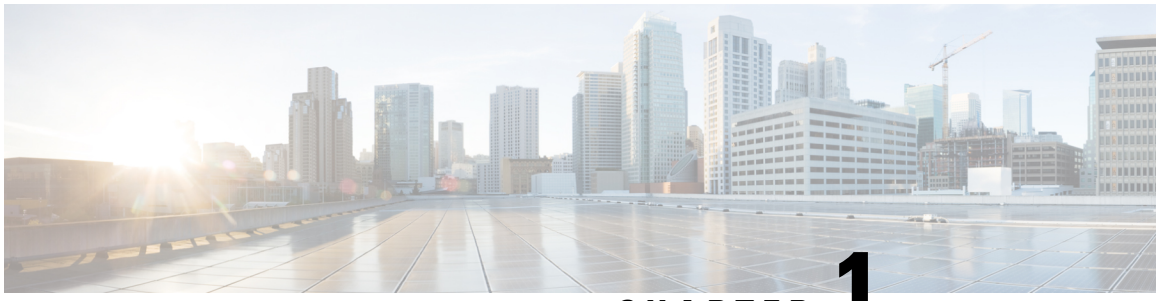
Cisco Smart PHY Application User Guide, Release 23.3

First Published: 2023-10-31

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

CONTENTS



CHAPTER 1

Information about Cisco Smart PHY

Cisco Smart PHY is a highly resilient cloud-native solution for installing, configuring, monitoring, and troubleshooting Remote PHY Devices (RPD) serviced by Cisco cBR-8 routers.

Smart PHY focuses on:

- Simplifying Distributed Access Architecture (DAA) deployment
- Providing Device Lifecycle management for RPDs
- Dynamic RPD Resource Management & CIN traffic engineering
- Enabling Common DHCP policy
- RPD GCP Redirect Management
- Surfacing Advanced Monitoring, Troubleshooting, and Cluster Health Metrics for network insights
- Enabling Programmatic API control for easy third party integration

Smart PHY significantly simplifies RPD deployments thereby improving operational efficiency and reducing the total cost of ownership for Communication Service Providers (CSPs).

- Benefits of Cisco Smart PHY, on page 1
- Configuring DAA Infrastructure, on page 2
- How to Use Cisco Smart PHY, on page 2

Benefits of Cisco Smart PHY

Below are some of the benefits of using the Cisco Smart PHY application:

- Zero-Touch discovery of RPDs as they are connected to the CIN
- Error free RPD Provisioning, which is validated by YANG data models
- Deployment validation ensures that unauthorized changes are detected and flagged
- RPD Software management
- REST-based API eases integration with third party systems

Configuring DAA Infrastructure

This section describes the steps that you should take to ensure your Distributed Access Architecture (DAA) infrastructure works with Smart PHY.

Configuring DHCP

To establish a GCP session with Smart PHY, and later to be GCP-redirected to the appropriate CCAP Cores, the RPDs must first discover Smart PHY's Converged Interconnect Network (CIN) virtual IP address.

Discovery is performed using DHCP. The DHCP servers assigning leases to RPDs must include the CIN virtual IP address of Cisco Smart PHY in the suboption 61 CCAP Cores, under DHCP option 43.

To configure suboption 61 CCAP Cores under DHCP option 43, contact your DHCP software vendor.

Configuring Cisco cBR-8 for Smart PHY

Smart PHY collects SNMP traps and syslog messages to determine and report the operational status of Cisco cBR-8 routers and RPDs.

Enabling Syslog

You can configure your cBR-8 routers to send syslog messages to Smart PHY, including the messages for Line Card high availability (HA) events.

To enable syslog, enter the following commands on your cBR-8 routers:

```
configure terminal
logging host <Smart PHY CIN Virtual IP Address> transport [tcp|udp]
port 8514
logging trap informational
cable logging layer2events
```

Enabling SNMP Traps

You can configure your cBR-8 routers to send SNMP traps to Smart PHY.

To enable SNMP traps on your cBR-8 router, enter the following commands:

```
configure terminal
snmp-server host <Smart PHY CIN Virtual IP address> version 2c public udp-port <port-number>
```

How to Use Cisco Smart PHY

Table 1: Feature History

Feature Name	Release information	Description
Modernized and Refreshed Smart PHY UI for System Settings and Appearance	Cisco Smart PHY 22.2	The Smart PHY UI has been completely refreshed and modernized with a new look and feel, and streamlined workflows.

For more innformation regarding how to use Cisco Smart PHY see Logging into Smart PHY UI, on page 3 and Provisioning an RPD, on page 4.

Logging into Smart PHY UI

Step 1 In the browser's address bar, enter `https://<fqdn>` or `https://<Cisco Smart PHY master virtual IP address>.nip.io`

The access URL is based on the initial cluster configuration.

When you access Cisco Smart PHY for the first time, the browser may display a warning that the site is untrusted or the connection is not private. The warning is due to Smart PHY's use of a self-signed certificate. Follow the browser prompts to add a security exception.

Step 2 Log in through the Cisco Operations Hub UI using the password that you provided during the initial installation.

The **Welcome** page appears.

Step 3 Click the **Cisco Smart PHY** box to open the application.

The Cisco Smart PHY **Overview** page appears.

To open the Cisco Smart PHY application each time after you log in, check the checkbox for **Open Smart PHY at login.**

Step 4 To exit the web GUI, close the browser window or log out using the option in the main menu.

Overview

Feature Name	Release information	Description
Enhancements to the **Overview** page	Cisco Smart PHY, Release 23.1	Additional Provisioning KPIs and new Application KPIs are available on the Overview page. The KPIs include: Provisioning Tasks (Succeeded and Failed), GCP Redirects, Cloud Node status, Micro Services status, API Server status, and Smart Licensing status.

When you access Smart PHY from Operations Hub's Welcome page, or if you have configured Smart PHY to open at login, your browser automatically loads the Smart PHY's Overview page.

The Smart PHY Overview provides you with a centralized view consisting of the following sections:

- **Inventory Overview**: Displays the number of RPDs, CCAP Cores, and Credential Profiles managed by Smart PHY.
- **Provisioning Overview**: Captures count of RPD Associations and Service Definitions along with insights into RPD provisioning activities, GCP message counts from RPDs.
- **Application Overview**: Provides health of the cluster nodes, application pods and status of Smart License.

The Overview page is accessible by selecting **Smart PHY** > **Overview** at the main menu.

For more information regarding viewing more detailed cluster specific Smart PHY metrics, see the Operations Hub's **Dashboards** section.

Smart Licensing

Cisco Smart Licensing is a new, flexible way of licensing to buy, deploy, track, and renew Cisco software. With Smart Licensing, you can configure, activate, and register your application. Smart Licensing establishes a pool of software licenses that you can use across your entire enterprise in a flexible and automated manner.

RPDs in the state other than **Defined**, **Inventory**, **Installed**, or **GcpUp** are considered for the license consumption.

For more information regarding the configuration of Smart Licence, see Configuring Smart License

Provisioning an RPD

Step 1 Create a Credential Profile.

For more information, see Creating a New Credential Profile, on page 6.

Step 2 Add the Cisco cBR-8 router to the inventory.

For more information, see Adding Devices Through GUI, on page 15 and Importing Devices in Bulk, on page 18.

Step 3 Create a Service Definition.

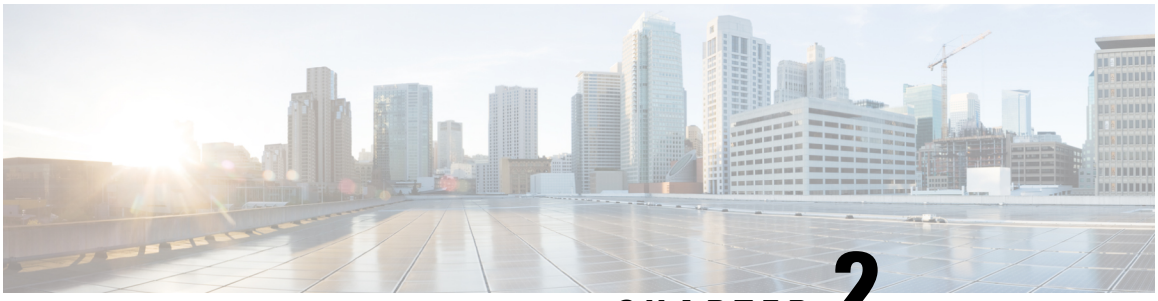
For more information, see Creating Service Definitions, on page 37.

Step 4 Create an RPD Association.

For more information, see Remote PHY Device Association, on page 26.

Step 5 Save the changes.

Note After providing all the mandatory parameters, Smart PHY pushes the RPD's configuration to the Cisco cBR-8 router. When the RPD boots, the RPD establishes a GCP session with Smart PHY. Smart PHY GCP-redirects the RPD to the DOCSIS Principal Core configured in the RPD Association, post which the RPD's status in Smart PHY is `Online`.



CHAPTER 2

Credential Profiles

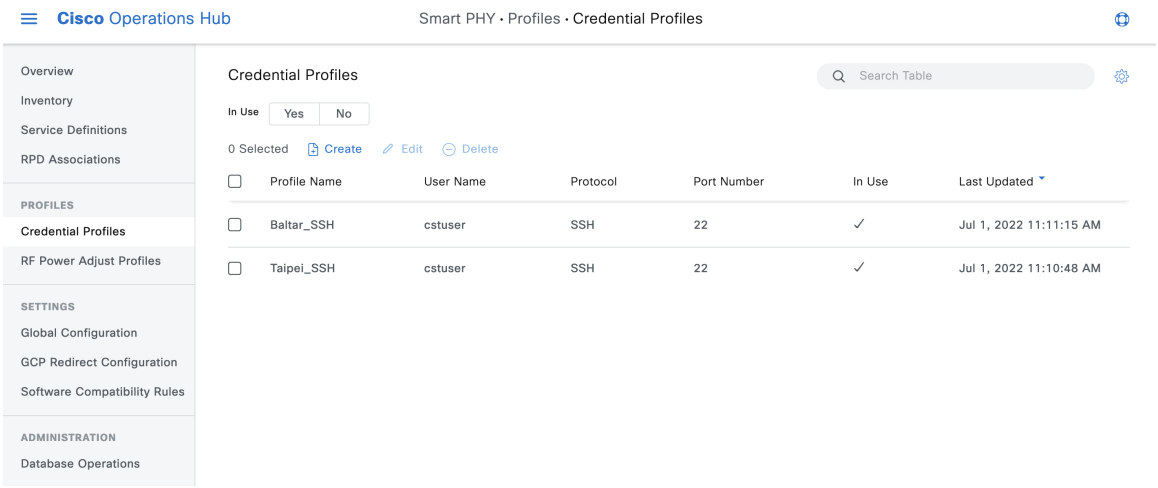
Table 2: Feature History

Feature Name	Release information	Description
Modernized and Refreshed Credential Management UI	Cisco Smart PHY 22.2	Modifications in the Credential Management Smart PHY UI: • Introduction of two new fields—**In Use** and **Last Updated** (in Date and time format) for the Credential profile. • Enhanced search facility to search based on credential profile parameters.

Overview

Credential profiles allow you to apply credential settings consistently across CCAP cores. When you add or import CCAP cores, you can specify the credential profile that you want to use. If you need to modify parameters such as changing a device password, you can edit the credential profile. Once the parameter is modified, it is applicable to all the CCAP cores that use the modified profile.

Figure 1: Credential Profile



Creating a New Credential Profile

This procedure creates a new credential profile.

Before you begin

Make sure that the SSH and SNMP are configured on Cisco cBR-8 router.

Step 1 At the main menu, click **Smart PHY** > **Credential Profiles**.

The **Credential Profiles** page appears.

Step 2 Click **Create** .

The **Add Credential Profile** window appears at the right side of the page.

Step 3 Enter the following details in the text fields.

If you have to add several credential profiles, then ensure that the credential **Profile Name** and **Description** are as informative as possible.

Field Name	Description
Profile Name	Name of the Profile
Username	Username of the Cisco cBR-8 router
Password	Password of the Cisco cBR-8 router

Field Name	Description
Enable Password	Enable Password of the Cisco cBR-8 router
Connectivity Type	SSH or Telnet
Port Number	22 for SSH and 23 for Telnet

Step 4 Click **Save**.

A success confirmation message appears that a new credential profile is added.

Note
- In a large network, devices may share the same credentials.
- Smart PHY leverages SSH to log in directly to the `exec` mode on the Cisco cBR-8 router.
- When a CCAP core is added or updated using this profile, the content you specify in the credential profile is applied to the device automatically.

Editing Credential Profiles

This procedure edits credential profiles.

Step 1 At the main menu, click **Smart PHY** > **Credential Profiles**.

The **Credential Profiles** page appears.

Step 2 Click the profile that you want to view or edit.

Step 3 Update the credential profile parameters as required.

Step 4 Click **Save**.

Note A credential profile is applied to multiple CCAP cores. Once the credential profile is updated, the new set of parameters is referred by the associated devices automatically.

Changing Credential Profile for existing CCAP Core

You can change the credential profile associated with a CCAP core at any time from Smart PHY's **Inventory** page.

This procedure changes the credential profile associated with a CCAP core.

Step 1 At the main menu, click **Smart PHY** > **Inventory**.

Step 2 Check the check box associated with the CCAP core that you want to update.

Step 3 Click **Edit** and then select a different credential profile from the **Credential Profile** drop-down list.

Step 4 Click **Save**.

Performing Bulk Credential Profile Update

We recommend that you use the Smart PHY's CSV import feature so that you can perform bulk credential profile updates to CCAP cores.

This procedure makes bulk credential profile updates to CCAP cores.

Step 1 At the main menu, click **Smart PHY** > **Inventory** > **Credential Profiles**.

The **Remote PHY Devices & CCAP Cores** page appears.

Step 2 Choose the CCAP cores that you want to update and click **Export**. A CSV file is generated and downloaded to your PC.

You can use the following **Export** options:

a. To include a complete list of devices in the **Remote PHY Devices & CCAP Cores** page, click **Export**.

b. To include the selected devices, check the device check boxes that you want to modify, and click **Export**.

c. To include the filtered list of devices, enter the text in the **Search** field to filter the list of devices, and click **Export**.

Step 3 **Edit** the new CSV file, update the rows with another Credential Profile and then **Save** the file. The file must be saved in the CSV format. The Credential Profile that you want to use must exist in Smart PHY before initiating the **Import** operation.

Step 4 Click **Import**. The updated CSV file is imported.

Step 5 Review the proposed changes in the **Replace Existing Node** panel window. Click **Yes to All** to accept the changes.

Step 6 Click **Save**.

Note This operation overwrites the existing associations between a CCAP Core and the credential profile.

Deleting Credential Profile

Smart PHY allows deleting one or more credential profiles as long as the selected profiles are not in use.

This procedure deletes the credential profile.

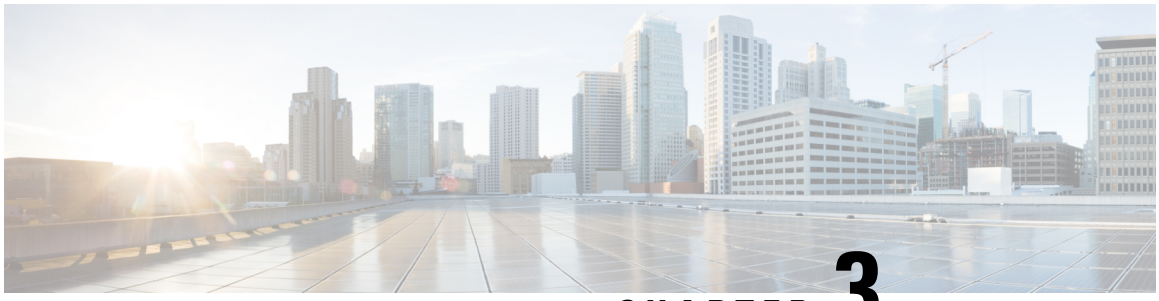
Step 1 At the main menu, click **Smart PHY** > **Credential Profiles**.

The **Credential Profiles** page appears.

Step 2 Select one or more profiles which are not in use.

Step 3 Click **Delete**.

A confirmation message appears that the credential profile is deleted.



CHAPTER 3

Managing Devices

Table 3: Feature History

Feature Name	Release information	Description
Modernized and Refreshed **Inventory** page UI	Cisco Smart PHY 22.2	Modifications in the Inventory Management Smart PHY UI: • Main menu navigation path. • Import of bulk inventory data for CCAP core and remote smart PHY devices. • Add tag to the devices. • Support to delete devices in bulk. • Filtering options based on device types or device management. • Addition of Credential profile information for the device. • Consolidation of managed CCAP actions to fetch SSH keys and enable maintenance mode for a device. • Export device data (single or bulk) in the UI. • Enhancement in table settings to edit the table columns and table appearance, and arrange the table columns as per requirement. • Enhanced search facility to search based on device parameters.
Delete RPD from Offline or under Maintenance cBR-8	Cisco Smart PHY, Release 22.4	Smart PHY allows you to delete RPDs when cBR8 is in maintenance or offline mode. Records get deleted only from Smart PHY, no transaction is performed on the CCAP device.

Feature Name	Release information	Description
Added a dedicated 360° View action	Cisco Smart PHY, Release 23.1	You can use the View 360° operation in the **Inventory** page to open CCAP 360° or RPD 360° view. You can also click on the Device Name hyperlink to open up the corresponding 360°.

Inventory and Device Management

Table 4: Feature History

Feature Name	Release Information	Description
Push Latitude and Longitude coordinates to cBR-8 routers	Cisco Smart PHY, Release 23.3	You can push latitude and longitude coordinates to all cBR-8 devices running Cisco IOS XE Dublin 17.12.1w or later, during RPD provisioning (for Principal and Aux Cores).

The **Inventory** page helps you manage, monitor, and organize Remote PHY and CCAP Core inventory. You can quickly view inventory details such as Device Name, Device IP address, MAC address, Product Type, RPD Software version, Tags, and so on. CCAP can be both managed and unmanaged; Non-Cisco RPDs, if supported by Cisco cBR-8, can also be added in Smart PHY.

Cisco Smart PHY supports 50,000 RPDs on a 3-node cluster. Because the number of RPDs provisioned by the Cisco Smart PHY scales into such huge numbers, we recommend that the Operators work on Cisco Smart PHY programmatically using its REST API.

The Following fields are available in the **Inventory** page.

Name	Description
Status	Status of the CCAP or RPD. The Status options are *resumingOp*, *fetchingKey*, *maintMode*, *offline*, *unknown*, *runningReconciliation*, *online*, *Defined*, *Maintenance*, *Processing*, *GCP*, *Warning*, or *Errored*.
Device Name	Host name of the device.
IP Address	IP address of the CCAP Core.
MAC Address	MAC address of the RPD.

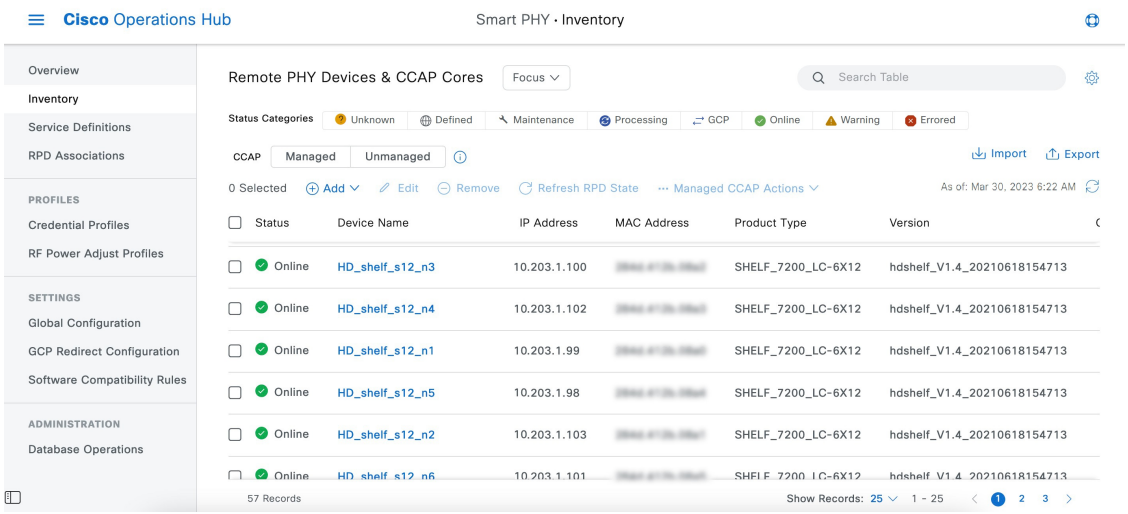
Name	Description
Product Type	Product type of the device.
Software Version	Software version of the device.
Credential Profile	Credential profile used in CCAP.
Model Number	Model number of the device.
Tags	Tags associated with the device.
Creation Date	Date and Time when the device was created.
Last Modified Date	Date and Time when the device was updated.

- Optional parameters for CCAP Cores: When adding a CCAP Core, you may add Device Name, Device description, Tags, latitude, longitude, and location information.
- Optional parameters for Remote PHY devices: When adding a Remote PHY device, you may add Device name, management IP, Tags, Smart PHY SSD profile, latitude, longitude, and location information. You may also enable/disable the selected SSD profile.

An administrator can perform the following operations from the Smart PHY inventory page.

Operation Name	Description
Add CCAP	Adding CCAP Core.
Add RPD	Adding RPD.
Edit	Editing parameters of an existing CCAP Core or RPD.
View	Opens CCAP 360° or RPD 360° view.
Remove	Remove a CCAP or RPD.
Refresh RPD State	Refresh the state of an RPD.
Fetch SSH Key	Fetches the latest SSH Key from a CCAP Core.
Enable Maintenance Mode	Moves a CCAP Core manually to Maintenance mode during a maintenance window.
Resume Normal Operation	Restores the normal mode of operation for a CCAP Core.
Import	Import Inventory data for CCAP Core(s) and RPD(s).
Export	Export Inventory data for CCAP Core(s) and RPD(s).

Figure 2: Inventory



Credential Profiles

Credential profiles are collections of device credentials to Telnet or SSH to cBR8 devices. When you add or import devices, you specify the credential profile the devices you want to use. You can apply same or different credential profiles across devices.

For information regarding Credential Management, see Credential Profiles.

Note

- We recommended that you add RPDs through Cisco Smart PHY RPD Association page and not through the Inventory page. The RPD Association page creates an inventory record automatically. For more information see, RPD Associations.
- If you are adding a Cisco cBR-8 router running Cisco IOS XE Dublin 17.12.1 or above, then you must run the **ip ssh server algorithm mac hmac-sha2-512** command on the cBR-8 router before adding it to Smart PHY. The cBR-8 router does not appear online, if you fail to run this command successfully.

Adding Devices Through GUI

Table 5: Feature History

Feature Name	Release Information	Description
Configuring Device Meta data	Cisco Smart PHY, Release 23.3	Smart PHY maintains and exposes meta data about Device Inventory additions and modifications as well as RPD Association creations and modifications. Inventory meta data can be seen in the Overview tab of the **CCAP 360° view** and **RPD 360° view** panels. Association meta data can be seen in the Associations tab of the **RPD 360° view** panels.

Use the following procedure to add a device.

Step 1 Click the main menu at the top-left of the home page, and select **Smart PHY** > **Inventory**

The **Remote PHY Devices & CCAP Cores** page displays.

Step 2 Click **Add** and choose either **CCAP Core** or **Remote PHY Device**.

Step 3 Enter the values for:

- **Managed CCAP Core**:
  - Management IP Address: Management IP address on the Cisco cBR-8 router that is reachable from the Smart PHY cluster.
  - Credential Profile: Specify the credential profile. Devices with the same credentials can use the same credential profile.
  - (Optional): Device Name
  - (Optional): Device Description
  - (Optional): Tags
  - (Optional): Location: Latitude, Longitude, and Location Name.
- **Unmanaged CCAP Core**:
  - CIN IP Address: IP address on the unmanaged Core that provides services to RPDs.
  - (Optional): Device Name
  - (Optional): Device Description
  - (Optional): Tags
  - (Optional): Location: Latitude, Longitude, and Location Name.
- **Remote PHY Device**:
  - MAC Address: MAC Address of the RPD.
  - Product Type: Specificy the RPD type. (Node, Shelf, Virtual, etc.)
  - (Optional): Device Name
  - (Optional): Management IP Address: Management IP address of the RPD.
  - (Optional): Device Description
  - (Optional): Tags
  - (Optional): Location: Latitude, Longitude, and Location Name.
  - (Optional): Exempt from Smart PHY initiated SSD operations
  - (Optional): Smart PHY SSD Profile

Step 4 Click **Add**.

Note

- Meta data about a Device including the date it was added to Smart PHY's inventory, the user who added it, the date of its last modification, and the user who last modified it can be seen in the Meta Data section of the **Overview** tab on the **Device 360° view** panel.
- If you wish to add devices in bulk, see Importing Devices in Bulk.

Accessing Device 360° Panel

Table 6: Feature History

Feature Name	Release information	Description
Device 360° Panel Enhancements	Cisco Smart PHY, Release 23.1	An Overview tab has been added to the RPD 360° View. An Uptime KPI has been added to the CCAP 360° View Overview tab.

Once a device is added, clicking on its name opens the **Device 360°** panel. The **Device 360°** panel provides you with a quick overview of the device, its state transitions and meta data such as create time, last updated time, and information about the user who added or modified the device. The **Device 360°** panel is available for both CCAP cores and RPDs.

CCAP 360°

- *Overview*: Information about the current CCAP State, Uptime, Vendor, Product Type, Software Version, Associated RPDs and Tags.
- *RPD Associations*: Information on the associated RPDs namely RPD Name, RPD status, RPD MAC Address and IP address.
- *Status History*: State transition details for the CCAP Core.

Note For Unmanaged CCAP Cores, Smart PHY only maintains information about Tags associated with the core.

RPD 360°

- *Overview*: Information about the RPD state, Hardware and Software Versions, Associated CCAP core(s) and RPD Location.
- *Association*: Information about RPD configuration parameters along with the associated Principal and Auxiliary Cores.
- *Status History*: History of all the RPD state transitions.
- *RPD Config History*: Historical list of cBR-8 CLI commands used by Smart PHY during RPD Configuration.

Importing Devices in Bulk

You can add devices to Smart PHY's Inventory by importing a CSV file. If you do not have a sample Inventory CSV file, click **Export** to create an empty Inventory CSV.

Step 1 Click the main menu at the top-left of the home page, and select **Smart PHY** > **Inventory**.

The **Remote PHY Devices & CCAP Cores** page displays.

Step 2 Click **Import**.

The **Import Devices** window displays.

Step 3 Click **Choose a file**, select the CSV file, and click **Import**.

Save the edited file in CSV format.

Note Smart PHY allows importing a maximum of 500 devices at a time using the CSV file.

Exporting Devices in Bulk

You can use the export functionality in Smart PHY to save all device information to a CSV file and download it to your PC. The generated Inventory CSV file lists all device details including: Device Name, IP Address, MAC Address, Product Type, Credential Profile, Device Location, Software Version, and so on.

Step 1 Click the main menu at the top-left of the home page, and select **Smart PHY** > **Inventory**

The **Remote PHY Devices & CCAP Cores** page displays.

Step 2 Click **Export**.

Note You can export device information in one of the following ways.

- Click **Export** to include all devices.
- Select the check boxes for the device that you want to export, and then click **Export** to include the selected devices.
- Filter the list of devices by entering text in the Search field, and then click **Export** to include the filtered list of devices.

Removing a Device from the Inventory

Step 1 At the main menu, click **Smart PHY** > **Inventory**.

The **Inventory** page displays.

Step 2 If your device isn't visible in **Remote PHY Devices & CCAP Cores** inventory table, you can use the **Search Table** field to locate it.

Step 3 Check the box that corresponds to your device, then click **Remove**.

Step 4 Review the confirmation dialog box, and then click **Remove** to proceed.

What to do next

Note

- By default, only RPDs without CCAP cores associations can be removed from Smart PHY's Inventory. When RPDs without CCAP core associations are removed, Smart PHY also deletes the RPD's association record.
- If the RPD you plan to remove from Inventory is associated with one or more CCAP cores, then you must first clear or delete the association record before proceeding with the inventory removal. You can view, clear, and delete RPD association records from the **RPD Associations** page.

Fetching SSH Keys from Cisco cBR-8

Use this procedure to fetch SSH keys.

1. Click the main menu at the top-left of the home page, and select **Smart PHY** > **Inventory**.

   The **Remote PHY Devices & CCAP Cores** page displays.
2. Select the check boxes of one or more cBR-8 routers as required.
3. Select **Fetch SSH Keys** in the **Managed CCAP Actions** drop-down list.
   - During the key fetch, the cBR-8 router's status appears as `SSHKEYFETCH_PROGRESS`.
   - The following pop-up message appears when the key fetch is successful:

     ```
     Successfully fetched SSH keys from the selected cBR-8(s)
     ```

Fetch SSH Keys Using REST API

Use the following asynchronous API to Fetch the SSH keys:

```
rpd-service-manager/rpdorch/v1/core-topology/fetch-ssh-key
```

You can fetch the SSH keys for all Cisco cBR-8 routers in the Cisco Smart PHY application, by setting the `allCore` parameter to `true` in the request message of `rpd-service-manager/rpdorch/v1/core-topology/fetch-ssh-key`.

```
{
"allCore": true,
"ipAddressList": [
"192.0.2.1", "192.0.2.100"
]
}
```

Check the status of fetching the SSH keys using the following API:

`inventory-manager/inventory/v1/device/query-device-list`

Limitations for Fetching SSH Keys

Smart PHY prohibits SSH key fetches for a cBR-8 router when:

- An SSH Key Fetch operation is already underway for a selected cBR-8 router.
- The status of the selected cBR-8 router is `Unknown`.

Note

1. Cisco Smart PHY 3.1.4 and later, supports fetching SSH keys from both online and offline Cisco cBR-8 routers.
2. Cisco Smart PHY 3.1.3 and earlier, supports fetching SSH keys only from online Cisco cBR-8 routers.

Disabling Southbound Communication to Cisco cBR-8 Router

During normal operation, Smart PHY periodically checks the managed cBR-8 routers for liveliness and configuration sync. You can disable those checks and GCP redirects to select cBR-8 routers by placing them in Maintenance Mode. Disabling the southbound communications allows the selected cBR-8 routers to undergo maintenance without interference from Smart PHY.

Setting Maintenance Mode

Use this procedure to set a cBR-8 router to maintenance mode:

1. Click the main menu at the top-left of the home page, and select **Smart PHY** > **Inventory**.

   The **Remote PHY Devices & CCAP Cores** page displays.
2. Check the check box of cBR-8 routers as required.
3. From the **Managed CCAP Actions** drop-down list, click **Enable Maintenance Mode**.

When a cBR-8 router is in the maintenance mode:

- The status of the router in the UI is `Maintenance Mode`.
- You are blocked from making any configuration changes through Smart PHY's UI or its V2 API.
- RPDs associated with the cBR-8 router are not GCP redirected.

Note Smart PHY does not block Version 1 (V1) of its RPD-pairing REST API when a cBR-8 router is in the maintenance mode. Smart PHY only blocks V2 API calls.

Resuming Normal Operation

Use this procedure to resume normal operation on a cBR-8 router:

1. Click the main menu at the top-left of the home page, and select **Smart PHY** > **Inventory**.

   The **Remote PHY Devices & CCAP Cores** page displays.
2. Select the check boxes of one or more cBR-8 routers that are in the maintenance mode.
3. From the **Managed CCAP Actions** drop-down list, click **Resume Maintenance Mode.**.
4. Review the Warning message, and then click **Resume Normal Operation**.

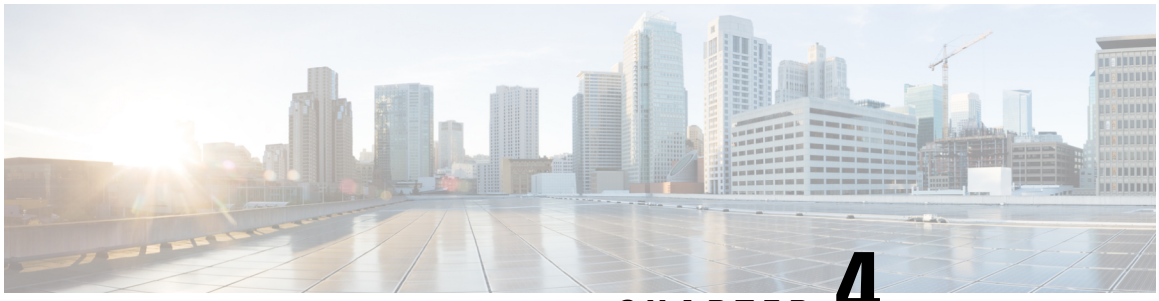
The consistency checks that Smart PHY performs when returning a cBR-8 router to normal operation often take several minutes to complete. While the checks are running the cBR-8 router's state displays as `NORMALOPS_PROGRESS`. Once the check is complete, the state of the router updates to reflect the results: `Online` or `Offline`

Restricted Cisco Smart PHY Operations

When Cisco Smart PHY detects a Cisco cBR-8 router as offline, Cisco Smart PHY does not allow you to do the following:

- Provision RPDs
- Fetch Details
- Import

However, you can edit, export, or delete the devices from the Inventory page.



CHAPTER 4

Managing RPDs

Smart PHY provides a single pane of glass to easily onboard Remote PHY Devices (RPDs). See:

Managing RPD Associations

Table 7: Feature History

Feature Name	Release information	Description
Modernized and Refreshed UI for RPD Association	Cisco Smart PHY 22.2	Modifications in the RPD Association Smart PHY UI: • Filtering based on all, provisioned and unprovisioned RPDs • Status for assigned RPDs • Import or export the database from/to local operations hub cluster or remote server. • (Optional) Password protect the database files (following password creation rules) during import and export operations. • Ability to view the history of Operations in a table format. • Enhanced search facility to search based on imported or exported RPD data. • Export the history of operations information.
US Port Description	Cisco Smart PHY 22.3	Smart PHY can be used to set a description for the Upstream Port level. Description can be set while creating and editing RPD operations. RPD-US Port Description can be set at Port 0, Port 1 or both Port 0 and Port 1 based on RPD segmentation (1x1, 1x2 and 2x2). RPD US Port Description can be Imported & Exported. US Port Description is not a service impacting change.

Feature Name	Release information	Description
Shelf and Base Power Enhancements	Cisco Smart PHY 22.3	When RPD is provisioned as a "SHELF", the ‘type shelf’ CLI is pushed to both Principal and Aux Core(s). Along with Base-power, if Tilt Pivot Freq and Tilt Slope are configured, then they are also be pushed to all the cores.
Configure US RF base-power level	Cisco Smart PHY 22.4	You can configure Upstream RF Base Power level. The valid range is -20 to 40 (dBmV).

The **RPD Associations** page enables you to add, organize, and update information about CMTS and RPD devices in the network. For more information, see:

- Remote PHY Device Association, on page 26
- Creating Service Definitions

Once an RPD is provisioned, the RPD may undergo state transitions as shown in the following table:

Table 8: RPD State Summary

RPD Summary	RPD State	Description
ERRORED	ConfigNotFound	RPD assignment is incomplete or not specified in the Cisco Smart PHY application.
ERRORED	ConfigPushError	Unable to push the RPD configuration to the CCAP core.
ERRORED	ConfigReadError	Unable to obtain the existing CCAP core configuration.
ERRORED	ConfigurationError	Assigned incorrect RPD in the Cisco Smart PHY application.
ERRORED	GcpRedirectError	Received an error from the RPD when redirecting to the CCAP core.
ERRORED	NotProvisioned	Cisco cBR-8 router is not provisioned with the RPD configuration. RPD configuration is not pushed to the Cisco cBR-8 router.
ERRORED	Offline	RPD is offline. However, RPD configuration is pushed to the CCAP core.
ERRORED	OFFLINE	RPD is offline.
ERRORED	ResourceAllocationError	Unable to allocate resources to an RPD for the assigned CCAP core or interface.
ERRORED	SSHKEYFETCH_FAILED	Unable to obtain the SSH key.

RPD Summary	RPD State	Description
GCP	GcpRedirected	Received an ACK from the RPD for the CCAP core redirect message. This redirect message captures the result of the redirect request, which is initiated by the Cisco Smart PHY application, along with the hostname, the IP address, and the interface of the redirected core.
GCP	GcpRedirectedWithException	Received an ACK from the RPD for the CCAP core redirect message. However, one of the following errors occurred: • RouterVersionIncompatible • StaticRouteNotConfigured
GCP	GcpRedirectStarted	RPD configuration is pushed to the CCAP core and the RPD is redirected to that core.
GCP	GcpRedirectStartedWithException	RPD configuration is pushed to the CCAP core and the process of redirecting the RPD to that core starts. However, one of the following errors occurs: • RouterVersionIncompatible • StaticRouteNotConfigured
GCP	GcpUp	Received GCP message from the RPD.
ONLINE	Online	RPD is online for the CCAP core.
PROCESSING	ConfigPush	Configuration push to CCAP is in progress.
PROCESSING	DeletePending	RPD pairing deletion is pending.
PROCESSING	NORMALOPS_PROGRESS	The CCAP is returning to Normal Operation.
PROCESSING	RECONCILIATION_PROGRESS	Reconciliation in progress
PROCESSING	SSHKEYFETCH_IN_PROGRESS	The process of obtaining the SSH key is in progress.
UNKNOWN	UNKNOWN	Unknown RPD State
WARNING	OnlineWithException	RPD is online, but NDF or NDR fails.
WARNING	PartialOnline	Partial services are available.
WARNING	RouterVersionIncompatible	RPD software version is incompatible with the CCAP core version.
WARNING	StaticRouteNotConfigured	Static route is not configured.

Remote PHY Device Association

The remote PHY device association feature enables you to create either a remote PHY device or in bulk using CSV upload.

Use the following table to configure the fields under **Create Remote PHY Device Association**:

Table 9: Creating Remote PHY Device Association

Field	Description
General	
RPD Device Name	Enter the RPD name. Smart PHY uses this name in the **cable rpd** command.
RPD MAC	Enter the MAC address of the RPD.
Description	Enter the RPD Description. The maximum limit is 80 characters
Tags	You can select one or more of the existing tags or create new tags and add it to the RPD Association.
Node Segmentation	Select one of the following Node segmentation options: • 1x1 • 1x2 • 2x2
Service Definition	Select the Service Definition as created in the **Service Definitions** page. If Cisco Smart PHY does not manage the principal CCAP core and if the **Principal Core** field is empty, then the **Service Definition** field is optional.
RPD Association Policies	
Allow Shelf Specific Configurations	Select the check box to configure Cisco Remote PHY Shelf 7200, Cisco Remote PHY Shelf 300, or Cisco Remote PHY Shelf 600. Cisco cBR-8 routers running Cisco IOS XE Gibraltar 16.12.1z or later support this feature. Select this check box to enable the following fields: • **Base Power (dBmV)** • **Tilt Pivot Freq (Hz)** • **Tilt Slope (dBmV)** **Note** When RF parameters and Auxiliary cores are configured for Shelf RPDs, Base Power, Tilt Pivot Frequency and Tilt Slope values are automatically configured for Aux Cores. These values are derived from DOCSIS Principal Core. RPD does not restart after updating these parameters.
Enforce Compatibility with Cisco IOS XE 17.6.1	If you select this check box, then Smart PHY generates Cisco IOS XE Bengaluru 17.6.1 compatible controller configurations for Cisco cBR-8 routers running versions of Cisco IOS XE earlier than 17.6.1.
Service Definition Overrides	
Do not Apply Network Delay	If you select this check box, then Smart PHY does not apply the selected Service Definition's Network Delay configuration to this Association. If the Network Delay is configured in the selected Service Definition, checking this box impacts the service.

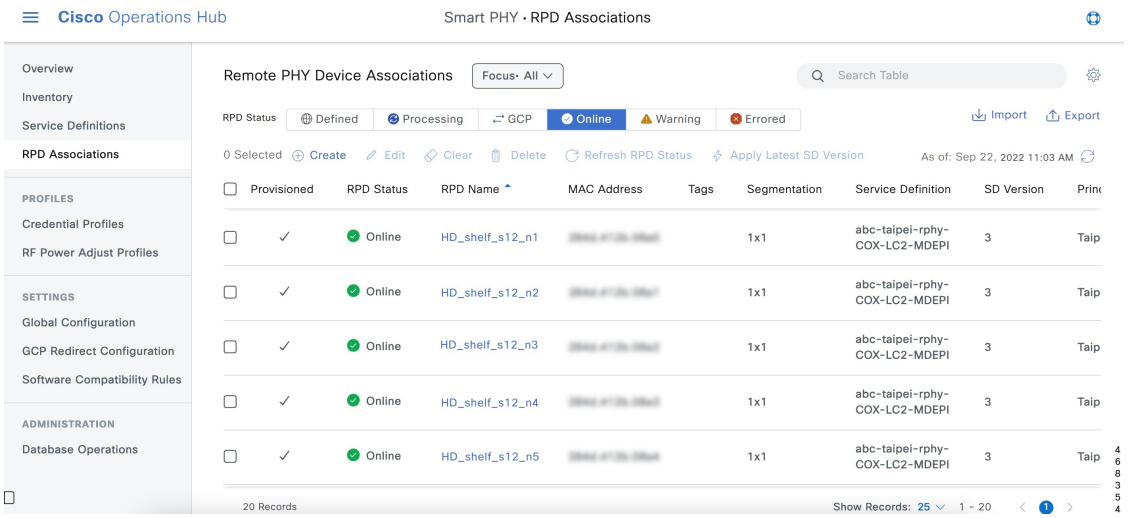
Field	Description
Override DSG Tunnel Group IDs	If you select this check box, Smart PHY overrides the selected Service Definition's DOCSIS Set-Top Gateway (DSG) Tunnel Group (TG) identifications list with the entries entered here. Seperate the entries must with a semicolon.
CCAP Cores & RF Parameters	
DOCSIS Principal Core	
Device Name	Select the name of the managed cBR-8 router or the unmanaged CCAP Core, which is the Principal CCAP Core for the RPD. If you choose a managed Principal Core, then the Core must provide the RPD with data and narrowband digital forward (NDF)/narrowband digital return (NDR) services. This core may also provide the following services: • Out-of-band (OOB) SCTE 55–1 • Video services: If there is no separate auxiliary Video Core.
Interface	If the Principal Core is a managed Cisco cBR-8 router, then select the DPIC interface used to deliver the data service. Leave this field empty if there is no Principal Core or if the Principal Core is unmanaged.
First and Second Logical DS/US Pairing	
RPD DS Port (Downstream Physical Port)	Select the Downstream RPD port of the logical pairing. The two options are `0` or `1`. Select `0` for the first pairing. This is not applicable to the second pairing for 1x1 or 1x2 node segmentation. You can select `0` or `1` for 2x2 node segmentation.
RPD US Port (Upstream Physical Port)	Select the Upstream RPD Port of the logical pairing. The two options are `0` or `1`. This is not applicable to second pairing for 1x1 node segmentation.
DS Service Group	Enter the name of the Downstream Service Group. All RPDs with the same data service group share the downstream controller for Data Service (Virtual Splitting for Data). This is not applicable to second pairing for 1x1 or 1x2 node segmentation.
US Service Group	Enter the name of the Upstream Service Group. Upstream data service group allows multiple RPDs to share the same upstream controller for upstream data traffic. Not applicable to second pairing for 1x1 node segmentation.
US Port Description	Enter a brief description for US Port, while creating and editing RPD operations. Description can be set at Port 0, Port 1 or both Port 0 and Port 1 based on RPD segmentation (1x1, 1x2 and 2x2).
Out-of-band Core	
Device Name	Enter the name of the Cisco cBR-8 router which is the CCAP core for the RPD that provides out-of-band (OOB) SCTE 55–1 service and NDF/NDR services. This field must match either the **DOCSIS Principal Core** or the auxiliary **Video Core**. Leave this field empty if the OOB 55–1 and NDF/NDR services are not used.
Interface	Select the DPIC interface to be used for out-of-band 55–1 and NDF/NDR service. If the OOB 55–1 and NDF/NDR services are not used, then leave this field empty.

Field	Description
Override OOB VOM & VARPD IDs	If you select this check box, then Smart PHY overrides the selected Service Definition's OOB Downstream & Upstream parameters (VOM ID, VOM Profile, VARPD ID, and VARPD Profile) with the values entered here.
Downstream VOM ID	OOB 55–1 Downstream Virtual out-of-band Modulator (VOM) Identification (ID). If you populate this field, it overrides the value in the Service Definition. Enter a value from 1 through 20.
Downstream VOM Profile	OOB 55–1 Downstream VOM profile. If you populate this field, it overrides the value in the Service Definition. Enter a value from 1 through 4294967295.
Upstream VARPD ID	OOB 55–1 Upstream Virtual Advanced Return Path Demodulator (VARPD) ID. If you populate this field, it overrides the value in the Service Definition. Enter a value from 1 through 32.
Upstream VARPD Profile	OOB 55–1 Upstream VARPD profile for first logical Downstream or Upstream (DS/US) pairing. If you populate this field, it overrides the value in the Service Definition. The upstream VARPD profile (upstreamVarpdProfile) and the second upstream VARPD profile (secondUpstreamVarpdProfile) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2, on page 43. Enter a value from 1 through 4294967295.
Second Upstream VARPD Profile	OOB 55–1 Upstream VARPD profile for second logical Downstream or Upstream (DS/US) pairing. If you populate this field, it overrides the value in the Service Definition. The upstream VARPD profile (upstreamVarpdProfile) and the second upstream VARPD profile (secondUpstreamVarpdProfile) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2, on page 43. Enter a value from 1 through 4294967295.
Video Core	
Device Name	Enter the name of the Cisco cBR-8 router, which is the auxiliary CCAP core for the RPD that provides video services. Leave this field empty if the principal core provides the video services.
Interfaces	Select the DPIC interfaces to be used for Video Services.

Field	Description
Video Service Groups	Video service group (VSG) names. Video is forwarded only in the downstream direction. Not applicable to second pairing for 1x1 or 1x2 node segmentation. Important**:**Cisco Smart PHY does not allow you to configure a VSG on a Downstream Port 1 (ds1) with `broadcast` keyword through the Cisco cBR-8 CLI. If you try to configure a VSG on a Downstream Port 1 (ds1) with `broadcast` keyword, then the CLI shows an error.Cisco Smart PHY maps a VSG to a video interface based on the order of the VSGs and interfaces if a VSG can map to more than one interface: • A VSG can map to more than one video interface if the video interface list includes both ports 0 and 2 or both ports 4 and 6 of one Cisco cBR-8 Series 8x10G Remote PHY Digital Physical Interface Card (CBR-DPIC-8X10G). • Cisco Smart PHY maps the first VSG to a matching Principal Core interface if present; otherwise, it maps the first VSG to the first matching video interface. • Cisco Smart PHY maps second, third, and fourth VSGs to the highest numbered matching video interfaces. Cisco Smart PHY reorders video interfaces and VSGs, so that a video interface that matches the Principal Core interface and the associated VSGs are listed first.
RF Parameters	
Base Power (dBmV)	Configure the base channel power level. Enter the value based on the type of RPD. • **Node RPDs: 20–22** • **Shelf RPDs: 24–61** If base power isn't provided by the Smart PHY, then application for Shelf RPDs, then a default value of 25 dBmV is set by cBR-8.
Tilt Pivot Freq (Hz)	Configure the frequency of the tilt pivot point. The valid range is 0–121800000. Tilt pivot point is the maximum frequency point where the Tilt Slope is applicable.
Tilt Slope (dBmV)	Configure the tilt slope. The valid range is 0–8.
RF Power Adjust Profile	You can override the RF Power Adjust Profile. This is optional. For more information, see Managing RF Power Adjust Profiles.
US Base Power RX (dBmV)	Configure Upstream RF Base Power level. The valid range is -20 to 40 dBmV.
Additional Cores	

Field	Description
Device Name	You can add additional unmanaged Cores to the GCP Redirect list by selecting them here. You can select multiple additional cores. You can configure multiple unmanaged Cores. If an unmanaged core is already selected as the **DOCSIS Principal Core**, it can't be configured again as an additional core. Thus, the unmanaged Principal Core and the unmanaged Additional Core fields are mutually exclusive. If a DOCSIS Principal Core supports dynamic addition of more Cores, then you can configure it through Smart PHY Global Configuration and avoid RPD reboot.
RPD Software	
Principal Core SSD Profile	If the Principal Core is a managed cBR-8 router, then you can use this option to set the Secure Software Download (SSD) profile ID. If the Principal Core is unmanaged or you do not wish to set the SSD profile ID, leave this field empty.

Figure 3: RPD Associations



RPD Associations

Creating an RPD Association

You can create Remote PHY Devices Associations from Smart PHY's RPD Associations page.

Step 1 At the main menu, select **Smart PHY** > **RPD Associations**.

Step 2 Click **Create** to add a single RPD Association.

The **Creating Remote PHY Device Association** page displays.

Step 3 Enter the values to the fields as seen in Table 9: Creating Remote PHY Device Association .

Step 4 Click **Save**.

Once created, you can quickly view RPD details by clicking on the RPD Name or View 360° action. In case of a *config push* and *config read* error while provisioning the RPD, you can select the **Try Again** option to retry the same operation without filling in the RPD provisioning parameters.

Meta data about an RPD Association including the date that the association was created, the user who created it, the date of its last modification, and the user who last modified it can be seen in the Meta Data section of the Associations tab on the **Device 360° view** panel.

Note

- Starting with Cisco IOS XE Dublin 17.12.1w, the latitude, longitude, and location information (configured for an RPD using the Smart PHY Inventory page), gets pushed to the CCAP Core automatically during the RPD association process. The CLI format can be seen in the **RPD 360° view > RPD Config History** tab.
- Smart PHY does not automatically push the latitude, longitude, and location information for RPDs which are already configured, when corresponding c-BR8/CCAP is upgraded to Cisco IOS XE Dublin 17.12.1w or higher.

Clearing an RPD Association

You can clear one or multiple Remote PHY Device association records from Smart PHY's RPD Associations page.

When you perform the clear operation, all provisioning related configuration parameters (Node Segmentation, Service Definition, CCAP Cores, etc.) are removed from the association record. Additionally, Smart PHY removes all relevant CLI configuration commands from CCAP cores previously associated with the now cleared record. The only values retained in a cleared association record are: RPD Name, MAC Address, and Description.

Step 1 At the main menu, select **Smart PHY** > **RPD Associations**.

Step 2 Check the box that corresponds to your RPD association record, then click **Clear**.

Step 3 Review the warning message, then click **Clear** to proceed.

Deleting an RPD Association

You can delete one or multiple Remote PHY Devices Associations from Smart PHY's RPD Association page. When you perform the delete operation, Smart PHY removes all relevant CLI configuration commands from CCAP cores associated with the record before permanently deleing the association record. The only value that remains in the RPD Associations page after deletion is the RPD MAC Address.

Step 1 At the main menu, select **Smart PHY** > **RPD Associations**.

Step 2 Check the box that corresponds to your RPD association record, then click **Delete**.

Step 3 Review the warning message, then click **Delete** to proceed.

Note

- If you delete an RPD association record when one or more of its associated CCAP Cores is in maintenance or offline mode, Smart PHY deletes the record. Smart PHY doesn't remove relevant CLI configuration commands from the associated CCAP Cores. At the end of the delete operation, we recommend that you manually review the CLI configuration of the relevant CCAP Cores. Any CLI configuration pertaining to the RPD in question should be manually removed.
- Once an RPD is added or modified, Smart PHY updates Creation Time, Last Modified Time, and information about the user who created or modified the RPD. The meta data is visible in **RPD 360°** page.

Refreshing RPD Status

You can refresh the status of Remote PHY Device from Smart PHY's RPD Associations page.

Step 1 At the main menu, select **Smart PHY** > **RPD Associations**.

Step 2 Select an RPD and click **Refresh RPD Status** to refresh its status from the associated CCAP device.

Applying Latest SD Version

YYou can apply the latest version of Service Definitions to one or multiple Remote PHY Devices from Smart PHY's RPD Associations page.

Step 1 At the main menu, select **Smart PHY** > **RPD Associations**.

Step 2 Select one or multiple RPDs.

Step 3 Click **Apply Latest SD Version**.

Creating RPD Associations in Bulk Through CSV Import

You can provision RPDs in bulk, using the **Import** option available in the **RPD Associations** page.

Step 1 At the main menu, select **Smart PHY** > **RPD Associations**.

Step 2 Click **Import**.

Step 3 Choose a CSV file containing RPD Association records. Ensure that all the provisioning parameters are present in the CSV file.

Step 4 Import

Note When you attempt to provision Data and Auxiliary services such as Video or OOB on two different cores, Smart PHY considers the operation as **atomic**. RPD is provisioned successfully when both Data and Auxiliary services are configured successfully. If it fails even in one of the cores, the entire operation is rolls back.

Task Viewer

Table 10: Feature History

Feature Name	Release Information	Description
Task Viewer Panel Enhancement	Cisco Smart PHY, Release 23.3	In the Task Viewer Panel, you can click an RPD in either the **Queued Tasks** tab or **Completed Tasks** tab to open the **RPD Panel**. The **RPD Panel** shows additional information about the selected RPD.
Task Viewer Panel	Cisco Smart PHY, Release 23.2	You can view the status of both queued and completed provisioning operations by opening Smart PHY's Task Viewer panel.

While most provisioning operations submitted to Smart PHY execute quickly, in some circumstances it may take Smart PHY several minutes, or even tens of minutes, to execute all pending operations. This is due to the asynchronous nature of RPD provisioning, which requires generating and then pushing CLI configuration commands to one, or more, managed cBR-8 routers.

Users can view the status of both queued and completed provisioning operations by opening Smart PHY's Task Viewer panel. To open the Task Viewer panel, click the Task List icon located in the top right corner of the Smart PHY WebUI, immediately to the left of the Support icon. By default, the Task Viewer panel opens with the **Queued Tasks** tab selected.

Queued Tasks

The **Queued Tasks** tab shows an ordered list of queued tasks that Smart PHY is either preparing to execute or actively executing.

The list includes the following information about each task:

- Date Initiated
- Task ID
- Operation (type)
- RPD Name
- CCAP Core Name
- Status (Preparing or Executing)

The user can filter the list by:

- Operation Type (Add, Remove, Modify)
- Status (Preparing, Executing)

A search field and export action are also available to the user. Once a task is executed, its result can be seen by clicking the **Completed Tasks** tab.

Completed Tasks

\

The **Completed Tasks** tab shows a sorted list of completed tasks.

The list includes the following information about each task:

- Date Initiated
- Result
- Task ID
- Operation (type)
- RPD Name
- CCAP Core Name

The user can filter completed tasks by:

- Operation Type (Add, Remove, Modify)
- Result (Success, Fail)
- Date Initiated (Last 24hr, Last 7 days, Last 30 days, All Time)

A search field and export action are also available in the panel.

Task Details

Clicking a Task ID in either the Queued Tasks tab or Completed Tasks tabs opens the Task Details panel. The Task Details panel shows additional information about the selected task.

Depending on the operation type and result, the additional information could include:

- Initiator Username
- Initiator Method
- Operation Type
- RPD Name
- CCAP Core Name
- Date & Time Initiated
- Duration
- Result
- Reason (in case of an error)
- Pushed CLI Configuration (in case of success)

RPD Details

Clicking an RPD in either the Queued Tasks tab or Completed Tasks tabs opens the RPD Panel. The RPD Panel shows additional information about the selected RPD.

Depending on the operation type and result, the additional information could include:

- Description

- MAC address
- Vendor & Model
- RPD type
- Software Version
- Tags
- Status
- CCAP Core Summary
- Location

Service Definitions

Feature History

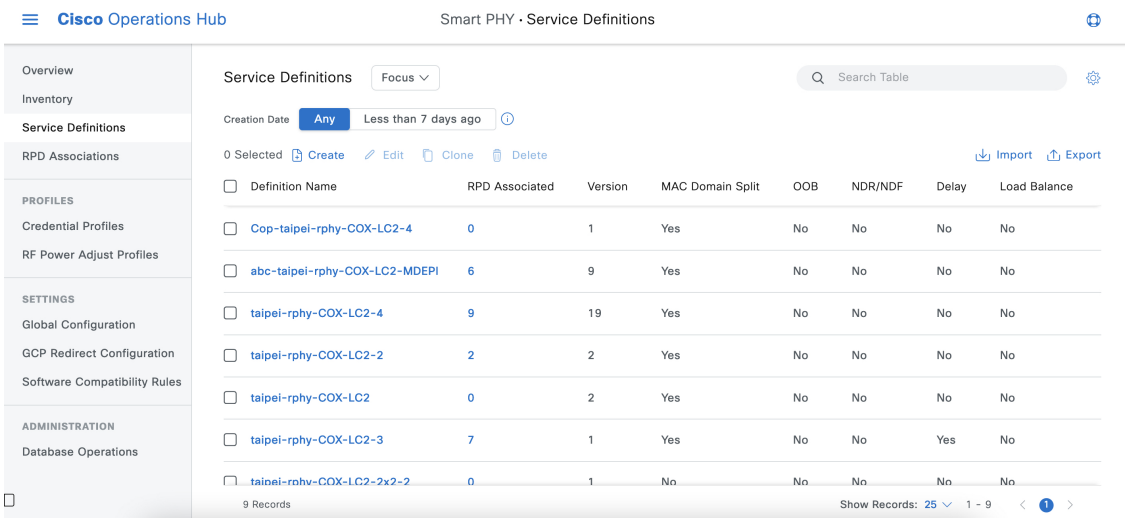
Feature Name	Release information	Description
Service Definition Enhancement	Cisco Smart PHY 22.2	• **Service Definition Versions**: Service definition now provides versioning and enables you to track the Service Definition changes. This identifys the RPDs running specific versions of a Service Definition. • **Forced Config Push**: You can edit Service Definitions and push service impacting changes to RPD(s) using the Force Config push option. Smart PHY deletes and re-adds the RPDs automatically. • **RF Profile Overwrite**: You can overwrite the RF Power Adjust Profile during RPD provisioning.
Modernized and Refreshed Service Definition UI	Cisco Smart PHY 22.2	• Support to create, edit, and clone service definitions. • Support to bulk delete the service definitions. • Filter based on with assigned and without assigned RPDs. • Ability to view device information, configuration, and version details in the Service definition name link. Ease to edit or clone from **Service Definitions Details** page. Enhanced Search option based on service definitions configured. • Export service definitions from GUI. • Import a maximum of 500 service definition using CSV file. • Enhancement in table settings to edit the table columns and table appearance, and arrange the table columns as per requirement.

Feature Name	Release information	Description
Apply Latest Service Definition Version	Cisco Smart PHY 22.3	You can assign the latest service definition to one or more RPDs in RPD Association page. Smart PHY handles service affecting changes smartly and reprovisions the RPDs in case service affecting changes are applicable in the latest version of the Service Definition.

Service Definitions are a logical grouping of the various configuration parameters that are needed to complete the RPD provisioning. You can manage Service Definitions on Smart PHY's **Service Definition** page.

When an RPD Association is created, or modified, the parameters that are configured in the selected Service Definition, are applied to the RPD.

Figure 4: Service Definitions



Creating Service Definitions

Step 1 At the main menu, select **Smart PHY** > **Service Definitions**.

The **Service Definitions** page appears.

Step 2 Click **Create**. The **Create Service Definition** page displays.

Step 3 Fill the **Name**, **Description**, and **Tags** fields. If you have multiple Service Definitions, then enter concise, informative, and detailed descriptions for these fields.

Step 4 Check the **Default** check box to make this the default Service Definition for Smart PHY. This is optional.

Step 5 Enter the remaining Service Definition parameters listed in the following table. All fields that are not marked as optional, are mandatory. Cisco Smart PHY supports unique downstream (DS) and upstream (US) configurations for each port of RPD 2x2.

Table 11: Service Definition Parameters

Field	Description	Service Affecting Parameter
Name	Name of the Service Definition.	No
Description	A brief description about the Service Definition	No
Tags	New or previously created user-defined tags can be assigned to the Service Definition.	No
General Parameters		
Event Profile ID	RPD Event Profile Set.	No
Remote DOCSIS Timing Interface ID	Remote DOCSIS Timing Interface (R-DTI) Set.	No
Pilot Tone Profile ID	Pilot tone profile.	Yes
Cable DSG TGs	DSG tag IDs.	Yes
Logical Pairings		
Split the MAC Domain	Select this box to have Smart PHY split the MAC Domain between two fiber nodes that share the same downstream controller.	Yes
First Logical DS/US Pairing		
Service Group Profile	Pre-existing Cable Service Profile-Group on the Cisco cBR-8 router.	Yes
Downstream Controller Profile	Primary downstream CCAP controller profile.	Yes
RF Power Adjust Profiles	You can adjust the power for the downstream RF channels using RF Power Profiles.	No
Upstream Controller Profile	Primary upstream CCAP controller profile.	Yes
Second Logical DS/US Pairing		
Switch	Use this option to enable the second logical DS/US pairing. The Cisco Smart PHY application supports different controller profiles and fiber node configurations for second logical pairing in 2x2 RPD.	Yes
Service Group Profile	Pre-existing Cable Service Profile-Group on the Cisco cBR-8 router.	Yes
Downstream Controller Profile	Secondary downstream CCAP controller profile.	Yes
RF Power Profiles	It allows you to adjust power for downstream RF channels using RF Power Profiles. For more information, see Managing RF Power Adjust Profiles.	No
Upstream Controller Profile	Secondary upstream CCAP controller profile.	Yes
Network Delay		

Field	Description	Service Affecting Parameter
Type:	Two options are available: • **DEPI Latency Measurement**—The cBR-8 router periodically measures the network latency between itself and the RPD, and dynamically updates the cable map advance. Range is the interval that is measured in seconds. The valid range for measuring DLM is 1–420 seconds.*Measure only*—Choose to measure network latency between the CCAP core and the RPD. This option is not for updating the cable map advance. You can select this option for a service definition in use, but cannot uncheck it. • **Static**—The cable map advance is adjusted by a fixed amount. The valid range is 30–100,000 microseconds.This range is the Converged Interconnect Network (CIN) delay in microseconds. CIN is the network between the CCAP core and RPD. For more information, see *DEPI Latency Measurement in the Service Template* section in this document.	No
Out Of Band		
Out Of Band Downstream		
Virtual out-of-band Modulator ID	OOB 55–1 Downstream Virtual out-of-band Modulator (VOM) identification (ID).	No
Virtual out-of-band Profile	OOB 55–1 Downstream VOM profile.	No
Out Of Band Upstream		
Virtual Advanced Return Path Demodulator ID	OOB 55–1 Upstream Virtual Advanced Return Path Demodulator (VARPD) ID.	No
Port 0 Virtual Advanced Return Path Demodulator Profile	OOB 55–1 Upstream VARPD profile for first logical downstream/upstream (DS/US) pairing.The upstream VARPD profile (upstreamVarpdProfile) and the second upstream VARPD profile (secondUpstreamVarpdProfile) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2, on page 43.	No
Port 1 Virtual Advanced Return Path Demodulator Profile	OOB 55–1 Upstream VARPD profile for second logical downstream/upstream (DS/US) pairing.The upstream VARPD profile (upstreamVarpdProfile) and the second upstream VARPD profile (secondUpstreamVarpdProfile) can have the same value. For more information, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2, on page 43.	No
Narrowband Digital Forward & Return		
Port	Choose Port 0, or Port 1.	No

Field	Description	Service Affecting Parameter
Pseudowire Name	ForwardNarrowband digital forward pseudowire name.Supports up to three pseudowire names and profile ID sets per DS port. ReturnNarrowband digital return pseudowire name. Supports up to three pseudowire names and profile ID sets per US port.	No
Profile ID	• NDF—NDF profile ID corresponding to the above NDF pseudowire. • NDR—NDR profile ID corresponding to above NDF pseudowire.	No
Load Balancing		
Text Field	Use the Cisco NSO Ntool to create a Load Balance group config-template encoded in XML. Enter the template in the text entry field.	No

Step 6 Click **Save** to save the information to Smart PHY or click **Save & Assign** to save the information and assign this Service Definition to one or more RPDs.

Note Once Service Definition is created, you can see more parameters such as **Service Definition Version**, **Create**, **Update timestamp** and **Owner information** which is the user who created this Service Definition in the Service Definition page.

Viewing and Editing Service Definitions

Once you create a Service Definition, you can view and edit it anytime. You can view the Service Definition information after a service is created and associated with the RPDs.

- You can view the Service Definition information after a service is created and associated with the RPDs. For more information, see Viewing Service Definitions, on page 41.
- You can dynamically edit the parameters of a Service Definition including its name even when the RPDs are associated to service definitions. For more information, see Editing Service Definitions, on page 41.

Applying Latest Version of a Service Definition

Once a Service Definition is edited, you can apply its latest version to one or multiple RPDs from 'Assigned RPDs' tab of Service Definition Details panel. To assign the latest version:

1. At the main menu, select **Smart PHY** > **Service Definitions** and click a Service Definition name. The **Service Definition Details** panel.
2. Select **Assigned RPDs** from the **Service Definition Details** panel.
3. Identify and select the RPDs where the latest version needs to be configured.
4. Click **Apply Latest SD Version** to apply the latest Service Definition version.

Once the operation is successful, you can see the **LATEST** tag in the version column, confirming that the RPD running the latest Service Definition version.

Viewing Service Definitions

The procedure enables you to view service definition details in the **Service Definitions** page.

Procedure

	Command or Action	Purpose
Step 1	At the main menu, click **Smart PHY** > **Service Definitions**.	The **Service Definitions** page appears.
Step 2	Click any **Service Definition** to view the following details:	***Table 12: Service Definition Fields***

Field Name	Details
Overview	Displays the overview of the Service Definition and contains the version, description, tags, create time, last modification details, and RPDs Assigned.
Configurations	Displays the details of the various configuration parameters that are used in the Service Definition.
Assigned RPDs	Displays the list of RPDs assigned to that Service Definition.
Version History	Displays the history of the changes for a Service Definition in chronological order.

Editing Service Definitions

You can dynamically edit the parameters of a Service Definition including its name even when the RPDs are associated to service definitions. You can then apply the changes to one or more RPDs that are already running that specific service definition. If a Service Definition is edited, then its version gets updated and is visible in the Service Definition page.

Editing a Service Definition may affect the service particularly, when you want to apply the changes to RPDs. On the Smart PHY UI, if a flag is visible next to a Service Definition parameter, it signifies that it is a service impacting field. You may get `config push error` from the Cisco cBR-8 router and may have to reprovision the RPD. However, if you don't want to reprovision the RPDs, you can use the updated service definition parameters to provision new RPDs in the network. For more details, see Service Definitions, on page 36.

Also, if the Cisco cBR-8 router is in maintenance mode, you cannot propagate these changes to the RPDs. In these scenarios, configuration error messages appear in the **RPD 360** page.

This procedure edits a Service Definition.

Step 1 At the main menu, click **Smart PHY** > **Service Definitions**.

The **Service Definitions** page appears.

Step 2 Select the service definition which you wish to update and click **Edit**.

Step 3 Update the required fields.

Step 4 Click **Save** or **Save & Assign**.

Note
- **Save** allows you to save the changes to the Cisco Smart PHY database.
- **Save & Assign** allows you to save the changes to the Cisco Smart PHY database and then recommends that you to apply the changes to one or more RPDs.

Once a service definition is updated, its version is incrementally updated and the changes are captured under **Version History**.

Cloning Service Definitions

You can create a new Service Definition by cloning an existing Service Definition. Cloning creates a copy of selected Service Definition, which you can edit. Cloning saves time if you only intend to make minor changes to an existing Service Definition.

Procedure

	Command or Action	Purpose
Step 1	At the main menu, click **Smart PHY** > **Service Definitions**.	The **Service Definitions** page appears.
Step 2	Select the check boxes of the Service Definitions that you wish to clone.	
Step 3	Click **Clone**.	The **Clone Service Definition** panel displays. The name of the cloned Service Definition is prefixed with **Copy-**.
Step 4	Edit the parameters that you wish to change and rename the Service Definition.	
Step 5	Click **Clone**.	

Provisioning an RPD for Video Support

Table 13: Feature History

Feature Name	Release Information	Description
Multi Core Atomic Provisioning	Cisco Smart PHY, Release 22.2	• Atomic transactions when multiple cores are involved. • Automatic rollback on transaction failure.
Support for two Video Core Chassis	Cisco Smart PHY, Release 23.1	Smart PHY supports the configuration of Video Services from more than one source chassis.

Cisco Smart PHY can be configured to use distinct Cisco cBR-8 routers as the DOCSIS Principal core and auxiliary video core.

The DOCSIS configuration is pushed to the Principal core and the video configuration is pushed to one or multiple Video Auxiliary cores. You can configure the OOB core to be either the Principal core or one of the Video Auxiliary cores. The OOB 55-1 and NDF/NDR configurations are pushed to the OOB core through the OOB core interface. You can configure only the Pilot tone, SSD, and DLM on the Principal core.

Important When integrating Viavi with RPD, NDF or NDR must be configured on the Principal Core. Viavi communicates with the core using SNMP MIBs that are only available on the Principal Core.

Cisco Smart PHY can also provision an RPD for supporting video using a standalone Cisco cBR-8 router or some other Core that is not managed by Cisco Smart PHY, as the Principal core.

If the principal core is not managed by Cisco Smart PHY and you do not have OOB 55–1 configuration on the auxiliary video core, the RPD Assignment does not require Service Definition configuration.

Note

- When you provision data and video services on two different cores simultaneously, Smart PHY considers it as an **atomic transaction**. In other words, an RPD is provisioned successfully when both data and video services are configured successfully. If the configuration of either core fails, then the entire operation is rolled back.
- When you provision data and video services on different cores at different point of time, each provisioning operation is considered as an independent transaction.
  - If RPD is online with both Principal Core and separate Video Auxiliary Core, and you remove the Video Core configuration, the RPD reboots and becomes online with only the Principal Core.
  - If the RPD is online with only the Principal Core, and later if you configure a separate Video Auxiliary Core, the RPD does not reboot automatically. You must manually reboot the RPD to get it to redirect to the new Video Core. After the RPD reboots, it becomes online with both cores.

Caution When you use the REST API to provision an RPD with separate video cores, you must use only version 2 (V2) RPD-pairing REST API. If you use V1 RPD-pairing API to provision an RPD with separate video cores, it may lead to data corruption. Also, version 1 (V1) of the RPD-pairing REST API does not support features such as 1x2 node segmentation, 2x2 node segmentation, OOB override, DLM, or separate video cores.

Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2

The Cisco cBR-8 router supports configuring the same profile to both upstream physical RF ports in an RPD. Service providers can expand the OOB 55–1 service group on to the second US port without the need for extra hardware.

This feature is available only in the following versions of Cisco cBR-8 series routers:

- Cisco IOS XE Fuji 16.8.1 and earlier
- Cisco IOS XE Amsterdam 17.3.1x and later

Note When you provision data and OOB services on two different cores, Smart PHY considers it as an **atomic transaction**.

Example

```
cable rpd SAME_OOB_US_PROFILE
identifier 2222.5555.2323
core-interface Te6/1/2
principal
rpd-ds 0 downstream-cable 6/0/1 profile 1
rpd-us 0 upstream-cable 6/0/1 profile 1
rpd-us 1 upstream-cable 6/0/2 profile 1
core-interface Te6/1/2
rpd-ds 0 downstream-oob-vom 1 profile 100
rpd-us 0 upstream-oob-varpd 1 profile 101
rpd-us 1 upstream-oob-varpd 1 profile 101
r-dti 1
rpd-event profile 0
cable fiber-node 2
downstream Downstream-Cable 6/0/1
downstream sg-channel 0 23 downstream-Cable 6/0/1 rf-channel 0 23
upstream Upstream-Cable 6/0/1
upstream sg-channel 0 1 upstream-Cable 6/0/1 us-channel 0 1
upstream sg-channel 2 3 peer-node-us
service-group managed md 0 Cable 6/0/1
service-group profile ram_SG1
cable fiber-node 3
downstream Downstream-Cable 6/0/1
downstream sg-channel 0 23 downstream-Cable 6/0/1 rf-channel 0 23
upstream Upstream-Cable 6/0/2
upstream sg-channel 2 3 upstream-Cable 6/0/2 us-channel 0 1
upstream sg-channel 0 1 peer-node-us
service-group managed md 0 Cable 6/0/1
service-group profile ram_SG1
```

In REST API, the following restrictions are applicable:

- OOB is enabled only if the following four parameters are configured within the specified range:
  - downstreamVomId
  - downstreamVomProfile
  - upstreamVarpdId
  - upstreamVarpdProfile
- The NDF configuration is independent of the OOB downstream and upstream configurations.
- NDR configuration is independent of OOB downstream and upstream configurations.

REST set-service-template

```
{
  "autoAccept": false,
  "defaultFlag": false,
  "dlmMeasureOnly": false,
  "dsgTunnelGroupIDs": "1",
  "elementsList": [
    {
```

```
      "description": "Service profile with 1.5Gbps Data Service. 16x4 DS/US SG channels",
      "downstreamControllerProfile": 0,
      "downstreamVomId": 1,
      "downstreamVomProfile": 1,
      "eventProfile": 0,
      "mdSplitting": false,
      "rdtiConfig": 0,
      "serviceGroupName": "SGProfile",
      "serviceType": "Data",
      "svcNdfProfiles": [
        {
          "portNum": 0,
          "profileId": 100,
          "pwName": "name1"
        }
      ],
      "svcNdrProfiles": [
        {
          "portNum": 0,
          "profileId": 100,
          "pwName": "name1"
        }
      ],
      "upstreamControllerProfile": 0,
      "upstreamVarpdId": 1,
      "upstreamVarpdProfile": 1
    }
  ],
  "loadBalanceXml": "XML String",
  "name": "Gold",
  "networkDelayDlm": 10,
  "networkDelayStatic": "null",
  "pilotToneProfile": 0,
  "secondUpstreamVarpdProfile": 1
}
REST  get-service-template Response Content Type

{
  "autoAccept": false,
  "defaultFlag": false,
  "dlmMeasureOnly": false,
  "dsgTunnelGroupIDs": "1",
  "elementsList": [
    {
      "description": "Service profile with 1.5Gbps Data Service. 16x4 DS/US SG channels",
      "downstreamControllerProfile": 0,
      "downstreamVomId": 1,
      "downstreamVomProfile": 1,
      "eventProfile": 0,
      "mdSplitting": false,
      "rdtiConfig": 0,
      "serviceGroupName": "SGProfile",
      "serviceType": "Data",
      "svcNdfProfiles": [
        {
          "portNum": 0,
          "profileId": 100,
          "pwName": "name1"
        }
      ],
      "svcNdrProfiles": [
        {
          "portNum": 0,
          "profileId": 100,
```

```
          "pwName": "name1"
        }
      ],
      "upstreamControllerProfile": 0,
      "upstreamVarpdId": 1,
      "upstreamVarpdProfile": 1
    }
  ],
  "error": {
    "errorCode": "RecordNotFound",
    "errorMessage": "Record not found : <Record type> <identifier>",
    "errorTag": "Record not found",
    "errorType": "User"
  },
  "loadBalanceXml": "XML String",
  "name": "Gold",
  "networkDelayDlm": 10,
  "networkDelayStatic": "null",
  "pilotToneProfile": 0,
  "rpdsAssigned": 0,
  "rpdsProvisioned": false,
  "secondUpstreamVarpdProfile": 1,
  "status": "Success or Failure. If Failure check Error field for error details."
}
```


Configuring Video Services

You can configure video service in a Cisco cBR-8 router using Cisco Smart PHY by wiring the video interfaces and video service groups (VSG).

Cisco Smart PHY provides a clear mapping between VSG and video interfaces. RPD node segmentation determines the number of VSGs that you can choose for a video interface.

Prerequisites

Create video service groups (VSG) in the Cisco cBR-8 router, before you configure a video service for each RPD. There are two ways to create VSGs:

- Manual method(Recommended): Provide a logical name for the VSG. Example: `cable virtual-service-group 18528 downstream-video 1/0/8 profile 101`
- Automatic method: When you assign a controller to a Cisco cBR-8 router profile that has video services, Cisco cBR-8 creates a VSG with a random name.

For more information, see Cisco cBR Converged Broadband Routers Video Configuration Guide for Cisco IOS XE Cupertino 17.9.

Adding a New Video Interface

Use the following task to add a new video interface.

1. Click the main menu at the top-left of the home page, and select > **Smart PHY** > **RPD Associations**. The **Remote PHY Device Associations** page displays.
2. Click the **Create** button. The **Create Remote PHY Device Association** page displays.
3. Add single or multiple entries in the **Video Core Interface** and **Video Service Group** fields.
4. Click the **Save** button.

You can also import CSV files from the previous versions of the Cisco Smart PHY application which have video configurations. You can also import a database that is exported from a previous version of the Cisco Smart PHY application.

Configuring VSG Using API

You can configure VSG using the Cisco Smart PHY API `setrpdpairinglist`.

This API is backward compatible. It has an extra `videointerfaces` field under `port-config`. The existing video service group mapping with the video interfaces, remains without any changes.

Example: Sample RPD Pairing API

```
{
  "setrpdpairinglist": [
    {
      "name": "rpd03",
      "previousname": "rpd03",
      "macaddress": "00049f320825",
      "description": null,
      "approvalstate": "approved",
      "servicetemplate": "d8-sg-split-rdti1",
      "gpslocation": {
        "genericlocation": "",
        "latitude": "",
        "longitude": ""
      },
      "ssdprofileid": 1,
      "disablenetworkdelay": false,
      "preconfigure": true,
      "nodesegmentation": "rpd_1x1",
      "additionalcores": [
        "2004:172:30:0:2eab:a4ff:feff:f36c"
      ],
      "assignedcores": [
        {
          "servicetype": "data",
          "mgmtcore": "video-lwr-s-d8.cisco.com",
          "rpdconnectioninterface": "tengigabitethernet9/1/0",
        },
        {
          "servicetype": "video",
          "mgmtcore": "video-lwr-s-d8.cisco.com",
          "rpdconnectioninterface": "tengigabitethernet9/1/0",
        },
       {
          "servicetype": "video",
          "mgmtcore": "video-lwr-s-d8.cisco.com",
          "rpdconnectioninterface": "tengigabitethernet9/1/6",
        },
        {
          "servicetype": "oob",
          "mgmtcore": "video-lwr-s-d8.cisco.com",
          "rpdconnectioninterface": "tengigabitethernet9/1/0",
        }
      ],
      "portconfigs": [
        {
          "dsport": 0,
          "usport": 0,
          "dsservicegroup": "sg-9-0-0",
          "usservicegroup": "sg-upstream-9-0-0",
          "videoservicegroups": [
```

```
            "vsg1",  // Index 0 is read along with video interface index 0
            "vsg2",  // Index 1 is read along with video interface index 1
            "vsg3"  // Index 2 is read along with video interface index 2
          ],
          "videointerfaces":[
            "tengigabitethernet9/1/0", // Index 0 is read along with vsg index 0
            "tengigabitethernet9/1/6", // Index 1 is read along with vsg index 1
            "tengigabitethernet9/1/6" // Index 2 is read along with vsg index 2
           ]
        }
      ]
    }
  ]
}
```

Limitations

- If you use the `setrpdpairinglist` API without the `videoInterfaces` attribute under `port-configs`, Cisco SmartPHY performs an ambiguity resolution. This process does not provide a clear one-to-one mapping.
- If two or more VSGs are configured under the same interface, the `videointerfaces` must repeat to match the one-to-one mapping.
- If you do not add the video interfaces under port-config and the assigned-cores, then the application shows an error.
- The size of the list of video interfaces and the VSGs must be the same.
- You can only map a VSG to a single interface. However, you can map the VSG to the same interface in a different port.
- If you configure a video interface without mapping to a VSG, then the application ignores the video interface.

Secure Software Download for RPD

Table 14: Feature History

Feature Name	Release Information	Description
RPD Secure Software Upgrade Enhancements	Cisco Smart PHY, Release 23.3	In this release: • Smart PHY SSD Profiles support the inclusion of an RPD Model. In previous Smart PHY releases, only the RPD Vendor is supported. • Software Compatibility Policies support attaching more than one Smart PHY SSD Profile. • The **History tab** in the **Secure Software Download** page is enhanced to include more information about each Smart PHY initiated SSD operation.

Feature Name	Release Information	Description
RPD Secure Software Upgrade	Cisco Smart PHY, Release 23.2	You can upgrade Remote PHY Device (RPD) from Smart PHY using the Secure Software Download (SSD) mechanism.

You can upgrade Remote PHY Device (RPD) from Smart PHY using the Secure Software Download (SSD) mechanism. To configure RPD software upgrades or downgrades, create SSD profiles and Software Compatibility Policies in Smart PHY. During RPD boot up phase (that is, GCP initialization), Smart PHY refers to these policies and triggers RPD upgrade using SSD IRA.

Creating SSD Profiles

You can control the RPD software that is deployed in the network by creating SSD profiles. Use the following steps to create a profile:

1. At the Main Menu, select on **Smart PHY** > **Secure Software Download**.
2. Click **Create SSD Profile** An SSD profile captures the following information.

Table 15: Create SSD Profile Fields

Name	Description
SSD Profile Name*	Name of the SSD profile
Make this a catch-all profile check box	A Catch-all SSD profile is used to ensure RPDs, that wouldn't otherwise be eligible for Smart PHY initiated SSD operations, are running a specific software image
Enforce this catch-all profile switch	This switch only applies to Catch-all SSD profiles. By default, the switch is off. When the switch is on, eligible RPDs that match the Catch-all SSD profile's criteria are instructed to execute an SSD operation
RPD Vendor*	Name of RPD Vendor
RPD Model	Model of the RPD
Transport*	TFTP or HTTP used to download RPD software image.
File Server IP Address or Hostname	Hostname or Server where the RPD Software (image) is available
File Path	Directory path to the image file
File Name*	Name of the File
Manufacturer CVC	Manufacturer CVC chain to enable the RPD to download the code file from the download server.
Cosigner CVC	Cosigner CVC chain to enable the RPD to download the code file from the download server

Note * indicates a mandatory field.

Editing and Deleting SSD Profiles

Once an SSD profile is created, you can edit and delete the SSD profile anytime. However, a profile which is associated with a Software Compatibility policy cannot be deleted till it is removed from the associated policy.

Rules for Upgrading RPD

Table 16: Rules for Upgrading RPD

Priority	Rule	Upgrade RPD
1	cBR-8 SSD Profile added for RPD	No
2	Exempt Flag set for RPD in Smart PHY Inventory page	No
3	Smart PHY SSD Profile added for RPD	Yes, when the condition is met
4	Smart PHY SSD Compatibility Policy applied to RPD's DOCSIS Principal Core	Yes, when the condition is met
5	Smart PHY SSD Profile marked as "Catch-All"	Yes, when the condition is met
6	None of the previous conditions are met	No

Creating Software Compatibility Policies

Once an SSD profile is created, it must be enforced to control the RPD software being deployed. Multiple SSD profiles can be attached to a Software Compatibility Policy. In a Smart PHY cluster, multiple policies can be active at any given point.

Restrictions

- Catch-all SSD profiles cannot be attached to a Software Compatibility Policy.
- SSD Profiles with matching RPD vendor names, but differing RPD software images cannot be attached to the same Software Compatibility Policy.
- SSD Profiles with matching RPD vendor names and RPD models, but differing RPD software images cannot be attached to the same Software Compatibility Policy.

A Software Compatibility policy contains the following information.

Table 17: Software Compatibility Policy

Name	Description
Policy Name	Name of the Policy.
Enforce Flag	To enforce a policy. Can be enforced during creation time or at a later time.
Cisco IOS-XE Software Version	Version of a CCAP core.
SSD Profile Name	The SSD profile which must be enforced.

Editing & Deleting Software Compatibility Policy

Once a Software Compatibility Policy is created, you can edit, enforce, and delete the SSD policy, anytime.

SSD History

The **SSD History** tab captures the list of RPDs upgraded from Smart PHY.

Exempting Smart PHY Initiated SSD Operation

You can exempt RPDs from Smart PHY initiated SSD operations by editing the RPD's Inventory record.

1. At the Main Menu, select on **Smart PHY** > **Inventory**.
2. Select the RPD to be exempted.
3. Click the check box, **Exempt from Smart PHY Initiated SSD Operations**.

As long as an RPD is marked as exempt, Smart PHY never instructs it to perform an SSD operation.

cBR-8 Configuration Reconciliation

Feature History

Table 18: Feature History

Feature Name	Release information	Description
cBR-8 Configuration Reconciliation Logic Wnhancements	Cisco Smart PHY, Release 23.3	Smart PHY's cBR-8 configuration reconciliation logic has been enhanced to include: Downstream RF Power Adjust values and RPD MAC Address. Additionally, Smart PHY's reconciliation error handling is improved and new reporting capabilities are added.
Enhanced Config Reconciliation Logic	Cisco Smart PHY, Release 23.2	In this release, we have enhanced reconcile logic to include additional parameters for Principal, OOB, and Video cores.
cBR-8 Configuration Reconciliation enhancements	Cisco Smart PHY, Release 23.1	You can perform Smart PHY Reconciliation using Smart PHY WebUI.
cBR-8 Configuration Reconciliation	Cisco Smart PHY, Release 22.2	You can now detect the configuration mismatches between the cBR-8 router and Smart PHY cluster. This helps in reconciling the configuration between both the entities so that the configuration set are in sync with each other and eliminates the need of reprovisioning of RPDs effectively and saves time.

Post upgrading the software on CBR-8 router, the CBR-8 software automatically converts its earlier CLI configuration syntax into a new form on the CBR-CCAP-LC-G2-R line card. Ambiguity and differences may be seen between the actual configuration in the cBR-8 router and the corresponding configuration that is stored in the Smart PHY cluster.

Manual changes to the RPD Association configuration directly performed on a cBR-8 device, can also result in configuration differences.

The Smart PHY reconciliation feature intelligently detects such configuration mismatches and updates its internal configuration. This reconciliation helps in maintaining the cBR-8 and Smart PHY configuration to be in sync and avoids reprovisioning of RPDs. During such reconciliation process, which can be triggered when cBR-8 transitions from maintenance to normal mode, Smart PHY takes care of the following aspects:

1. Detects the configuration differences and prepares a report of the configuration difference between cBR-8 and Smart PHY.
2. Updates the Resource Allocation information and CLI details in Smart PHY when there is any discrepancy.
3. Ensures that existing RPDs are not reprovisioned and the new RPDs use the correct set of resources.

Note In Smart PHY, the reconciliation feature assumes that the RPDs are configured with the same name in both Smart PHY and the cBR-8 router.

Smart PHY Reconciliation Operation

Use the following procedure to perform a Smart PHY Reconciliation Operation.

1. At the main menu, select **Smart PHY > Inventory**. The **Remote PHY Devices & CCAP Cores** page displays.
2. Select a CCAP router and from the **Managed CCAP Actions** drop-down list, click **Check for Config Deviation**. Smart PHY triggers a check to detect config deviation. This process may take few minutes to complete.
3. If a config deviation is found, you can view the configuration difference and get an option to reconcile the data.
4. Click **Save to Smart PHY** to reconcile the Smart PHY database. During reconciliation, the Smart PHY database is updated with the configuration data from the selected CCAP.
5. You can download the reconciliation report by clicking the **Download Reconciliation Report** button.

Smart PHY Reconciliation using Maintenance Mode

Use the following procedure to perform Smart PHY Reconciliation using Maintenance Mode

1. At the main menu, select **Smart PHY > Inventory**. The **Remote PHY Devices & CCAP Cores** page displays.
2. Select the check boxes of one or more cBR-8 routers that are in the maintenance mode.
3. From the **Managed CCAP Actions** drop-down list, click **Resume Maintenance Mode**.
4. Review the Warning message and select the **Reconcile cBR-8 configuration** check box. The reconciliation operation takes place. The CCAP core is moved out of the maintenance state and reconciliation is performed.
5. Click **Resume Normal Operation**.

Reconciliation can be performed only for a single cBR-8. The following table shows the RPD Attributes that are reconciled.

Attribute	Reconciliation Status
RPD Device Name	Not Applicable as this attribute is the identifier for reconciliation
RPD Description	Reconciled
RPD MAC	Reconciled
Tags	Not Applicable as this attribute isn't a cBR-8 or RPD property
Node Segmentation	Reconciled
Service Definition	Not reconciled
Principal Core	
Device name for principal core	Not reconciled as we're triggering from cBR-8
Principal core interface	Reconciled
Downstream port 0	Reconciled
Upstream port 0	Reconciled
Downstream port 1	Reconciled
Upstream port 1	Reconciled
US Service Group for both ports	Reconciled
DS Service Group for both ports	Reconciled
US port 0 Description	Reconciled
US port 1 description	Reconciled
US base power for port 0	Reconciled
US base power for port 1	Reconciled
1st pairing downstream RF Pwr Adj profile	Reconciled
1st pairing DS base power	Reconciled
1st pairing tilt freq	Reconciled
1st pairing tilt slope	Reconciled
2nd pairing downstream RF Pwr Adj profile	Reconciled
2nd pairing DS base power	Reconciled
2nd pairing tilt freq	Reconciled
2nd pairing tilt slope	Reconciled
SSD Profile	Reconciled
Video Core Interface	
Video core Interface	Reconciled
VSG	Reconciled

Attribute	Reconciliation Status
OOB	
OOB interface	Reconciled
OOB parameters if overwritten	Reconciled
OOB parameters if overwritten for port 2	Reconciled

Note Once a cBR-8 router is reconciled, Smart PHY automatically updates the Last Modified Date and Last Modified By (user) meta data values.

For More information about the RPD attributes, see Remote PHY Device Association, on page 26.

Viewing RPD History

Step 1 Click the main menu at the top-left of the home page, and select **Smart PHY** > **RPD Associations**. The **Remote PHY Device Associations** page displays.

Step 2 Click the desired **RPD Name** to view the RPD information.

Step 3 Click **Status History** and **RPD Config History** to view the historical information.

Managing RF Power Adjust Profiles

Feature History

Feature Name	Release information	Description
RF Power Adjust Profile Enhancement	Cisco Smart PHY, Release 22.2	You can overwrite the RF Power Adjust Profile during RPD provisioning.

Smart PHY allows you to adjust the power levels for a single or a group of downstream RF channels using an RF Power Adjust Profile. An RF Power Adjust Profile consists of a profile name, an RF channel identifier (or identifiers), and a power adjust value. You can manage RF Power Adjust Profiles from Smart PHY's RF Power Adjust Profiles page.

RF channel power adjustment does not affect the service of the RPDs.

Limitations for RF Power Adjust Profile

- You cannot delete an RF Power Adjust Profile that is already used in a Service Definition.
- If you modify an RF Profile, the updated configuration is not applied to the RPDs that have already been provisioned. You can access the appropriate **Service Definition** page, select **Save & Assign**, select the specific RPD, and click **Assign** to apply the modified RF Power Adjust Profile parameters.

Creating an RF Power Adjust Profile

This procedure creates an RF power adjust profile.

Step 1 At the main menu, select **Smart PHY** > **Profile** > **RF Power Adjust Profiles**.

The **RF Power Adjust Profiles** page displays.

Step 2 Click **Create**.

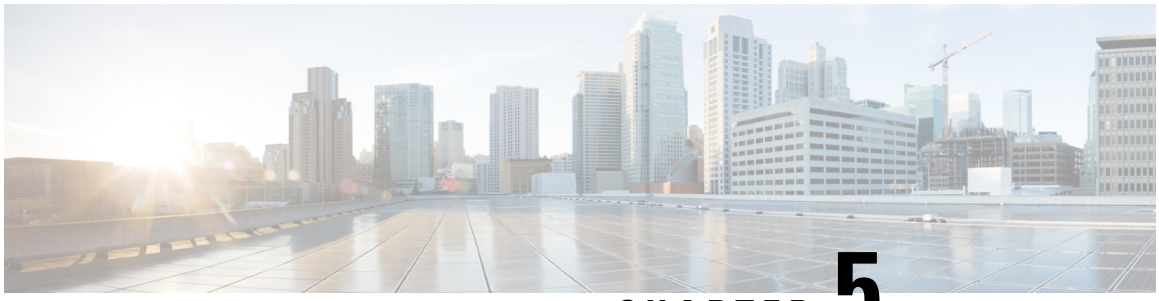
The **RF Power Adjust Profiles** page appears.

Step 3 Enter values for the following fields in the **RF Power Adjust Profiles** page.

Table 19: RF Power Adjust Profiles

Field	Value
Profile Name	Profile name can be up to 21 alphanumeric characters
Power Adjust (dBmV)	The Power Adjust range is from –10 to 10 dBmV
RF Channel	The RF Channel ID can be: • A single RF channel (for example: 6) • Multiple RF channels (for example: 6, 12, or 14) • Multiple consecutive RF channels (for example: 15–20) • A combination of the previous items (for example: 6.12, or 15–20)

Step 4 Click **Create**.



CHAPTER 5

Security and Administration

Smart PHY is hosted on Operations Hub, which provides comprehensive Role Based Access Control (RBAC) and User Management. Administrator can configure local or LDAP-based user authentication, create custom login banners, import and export Operations Hub configuration, monitor Audit and Debug logs, and create custom Kibana dashboards.

Refer to the Cisco Operations Hub User Guide for additional details.

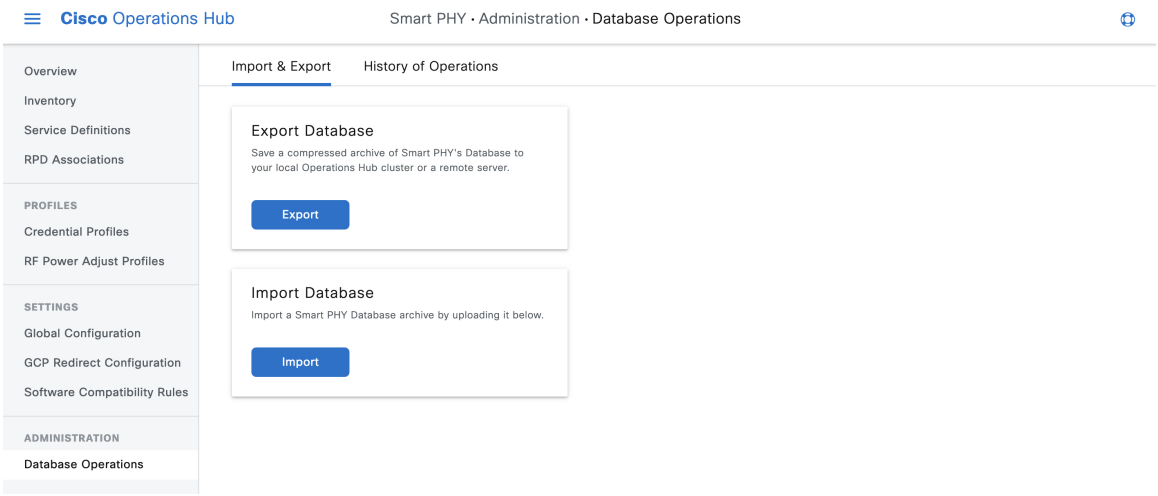
Database Operations

Table 20: Feature History

Feature Name	Release information	Description
Clear Smart PHY database without redeploying the cluster	Cisco Smart PHY, Release 23.1	You can clear (delete) all the data within the Smart PHY database without having to redeploy the cluster. This operation is similar to a factory reset.
Exporting Smart PHY Database to Local Computer	Cisco Smart PHY, Release 23.2	You can export the Smart PHY database to you local computer. You can also import previously saved Smart PHY databases.

Smart PHY stores all its inventory and provisioning data in an internal database. You can execute database import and export operations and view a history of previous operations from Smart PHY's Database Operations page.

Figure 5: Database Operations



Exporting Smart PHY Database to Local Computer

Smart PHY's Database is compressed and saved to the `/var/smartphy/backup` directory on the local filesystem. The filename format is `<cluster-name>_backup_<YYYYMMDD_HHMMSS>.tar.gz`.

Use this task to export the database from local filesystem

Step 1 At the main menu, click **Smart PHY** > **Administration** > **Database Operations**.

The **Import & Export** page appears.

Step 2 Click **Export**.

The **Export Database** panel appears at the right side of the page.

Step 3 Under Destination, select the **My Computer** radio button.

If you wish to password protect the exported database, check the **Password Protect Database** checkbox, and then enter a password.

Step 4 Click **Export**.

Use the **Import** option to import previously saved Smart PHY databases.

Exporting Smart PHY Database to Local Operations Hub Cluster

Smart PHY's Database is compressed and saved to the `/var/smartphy/backup` directory on the local filesystem. The filename format is `<cluster-name>_backup_<YYYYMMDD_HHMMSS>.tar.gz`.

Use this task to export the database from local filesystem

Step 1 At the main menu, click **Smart PHY** > **Administration** > **Database Operations**.

The **Import & Export** page appears.

Step 2 Click **Export**.

The **Export Database** panel appears at the right side of the page.

Step 3 Under Destination, select the **Local Operations Hub Cluster** radio button.

If you wish to password protect the exported database, check the **Password Protect Database** checkbox, and then enter a password.

Step 4 Click **Export**.

Exporting Database to a Remote Server

Smart PHY's Database is compressed and then copied to the specified file path on the remote server using SCP. The filename format is `<cluster-name>_backup_<YYYYMMDD_HHMMSS>.tar.gz`.

Step 1 At the main menu, click **Smart PHY** > **Administration** > **Database Operations**.

The **Import & Export** page appears.

Step 2 Click **Export**.

The **Export Database** panel appears at the right side of the page.

Step 3 Under **Destination**, select the **Remote Server** radio button.

Enter the following details for the remote server:

- Server IP Address
- Server File Path
- Select your desired Server SSH Authentication Method: **Username/Password** or **SSH Key**. If you select **Username/Password**, enter the: Server Username and Server Password. If you select **SSH Key**, select the appropriate SSH Private Key Profile from the dropdown list.
- If you wish to password protect the exported database, check the **Password Protect Database** checkbox, and then enter a password.

Step 4 Click **Export**.

Importing Database

If you have not yet added inventory or provisioning data to your Smart PHY cluster, then you can import a previously exported Smart PHY Database.

Note: Smart PHY only allows database import operations to occur when its internal database is empty. If inventory or provisioning data is present in its internal database, then Smart PHY blocks database import operations.

This procedure imports a database.

Step 1 At the main menu, click **Smart PHY** > > **Adminsitration** > **Database Operations**.

The **Import & Export** page appears.

Step 2 Click **Import** under the **Import Database** area.

The **Import Database** window appears at the right side of the page.

Step 3 Under Source, select either the **Local Operations Hub cluster** or **Remote Server** radio button.

- For Local Operations Hub Cluster, enter the following details:
  - Database filename (The filename must end with `tar.gz`)
  - Optionally enter the password, if your password protected the exported database during export.
- For Remote Server, enter the following details:
  - Server IP Address
  - Server File Path
  - Database filename (The filename must end with `tar.gz`)
  - Select your desired Server SSH Authentication Method: **Username/Password** or **SSH Key**. If you select **Username/Password**, enter the: Server Username and Server Password. If you select **SSH Key**, select the appropriate SSH Private Key Profile from the dropdown list.
  - If you wish to password protect the exported database, check the **Password Protect Database** checkbox, and enter a password.

Step 4 Click **Import**.

Smart PHY allows database import operations to occur only when its internal database is empty. If the database isn't empty, you're prompted to erase the existing database. On confirmation, existing database is erased, GCP communication is disabled internally and the new database is imported.

After importing the database, Smart PHY automatically reenables the GCP communication, verifies, and synchronizes the imported data. Once synchronizing is complete, all data including Smart PHY Inventory, Service Definition and RPD pairing information re-appears.

Configuring SSH Private Key Profiles

Table 21: Feature History

Feature Name	Release information	Description
SSH Private Key Profiles	Cisco Smart PHY, Release 23.2	Smart PHY allows you to upload SSH Private Keys and then use those keys to securely connect to remote systems for Import and Export Database operations.

Smart PHY allows you to manage SSH private key profiles and then securely connect to remote servers. These SSH profiles, which are stored securely in Operations Hub platform, can be used during export and import operations of Smart PHY databases.

Creating SSH Private Key Profiles

1. Access the SSH profiles page from the main menu, and select **Smart PHY > Settings > SSH Private Key Profiles**.
2. Enter **SSH Profile Name**, **SSH User Name** and upload the **SSH Private Key (PEM file)**
3. If SSH Private Key is encrypted with a passphrase, then enter a passphrase.
4. Click **Create**.

Note:

- Only AES-128 CBC passphrase encryption is supported. If private key is passphrase encrypted with AES-128 CBC, the private key PEM file should have DEK-Info.
- SSH private key can be of RSA-2048, RSA-4096 or AES-128-CBC encrypted PEM format.

The RSA PEM Key format example is given below:

```
-----BEGIN RSA PRIVATE KEY-----
<... Your Private Key ... >
-----END RSA PRIVATE KEY-----
```

When private key is passphrase encrypted:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,D6BF782F43A083F8303F55EEC3624D0B
.............................
-----END RSA PRIVATE KEY----
```

Validating SSH Private Key Profiles

Once an SSH private key profile is created, you can validate the profile. During validation, Operations Hub attempts to open an SSH session with the Remote Server using the SSH Private Key from the selected SSH Profile.

1. Access the SSH profiles page from the main menu, and select **Smart PHY > Settings > SSH Private Key Profiles**.
2. Select an SSH profile and click **Validate**.

3. Enter an IPv4 remote server IP Access the SSH profiles page from the main menu, and select address and click **Validate**.

Note: For the validation to be successful, the public key should be present in the remote server as part of SSH authorization keys. This enables passwordless login to the remote server.

Editing SSH Private Key Profiles

An SSH private key profile can be edited anytime.

1. Access the SSH profiles page from the main menu, and select **Smart PHY > Settings > SSH Private Key Profiles**.
2. Select an existing SSH private key profile and click **Edit**.
3. You can edit or correct any of the following parameters: SSH Profile Name, SSH User Name, SSH Private Key and optionally the SSH Private Key passphrase.

Note The private key can't be edited. However, it can be replaced by pasting or uploading a new private key during the edit operation.

Deleting SSH Private Key Profiles

If you are not using an SSH private key profile, you can delete it.

1. Access the SSH private key profiles page from the main menu, and select **Smart PHY > Settings > SSH Private Key Profiles**.
2. Select one or more SSH private key profiles and click **Delete**.

Viewing History of Database Operations

Smart PHY maintains a history of all database Operations.

The history contains the following information:

- Operation Status
- Type of Operation (Import or Export)
- Start Time
- End Time
- Result

This procedure enables you to view the history of database operations.

Step 1 At the main menu, click **Smart PHY** > **Database Operations**.

Step 2 Click the **History of Operations** tab to view the history of database operations.

You can also perform the following tasks:

- Click the **Export** icon to export history information into CSV format.
- Enter specific text in the the **Search Table** field to search and return specific information.

Customizing Smart PHY Settings

Feature History

Feature Name	Release Information	Description
Aux Core Configuration for RPD	Cisco Smart PHY, Release 22.4	You can use this option to configure additional cores on RPD's DOCSIS Principal Core using TLV 88.1.
Decision Pending IRA	Cisco Smart PHY, Release 22.4	Decision Pending IRA functionality is introduced to handle GCP redirect delays.

Smart PHY offers several ways to customize its behavior to fit your needs:

- Global Configuration
- GCP Redirect Configuration
- Software Compatibility Rules

To customize Smart PHY's behavior, click the Operations Hub main menu, and then select **Smart PHY** > **Settings**.

Global Configuration

To suit your requirements, you can customize the following configurations using Global Configuration options:

- Configure Static Routes—For more details, see the Static Routes section.
- Validate Software Compatibility—When enabled, Smart PHY performs a compatibility check based on the configured Software Compatibility Rules.
- Persist Running Configuration—When enabled, Smart PHY saves the changes that are made to the cBR-8 router's running configuration.
- Configuration Save Interval—This value determines the interval at which the changes are saved (Defaults to 60 minutes).

Static Routes

To route traffic and for communication between an RPD and a Cisco cBR-8 router, static routes to the Cisco cBR-8 router are created when you create an RPD association. When enabled, Smart PHY automatically creates a static route for the RPD if the cBR-8 router's DPIC interface is configured with a 31 (IPv4 networks) or 127 (IPv6 networks) subnet. The static route is determined by calculating the gateway IP address and routing traffic through the gateway for the RPD.

Note

- The DPIC must be a /31 or /127 subnet.
- Wait for the RPD to push the static route configuration.

Sample of a Cisco Smart PHY-Generated Configuration

```
cable rpd <the name assigned to the RPD>
  identifier a0f8.496f.6506
  type shelf
  rpd-ds 0 base-power 25
  rpd-ds 1 base-power 25
  core-interface Te9/1/6
   principal
   rpd-ds 0 downstream-cable 9/0/16 profile 100
   rpd-us 0 upstream-cable 9/0/1 profile 4
  r-dti 2
  rpd-event profile 0
 rpd-55d1-us-event profile 0

 cable fiber-node <next available fiber-node>
  downstream Downstream-Cable 9/0/16
  upstream Upstream-Cable 9/0/1
  downstream sg-channel 0 23 downstream-Cable 9/0/16 rf-channel 0 23
  upstream sg-channel 0 3 Upstream-Cable 9/0/1 us-channel 0 3
  service-group managed md 0 Cable 9/0/1
  service-group profile SG1
```

Programming Additional Cores

By default, Smart PHY passes CCAP Core IP addresses to RPDs via GCP Redirect IRA messages. A Redirect IRA message contains a complete list of the CCAP Cores an RPD must connect to. It's sent as a response to a Startup Notification message received from an initializing RPD. The CCAP Core list, which is generated by examining an RPD's association record, contains a DOCSIS Principal Core plus any configured Video Cores and any Additional Cores.

Additional Cores can optionally be passed to RPDs by a different method, which leverages a capability in the DOCSIS Principal Core to send TLV 88.1 (ConfiguredCoreTable) updates. When the DOCSIS Principal Core (TLV 88.1) method is selected, Smart PHY excludes Additional Cores from GCP Redirect IRA messages. Instead, Smart PHY dynamically adds or removes Additional Cores to, or from, the appropriate DOCSIS Principal Core. (Smart PHY updates the DOCSIS Principal Core by pushing "external core" CLI configuration commands.) The DOCSIS Principal Core then passes the IP addresses of the Additional Cores to the RPD by sending TLV 88.1 updates.

Should an RPD's DOCSIS Principal core be Unmanaged or run an IOS-XE software release without support for TLV 88.1, Smart PHY ignores this selection and programs Additional Cores via GCP Redirect.

Configuring Decision Pending IRA Message

By default, the Send Decision Pending IRA Messages feature is disabled.

When large numbers of RPDs boot-up or initialize at the same time, Smart PHY may not be able to process and reply to every incoming GCP Startup Notify message in a timely manner. RPDs with long waits may

send multiple Startup Notify messages or even timeout and reboot before Smart PHY is able to reply with a GCP Redirect IRA message.

To prevent RPDs from sending multiple Startup Notify messages or rebooting unnecessarily, you can enable the Send Decision Pending IRA Messages feature. When enabled, any time Smart PHY is unable to reply to an RPD's Startup Notify message with a GCP Redirect IRA message before a user configurable wait timer expires, Smart PHY replies with a Decision Pending IRA message.

Per the CableLabs Remote PHY specification, RPDs that receive a Decision Pending IRA message must wait for further messages from their connected CCAP core before proceeding with initialization. After sending a Decision Pending IRA message Smart PHY continues processing the RPD's initial Startup Notify message. A GCP Redirect REX message is sent to the RPD when the processing of the initial Startup Notify message is complete.

The Send Decision Pending IRA Message wait timer defaults to 90 seconds and can be configured anywhere from a minimum of 15 seconds to a maximum of 600 seconds. You can configure this parameter from the Smart PHY **Global Configuration** page by accessing **Smart PHY > Global Configuration** from the main menu.

GCP Redirect Configuration

Smart PHY supports GCP-redirects in compliance with the I15 revision of the CableLabs Remote PHY specification. By default, the pre-I15 GCP-redirect behavior is applied to all RPDs. Ensure that you enable the I15 GCP-redirect behavior.

I15 GCP Redirect Configuration

Smart PHY provides the flexibility to configure I15 compliant GCP redirect behavior. I15 GCP redirect messages are enabled based on the RPD vendor and the RPD software version. If a matching pattern is available, then Smart PHY initiates a GCP redirect message in I15 format, otherwise Smart PHY continues to send pre-I15 GCP-redirect messages. In such an environment, Cisco Smart PHY provides both exact pattern match and regex patterns.

Creating I15 GCP Redirect entry

Step 1 At the main menu, click **Smart PHY** > **Settings** > **GCP Redirect Configuration**.

The **GCP Redirect Configuration** page appears

Step 2 Click **Create** to open the **Add GCP Redirect Configuration** window appears at the right side of the page.

Step 3 Enter the RPD Vendor (For example: *Cisco* or *Cisco.*) and RPD Software Version (For example: *v.9.4* or *v.9.*).

Step 4 Click **Add**

I15 GCP-redirect Result Notification

Smart PHY displays the result of the RPD's `GCP Redirect Notification` message in the **RPD 360** panel. When redirect errors occur, Smart PHY displays the RPD status as **GcpRedirectError**. The **GcpRedirected** status indicates that the redirect message is processed successfully by the RPD.

Software Compatibility Rules

Smart PHY allows you to add, edit, or delete software compatibility rules. Leveraging these rules, Smart PHY can detect software incompatibility between an RPD and a Cisco cBR-8 route and alert you to this incompatibility.

After an alert message appears, you have to either manually upgrade the RPD software or update the RPD's association with the appropriate SSD Profile.

Creating a Software Conmpatibility Rule

This procedure creates a software compatibility rule.

Step 1 At the main menu, click **Smart PHY** > **Settings** > **Software Compatability Rules**.

The **Software Compatibility Rules** page appears.

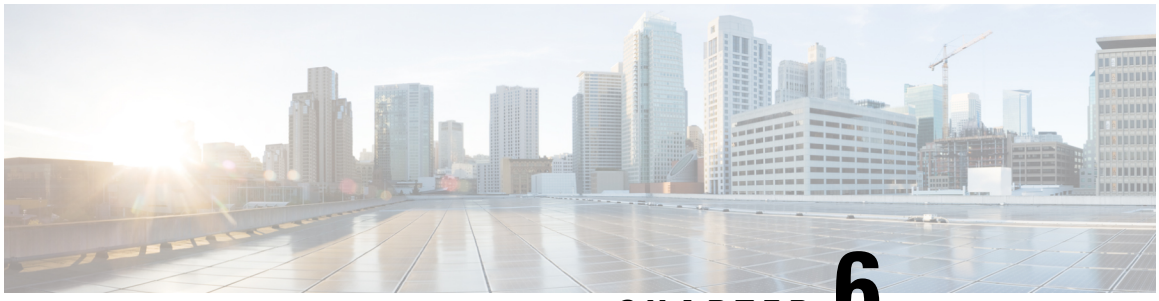
Step 2 Click **Create**.

The **Add Rule** window appears at the right side of the page.

Step 3 Enter the following information:

Name	Description
RPD Vendor	Name of the RPD vendor.
RPD Software Version	Software version running on the RPD.
Router Product Type	Product type of the router in the Inventory. Example: CBR-8-CCAP-CHASS.
Router Software Version	Software version of the router.

Step 4 Click **Add**



CHAPTER 6

Monitoring and Troubleshooting

Refer the following topics for some troubleshooting tips for installing and using Smart PHY.

Monitoring Host Resources

You can use Operations Hubs prepackaged Dashboards to monitor cluster and host resources.

Step 1 Click the main menu at the top-left of the home page.

Step 2 Select**Dashboards**.

The **Dashboards** page displays. The following types of dashboards are available:

- **Operations Hub Dashboard**: Capturing Kubernetes, Open Source, Infrastructure, and KPI metrics.
- **User Created Dashboards**: Customized dashboards (if any).

Accessing API Explorer

Smart PHY comes with comprehensive online API documentation, which is accessible from Operations Hub's API Explorer. Smart PHY's APIs are divided into two categories: **RPD Service Manager** and **Inventory Management**.

Use the following procedure to access Smart PHY's APIs.

Step 1 At the main menu, select **API Explorer**.

The **API Explorer** page displays.

Step 2 Locate **SMARTPHYAPI** in the left navigation menu.

Step 3 Click **RPD Service Manager** or **Inventory Manager** under **SMARTPHYAPI**.

Debugging RPD SSD on Cisco Smart PHY

The SSD related logs in Cisco Smart PHY application are available at: `/var/log/rpd-service-manager/rpd-service-manager.log`.

Checking SSD on NSO

The Cisco Network Services Orchestrator (NSO) supports the SSD profile from the iosNed 6.28.

1. Access the `robot-cfgsvc` container and check the SSD configuration on the NSO side.
2. Wait until the device moves into in-sync.

```
router# devices device _DEVICE_20.5.30.13 check-sync
result out-of-sync
info got: 4a0ba9b4ecdaa8710a9202e8656bfe82 expected: c22a63a573c84e40c1ad5e735888461c
router# devices device _DEVICE_20.5.30.13 check-sync
result in-sync
show running-config devices device _DEVICE_20.5.30.13 | begin ssd
  ios:cable profile ssd 1
   ssd 12.2.2.2 tftp xxx
  !
  ios:cable profile ssd 2
   description ssd 2
   ssd 10.1.1.1 tftp abc
```

The SSD configuration on NSO must be the same as with the Cisco cBR-8 router.

Checking SSD using RestAPI

1. Get the SSD profiles, which are read by NSO from the Cisco cBR-8 router, use the **query-core-details** command.

   `https://{{controller}}:{{new-port}}/rpd-service-manager/rpdorch/v2/core-topology/query-core-details`

   Output:

   SSD profile info must be the same as that with the Cisco cBR-8 router.

```
Input:
{
  "ipAddress": "10.0.0.1"
}


Result:
{
    "status": "Success",
```

```
    "coreList": [
        {
            "ipAddressList": [
                "10.0.0.1"
            ],
            "uuid": "_DEVICE_10.0.0.1",
            "gpsLocation": {},
            "hostName": "NG03.cisco.com",
            "interfacesList": [...],
            "virtualSGs": [],
            "ndfProfiles": {},
            "ndrProfiles": {},
            "ssdProfiles": [
                {
                    "id": 1,
                    "name": "xxx"
                },
                {
                    "id": 2,
                    "name": "abc"
                },
                {
                    "id": 3,
                    "name": "aaa"
                },
                {
                    "id": 4,
                    "name": "abcdef"
                },
                {
                    "id": 5,
                    "name": "abbbc"
                },
                {
                    "id": 6,
                    "name": "acde"
                },
                {
                    "id": 7,
                    "name": "xxx"
                },
                {
                    "id": 9,
                    "name": null
                },
                {
                    "id": 10,
                    "name": "abcc"
                }
            ],
            "state": "ONLINE",
            "productType": "CBR-8-CCAP-CHASS",
            "swVersion": "16.10.1f",
            "vendorName": "Cisco",
            "protectedLC": -1
        }
    ]
}
```


2. Check the RPD paring details, use the **query-rpd-pairing** command.

   ```
   https://{{controller}}:{{new-port}}/rpd-service-manager/rpdorch/v2/rpd-pairing/query-rpd-pairing
   ```

   Output:

The value of ssdProfileId must be correct.

```
Input:
{
}

Result:
{
    "status": "Success",
    "rpdPairingRspList": [
        {
            "macAddress": "aabb11112124",
            "name": "1",
            "serviceTemplate": "C02",
            "approvalState": "Approved",
            "assignedCores": [
                {
                    "serviceType": "Data",
                    "mgmtCore": "C02.cisco.com",
                    "rpdConnectionInterface": "TenGigabitEthernet7/1/0",
                    "primaryUsPort": 1
                }
            ],
            "pairingChangeTimestamp": 1563823890549,
            "description": "",
            "state": "ResourceAllocationError",
            "gpsLocation": {
                "latitude": 77,
                "longitude": 99,
                "genericLocation": "Shanghai"
            },
            "ssdProfileId": 1
        }
    ],
    "nextFrom": null
}
```

3. Verify the SSD profile ID and the image name in the **Edit** window of the RPD paring table.
4. Verify whether the RPD Details contain the SSD command.

Checking SSD on Cisco cBR-8

Run the following command to check the SSD on the Cisco cBR-8 router.

```
cable rpd PRPD
 identifier a0f8.496f.6506
 type shelf
 rpd-ds 0 base-power 25
 rpd-ds 1 base-power 25
 core-interface Te9/1/6
  principal
  rpd-ds 0 downstream-cable 9/0/16 profile 100
  rpd-us 0 upstream-cable 9/0/1 profile 4
 r-dti 2
 rpd-event profile 0
 ssd 1
 rpd-55d1-us-event profile 0
```

Debugging SSD on Cisco cBR-8

Use the following command to check the upgrading state on the Cisco cBR-8 router.

```
cable rpd xxxx.xxxx.xxxx ssd status
```

DEPI Latency Measurement in Service Template

If a Service Definition is already in use, then you can update only the DLM fields (Static delay, DLM sampling value, Measure Only), and the existing behavior is maintained for all other fields.

Following operations are allowed when a Service Template is already in use:

- If there is no existing DLM configuration in the service template, you can add network-delay static <delay-val>, network-delay dlm <interval>, and network-delay dlm <interval><measure-only>.

  If the network-delay static <delay-val> is configured in the service template, then user can modify the <delay-val> for static.

  If the network-delay dlm <interval> is configured in the service template, then user can modify the dlm <interval> and <measure-only> parameters.

  If the network-delay dlm <interval><measure-only> is configured in the service template, then user can modify only the dlm <interval>.

The RPD detailed information contains the DLM command.

Before you update a Service Definition, you should check whether any Cisco cBR-8 line cards are in a high availability state an active secondary line card.

The DLM configuration gets automatically applied to all RPDs assigned to the Service Definition. However, the RPD configuration is rejected if the Cisco cBR-8 line card for DOCSIS controllers is in high availability mode. In addition, because this operation might take more time, you may see a network connectivity issue.

After updating a Service Definition, you should check the RPD service manager logs for errors. To recover an RPD with a configuration rejection or error, do the following:

- If the secondary line card is active:
  1. Revert to the primary line card.
  2. Wait until the primary line card is active.

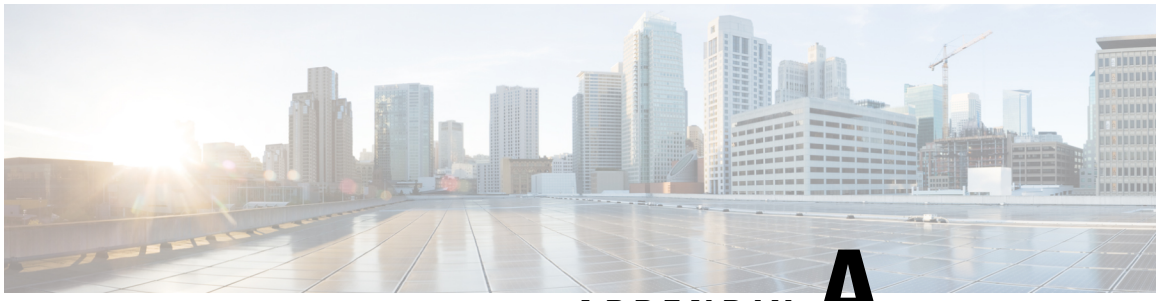
- For each RPD with a configuration rejection or error:
  1. In the **RPD Association** page, click **Edit** for that RPD.
  2. On the **Edit** page, click **Save**.

Related Topics

Checking New DLM Configuration on Cisco cBR-8, on page 72

Checking New DLM Configuration on Cisco cBR-8

```
cable rpd <RPD Name>
 identifier a0f8.496f.6506
 type shelf
 rpd-ds 0 base-power 25
 rpd-ds 1 base-power 25
 core-interface Te9/1/6
  principal
  rpd-ds 0 downstream-cable 9/0/16 profile 100
  rpd-us 0 upstream-cable 9/0/1 profile 4
  network-delay dlm 100
 r-dti 2
 rpd-event profile 0
 ssd 1
 rpd-55d1-us-event profile 0
!
```



APPENDIX A

Best Practices

This section provides some best practices that you can follow for configuring and using the Cisco Smart PHY application.

- Best Practices, on page 73

Best Practices

Do not use `systemctl network restart` or `ifup` and `ifdown` commands. `keepalived` does not monitor these Linux commands. Hence, use the following commands as `keepalived` monitors them:

- `ip link set down dev <interface>`
- `ip link set up dev <interface>`

System and Cluster Recommendations

On multinode installations, we recommend exporting the Database to a remote server. Exporting the Database to the local Operations Hub cluster isn't recommended because the Database could be saved on any one of the three worker nodes.

Smart PHY Application User Recommendations

Cisco cBR Router

- The Management IP address that is configured in Smart PHY's Inventory should belong to the interface the cBR-8 router uses to send SNMP traps.
- Use the following cBR-8 router command to configure the SNMP trap source: `snmp-server trap-source <interface>`
- We advise against specifying a device name when adding a cBR-8 router to Smart PHY's Inventory. Smart PHY automatically retrieves the hostname and uses it as the router's device name after it connects to the cBR-8 router. Retrieving the hostname prevents any human errors due to incorrect entries of hostname or the IP address.
- If there is a network outage or loss of connectivity, confirm the cBR-8 router's state is *Online* in Smart PHY before modifying the RPD associations.
- Unprovision all RPDs assigned to a cBR-8 router before deleting the router from Smart PHY.

RPD Provisioning

- When MD splitting is enabled, clear RPDs in the RPD Assignment UI before making changes to the existing RPD assignments. Make sure that all cleared RPDs are in Installed, Inventory, or NotProvisioned state before provisioning them again. If the RPD status does not change, manually verify whether the RPD and fiber node configurations are cleared on the Cisco cBR-8 router.
- Modifications to RPDs provisioning do not require clear or delete. Except for the above mentioned scenario, RPD fields should be modified directly via API/UI/CSV uploads.
- In case of clear of RPDs, make sure that the RPDs have reached the Installed, Inventory, or the NotProvisioned state before provisioning them again. If you are deleting RPDs, make sure that the delete transactions are complete before provisioning them again.
- If pilot-tone is being configured for the RPDs, we recommend that not more than 10 RPDs be provisioned in one CSV upload or REST API call. The Cisco cBR-8 router needs more time to configure RPDs with the pilot-tone and it rejects all subsequent RPD configurations if there are more than ten pending RPD transactions in the Cisco cBR-8 router internal queue.
- Any assignment or configuration change to an online RPD results in the RPD service being interrupted. We recommend that you provision all needed parameters before the RPD is brought Online.