Cisco Cloud Native Broadband Router Maintenance

Cisco cnBR enables you to perform software upgrades seamlessly, and without disrupting any of the services. You can continuously deploy new services and features with minimal downtime.

RPD Secure Software Download

The cnBR Manager provides automated ways to securely download and activate software images to RPDs.

The secure software download (SSD) feature helps you to authenticate the source of a file and verify the integrity of the downloaded code before you use it in your system. The SSD feature is applicable to Remote PHY (R-PHY) devices installed in unsecure locations.

Prerequisites

To use SSD, the following prerequisites must be met:

- For Non-Express mode: The RPD software image is available at an external TFTP or HTTP image server. The image server is where the software image is stored, and can be accessed by RPD.
- For Express mode: The RPD software image is available in the Cisco Operations Hub. Ensure that RPD has connectivity to the management IP of Cisco Operations Hub.
- Ensure that code validation certificates are available. For more information, go through the Add Code Validation Certificates topic.

Upload Software Image for RPD

For Express-mode of SSD, upload the software image to the cnBR Manager. Complete the following steps:

Step 1 Log in to the Cisco Operations Hub.

Step 2 Choose **cnBR Manager** > **Remote PHY Device Management** from the Cisco Operations Hub main menu and click **Image Management**.

Step 3 Click **Choose file** to select the RPD software image file that you want to upload.

Step 4 Click **Upload**.

To delete any of the listed software image files, click the **X** icon that appears against the image name.

Download Software Image for RPD

Download the software image from the specified server. The software image is available on an external TFTP or HTTP image server.

To download an RPD software image using SSD, complete the following steps:

Step 1 Manually upload the software image to the external image server.

Step 2 Add code validation certificates.

Step 3 Upgrade the software image.

Note You need to download the software image for RPD only for Non-Express mode. For Express mode, the image is available in the Operations Hub.

Add Code Validation Certificates

To authenticate the source and verify the integrity of the software image, Cisco cnBR uses the following two types of RPD code validation certificates (CVC).

- M-CVC: The type of CVC released along with the Cisco RPD software image. Contact Cisco Support to get the M-CVC.
- C-CVC: The type of CVC created and signed through Manufacturer’s Statement of Origin (MSO). When CVCs are available, upload them using the following procedure:

Step 1 Log in to the Cisco Operations Hub.

Step 2 Choose **cnBR Manager** > **Remote PHY Device Management** from the Cisco Operations Hub main menu and click **Code Validation Check**.

Step 3 Copy the contents from the CVC file to the appropriate text box and click **Add**.

Upgrade the Software Image

To upgrade the software, complete the following steps:

Step 1 Log in to the Cisco Operations Hub.

Step 2 Choose **cnBR Manager** > **Remote PHY Device Management** from the Cisco Operations Hub main menu and click **Secure Software Download**.

Step 3 Scroll down the page and use the toggle button to choose to upgrade using either of the following options:

- Express Mode
- Non-Express Mode

Upgrade RPD in Express Mode

Complete the following steps to upgrade the RPD software in Express mode:

Note Express mode works only with HTTP on PORT 80.

Step 1 Log in to the Cisco Operations Hub.

Step 2 Choose **cnBR Manager** > **Remote PHY Device Management** from the Cisco Operations Hub main menu and click **Secure Software Download**.

Step 3 Click **On** in the toggle button to choose the Express Mode option.
This step enables the Express mode, and the corresponding text fields are visible.

Step 4 Enter the following details in the appropriate text fields:

Field	Description
RPD Image	Choose the image from the list of available images in the drop-down list.

Ensure that the RPD is able to reach the Cisco Operations Hub management IP.

Step 5 Filter out the required RPDs by using the search field in the **RPD Summary** section. The list depicts the target RPDs for upgrade.

Step 6 Click **Upgrade Now** to upgrade the image without a reboot. Alternatively, you can also choose to upgrade during the next reboot by clicking **Save Configuration**.

Upgrade RPD in Non-Express Mode

Complete the following steps to upgrade the RPD software in Non-Express mode:

Step 1 Log in to the Cisco Operations Hub.

Step 2 Choose **cnBR Manager** > **Remote PHY Device Management** from the Cisco Operations Hub main menu and click **Secure Software Download**.

Step 3 Click **Off** in the Express Mode toggle button to choose the non-Express Mode option.

This step enables the Non-Express mode.

Step 4 Enter the following details in the appropriate text fields:

Field	Description
Image Server	Address of the server that stores the software image, and from where RPDs can access the software images.
Image Path	The relative path of the RPD software image on the server. The file is available in the default directory of the image server.
Method	HTTP or TFTP for RPD download SSD image.
M-CVC	Indicator showing whether the certificate is valid or not.
C-CVC	Indicator showing whether the certificate is valid or not.

Ensure that the RPD is able to reach the Cisco Operations Hub management IP.

Step 5 Filter out the target RPDs by using the search field in the **RPD Summary** section. The RPDs in this list of RPDs are the target RPDs for upgrade.

Step 6 Click **Upgrade Now** to upgrade the image without a reboot. Alternatively, you can also choose to upgrade during the next reboot, by clicking **Save Configuration**.

Monitor RPD and SSD State

The RPD SSD window provides options to monitor and trigger SSD operations. A dashboard, displaying three pie charts, provides details of the RPD status and metrics. Access this dashboard under the **Cisco Operations Hub** > **cnBR Manager** > **Remote PHY Device Management** > **Secure Software Download**.

- RPD State: Displays the states of RPDs that are upgraded. During the upgrade process, the RPD becomes offline and then returns online.
- Software Version: Shows the number of RPDs for each RPD software version.
- SSD State: Shows various phases of the SSD progress of RPDs.

RPD Summary

The **RPD Summary** table provides details of RPDs which can be upgraded. You can also search for a specific RPD or set of RPDs that can be upgraded. The following table explains the fields in the **RPD Summary** pane.

Field	Description
Name	Name of the RPD.

Field	Description
MAC Address	MAC address of the RPD.
Service Group	Service group ID of the RPD.
IPv4 Address	IPv4 address of the RPD.
IPv6 Address	IPv6 address of the RPD.
State	Status of the RPD: • online • offline
CCMTS ID	Host name of the Cisco cnBR application. Example: `cnbr1.cisco.com`
SSD State	Phase of the SSD progress.
Software Version	Version of the software running on the RPD.
Online Timestamp	Time when the RPD became online.

Offline Image Upgrade

Cisco cnBR supports offline image upgrade. The image upgrade workflow provides a dashboard that simplifies the image upgrade for both Cisco cnBR and Cisco Operations Hub.

Note The image upgrade workflow supports only the upgrade of the `cmts-app`, `opshub-app`, and `cloud-infra-app` charts.

Image Upgrade Preparation

Use the following steps to prepare an image for upgrade:

Step 1 Log in to the Cisco Operations Hub.

Step 2 Choose **cnBR Manager** > **Core Management** from the Cisco Operations Hub main menu and click **Add cnBR Core**.

Step 3 Provide a unique name to the Cisco cnBR core, a namespace, and Core Ingress-host-name.

See the following example:

```
cnBR-Core Name: Upgrader-demo
Core Namespace: ccmts-infra
Core Ingress-host-name: cnbr1.cisco.com
```

Step 4 Enter the Cisco cnBR username and password.

Step 5 Click **ADD**.

Step 6 Copy the `cnbr-installer-v20.2-06042020.tar.gz` installer bundle image to a staging server.

The installer bundle name `<06042020>` denotes the date MMDDYYYY.

Step 7 Decompress the image into the directory.

Step 8 Set up the configuration file by following the steps at Environment Configuration and Deployer Configuration.

Step 9 Run the following autodeploy command to update the image on the deployer:

```
./deploy -c <day0 config file> -u
```

The image update process takes 30–45 minutes on the deployer.

The new image URL format is as follows:

```
http://chart.<deployer's ip>.nip.io/<image name>/
```

Based on the product type, the `<image name>` is either `cnbr-master` or `opshub-master`.

Image Upgrade

Complete the following steps to upgrade the image:

Step 1 Log in to the Cisco Operations Hub.

Step 2 Choose **cnBR Manager** > **Core Management** from the Cisco Operations Hub main menu and click **Upgrade cnBR**.

Step 3 Select the Cisco cnBR cluster that you want to upgrade.

Step 4 Enter the username and password.

Step 5 Click **Connect**.

You can upgrade only the Cisco Operations Hub that is currently in use. You cannot choose a cluster when you want to upgrade the Cisco Operations Hub.

Step 6 Enter the image that you want to upgrade. Provide the target URL obtained from Image Upgrade Preparation, on page 5.

Step 7 Click **Next**.

Step 8 Check the following before performing image upgrade:

- Helm status: Ensure that the Helm releases status is **DEPLOYED**. To recover failed images, go through the steps that from Image Recovery, on page 7.
- Updates of the new image: Lists the differences between the current and target versions.
- Target cluster pod status: Lists the status of all Pods.

Step 9 Click **Upgrade**. During the Cisco Operations Hub upgrade, the page may redirect you to the Cisco Operations Hub login page. The redirect can happen due to any back-end service downtime. To resolve the issue, log in to the Cisco Operations Hub and go through step #unique_255 unique_255_Connect_42_step1. The workflow jumps to step Step 4, on page 6 and continues the monitoring progress.

The Cisco Operations Hub displays the Image upgrade report.

Step 10 Click **SHOW** to view detailed differences of image and pod statuses before and after upgrade.

Image Recovery

To recover from an environment failure during the upgrade process, go through the following steps:

Step 1 Label all the DOCSIS worker node with the following label using deployer CLI:

```
config terminal
cluster <cluster-name>
nodes docsis-1
no k8s node-labels type_cmts no
k8s node-labels smi.cisco.com/node-type docsis
exit
exit
nodes docsis-2
no k8s node-labels type_cmts no
k8s node-labels smi.cisco.com/node-type docsis
exit
exit
nodes docsis-3
no k8s node-labels type_cmts no
k8s node-labels smi.cisco.com/node-type docsis
exit
exit
```

Note The value `<docsis-n>` denotes a number of K8s nodes. If there are more UCS servers or nodes in the system, you must repeat the steps for every worker node.

Step 2 Clean up environment. To clean up the ops-center in deployer:

```
config terminal
cluster <cluser-name>
no ops-centers cnBR infra
commit
end
clusters <cluster-name> actions sync run
```

You can check the synchronization progress by using the following CLI:

```
clusters <cluster-name> actions sync status
```

Step 3 Reconfigure the ops-centers image with the new image:

```
conf t
cluster <cluser-name>
ops-centers cnBR infra
  repository <image url>
  initial-boot-parameters use-volume-claims true
  initial-boot-parameters first-boot-password <password>
  initial-boot-parameters auto-deploy true
  initial-boot-parameters single-node false
commit
```

```
end
clusters <cluster-name> actions sync run
```

Service Group Operations

Table 1: Feature History

Feature Name	Release Information	Feature Description
Service Group Operations	Cisco cnBR 21.1	You can view the worker-node each service group is running on and move service groups from one worker-node to another. This allows you to balance workloads across worker-nodes. You have better visibility and management on the service groups and the worker-nodes that they are running on.

Cisco cnBR enables you to move Data-over-Cable Systems Interface Standard (DOCSIS) service group workloads to other Cisco cnBR nodes during maintenance and troubleshooting activities. The Service Group related operations help avoid service interruptions during maintenance activities and help balance workloads across nodes.

Move Service Groups

You can move DOCSIS service groups across nodes. Moving Service Groups allows nodes to balance the Service Group workloads effectively. You can move one or multiple Service Groups using the cnBR Manager.

Perform the following steps to move Service Groups.

Step 1 On the Cisco Operations Hub main menu, click **cnBR Manager** > **Core Management** > **Service Group Operations**.

Step 2 Select an available Cisco cnBR cluster from the drop-down list.
The table displays the nodes for the selected cluster.

Step 3 Select a node, click **Move Service Groups**.
The right panel lists down the available Service Groups for that node.

Step 4 Click the plus icon next to the Service Group to select the target Service groups.

Step 5 Select the destination node from the drop-down list.

Step 6 Click **Move** to trigger the move operation.
The status of the host and destination nodes changes to **SG Moving**. On completion of the operation, the Cisco Operations Hub updates Service Group information in the table.

Drain the Node

You can drain a node by moving all the DOCSIS service group workloads from the node. Draining allows you to safely remove the node from the cluster, allowing other nodes to take up workloads.

Perform the following steps to drain a node.

Step 1 On the Cisco Operations Hub main menu, click **cnBR Manager** > **Core Management** > **Service Group Operations** to launch the Service Group Operations panel.

Step 2 Select an available Cisco cnBR cluster from the drop-down list.
The table displays the nodes for the selected cluster.

Step 3 Select a node, click **More Action > Drain & Deactivate**, and confirm the drain operation.
On confirmation, the status of the node changes to **SG Moving**. On completion, the status changes to **Inactive**. A drained node has no associated Service Groups.

Activate the Node

A drained node appears as Inactive in the **Service Group Operations** dashboard (**cnBR Manager > Core Management > Service Group Operations**). To move a drained node back to the working pool after maintenance, perform the following steps:

Step 1 Select an available Cisco cnBR cluster from the drop-down list.
The table displays the nodes for the selected cluster.

Step 2 Select an Inactive Node and click ****More Action > Activate****.
On successful activation, the selected node appears as *Active* in the Service Group Operations dashboard.

Audit of Service Group Operations

The Cisco Operations Hub records all Service Group related moves in the cnBR Manager for auditing.

To view the service group move, drain or activation history, perform the following step:

Navigate to **cnBR Manager > Core Management > Service Group Operations** and click **Operations History**.
The **Operations History** table provides the following information:

- Task ID
- Action undertaken
- Status of the operation
- Cluster ID
- Source and Destination Node
- Service Groups that moved successfully

- Service Groups that failed during movement (if any)
- The initiation time of the operation

Service Group Operations Errors and Warnings

Service Group Operations have the following errors and warnings:

Error

Error: Failed to drain node <*node-name*>, reason: job failed. Please try again later.

Diagnosis: The common cause for a draining job failure is a timeout occurring while waiting for responses from other microservices.

Solution: Attempt the operation later and see whether the issue is resolved.

Warning

Warning: Unable to drain <*node-name*>, reason: Insufficient SG capacity in other worker node.

Diagnosis: When draining a DOCSIS node, the Cisco cnBR moves the service groups to other DOCSIS nodes to keep the services running. Sometimes, the other DOCSIS nodes do not have the capacity to hold all service groups. In such cases, an error-dialog warns of the insufficient capacity.

Solution: To resolve the issue, click **Cancel** and stop the drain operation. You can alternatively drain the node with **Force Drain**.

Note We do not recommend the **Force Drain** method. This method may cause the clusters to become unable to service several service groups. These unserved service groups may increase service downtime.

Export and Import Configuration

The system administrator perform import and export Cisco cnBR and Cisco Operations Hub configurations using the Cisco Operations Hub UI or RESTful APIs. The system administrator can store the exported configuration at a secure location. For Disaster Recovery, the system administrator performs the import operation, to restore the Cisco cnBR, the Cisco Operations Hub, or both to their original configurations.

Export Cisco cnBR Configuration using cnBR Manager

To export the Cisco cnBR configuration, complete the following steps:

Step 1 Click **Cisco Operations Hub** > **cnBR Manager** > **Core Management** > **Import & Export cnBR**.

Step 2 Select the target Cisco cnBR from the drop-down list in the **Export cnBR Configuration** section.

Step 3 Click **Export**.

Step 4 Rename the file and save it at a secure location.

Export Cisco cnBR Configuration using RESTful API

Run the following command in a UNIX shell to export the Cisco cnBR configuration:

```
curl -k -X GET 'https://{opsHUBHost}/api/configurator/v1/cmts/config/{cmts-id}' -H 'Accept:
application/json' -H 'Authorization: Bearer <token>' | tee path/to/backup/config
```

Example

```
hostname#curl -k -X GET
'https://opshub1.cisco.com/api/configurator/v1/cmts/config/cnbr1.cisco.com' -H 'Accept:
application/json' -H 'Authorization: Bearer <token>' | tee
cnbr-10.79.193.236-configuration.json
```

Export Cisco Operations Hub Configuration using Cisco Operations Hub

To export the Cisco Operations Hub configuration, complete the following steps:

Step 1 Click **Cisco Operations Hub** > **System** > **Configurations & Upgrade**.

The **Cisco Operations Hub** Export/Import pane is displayed.

Step 2 On the **Export Operations Hub Configuration** section, click **Export**.

Step 3 Rename the file and save it to a secure location.

Export Cisco Operations Hub Configuration using RESTful API

Run the following command in a UNIX shell to export the Cisco Operations Hub configuration:

```
curl -k -X GET 'https://{opsHUBHost}/configurator/opshub/export' -H 'Accept: application/json' -H
'Authorization: Bearer <token>' | tee path/to/backup/config
```

Example

```
hostname#curl -k -X GET 'https://opshub1.cisco.com/configurator/opshub/expor' -H 'Accept:
application/json' -H 'Authorization: Bearer <token>' | tee
opshub-172.22.29.221-configuration.json
```

Import Cisco cnBR Configuration using cnBR Manager

To import the Cisco cnBR configuration, complete the following steps:

Step 1 Click **Cisco Operations Hub** > **cnBR Manager** > **Core Management** > **Import & Export cnBR**.

Step 2 Select the target Cisco cnBR Name from the drop-down list in the **Import cnBR Configuration File** section.

Step 3 Select the configuration file.

Step 4 Click **Import**.

Step 5 Rename the file and save it at a secure location.

Import Cisco cnBR Configuration using RESTful API

Run the following command in a UNIX shell to import the Cisco cnBR configuration:

```
curl -k -X PUT 'https://{opsHUBHost}/api/configurator/v1/cmts/config/{cmts-id}' -H 'Accept:
application/json' -H 'Content-Type: application/json' -H 'Authorization: Bearer <token>' -d
'@path/to/backed/up/config
```

Example

```
hostname#curl -k -X PUT
'https://opshub1.cisco.com/api/configurator/v1/cmts/config/cnbr1.cisco.com' -H 'Accept:
application/json' -H 'Content-Type: application/json' -H 'Authorization: Bearer <token>'
-d '@cnbr-10.79.193.236-configuration.json
```

Import Cisco Operations Hub Configuration using Cisco Operations Hub

To import the Cisco Operations Hub configuration, complete the following steps:

Step 1 Click **Cisco Operations Hub** > **System** > **Configurations & Upgrade**.

The **Cisco Operations Hub** Export/Import pane is displayed.

Step 2 On the **Import Operations Hub Configuration File** section, browse and choose an Operations Hub configuration file.

Step 3 Click **Import**.

Import Cisco Operations Hub Configuration using RESTful API

Run the following command in a UNIX shell to import the Cisco Operations Hub configuration:

```
curl -k -X PUT "https://{opsHUBHost}/configurator/opshub/import" -H "accept: application/json" -H
"Content-Type: application/json" -H 'Authorization: Bearer <token>' -d "@path/to/backed/up/config
```

Example

```
hostname#curl -k -X PUT 'https://opshub1.cisco.com/configurator/opshub/import' -H 'Accept:
 application/json' -H 'Content-Type: application/json' -H 'Authorization: Bearer <token>'
-d '@opshub-172.22.29.221-configuration.json
```