



Access Cisco Smart PHY Application

This section describes how to access the Cisco Smart PHY application and how to bring an RPD online.

- [Configure Cisco cBR-8 for Smart PHY Application, on page 1](#)
- [Log in Using a Browser, on page 2](#)
- [Bring Up the RPD, on page 2](#)
- [Create a New Credential Profile, on page 3](#)
- [Apply Device Credential from Credential Profiles, on page 4](#)
- [Apply a Different Credential Profile to Existing Devices, on page 4](#)
- [Apply Different Credential Profile in Bulk, on page 5](#)
- [Delete a Device from the Inventory, on page 5](#)
- [Create CSV File for Importing Devices, on page 6](#)
- [Export Device Information to a CSV File, on page 6](#)
- [Add Devices through GUI, on page 7](#)
- [Import Device Information in Bulk, on page 8](#)
- [Delete a Credential Profile, on page 8](#)
- [Create a New Service Definition, on page 9](#)
- [Add and Assign RPDs, on page 12](#)
- [View RPD History, on page 17](#)
- [Database Backup, on page 17](#)
- [Manage Users, on page 18](#)
- [Basic and LDAP Authentication, on page 19](#)

Configure Cisco cBR-8 for Smart PHY Application

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

Enable Syslog

Configure the Cisco cBR-8 router to send syslog messages to the Cisco Smart PHY application, including the messages for Line Card high availability (HA) events.

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

```
logging trap informational
cable logging layer2events
```

Enable SNMP Traps

Configure the Cisco cBR-8 router to send syslog and SNMP messages to the Cisco Smart PHY application.

The Cisco Smart PHY application uses syslog messages to monitor the state of the RPD on the Cisco cBR-8 router. Run the following command on the Cisco cBR-8 router:

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

Log in Using a Browser

- 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.
- 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 **Dashboards** 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.
When you access Cisco Smart PHY for the first time, if the browser displays a warning that the site is untrusted follow the prompts to add a security exception and download the self-signed certificate from the Cisco Smart PHY server. After you add the certificate, the browser accepts the Cisco Smart PHY server as a trusted site in all future login attempts.
Exiting a Cisco Smart PHY web GUI session does not shut down Cisco Smart PHY on the server.
If a system administrator stops the Cisco Smart PHY server during your Cisco Smart PHY session, your session ends. When the server restarts, you should start a new Cisco Smart PHY session.
-

Bring Up the RPD

- Step 1** Log into the Cisco Smart PHY application.
Go to `https://<fqdn>` OR `https://<Cisco Smart PHY master virtual IP address>.nip.io`.
- Step 2** Create a Credential Profile.
For more details, see the section [Create a New Credential Profile, on page 3](#).
- Step 3** Add the Cisco cBR-8 router to the inventory and reference the credential profile.

Add a device manually or by importing from a CSV file. For more details, see sections [Add Devices through GUI, on page 7](#) and [Import Device Information in Bulk, on page 8](#).

Step 4 Create a Service Template.
For more details, see the section [Create a New Service Definition, on page 9](#).

Step 5 Pair an RPD with the RPD MAC address in the RPD assignment table.

Adding RPD through a Web GUI

Note Fields with an asterisk are mandatory.

Add RPD devices through the **RPD Automation > RPD Assignment** menu options and not through the **Inventory** menu.

You can assign RPDs manually or by importing a CSV file.

For more details, see [Add and Assign RPDs, on page 12](#).

Click **Save**.

After assigning the RPD MAC address to the RPD name, the RPD is provisioned on the Cisco cBR-8 router and comes online on that Cisco cBR-8 router after getting redirected by the Cisco Smart PHY application.

Create a New Credential Profile

Before you begin

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

Step 1 Choose Cisco Operations Hub main menu > **Smart PHY > Smart PHY Inventory > Credential Profiles**.

Step 2 Click **Create New**.

Step 3 Enter the following details in the text fields.

If you have many credential profiles, make the name and description as informative as possible, because that information is displayed on the **Credential Profiles** panel.

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
Connectivity Type	SSH
Port Number	22
Save/Delete/Cancel	Use these buttons to complete your action.

Note The Cisco Smart PHY application requires SSH to log in directly to the `exec` mode on the Cisco cBR-8 router.

When a device is added or updated using this profile, the content you specify here is applied to the device.

Step 4 Click **Save**.

Apply Device Credential from Credential Profiles

Using credential profiles lets you apply credential settings consistently across devices. When you add or import devices, you specify the credential profile the devices use. If you need to make a credential change, such as changing a device password, you can edit the profile to update the settings across all devices that use that profile.

Step 1 To view the existing profiles, choose Cisco Operations Hub main menu > **Smart PHY** > **Smart PHY Inventory** > **Credential Profiles**.

Step 2 Click the profile you want to view.

Credential profiles can be shared by multiple devices. Large networks might have similar credentials for hundreds of devices.

The mandatory fields are:

- Profile Name
 - Username
 - Password
 - Connectivity Type
 - Port Number
-

Apply a Different Credential Profile to Existing Devices

You can use the Inventory user interface to edit device information, including changing the credential profile in the inventory record. This operation overwrites any existing association between a device and a credential profile. You can also use this operation to synchronize device configurations with new settings.

Before you begin

You need a credential profile to complete this task.

Step 1 To view inventory, choose Cisco Operations Hub main menu > **Smart PHY** > **Smart PHY Inventory** > **Inventory**.

Step 2 (Optional) In the **Inventory** section, filter the list of devices by entering text in the **Search** field or filtering on the individual headings.


- Step 3** Check the check boxes of the devices you want to change, and click the **Edit** icon.
- Step 4** Choose a different credential profile from the **Credential Profile** drop-down list, for example, or make other changes in the device records.
- Step 5** Click **Save**.
-

Apply Different Credential Profile in Bulk

This is an alternative to changing the credential profile for devices within the Cisco Smart PHY Inventory Manager GUI. If you are changing the credential profile for a large number of devices, you may find it more efficient to make the change by using a CSV file rather than the Cisco Smart PHY UI. Export a CSV file, make the changes, and import the changed CSV file. This operation overwrites any existing association between a device and a credential profile. You can also use this operation to synchronize device configurations with new settings.

- Step 1** (Optional) To review the contents of a credential profile, choose Cisco Operations Hub main menu > **Smart PHY** > **Smart PHY Inventory** > **Credential Profiles**.
- Step 2** Click the profile you want to use. Else, create a new profile.
- Step 3** To view device inventory, click the **Inventory** tab.
- Step 4** Choose which device records to change by including them in the CSV file.
Do one of the following:
- Click the **Export** icon to include all devices.
 - Filter the list of devices by entering text in the **Search** field or by filtering on the individual headings, and then click the **Export** icon to include the filtered list of devices.
 - Check the check boxes for the device records you want to change, and then click the **Export** icon to include the selected devices.
- Step 5** Edit and save the new CSV file. Note: You must save the file opened in MS Excel as a CSV file only.
- Step 6** In the Import CSV File dialog box, click **Browse**, select the new CSV file, and click the **Import** icon.
- Step 7** In the **Replace Existing Node** dialog box, click **Yes to All**.
- Step 8** Click **Save**.
-

Delete a Device from the Inventory

- Step 1** Choose Cisco Operations Hub main menu > **Smart PHY** > **Smart PHY Inventory** > **Inventory**.
- Step 2** (Optional) In the **Inventory** section, filter the device list by entering text in **Search** or filtering specific columns.
- Step 3** Check the check boxes for the devices you want to delete.
- Step 4** Click delete icon ()


Step 5 In the confirmation dialog box, click **Delete**.

Deleting an RPD from the Inventory does not delete the corresponding RPD Assignment from the **RPD Assignment** table. Similarly deleting an RPD Assignment does not delete an RPD from the Inventory.

Create CSV File for Importing Devices

To add information for multiple devices to Inventory Manager, create a CSV file. Inventory Manager contains a sample template CSV file. The GUI for adding individual devices contains field information that also applies to the contents of the CSV files that you create for device import.

Step 1 Choose Cisco Operations Hub main menu > **Smart PHY** > **Smart PHY Inventory** > **Inventory**.

Step 2 In the **Inventory** section, click the import icon (.

(Optional) Click the link **Download sample 'Inventory template (*.csv)' file** to download the sample CSV file .

Step 3 Edit the CSV file and save it as a CSV file on your system. Upload this CSV file to import devices.

The mandatory fields are:

- Key Type
 - IP Address
 - Product Type
 - Credential Profile
-

Export Device Information to a CSV File

When you export the device list to a file, all device information is exported into a CSV file.




Caution The CSV file lists all the credentials for the exported devices. Handle the CSV file with care. Ensure that only users with special privileges can perform a device export.

Step 1 Choose Cisco Operations Hub main menu > **Smart PHY** > **Smart PHY Inventory** > **Inventory**.

Step 2 (Optional) In the **Inventory** section, filter the device list by entering text in the **Search** field or filtering specific columns.

Step 3 Check the check boxes for the devices you want to export.

Step 4 Click the export icon (.

Add Devices through GUI

If you have many devices to add to the Inventory Manager, you may find it more efficient to put the information in a CSV file and import the file.

Step 1 Choose Cisco Operations Hub main menu > **Smart PHY** > **Smart PHY Inventory** > **Inventory**.

Step 2 In the **Inventory** section, click the add icon (+).

Step 3 Choose a **Core Type**: Managed or Unmanaged

Step 4 Enter the values for the Cisco cBR-8 device.

- **Managed**: The following fields are mandatory:

- Device Key Type: IP address

- Management IP Address: Management IP address on the Cisco cBR-8 router that can reach the Cisco Smart PHY application

- Product Type: CBR-8-CCAP-CHASS

- Credential Profile: Specify the credential profile. Devices with the same credentials can use the same credential profile

- **Unmanaged**: The following fields are mandatory:

- CIN IP Address: IP address on the unmanaged Core that provides services to RPDs

- Product Type: UNMANAGED (The field is not editable.)

The screenshot displays the 'Add Inventory' form in the Cisco Smart PHY Inventory Manager. The form is titled 'Add Inventory' and has a close button (X) in the top right corner. It features a 'Core Type' section with radio buttons for 'MANAGED' (selected) and 'UNMANAGED'. Below this, there are several input fields: 'Device Key Type * IP ADDRESS' (with a dropdown arrow), 'Management IP Address * IP Address' (with a calendar icon), 'MAC Address MAC Address', 'Product Type * Product Type' (with a dropdown arrow), 'Credential Profile *' (with a dropdown arrow), 'Host Name Host Name', 'Latitude -90 to 90', 'Longitude -180 to 180', 'Location Location', and 'Description Description'. At the bottom of the form are 'Save' and 'Cancel' buttons.

In the background, the 'Inventory' table is visible, showing a list of devices with columns for Status, Host Name, and Key. The table contains several rows, including dummy devices and a device named 'sphy-c2.cisco.com' with a status of 'ONLINE' and a key of 'IP ADDRESS'.


Status	Host Name	Key
OFFLINE	MK_DB_DUMMY_07	MAC ADDRESS
OFFLINE	HA_SQUIMKC	MAC ADDRESS
OFFLINE	MK_898	MAC ADDRESS
OFFLINE	MK_DB_DUMMY_04	MAC ADDRESS
ONLINE	sphy-c2.cisco.com	IP ADDRESS
OFFLINE	BidiptaRPDEDITWOR...	MAC ADDRESS
OFFLINE	MK_DB_DUMMY_03	MAC ADDRESS

- Step 5** Click **Save**.
- Step 6** (Optional) Repeat to add more devices.

Import Device Information in Bulk

Before starting this procedure, create a CSV file that contains the device information.

Step 1 Choose Cisco Operations Hub main menu > **Smart PHY** > **Smart PHY Inventory** > **Inventory**.

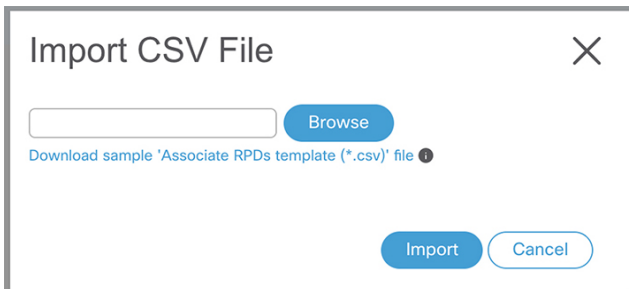
Step 2 Click the import icon ().

Step 3 In the **Import CSV File** window, click **Browse**, select the CSV file, and click **Import**.

The **Import** dialog box also has a link to a sample CSV file which you can download for reference. Make sure you save the edited file in CSV format.

Set the following values for a Cisco cBR-8 device.

- Key Type: IP address
- IP Address: IP address on the Cisco cBR-8 router that can reach the Cisco Smart PHY application.
- Product Type: CBR-8-CCAP-CHASS
- Credential Profile: Specify the credential profile



If any primary keys are duplicates with existing device records, Inventory Manager alerts you.

Delete a Credential Profile

To delete a credential profile from Inventory Manager, disassociate the profile from any devices. Inventory Manager displays an alert if you attempt to delete a credential profile that is associated with devices.

(Optional) Check whether any devices are using the obsolete credential profile and change the credential profile before deleting the profile.

1. Choose Cisco Operations Hub main menu > **Smart PHY** > **Smart PHY Inventory** > **Inventory**.
2. In the **Inventory** section, enter the obsolete credential profile name in the **Search** field.

3. Check the check boxes for the devices that use the obsolete credential profile, and click **Edit**.
4. Choose a different credential profile from the **Credential Profile** drop-down list.
5. Click **Save**.

Step 1 Choose Cisco Operations Hub main menu > **Smart PHY** > **Smart PHY Inventory** > **Credential Profiles**.

Step 2 Click the profile, and click **Delete**.

The screenshot displays the 'Credential Profiles' management interface. On the left, a list of profiles is shown, with 'sil' selected. On the right, the 'Edit Profile' form is open, showing the following details:

- Profile Name * sil
- Username * lab
- Password *
- Enable Password
- Connectivity Type * SSH
- Port Number * 22

At the bottom of the form, there are three buttons: Save, Delete, and Cancel. A vertical ID number '520634' is visible on the right side of the form area.

Create a New Service Definition

Step 1 Choose Cisco Operations Hub main menu > **Smart PHY** > **RPD Automation** > **Service Definitions**.

Step 2 Click + **Create New**.

Step 3 Enter a name and description.

If you have many service definitions, make the name and description as informative as possible because that information is displayed on the **RPD Assignment** and **Overview** tabs.

Step 4 (Optional) Check the **Set as Default** check box.

Step 5 Enter the definitions for the Service Definition.

When a device is added or updated using this service definition, the content you specify here is applied to the device. 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 1: Service Definition Parameters

Name	Description	Service Affecting Parameter
Name	Name of the service definition	NA
Description	A brief description on service definition	No
Event Profile	RPD Event Profile Set	No
R-DTI Profile	Remote DOCSIS Timing Interface (R-DTI) Set	No
Pilot Tone Profile	Pilot tone profile.	Yes
Cable DSG TGs	DSG tag IDs.	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 Profiles	Apply one or more RF Power Adjust Profile(s) to modify the RPD's Downstream RF channel power output.	No
Upstream Controller Profile	Primary upstream CCAP controller profile.	Yes
Second Logical DS/US Pairing		
Enable	Select the check box 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	Apply one or more RF Power Adjust Profile(s) to modify the RPD's Downstream RF channel power output.	No
Upstream Controller Profile	Secondary upstream CCAP controller profile.	Yes
Enable MAC Domain Splitting	Select the check box to split a MAC domain between two fiber-nodes that share the same downstream controller.	Yes

Name	Description	Service Affecting Parameter
Network Delay	<p>Network delay has two options:</p> <ul style="list-style-type: none"> • DLM—System periodically measures the network latency between the CCAP core and the RPD, and dynamically updates the cable map advance. Range is interval in seconds. The valid range for measuring DLM is 1–420 seconds. <p><i>Measure only</i>—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 deselect it.</p> <ul style="list-style-type: none"> • Static—The cable map advance is adjusted by a fixed amount. The valid range is 30–100,000 microseconds. <p>This range is the Converged Interconnect Network (CIN) delay in microseconds. CIN is the network between the CCAP core and RPD.</p> <p>You can change the network-delay range for a service definition in use.</p> <p>For more details, see <i>DEPI Latency Measurement in the Service Template</i> section in this document.</p>	No
Out Of Band		
Downstream VOM ID	OOB 55–1 Downstream Virtual out-of-band Modulator (VOM) identification (ID).	No
Downstream VOM Profile	OOB 55–1 Downstream VOM profile.	No
Upstream VARPD ID	OOB 55–1 Upstream Virtual Advanced Return Path Demodulator (VARPD) ID.	No
Upstream VARPD Profile	<p>OOB 55–1 Upstream VARPD profile for first logical downstream/upstream (DS/US) pairing.</p> <p>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.</p>	No
Second Upstream VARPD Profile	<p>OOB 55–1 Upstream VARPD profile for second logical downstream/upstream (DS/US) pairing.</p> <p>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.</p>	No


Name	Description	Service Affecting Parameter
NDF/NDR		
Pseudowire Name	<p>NDF</p> <p>Narrowband digital forward pseudowire name.</p> <p>Supports up to three pseudowire names and profile ID sets per DS port.</p> <p>NDR</p> <p>Narrowband digital return pseudowire name. Supports up to three pseudowire names and profile ID sets per US port.</p>	No
Profile ID	<ul style="list-style-type: none"> • NDF—NDF profile ID corresponding to the above NDF pseudowire. • NDR—NDR profile ID corresponding to above NDF pseudowire. 	No
NDF : Port	Downstream port, Port 0, or Port 1 to apply NDF pseudowire name and profile ID for a 2x2 RPD.	No
NDR : Port	Upstream port, Port 0, or Port 1 to apply NDR pseudowire name and profile ID for a 2x2 RPD.	No
Load Balance	Paste the load balance XML text in the text field. Use the ntool to convert the XML configuration from the Cisco cBR-8 router to the required XML format.	No

Step 6 Click **Save** or **Save & Assign**.

Add and Assign RPDs

Step 1 Choose Cisco Operations Hub main menu > **Smart PHY** > **RPD Automation** > **RPD Assignment**.

RPD Assignment can be specified manually or by importing a CSV file.

Step 2 Click  icon to assign a service template to an RPD.

Fill in all the fields.

Field Name	Description
RPD Parameters	

Field Name	Description
Shelf	<p>Select the check box to configure Cisco Remote PHY Shelf 7200, Cisco Remote PHY Shelf 300, or Cisco Remote PHY Shelf 600.</p> <p>This feature is supported only from Cisco IOS XE Gibraltar 16.12.1z on Cisco cBR-8 routers.</p> <p>The following fields are enabled when you select this check box:</p> <ul style="list-style-type: none"> • Base Power (dBmV) • Tilt Pivot Freq (Hz) • Tilt Slope (dBmV) <p>RPD does not restart after updating these high availability (HA) parameters.</p>
Enforce Controller compatibility with IOS XE 17.6.1	When you enable this option, Cisco 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.
RPD Name	<p>Name for the RPD.</p> <p>This RPD name is also used in the <code>cable rpd</code> CLI command.</p>
RPD MAC Address	MAC address of the RPD.
Node Segmentation	Node segmentation of the RPD: 1x1, 1x2, or 2x2.
Service Definition	Service Definition as created in the Service Definitions tab. If Cisco Smart PHY does not manage the principal CCAP core and if the Principal Core field is empty, then this Service Definition field is optional.
Disable Network Delay	<p>The default is value is No.</p> <ul style="list-style-type: none"> • No—Apply network delay from service definition to RPD. • Yes—Do not apply network delay from service definition to RPD. <p>Changing this value to <code>yes</code> is service impacting, if the RPD's assigned Service Definition/Template has network-delay configured.</p>
Latitude	Latitude of the RPD (GPS coordinates)
Longitude	Longitude of the RPD (GPS coordinates)
RPD Description	Description for the RPD
Cable DSG TGs	Semicolon separated list of DOCSIS Set-Top Gateway (DSG) Tunnel Group (TG) identifications. If present, this list overrides the list from the Service Definition.
Data / Principal Core	

Field Name	Description
Principal Core	<p>The name of the managed Cisco cBR-8 router or the unmanaged Core, which is the Principal Converged Cable Access Platform (CCAP) Core for the RPD.</p> <p>If you choose a managed Principal Core, 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:</p> <ul style="list-style-type: none"> • Out-of-band (OOB) SCTE 55–1 • Video services: If there is no separate auxiliary Video Core
Principal Core Interface	<p>If the Principal Core is a managed Cisco cBR-8 router, choose the complete name of the TenGigabitEthernet DPIC interface used to deliver data service.</p> <p>Leave this field empty if there is no Principal Core or if the principal core is unmanaged.</p>
SSD Profile	<p>If the Principal Core is a managed cBR-8 router, enter the Secure Software Download (SSD) profile ID. If the Principal Core is Unmanaged, leave this field empty.</p>

Table 2: First and Second Logical DS/US Pairing

Field Name	Description
Downstream Physical Port	<p>Downstream RPD port of the logical pairing.</p> <p>Always 0 for the first pairing and not applicable to second pairing for 1x1 or 1x2 node segmentation. May be 0 or 1 for 2x2 node segmentation.</p>
Base Power (dBmV)	<p>The base channel power for Compact Shelf. Set the base power level. Following is the available ranges for the Base Power:</p> <ul style="list-style-type: none"> • Node RPDs: 20 -22 • Shelf RPDs: 24–61
Tilt Pivot Freq (Hz)	<p>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.</p>
Tilt Slope (dBmV)	<p>Set the tilt slope. The valid range is 0–8.</p>
Upstream Physical Port	<p>Upstream RPD Port of the logical pairing. May be “0” or “1.” Not applicable to second pairing for 1x1 node segmentation.</p>
DS Data Service Group	<p>All RPDs with the same data service group share the downstream controller for Data Service (Virtual Splitting for Data). Not applicable to second pairing for 1x1 or 1x2 node segmentation.</p>
US Data Service Group	<p>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.</p>

Table 3: Video Configuration

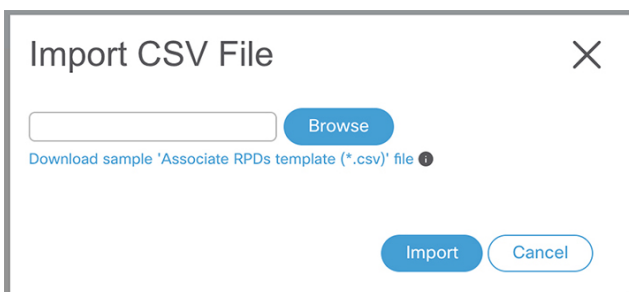
Field Name	Description
Video Core	Name of the Cisco cBR-8 router, which is the auxiliary CCAP core for the RPD that provides video services. Leave this field empty if principal core provides the video services.
Video Core Interfaces	List of complete names of the TenGigabitEthernet DPIC interfaces to be used for Video Services.
Video Service Groups	<p>Video service group (VSG) names. Video is forwarded only in the downstream direction.</p> <p>Not applicable to second pairing for 1x1 or 1x2 node segmentation.</p> <p>Important Cisco Smart PHY does not allow configuring a VSG on a Downstream Port 1 (ds1) with <code>broadcast</code> keyword through the Cisco cBR-8 CLI. If you try to configure, the CLI shows an error.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>

Table 4: OOB & Additional Core Configuration

Field Name	Description
OOB Core	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 Principal Core or the auxiliary Video Core . Leave this field empty if the OOB 55–1 and NDF/NDR services are not used.
OOB Core Interface	Complete name of the TenGigabitEthernet DPIC interface to be used for out-of-band 55–1 and NDF/NDR service. Leave this field empty if the OOB 55–1 and NDF/NDR services are not used.
Downstream VOM ID	OOB 55–1 Downstream Virtual out-of-band Modulator (VOM) Identification (ID). If present, this value overrides the value from the Service Definition.

Field Name	Description
Downstream VOM Profile	OOB 55–1 Downstream VOM profile. If present, this value overrides the value from the Service Definition.
Upstream VARP ID	OOB 55–1 Upstream Virtual Advanced Return Path Demodulator (VARPD) ID. If present, this value overrides the value from the Service Definition.
Upstream VARP Profile	OOB 55–1 Upstream VARP profile for first logical Downstream/Upstream (DS/US) pairing. If present, this value overrides the value from the Service Definition. The upstream VARP profile (upstreamVarpdProfile) and the second upstream VARP profile (secondUpstreamVarpdProfile) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2 .
Second Upstream VARP Profile	OOB 55–1 Upstream VARP profile for second logical Downstream/Upstream (DS/US) pairing. If present, this value overrides the value from the Service Definition. The upstream VARP profile (upstreamVarpdProfile) and the second upstream VARP profile (secondUpstreamVarpdProfile) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2 .
Additional Cores	Add additional unmanaged Cores to the <code>GCP Redirect</code> list by selecting them here. You can select multiple additional cores. You can configure multiple unmanaged Cores. If an unmanaged core is added as a principal Core, the same core cannot be configured again as an additional core. Thus, the unmanaged Principal Core and the unmanaged Additional Core fields are mutually exclusive.
Downstream Controller Profile	Primary downstream CCAP controller profile.
Upstream Controller Profile	Primary upstream CCAP controller profile.

Or to import a CSV file, click the  icon, select the file and click **Import**.



Import CSV File

Browse

[Download sample 'Associate RPDs template \(*.csv\)' file](#)

Import Cancel

520637

Step 3 Click **Save**.

Step 4 Click **Assign**.

View RPD History

Step 1 Choose Cisco Operations Hub main menu > **Smart PHY** > **RPD Automation** > **RPD Assignment**.

Step 2 Select the RPD and click the **Details** button.

The RPD window shows the RPD Summary, RPD State History, RPD CLI, and RPD Automation Errors.

The screenshot displays the 'RPD Assignment' window for 'MK_DB_DUMMY_02'. The window is divided into several sections:

- RPD Summary:** Shows the RPD MAC as a0f8.496f.6110.
- RPD State History:** Shows a list of events:
 - 03/19/2021 5:12:11 PM UTC (GMT0:00) : Configured
 - 03/19/2021 5:12:06 PM UTC (GMT0:00) : Inventory
 - 03/19/2021 5:12:06 PM UTC (GMT0:00) : Defined
- RPD CLI:** Shows the configuration commands for the RPD:


```
[172.22.10.37 2021-03-19 17:12:06.838]
cable rpd MK_DB_DUMMY_02
  identifier a0f8.496f.6110
  core-interface Te3/1/5
  principal
  rpd-ds 0 downstream-cable 3/0/20 profile 100
  rpd-ds 1 downstream-cable 3/0/20 profile 100
  rpd-us 0 upstream-cable 3/0/0 profile 4
  rpd-us 1 upstream-cable 3/0/0 profile 4
  r-dti 1
  rpd-event profile 0
  cable fiber-node 1
  downstream Downstream-Cable 3/0/20
  downstream sg-channel 0 99 downstream-Cable 3/0/20 rf-channel 0 99
  upstream Upstream-Cable 3/0/0
```

A 'Cancel' button is visible at the bottom of the window.

Database Backup

The *Database Backup* section includes the following entry fields:

- Server
- Username
- Password
- Directory

- Filename (Used exclusively for the Database Import function.)

The data that you enter in the **Server** field determines the location of the DB operation.

- Local backup—localhost
- Remote operation—IP address or hostname.domain.com

Manage Users

Administrators on the Cisco Smart PHY application can perform the following tasks from the Cisco Operations Hub main menu > **Systems** > **Users & Roles**.



Note Only administrators can access the **User & Roles** option.

Add Users Through CLI

Use the following procedure to create a new user:

Step 1 Define a new user using the following sample commands:

```
product opshub# smiuser add-user username <username> password <password>
message User added
product opshub#
product opshub# smiuser show-user username <username>
User: <username>, Group(s): <username>, Password Expiration days: 90
```

Note The default password expires in 90 days.

Example:

```
product opshub# smiuser add-user username user123 password Abcd123@
message User added
product opshub#
product opshub# smiuser show-user username user123
User: user123, Group(s): user123, Password Expiration days: 90
```

Step 2 Add a new user to the API group using the following commands.

Applicable groups for Cisco Smart PHY are `admin` and `api-admin`. By default, the `admin` user is mapped to group `admin`.

```
product opshub# smiuser assign-user-group username <username> groupname <groupname>
message User assigned to group successfully
product opshub
```

Example:

```
product opshub# smiuser assign-user-group username user123 groupname api-admin
message User assigned to group successfully
product opshub
```

Basic and LDAP Authentication

The Cisco Smart PHY application supports the following two different authentication mechanisms:

- Basic authentication
- LDAP authentication

The default method is the Basic authentication. You can configure and switch to LDAP and vice versa using the following CLI procedures.

Switch from Basic Authentication to LDAP Authentication



Note LDAP support is limited to Microsoft Active Directory (AD) only. Open LDAP is not supported.

Step 1 Log in to any one of the control-plane nodes using the following command:

```
ssh -i <private-key-file> <smartphy-user>@<control-plane-node-ip>
```

Step 2 Enter the following command.

```
kubectl get svc ops-center-smartphy-data-ops-center -n smartphy-data
```

Note the cluster IP address and TCP ports of the service ops-center-smartphy-data-ops-center.

```
Ops-center-smartphy-data-ops-center   ClusterIP      10.x.x.x   <none>
8008/TCP,8080/TCP,2024/TCP,2022/TCP,7681/TCP   19d
```

Step 3 Enter the following command to log in to the service resource using the password previously set by the deployer.

```
ssh admin@<cluster-ip-of-svc> -p <port-number>
```

Example:

```
smartphyuser: ~$ ssh admin@10.x.x.x -p 2024
Warning: Permanently added '[10.x.x.x]:2024' (RSA) to the list of known hosts.
admin@10.x.x.x's password:
Welcome to the smartphy CLI on user/data
admin connected from172.x.x.x using ssh on ops-center-smartphy-data-ops-center-774b8cc6fb-n6qmz
[user/data] smartphy#
```

Step 4 Run the following command to enter the configuration mode and get a list of available commands.

```
config
```

Use the `kong` command and its sub-commands.

Step 5 Display a list of configuration options available to configure the LDAP authentication plugin using the following command.

```
kong ldap_plugin configure ?
```

Step 6 Enter the required details of the Active Directory you want to use with the LDAP authentication plugin and enter `commit` to save.

Example:

Switch from LDAP Authentication to Basic Authentication

```
kong ldap_plugin configure attribute cn ldap_host ldap.example.com ldap_port 309 base_dn
dc=example,dc=com
```

Step 7 Enter the following command to enable the LDAP authentication plugin.

```
kong ldap_plugin enable true
commit
```

By default, the LDAP plugin is disabled. However, the Basic authentication plugin is enabled.

If you are using the LDAP authentication plugin for the first time, you should configure before enabling it.

Step 8 Enter `end` to exit the config mode and `exit` to exit the service resource.

You can log in to the UI using an LDAP user credentials.

Switch from LDAP Authentication to Basic Authentication

Local authentication is enabled by default in the Cisco Operations Hub.

Step 1 Go to the Cisco Operations Hub main menu > **Systems** > **Authentication** to change the authentication method to basic.

Step 2 If the LDAP authentication is enabled, click **Edit** and select the **Authentication Method** as **Local**.

Step 3 Save your changes.
