- Install boot mode is a software operating mode in Cisco IOS XE devices in which the device boots and runs the operating system from a set of extracted software package files, rather than from a single monolithic image.
- You require minimum free space of upto 800 MB, in the `bootflash` directory to use the **Install Boot Mode**.
- You can't downgrade to versions that exclusively support only **Bundle Boot Mode** if the device is already operating in Install Mode.

Step 7 Select an image from the **Select an Image** drop-down list.



Note In Cisco IoT FND Release 5.0, you can use the **Remove unused firmware images from bootflash** checkbox when uploading Cisco IOS-XE images. If there isn’t enough space for the new image, checking the checkbox deletes all unused .bin files from `bootflash` and `bootflash:/managed/images`, keeping only those required for boot parameters and active images. This ensures enough disk space for the upload.

Step 8 Click **Upload Image Now** to initiate the firmware upgrade process instantly.

Note Use the **Cancel** or **Pause** buttons to either cancel or pause the firmware image upload.

Step 9 Click **Schedule** to execute the firmware upgrade process at a preferred time. Check the **Enable timeout for scheduled upload** check-box to set a timeout for the uploading operation.

Note If you want to reschedule a future scheduled Firmware job, you need to cancel this firmware job and schedule again.

You can view the firmware upload percentage in the **Update Progress** column in the firmware images table.

What to do next

Install firmware images.

Install firmware images

Use this task to install a firmware image to a router group after you upload a firmware image to Cisco IoT FND.

Before you begin

- If you cancel the firmware upload for some devices, firmware installation proceeds only on devices that successfully completed the upload. For errored or cancelled devices, move them to a separate install group and repeat the upload and installation process.
- For Cisco IOS XE devices, Cisco IoT FND automatically performs bootflash space cleanup during every firmware upload, install, and post-reload registration. Any image not part of the active boot parameters or referenced in before-tunnel-config, before-registration-config, express-setup-config, or factory-config is proactively removed from `bootflash` and `bootflash:/managed/images`, regardless of whether a space issue is detected.

  If, after this proactive cleanup, a router group still does not have enough free space, Cisco IoT FND continues space-recovery cleanup by removing additional unused files until sufficient space is available to upload the new image. If there is still not enough space, you must manually delete unused files on the router.
- Auto-cleanup is applicable to both Bundle and Install boot modes. Cisco IoT FND checks both `bootflash:` and `bootflash:/managed/images` during cleanup. In Install boot mode, cleanup removes unwanted package files, .conf files, and .bin files from both locations.
- Firmware image upload and installation require the following free disk space:
  - For bundle boot mode: 20 MB + uploaded file size
  - For install boot mode: 800 MB

- Starting from Cisco IoT FND Release 5.1, you'll see an auto-cleanup error when there is not enough space for the firmware install to progress.
- Once the new firmware is installed and during the device registration, the copy of new firmware image is copied copied to the bootflash directory for failsafe and is also configured in bootparams.
- The automatic bootflash cleanup is not supported in PnP (Plug and Play) workflow.

Procedure

Step 1 In the Cisco IoT FND menubar, choose **CONFIG** > **Firmware Update**.

Step 2 Click the **Groups** tab.

Step 3 In the **Groups** tab, select the router group for which you want to install the firmware.

Step 4 Click **Install Image**.

Step 5 In the **Install Image to:** dialog box, select **Install Image Now** to install the image instantly.

Step 6 Select **Schedule** to schedule the installation based on your requirement.

Note If you want to reschedule a future scheduled Firmware job, you need to cancel this firmware job and schedule again.

Step 7 Check the **Enable timeout for scheduled install** check box if you want to set a timeout for the installation.

Step 8 Use the **Cancel** or **Pause** buttons to cancel or pause the firmware installation.

Note
- If you restart Cisco IoT FND during the image installation process, it automatically resumes any firmware installations that were in progress before going offline.
- The firmware installation operation can time out on some routers. During installation, a job scheduler runs every two hours to terminate any firmware install jobs that are stuck at 35% progress. You can adjust the scheduler's default interval by setting the "firmware-install-timeout-schedule-cron-hour" key in the cgms.properties file to any value greater than 0 and less than 24. This scheduler applies only to jobs stalled at the 35% mark.
- When a firmware install or image upload operation for routers takes too long, it can cause other jobs in the queue to wait longer. You can set the timeout duration for stuck firmware jobs using the `router-firmware-upload-timeout-minutes` and `router-firmware-install-timeout-minutes` keys in the cgms.properties file; the default is 8 hours (480 minutes).

What to do next

View the firmware images

Firmware upgrade behavior

This topic describes how Cisco IoT FND manages device firmware upgrades across greenfield and brownfield deployments, covering install versus bundle boot modes, storage locations (`bootflash` and `managed/images`), progress/status milestones (35%, 50%, 75%, 100%), space requirements for install mode (800 MB), file cleanup at defined checkpoints (success, failure, registration, and retries), error/skip conditions related to install-mode support, and rollback handling using `packages.conf` and `prev_packages.conf` to prevent `prev_packages.conf.xx` accumulation.

- Covers greenfield and brownfield upgrade paths, including install and bundle boot modes.
- Identifies storage locations used during upgrades: `bootflash` and `managed/images`.
- Outlines file cleanup behavior on success and failure, including actions during registration and retry phases.
- Details status and progress updates, including milestones at 35%, 50%, 75%, and 100% with `UPDATING_FIRMWARE` and "update complete."
- Requires at least 800 MB free space before starting an install-mode upgrade.
- Describes rollback handling with `packages.conf` and `prev_packages.conf`, including an additional reload to avoid `prev_packages.conf.xx` file sprawl.
- Highlights brownfield two-reload behavior and associated cleanup in `managed/images` and `bootflash`. Notes that Cisco IoT FND retries deletions and can enforce cleanup across boot modes when initial deletion fails.
- All firmware related activities on Cisco IoT FND are captured in the **Audit Trail** page. Starting from Cisco IoT FND Release 5.1, you can see the **Mode of installation** used to perform the firmware upload or install.

Table 7: Terminology

Term	Details
Greenfield	Device uses images in `bootflash` (previous package is in `bootflash`).
Brownfield	Device previously used bundle boot mode with images under `managed/images`, now upgrading using install boot mode in `bootflash` (requires two reloads).
`bootflash`	Device's local storage.
`managed/images`	Directory used by bundle boot mode.
Install boot mode	Boots using installed packages in `bootflash`.
Bundle boot mode	Boots using a single `.bin` image (often under `managed/images`).
`packages.conf` / `prev_packages.conf`	Boot configuration files; `prev_packages.conf` is used for rollback/revert.

Table 8: File cleanup behavior

Scenario	Cleanup Actions
Greenfield, install succeeds.	During registration, Cisco IoT FND deletes unused extracted files, the uploaded `.bin`, unused `.bin` file and `prev_packages.conf` (if not needed) from `bootflash`.
Greenfield, install fails.	Device rolls back; Cisco IoT FND removes the uploaded `.bin` and any unused files from `bootflash`.
Brownfield, install succeeds (first reload).	At first registration, Cisco IoT FND removes the unused `.bin` under `managed/images`.
Brownfield, install succeeds (second reload).	Cisco IoT FND removes any unused `.bin` from `bootflash`.
Brownfield, install fails (first reload still works).	Cisco IoT FND cleans up the `.bin` under `managed/images`.
Brownfield, second upgrade attempt fails.	Cisco IoT FND removes unwanted extracted files and the uploaded `.bin` from `bootflash`.
Deletion fails right after install.	Cisco IoT FND retries deletion during upload and install phases; can enforce cleanup of leftover files related to the other boot mode.

Table 9: Status and progress

Flow	Status	Progress	Message
Generic: while installing	`INSTALLING FIRMWARE`	0% → 10%	—
Generic: after commands sent.	`UPDATING_FIRMWARE`	0% → 35%	—
Generic: successful installation and reload, upon registration.	Update complete	100%	—
Brownfield with install boot mode.	`UPDATING_FIRMWARE`	35%	—
Brownfield with install boot mode: after first reload and registration.	`UPDATING_FIRMWARE`	50%	“Two reloads are required as firmware already installed in managed/images using bundle boot mode is upgrading using install boot mode in bootflash directory.”
Brownfield with install boot mode: second installation commands sent for `bootflash`.	`UPDATING_FIRMWARE`	75%	Same as above.
Brownfield with install boot mode: successful completion.	Update complete	100%	—
Any failure.	Error/failure state	—	Status updates accordingly.

Table 10: Error and skip conditions

Category	Condition	FND Response	Message
Error	Device already in install boot mode; user uploads a bundle-mode image.	Show `ERROR`; advise using install boot mode.	"Firmware has already installed using install boot mode. Please select install boot mode for upgrade."
Skip (upload)	Running firmware does not support install boot mode (< 17.09.01).	Skip upload with message.	"The running firmware version is not supporting install boot mode. Firmware upgrade using Install mode is supported in 17.09.01 or later."
Skip (test-only)	Property `skip-install-bootmode-firmware-version-check` used.	Bypass version check (testing only; not for production; not documented).	—
Upload error	Uploaded image does not support install boot mode (< 17.09.01).	Show error popup and fail upload.	Appropriate error presented.
Note	Skip checks apply to upload.	Installation-phase skip logic remains unchanged.	Existing behavior is preserved.

Table 11: Handling `prev_packages.conf` reverts

Condition	FND Actions	Rationale
Device reverts during install-mode upgrade and boots using `prev_packages.conf`.	Upon registration: set boot parameter to `packages.conf`, copy `prev_packages.conf` to `packages.conf`, then reload.	Prevents staying on `prev_packages.conf`, which would create `prev_packages.conf.01`, `.02`, etc.; platform does not allow normal deletion of older `prev_packages.0x` files, so FND avoids accumulation.

Upgrade the cellular modem

Starting from Cisco IoT FND Release 5.1, you can upgrade the firmware of the cellular modem of Cisco IoT routers based on cellular technologies like 5G and LTE using Cisco IoT FND. Here are the supported devices:

- Cisco Catalyst IR1100
- Cisco Catalyst IR8100
- Cisco Catalyst IR1800

Here are the steps involved in upgrading the cellular modem of a supported Cisco IoT router:

1. Upload the firmware image to Cisco IoT FND.

2. Upload the firmware image from Cisco IoT FND to the supported Cisco IoT router.
3. Install the firmware image to the supported Cisco IoT router.

Before you begin

- Ensure to identify the modem type and Stock Keeping Unit (SKU) as the upgrade sequence might vary. The cellular modems in some cases require upto 3 firmware related files depending on the modem and the carrier. Here are the 3 files that can help you upgrade the firmware of cellular modems:
  - Firmware file
  - Carrier PRI file (.nvu)
  - OEM PRI file

  Here are some SKU examples:

SKU ID	Modem Type	Firmware Download Link
P-LTE-GB	WP7607	Download
P-LTE-IN	WP7608	Download
P-5GS6-GL	FN980	Download

- Each firmware file must be uploaded individually. Don't group the firmware image files in a single folder.
- If you have Semtec modems, you can place the Firmware and the Carrier PRI files in the same folder and upgrade them together. Upgrade the OEM PRI file separately.
- If you have Telit modems, use .bin files for upgrading the firmware.
- If the uploaded firmware image file doesn't match the required modem or slot details, Cisco IoT FND skips the upload or installation with a warning.
- Once the installation is completed, the uploaded file is auto-deleted.
- We don't recommend downgrading the cellular modem using Cisco IoT FND.
- That firmware progress time is converted to server time zone and is scheduled accordingly. Similarly, the status of the upgrade is converted back to your time zone.
- If the modem supports three files, upload the Firmware file and Carrier PRI file, and install them. After successful installation, upload the OEM PRI file and install it. If the modem supports two files, upload the Firmware file and install it. After successful installation, upload the OEM PRI file and install it. If the modem supports one file, upload and install it.

Here are the instructions to upgrade the firmware of cellular modems of Cisco IoT routers using Cisco IoT FND:

Procedure

Step 1 From the Cisco IoT FND menubar, choose **CONFIG** > **Firmware Update**.

Step 2 Click the **Images** tab and select either **LTE** or **5G** based on the cellular technology. Click the **+** icon.

Step 3 Choose a **Modem**, a **Carrier**, and browse for the firmware image file to select it. Click **Add File**.
You'll see the file you just added, listed in the **Cellular Firmware Images** table.

If the cellular modem doesn't exist on the registered device, Cisco IoT FND doesn't display the modem model while you upload the images to Cisco IoT FND.

Step 4 Click **Groups** tab, select a supported Cisco IoT router from the list and click **Upload Image**. Uploading an image with the same extension overwrites the existing image.

Step 5 Select the appropriate options from the **Select Type**, **Modem**, **Carrier**, **Slot** drop-down lists. Ensure to select the image that you just uploaded to Cisco IoT FND in the **Select an Image** drop-down list. Click either **Upload Image Now** or **Schedule as** based on your requirement. Check the **Clean cellular image Directory** check box to delete the existing cellular directory and its images before uploading the new image.

Step 6 Once the image is uploaded to the router, click **Install Image**. For more information see, Install firmware images.

You've successfully upgraded the firmware of the cellular modems of Cisco IoT routers.

What to do next

- The cellular images are uploaded to the device on the cellular directory. If the directory doesn't exist, Cisco IoT FND creates a directory on the device and will upload the images to the path `bootflash:/managed/cellular/`
- We recommend that you don't downgrade the cellular modems.
- When the installation is triggered from Cisco IoT FND, the cellular modem will reboot to upgrade the image. During this time, connectivity between the cellular modem and the Cisco IoT FND will be unavailable.
- The Cisco IoT FND pushes the applet `checkCellularManagedDir` and the cgna-profile `cg-nms-cellularFWIntfMetrics`.
- The applet runs every 15 minutes and executes the profile to communicate with the Cisco IoT FND. If successful, the cellular directory is removed, and the firmware activity in the Cisco IoT FND will be marked as `UPDATE_COMPLETE`.
- After successful installation, Cisco IoT FND removes the cellular directory on the router. In addition, Cisco IoT FND removes `aplet checkCellularManagerDir` and `cgna-profile cg-nms-cellularFWIntfMetrics`.
- After successful installation, verify the Firmware Version, Carrier, and OEM PRI version on the **Device Info** page in the **Cellular Link Settings** section.
- If the installation fails, the cellular directory will be removed after five retry attempts if the connection between the router and Cisco IoT FND fails. In addition, Cisco IoT FND removes `aplet checkCellularManagerDir` and `cgna-profile cg-nms-cellularFWIntfMetrics`.
- If the cellular modem upgrade fails and the modem comes up with the old image version, Cisco IoT FND still marks the router as `UPDATE_COMPLETE`. Cisco IoT FND allows upgrading the same cellular image that is currently running on the cellular modem.

  In a dual-modem router, Cisco IoT FND marks the upgrade as `UPDATE_FAILED` if modem 1's upgrade fails or its interfaces go down even when modem 2 establishes a connection between the router and Cisco IoT FND.

Cisco IoT FND marks the upgrade as `UPDATE_COMPLETE` if modem 1's interfaces come up after the upgrade but modem 1 fails to connect and modem 2 establishes the connection; if no connection is established, the upgrade times out per configuration.

View firmware images

Use the following instructions to view the firmware images on Cisco IoT FND:

Procedure

Step 1 From the Cisco IoT FND menubar, choose **CONFIG** > **FIRMWARE UPDATE**.

Step 2 Click the **Images** tab.

Step 3 Select a ROUTER or an ENDPOINT to display all firmware images for those devices in the Cisco IoT FND database. You can view a list of firware images associated with the particular device type. You can view details such as name, version, hardware ID, vendor hardware ID, size, active download etc.

Step 4 Click **Delete** to delete a particular firmware image.

Export firmware images data

This task helps you export the existing firmware images data from Cisco IoT FND.

Before you begin

- Ensure that your local system has enough space to download the firmware and configuration data.
- Ensure that your local system supports .csv files.

Here are the instructions for you to export firmware images data from Cisco IoT FND:

Procedure

Step 1 From the Cisco IoT FND menubar, choose **CONFIG** > **Firmware Update**.

Step 2 Select the firmware group. Select multiple group members or filter them using the firmware group's search filter. Find the export icon for endpoints on the **Devices** tab of each endpoint firmware group.

Step 3 Click the export icon adjacent to the refersh icon.
The firmware images data is downloaded as a .csv file to your local system.

You've successfully exported the fimrware images data.

What to do next

Search Firmware Updates

Search Firmware Updates

Search Firmware Updates

Table 12: Feature History

Feature Name	Release	Description
Search Firmware Updates	Cisco IoT FND Release 5.0	Search through the existing firmware updates using the filters introduced in this release. This feature aims to make the firmware updates page searchable.

Information About Search Firmware Updates

Starting from Cisco IoT FND Release 5.0, search through the firmware updates in the **Firmware Update** page. Use the exhaustive filters provided along with the search option to narrow down your search.

Benefits of Search Firmware Updates

- Quickly locate specific devices, data, or configurations, and reduce the time spent navigating through the system.
- As the network grows, the functionality can help you handle larger datasets, ensuring that performance and usability remain consistent.

Perform a Search Using Search Firmware Updates

1. From the Cisco IoT FND menubar, choose **CONFIG** > **Firmware Updates**.
2. In the default page, perform a search using the search bar. Click **Show Filter**.
3. In the Filters pane, click the first drop-down box and choose from the following options:

Option	Description
Status	Choose Status as a search criteria if you want to filter the devices based on their statuses. Here are the statuses that you can choose from: • blocked • bootstrapped • bootstrapping • down • outage • outofservice • registering • restored • unheard • unmanaged • unsupported • up
Name	Type in the name of the device that you are looking for in the text box.
EID	Type the EID of the device that you are looking for in the text box.
IP Address	Enter the IP address of the device that you are looking for in the text box.
Firmware Version	Use the firmware version of the device to filter the devices running a particular firmware version.

Option	Description
Activity	Choose Activity as a filter if you want to filter out devices based on their activity. Here are some of the device activities: • Unknown • Partially Uploaded • Awaiting Upload • Skipped • Error • Fully Uploaded **Note** You can use any VM on which Cisco IoT FND is installed to monitor all the activities.
Update Progress	You can filter the devices that are going through a firmware update process. Choose **between** in the second drop-down box and enter the firmware upgrade versions in the text boxes provided.
Last Firmware Status Heard	Use this filter if you want to filter devices based on the date and time they broadcasted their firware update status.

4. Click + button to populate the search bar.
5. Click the **Search** icon to perform a search based on the filters.

Push StackMode

Starting from Cisco IoT FND Release 4.8.1, Cisco IoT FND supports multiple mesh networking modes for IoT deployments. You must be an admin or you should have firmware upgrade permission to perform the switch from CR-Mesh to Wi-SUN stack mode. Switching from CR-Mesh to Wi-Sun mode changes the underlying radio protocol used by devices in the network. CG-Mesh is Cisco mesh technology, while Wi-Sun leverages the IEEE 802.15.4g standard with Wi-SUN profiles for interoperability within a broader ecosystem. During the switching process, a single or multiple PAN nodes are grouped and scheduled for switching devices from CG-Mesh to Wi-SUN stack. Wi-SUN stack supports both unicast and multicast transmissions. For more information see, Mesh protocol modes.

Supported Platforms

Cisco IoT FND supports the following platforms for switching devices from CG-Mesh to Wi-SUN stack:

- ITRON30
- CR-Mesh

- Cisco 500 Series WPAN Industrial Routers

Table 13: Feature History

Feature Name	Release Information	Description
Support For Wi-SUN Stack Switch	Cisco IoT FND Release 4.8.1	Switch devices from CR-Mesh to Wi-SUN StackMode.
Abort StackMode jobs	Cisco IoT FND Release 5.1	Abort the StackMode jobs using Cisco IoT FND. You can abort the operations you performed using **Push StackMode**, **Push StackMode Time**, and **Cancel StackMode** options.
Abort backup and reload	Cisco IoT FND Release 5.1	Abort both the **Schedule Install and Reload** and **Set as Backup** operations.

Prerequisites

Here are the prequisites for switching to Wi-SUN mode from CR-Mesh mode using Cisco IoT FND:

- Ensure that the following supported devices are running the minimum required versions
  - Cisco CGR: Cisco IOS Release 15.9(3)M1 and later releases.
  - Cisco IR8140: Cisco IOS-XE 17.x and later releases.
- Once you are done with switching of the devices from CR-Mesh to Wi-SUN stack mode, ensure to update the WPAN OFDM/FSK stack mode to Wi-SUN stack. If the WPAN OFDM/FSK is not updated, the node can't join back the network and will move to **Down** state in Cisco IoT FND.
- Ensure that the firmware version is 6.2.35 MR and later versions to use Push Stack Mode.

Note Starting from Cisco IoT FND 5.1.2, you can execute the Push Stack Mode even when the devices in a PAN are running 6.2.35 MR or lower versions. You can still execute the Push Stack Mode which ignores the devices that don't match the version criteria.

Switch from CR-Mesh to Wi-SUN StackMode

You can push your devices to Wi-SUN mode from CR-Mesh mode by scheduling the task at your convenience.

Configure Push StackMode

Here are the instructions to push devices to Wi-SUN stack mode:

Procedure

Step 1 From the Cisco IoT FND menubar, choose **CONFIG** > **Firmware Update**.

Step 2 Click the **Groups** tab in the left pane.

Step 3 Select the default or user-defined firmware group from the **ENDPOINT**.

Step 4 Check the **PAN ID** check box in the **StackMode Switch** table.

Step 5 Click **Push StackMode** to set your device mode to Wi-SUN stack mode.

Step 6 A confirmation dialog-box appears, click **Yes**. If you see a stack mode failure message, retry pushing to StackMode.

Step 7 Based on the status of the push stack mode process, the following states are displayed for the selected PAN ID in the **StackMode Switch** table:

Field	Description
Stack Operation Type	Displays the following states for the Push StackMode operation: • **StackMode Push Initiated**: Displays initiation of the stack mode operation. • **StackMode Push Completed**: Displays the completion of the stack mode operation. • **No operation** when no operation is initiated.
Stack Operation Status	Displays the overall success and failure status of the devices for the selected PAN during the StackMode operation.
Job Status	Displays the following statuses: • In-progress • Success • Aborted
Abort StackMode Operation	Click the **Abort** button if you'd like to abort the Push StackMode operation.

Your device modes are set to Wi-SUN stack mode.

Schedule Push StackMode Time

Here are steps to configure Push StackMode Time:

Procedure

Step 1 From Cisco IoT FND menubar, choose **CONFIG** > **Firmware Update**.

Step 2 From the **StackMode Switch** table, check the **PAN ID** check box.

Note You can select only the PAN ID that has successfully completed the push StackMode configuration.

Step 3 Click **Push StackMode Time**.

A **Confirm** dialog box appears to schedule the switching initiation process for moving CR-Mesh devices to Wi-SUN stack.

Based on the status of the StackMode time process, the following states are displayed for the selected PAN ID in the **StackMode Switch** table.

Table 14: PAN ID Status

Field	Description
Stack Operation Type	Displays the following states for the Push StackMode operation: • **StackMode Switch Time Push Initiated** : Displays initiation of the stack mode schedule operation. • **StackMode Switch Time Completed**: Displays the completion of the stack mode schedule operation.
Stack Operation Status	Displays the overall success and failure status of the devices for the selected PAN during the StackMode operation.
Job Status	Displays the following statuses: • In-progress • Success • Aborted
Abort StackMode Operation	Click the **Abort** button if you'd like to abort the Push StackMode Time operation.

Note

- If you abort an in-progress Push StackMode Time job, the job stops immediately and retains all progress completed before the abort. To complete Push StackMode Time for the remaining devices, run Push StackMode Time again to restart the workflow.
- When you run Push StackMode Time again for an aborted or unsuccessful workflow, Cisco IoT FND sends requests only to the pending devices. It ignores devices that successfully received the Push StackMode Time request during the previous run.
- When you perform Push StackMode Time more than once on a workflow, the timestamp on devices in the same PAN might vary depending on the time configured in each run. We recommend that you push the same timestamp each time. If different timestamps are configured across devices in the same PAN, the devices switch to Wi-SUN mode according to their configured time, which might prevent some nodes from rejoining the network.
- If you want to reschedule the Push StackMode Time and set the same for all devices in the same PAN ID, we recommend that you cancel Push StackMode and run Push StackMode and Time as a fresh workflow.

Step 4 Select the time and date in the **Schedule Switch Wi-SUN Stack** dialog box and click **Schedule** .

Note Ensure that the scheduled time is not more than 49 days from the current date.

Note If the scheduled time is in the past, an error message appears.

Step 5 Click **Yes** to confirm the stack switching operation.

On confirming the stack switching process, the stack operation type gets updated to **Stack Switch Time Push Initiated** state for the selected PAN ID.

Step 6 Click **OK** in the **Success** dialog box.

On successful completion of the stack switch process, the stack operation type column in the table gets updated to **Stack Switch Time Push Completed** state for the selected PAN ID.

Note We recommend that you wait until all the devices in the selected PAN get switched to Wi-SUN stack, as there is a possibility of some devices failing to switch in the scheduled time. However, the failed devices automatically switch to Wi-SUN StackMode after a one-day time period.

If you don't schedule Push Stack Mode Time after you Push StackMode, the endpoint devices switch to Wi-SUN mode after 24 hours.

Note If you want to reschedule the stack time for some reason, then you have to cancel the current stack switch operation, push the StackMode again, and reinitiate the scheduling stack switch process.

Cancel Wi-SUN Stack Switch Operation

Here are the steps to cancel Wi-SUN stack switch operation:

Before you begin

- Starting from Cisco IoT FND Release 5.1.2, use the cancel switch operation during any stage of the Push StackMode workflow.
- Cancel switch operation cancels the scheduled Push StackMode workflow as well.

Procedure

Step 1 From the Cisco IoT FND menubar, Choose **CONFIG** > **Firmware Update**.

Step 2 In the **Firmware Management** page, check the **PAN ID** check box for which you have completed either configuration or scheduling operation.

Step 3 Click **Cancel StackMode**.

Based on the status of the StackMode cancellation process, the following states are displayed for the selected PAN ID in the **StackMode Switch** table.

Table 15: PAN ID Status

Field	Description
Stack Operation Type	Displays the following states for the Push StackMode operation: • **StackMode Cancel Initiated:** Displays the intitiation of cancelling the StackMode operation. • **StackMode Cancel Completed**: Displays the completion of cancelling the StackMode Operation.
Stack Operation Status	Displays the overall success and failure status of the devices for the selected PAN during the StackMode operation.
Job Status	Displays the following statuses: • In-progress • Success • Aborted

Field	Description
Abort StackMode Operation	Click the **Abort** button if you'd like to abort the cancel Push StackMode push operation.

Step 4 Click **Yes** to cancel the stack switch operation.

A **Success** dialog box appears to indicate the successful cancellation of the Wi-SUN stack switch operation.

Validate Push StackMode

In the **StackMode Push Initiated** state, the devices in the selected PAN ID are validated based on the following parameters:

- Firmware version
- StackMode configuration

Table 16: Push StackMode Validation

Scenarios	System Validation	User Action
Firmware version 6.2 MR.	Checks if the devices in the selected PAN ID are running firmware version 6.2 MR. • If the firmware version is lower than 6.2 MR, then an error message appears. **Note** for more information on the devices that are running a lower version go to the **Devices** tab.	• You must upgrade the devices to firmware version 6.2 MR or later versions. • After upgrading the devices, you must again push new StackMode for the selected PAN ID.
	• If the firmware version is greater than 6.2 MR, then the devices are already in Wi-SUN stack.	

Scenarios	System Validation	User Action
StackMode configuration.	Checks if all devices in the selected PAN ID received the StackMode configuration. • Some devices in the selected PAN ID fail to receive the configuration.	• Push StackMode again for the selected PAN ID. or • Remove the devices that are in Down state from FND and again push StackMode for the remaining devices in the PAN ID.
	• If all the devices in the selected PAN ID received the StackMode configuration, then you can schedule the devices for stack switch operation initiation.	You can schedule the devices for Wi-SUN stack switch only on successful completion of pushing StackMode configuration to all devices in the selected PAN.



Note On successful completion of the validation, the stack operation state for the selected PAN ID changes to **Stack Mode Push Completed**.

Abort backup and reload

Starting from Cisco IoT FND 5.1, you can abort both the **Schedule Install and Reload** and **Set as Backup** operations.

Before you begin

Here are the steps that you need to follow to abort the schedule and reload operations

Procedure

Step 1 From the Cisco IoT FND menubar, choose **CONFIG** > **Firmware Update**

Step 2 Click the **Groups** tab and select an **ENDPOINT** of your choice.

Step 3 From the available list of images in the **Image Status** table, click either **Schedule Install or Reload** or **Set as Backup** based on your requirement.

Step 4 The current status of the schedule install or reload or set as backup is displayed in the **Current Status** field.

Step 5 Click either **Abort Reload** or **Abort Backup** to cancel the operation.

You've aborted the backup or reload operation.

View StackMode information

From the **Devices** tab, you can view the StackMode status and StackMode time of each device for the following processes:

- Pushing Devices to Wi-SUN StackMode
- Scheduling Devices for Wi-SUN Stack Switch
- Canceling Wi-SUN Stack Switch Operation

Procedure

Step 1 From the Cisco IoT FND menubar, choose **CONFIG** > **FIRMWARE UPDATE** > **Groups** tab.

Step 2 Select the default or user-defined firmware group from the **ENDPOINT**.

Step 3 Select the **PAN ID** from the StackMode Switch table.

Step 4 Click the **Devices** tab.

The **Stack Change Status** column displays the following states:

Table 17: Device State

Device State	Description
Not Started	Indicates the supported devices that are not initiated for Wi-SUN stack switch.
Not Applicable	Indicates the devices that are not supported for Wi-SUN stack switch.
Configuring StackMode	Indicates the devices that are pushed for StackMode operation.
Configured Stackmode	Indicates the devices that are successfully configured with StackMode.
Scheduling Stackmode time	Indicates the devices that are scheduled for StackMode switch.
Success	Indicates the devices that are successfully switched from CG-Mesh to Wi-SUN stack.
Canceling stackmode switch	Indicates the devices that are scheduled for canceling StackMode switch.
Cancelled stackmode switch	Indicates the devices that are successfully cancelled from switching to Wi-SUN stack.

Filtering Options

a) Click **Show Filter**. The page displays three drop-down lists.

b) Select the search option from the first drop-down list. For example, if you select Status from the first drop-down list, the available list of states appears in the third drop-down list.
c) Select the required option in the third drop-down list and click +.

Your selection is displayed in the text box above the drop-down lists.

d) Click the search icon.

The table displays information based on the search criteria set by you.

View logs for Wi-SUN stack switch

To view logs for Wi-SUN stack switch:

Procedure

Step 1 From the Cisco IoT FND menubar, choose **CONFIG** > **Firmware Update**.
Step 2 Select the firmware group from the **ENDPOINT** in the left pane.
Step 3 In the **Firmware Management** page, select the **PAN ID** for which you want to see the logs.
Step 4 Click the **Logs** tab.

In the **Logs** page, you can view the events that are recorded for the selected PAN ID.

View Audit Trail for Wi-SUN stack switch

To view audit trail for Wi-SUN stack switch :

Procedure

Step 1 From the Cisco IoT FND menubar, choose **ADMIN** > **System Management** > **Audit Trail**.
Step 2 In the Audit Trail page, click the **Date/Time** drop-down arrow to filter the audit trail based on the date and time.

You can view the audit trail of the stack operations that were performed on the selected PAN ID.

Upgrading Firmware Image during Bootstrapping

During bootstrapping, you can enter a different image if the installed image at manufacturing is inappropriate. This is supported for IR1800 and IR8100 devices from the versions 17.13.01 and above. Plug and Play (PnP) must be supported on these devices.

Note Ensure that IR8100 device has the network-essentials license to register the device to IoT FND.

PnP Device Information service retrieves current firmware version on the device and the PnP ImageInstall service performs the image installation. The CGNA ‘image-retrieve' service transfers the image file from IoT FND to router.

Procedure

Step 1 Set the firmware-update-bootstrap property in cgms.properties to ‘true’.

Step 2 On the Tunnel Provisioning Page, navigate to **CONFIG** > **TUNNEL PROVISIONING** > **ROUTER BOOTSTRAP CONFIGURATION**.

Step 3 Select the device group in the left pane, choose the Target Firmware Version from the drop down that lists the images in IoT FND, and click **Save**.

The PnP workflow configures the device to load the new image upon the next reload by executing the boot system command. The configuration changes are saved on the device. The PnP reload happens and sends a message to the PnP server after which an event is generated denoting image installation.

Note The PnP workflow supports device upgrade only if the target image version is higher than the running (current) image version.

If the target image runs the same or lower version, then the device upgrade is skipped during the PnP workflow.

During PNP, you also have the option to skip the firmware upgrade and proceed with PNP if the source operating system on these devices is found to be unreliable. Enter the image versions as comma separated values in **pnp-skip-update-ios-xe-fw-versions** property in cgms.properties file. This property is applicable for all IR1100, IR1800, and IR8100 devices. For more information, see Skipping Firmware Upgrades during PNP, on page 45.

Skipping Firmware Upgrades during PNP

During Zero Touch Deployment (ZTD), certain scenarios may arise where Plug-and-Play (PNP) devices come bundled with software that exhibits instability or issues. If the source operating system (OS) on these devices is found to be unreliable, it can potentially disrupt the entire registration process. In such instances, during the PNP process, you can skip the firmware upgrade step while allowing PNP to proceed seamlessly. However, you can upgrade the firmware once the PNP process is complete.

To perform a PNP with firmware upgrade skip:

Procedure

Step 1 Set the image versions in pnp-skip-update-ir1100-fw-versions property in cgms.properties file.

Note The pnp-skip-update-ir1100-fw-versions property is applicable for IOS-XE routers only.

Step 2 Set the image versions in pnp-skip-update-ios-xe-fw-versions property in cgms.properties file.

Note The pnp-skip-update-ios-xe-fw-versions property is applicable for IOS-XE routers only.

Step 3 Choose **CONFIG** > **Tunnel Provisioning**. Select the router group for which you intend to execute the PNP process.

Step 4 Click **Router Bootstrap Configuration** tab.

Step 5 Under Target Firmware Version, specify the image version you want to skip and click **Save**.

The template is saved. However upon performing PNP, during router bootstrap configuration, a warning popup appears if any invalid entry is found. In that case, modify the field and restart server.

If firmware install is skipped during PnP process, the log details are stored in server.log file. The sample INFO log is shown below:

```
Aug 03 2023 19:24:26.854 +0000: %IOTFND-6-UNSPECIFIED:
 %[ch=WorkResponseHandler][eid=IR1101-K9+FCW23500HJ3][ip=1.1.1.121]
[sev=INFO][tid=tunnelProvJetty-67]: Retrieved device image version
[17.9.3] is present in PnP firmware image skip list. Firmware image update
 during PnP process will be skipped.
```

Note In order to upgrade the device with the latest firmware version, skip entering the current image version in cgms.properties and proceed with PNP.

Step 6 Navigate to the Bootstrapping tab where the Error Message field is updated though the PNP progresses as is.

The Bootstrapping tab shows the status of the PNP under the Bootstrap State field.

Update Target Firmware Versions For All Users

In the Cisco IoT FND Release 4.12.x and earlier releases, when you change the target firmware versions in the **Router Bootstrap Configuration** tab as a root user. The target firmware changes don't reflect in Cisco IoT FND when you're logged in as a different user with specific roles assigned to you by the root user. For more information on managing roles and permissions see, Managing Roles and Permissions.

Starting from Cisco IoT FND Release 5.0, when the root user changes the target firmware version, the changes reflects for all the other associated Cisco IoT FND users.