



Cisco Smart PHY Application User Guide, Release 21.3

First Published: 2021-11-17

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	1
	Benefits of Cisco Smart PHY	1
	Dashboard	2
	Inventory	3
	RPD Automation	6
	User Management	17

CHAPTER 2	Configure DAA Infrastructure	19
	Configure DHCP	19
	Configure Cisco cBR-8 for Smart PHY Application	19

CHAPTER 3	Access Cisco Smart PHY Application	21
	Log in Using a Browser	21
	Bring Up the RPD	22

CHAPTER 4	Configure Credential Profiles	23
	Create a New Credential Profile	23
	Apply Device Credential from Credential Profiles	24
	Apply a Different Credential Profile to Existing Devices	24
	Apply Different Credential Profile in Bulk	25
	Delete a Credential Profile	25

CHAPTER 5	Manage Devices	27
	Add Devices through GUI	27
	Create CSV File for Importing Devices	28
	Import Device Information in Bulk	29

Export Device Information to a CSV File	29
Delete a Device from the Inventory	30
Fetch SSH Keys from Cisco cBR-8	30
Disable Southbound Communication to Cisco cBR-8 Router	31
Restricted Cisco Smart PHY Operations	31

CHAPTER 6**Manage RPDs 33**

Add and Assign RPDs	33
Create a New Service Definition	37
Edit Service Definition	40
Provision RPD for Video Support	41
Configure Video Service	44
View RPD History	47
Manage GCP Redirection	48
Configure I15 GCP Redirect	48
I15 GCP Redirect APIs	49
I15 GCP-redirect Result Notification	50

CHAPTER 7**Security and Administration 51**

Manage Users	51
Add Users Through Cisco Operations Hub	51
Add Users Through CLI	52
Update User Password	52
Edit Users	53
Delete a User	53
Filter Users	53
View Session History	53
Authentication	53
Switch from Basic Authentication to LDAP Authentication	54
Switch from LDAP Authentication to Basic Authentication	54
Customize Login Banner	54
Database Backup	55
Local Backup	55
Remote Backup	55

Import Database	56
Renew Kubernetes Client TLS Certificate	56

CHAPTER 8**Monitor and Troubleshoot 57**

Monitor Host Resources	57
API Explorer	57
Debug RPD SSD on Cisco Smart PHY	57
Check SSD on NSO	58
Check SSD using RestAPI	58
Check SSD on Cisco cBR-8	61
Debug SSD on Cisco cBR-8	61
DEPI Latency Measurement in Service Template	62
Check New DLM Configuration on Cisco cBR-8	62

APPENDIX A**Best Practices 65**

Best Practices	65
----------------	----





CHAPTER 1

Information about Cisco Smart PHY

The Cisco Smart PHY application simplifies the installation, configuration, monitoring, and troubleshooting of Remote PHY Devices (RPD) serviced by Cisco cBR-8 routers. It enables multiple use cases, including:

- Distributed Access Architecture (DAA) deployment simplification
- RPD deployment automation
- RPD software lifecycle management
- CIN Traffic engineering
- Common DHCP policy

These are some general instructions and information for using the Cisco Smart PHY:

Icon	Description
	Information button. Click this button to display more information.
	Context Menu button. Move the mouse over this button to display a context menu.

- [Benefits of Cisco Smart PHY, on page 1](#)
- [Dashboard, on page 2](#)
- [Inventory, on page 3](#)
- [RPD Automation, on page 6](#)
- [User Management, on page 17](#)

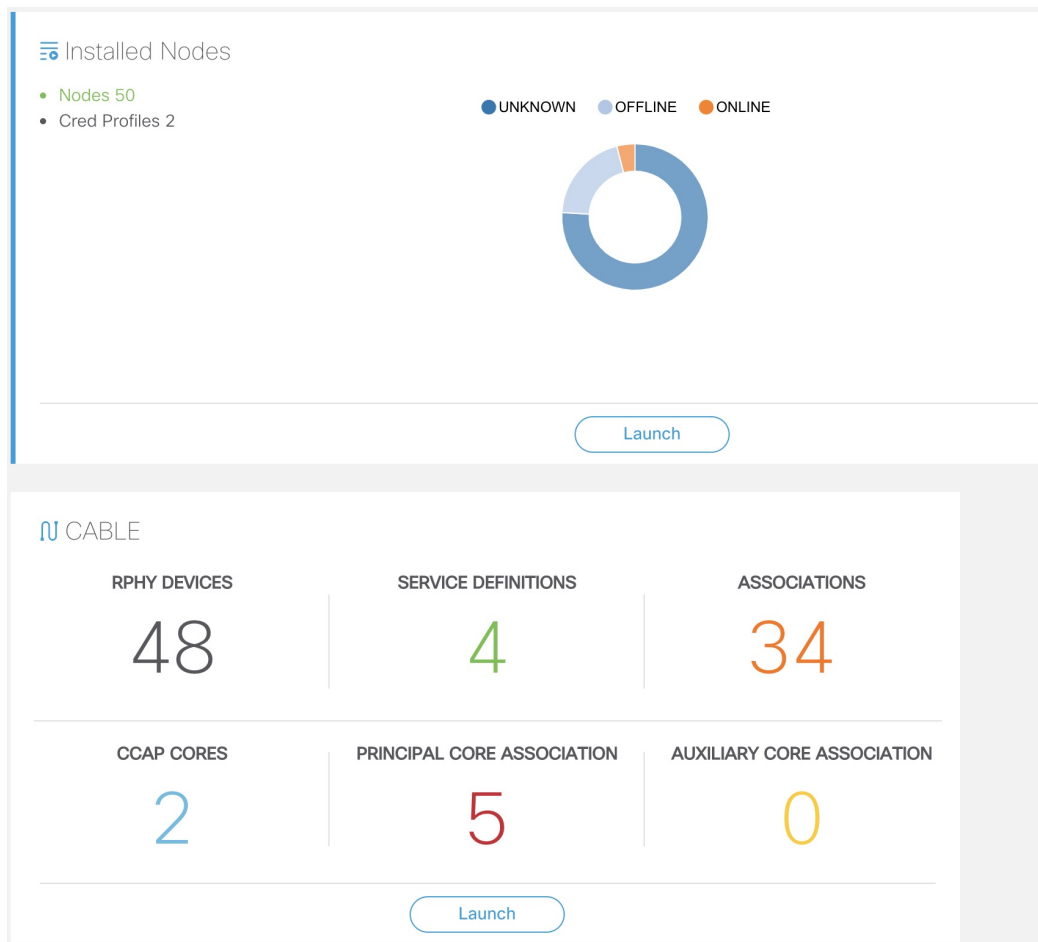
Benefits of Cisco Smart PHY

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

- **Initial RPD Zero-Touch Automation:** Initial RPD installation and provisioning with Zero-touch of the Cisco CMTS.
- **Inventory:** Tracks RPD and CCAP resources, allowing operators to perform searches on several provisioning-specific criteria.

- Configuration generation and push: Generates error free Cisco cBR-8 RPD configuration and ensures that the configuration is pushed to the appropriate DOCSIS Principal and Video CCAP Cores.
- RPD SW management: Manages RPD software.
- API centric design: Direct programmatic access for operators to various Cisco Smart PHY services and functions using open interfaces and tools.
- Deployment validation: Monitors Cisco cBR-8 routers for unauthorized out-of-band changes to RPD configurations.

Dashboard



Following are the field descriptions:

Name	Description
Dashboard	Snapshot view of all devices managed and monitored by the Cisco Smart PHY application.

Name	Description
Installed Nodes	Shows the number of nodes installed using the Cisco Smart PHY application. This panel also shows the number of Credential Profiles available in the application. The pie chart shows the offline, online, and unknown (unmanaged cores) nodes.
Launch	Takes you to the specific page view.
Cable	Shows the following details in this pane: configured and managed using the RPD Automation page. <ul style="list-style-type: none"> • RPHY Devices • Service Definitions • Associations • CCAP Cores • Prinicpal Core Association • Auxiliary Core Association Click the number to view more details. Click the Launch link to go to the RPD Automation page.

Inventory

Inventory has two tabs; Inventory and Credential Profiles.

The screenshot displays the 'Inventory' tab in the Cisco Smart PHY application. At the top, there are three summary charts: 'Status' (a pie chart showing Offline, Unknown, and Online nodes), 'Type' (a gauge chart showing Node-Unknown, Node-Virtual, CBR-8-CCAP-Chassis, and Shelf-600-6X12), and 'Manufacturer' (a gauge chart showing Cisco). Below these charts is a table with columns for Status, Host Name, Key Type, IP Address, MAC Address, UUID, Product Type, Credential Pr..., Latitude, Longitude, and Loc. The table contains several rows of data, with the last row selected and highlighted in blue.

Status	Host Name	Key Type	IP Address	MAC Address	UUID	Product Type	Credential Pr...	Latitude	Longitude	Loc
✗	MK_DB_DUMMY_07	MAC ADDRESS		A0F8.496F.6117	_DEVICE_A0F8496F...	NODE-UNKNOWN				
✗	HA_SQUMIKC	MAC ADDRESS		4444.5555.3333	_DEVICE_44445555...	NODE-UNKNOWN				
✗	MK_898	MAC ADDRESS	10.40.5.221	C000.0000.0001	_DEVICE_C0000000...	NODE-VIRTUAL		-9.2322424	-7.7878787	
✗	MK_DB_DUMMY_04	MAC ADDRESS		A0F8.496F.6114	_DEVICE_A0F8496F...	NODE-UNKNOWN				
⏸		MAC ADDRESS		A0F8.496F.9999	_DEVICE_A0F8496F...	NODE-UNKNOWN				
☑	sphy-c2.cisco.com	IP ADDRESS	172.22.9.171		_DEVICE_172.22.9...	CBR-8-CCAP-CHASS gold				

Inventory

The **Inventory** tab enables you to onboard and organize your managed and unmanaged CCAP Cores.















Note Add the RPDs through the Cable Pairing table in the Cisco Smart PHY application and not through the Inventory tab.

Cisco Smart PHY supports 50000 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 through its REST API.

Following are the field descriptions for Inventory:

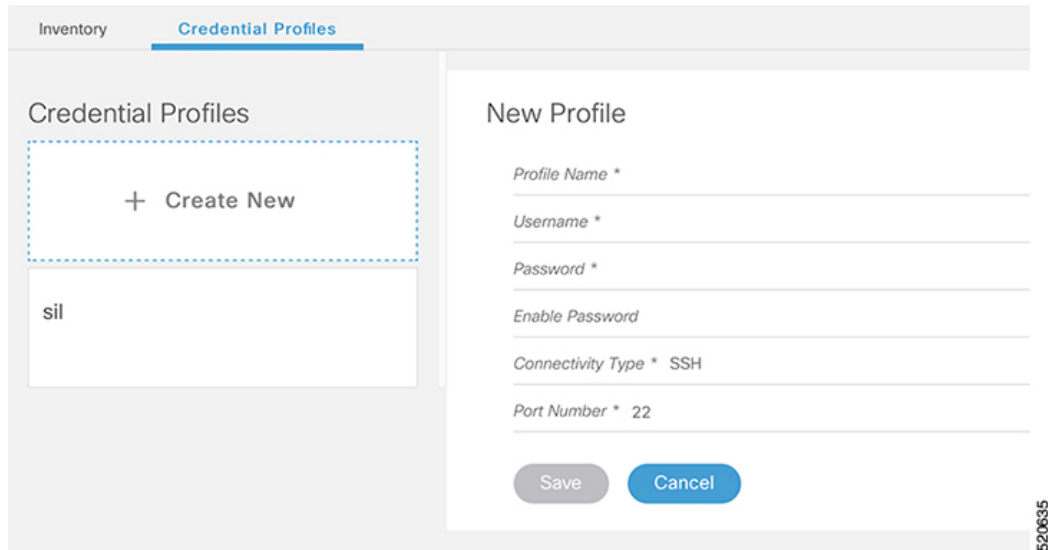
Name	Description
Status	Shows a graphical pie chart of all devices in the network, categorized by status: <ul style="list-style-type: none"> • ONLINE • OFFLINE • UNKNOWN • SSHKEYFETCH • MAINTENANCE • NORMALOPS_PROGRESS
Host Name	Host name of the device.
Key Type	Two types: <ul style="list-style-type: none"> • MAC ADDRESS • IP ADDRESS
IP Address	IP address of the device.
MAC Address	MAC address of the device.
UUID	Universally unique identifier of the device.
Product Type	Product type of the device.
Credential Profile	Credential profile name.
Latitude	Latitude of the device.
Longitude	Longitude of the device.
Location	Location of the device.
Description	Description of the device.
Software Version	Software version of the device.
Model Number	Model number of the device.

Name	Description
	Adds a device to the existing inventory.
	Edits the device information.
	Deletes a device from the inventory.
	Imports devices by using a CSV file.
	Exports device information to a CSV file.
	Synchronizes RPD states manually by fetching the latest RPD status.
	Enables maintenance mode on one or more Cisco cBR-8 routers. Applicable only to Cisco cBR-8 routers.
	Resumes normal operations on one or more Cisco cBR-8 routers. Applicable only to Cisco cBR-8 routers.
	Fetches the SSH key on one or more Cisco cBR-8 routers. Applicable only to Cisco cBR-8 routers. Cisco Smart PHY 3.1.4 and later, supports SSH key fetch from offline and online Cisco cBR-8 routers. The SSH key fetch states are the following: <ul style="list-style-type: none"> • SSHKEYFETCH_IN_PROGRESS • SSHKEYFETCH_FAILED For more details, see the section Fetch SSH Keys from Cisco cBR-8, on page 30 .
	Status showing SSH key failure.
	Status shows one of the following states: <ul style="list-style-type: none"> • Fetching SSH Keys • Resuming Normal Operations from the maintenance mode
Details	Shows the details of the devices, such as Device Summary and Device State History
	Sets the columns in the device table.
Search	Allows you to search for and filter the network devices.
Devices table	Shows detailed information about each device in the network.

Credential Profiles

Credential profiles are collections of device credentials for Telnet or SSH network devices. 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.

Figure 1: Credential Profiles



Following are the field descriptions for Credential Profiles:

Name	Description
+ Create New	Allows you to add or edit a credential profile. Note Mandatory fields are marked with an asterisk.
New Profile	You can create a new profile by entering the required details and saving the profile.

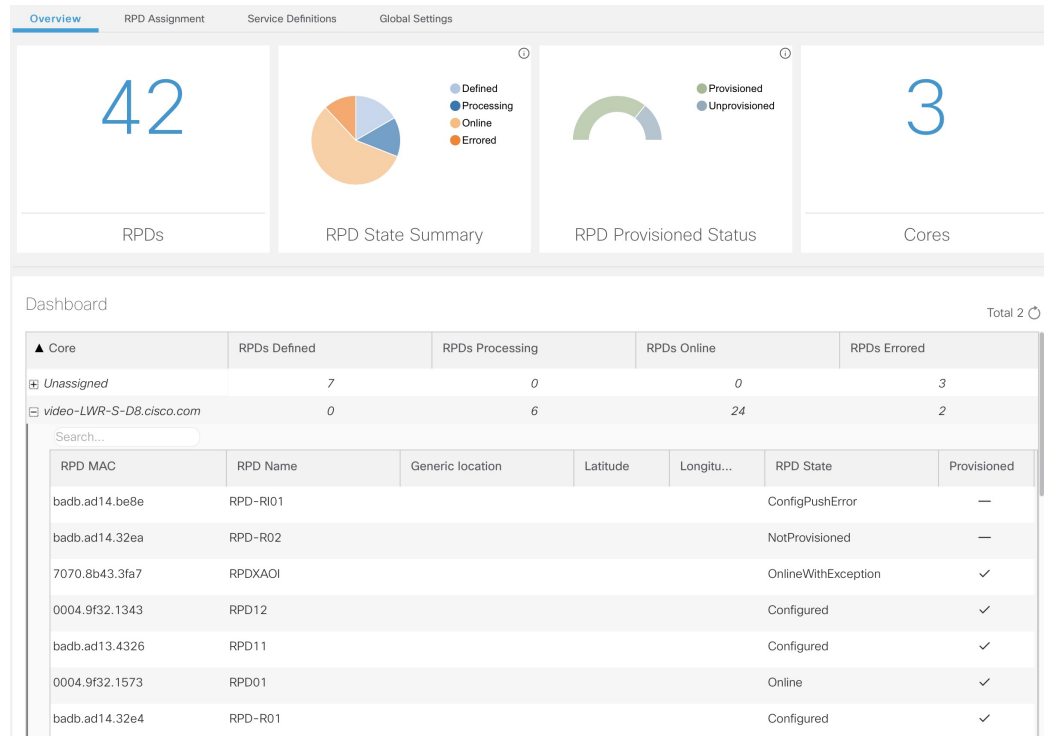
RPD Automation

The **RPD Automation** page enables you to add, organize, and update information about CMTS and RPD devices in the network. The information available in the view is focused on CCAP Cores and Remote PHY Devices.

The **RPD Automation** page has four tabs; Overview, RPD Assignment, Service Definitions, and Global Settings.

Overview

Provides a view of the number of RPDs, their status, and the number of Cores. Also, it provides a dashboard view of the Core and the RPDs in different states.



You can view the following RPD State Summary table by clicking the icon in the RPD State Summary dashlet.

Table 1: RPD States Summary

RPD Summary	RPD State	Description
DEFINED	Defined	RPD pairing is defined. However, MAC address is not yet assigned.
DEFINED	Installed	Installed RPD. RPD name, MAC address, and the GPS location are available.
DEFINED	Inventory	Added RPD MAC address to the inventory without the GPS details.
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 get the existing CCAP core configuration.
ERRORED	ConfigurationError	Assigned incorrect RPD in the Cisco Smart PHY application.

RPD Summary	RPD State	Description
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	ResourceAllocationError	Unable to allocate resources to an RPD for the assigned CCAP core or interface.
ONLINE	Online	RPD is online on the CCAP core.
ONLINE	OnlineWithException	RPD is online, but NDF or NDR fails.
ONLINE	PartialOnline	Partial services are available if the RPD is not online on all cores.
PROCESSING	Configured	CCAP core is configured. RPD configuration is pushed to the CCAP core.
PROCESSING	DeletePending	RPD pairing deletion is pending.
PROCESSING	GcpRedirected	Received an ACK from the RPD for the CCAP core redirect message. This redirect message captures the result of the redirect request, initiated by the Cisco Smart PHY application, along with the hostname, the IP address, and the interface of the redirected core.
PROCESSING	GcpRedirectStartedWithException	RPD configuration is pushed to the CCAP core and redirecting the RPD to that core has started. However, one of the following errors occurred: <ul style="list-style-type: none"> • RouterVersionIncompatible • StaticRouteNotConfigured
PROCESSING	GcpRedirectStarted	RPD configuration is pushed to the CCAP core and the RPD is redirected to that core.
PROCESSING	GcpRedirectedWithException	Received an ACK from the RPD for the CCAP core redirect message. However, one of the following errors occurred: <ul style="list-style-type: none"> • RouterVersionIncompatible • StaticRouteNotConfigured

RPD Summary	RPD State	Description
PROCESSING	GcpUp	Received GCP message from the RPD.
WARNING	RouterVersionIncompatible	RPD software version is incompatible with the CCAP core version.
WARNING	StaticRouteNotConfigured	Static route is not configured.






RPD Assignment

Allows you to add, edit, import, or export the details of RPD assignments. Search allows you to search for or filter the RPD information.

The screenshot shows the 'Associate RPDs' window. On the left, the 'Select Service Definition' sidebar lists various service definitions with their assigned RPD counts. The main area displays a table of RPDs with columns: RPD Name, MAC, Service Definition, Principal Core, and DS Port. The table contains several rows, with the row for 'MK_DB_DUMMY_07' selected. Above the table, there are buttons for '+', '-', 'Assign', 'Clear', and 'Details', along with a search bar and a status indicator 'Selected 1 / Total 21'.

Following are the menu options available on the RPD Assignment window:

Options	Description
	To assign an RPD for a specific RPD name or to add an RPD MAC address to the RPD Inventory. You can assign additional RPD information only after specifying a name for the RPD MAC address.
	To edit an existing RPD assignment. You can edit the name, the MAC address information, and so on.

Options	Description
	<p>To delete an RPD name and its RPD assignment information.</p> <p>When you delete the RPD Assignment details, the RPD MAC address that is assigned to the RPD name is moved back to the Inventory and is retained in the system.</p> <p>To delete the RPD MAC address, delete it from the main Inventory page.</p> <p>Similarly, deleting an RPD MAC address from the Inventory does not delete the RPD name and its assignment information in the RPD Assignment table. This deletion removes only the RPD MAC address from the RPD Assignment table.</p>
	<p>Imports the details of RPD assignments using a CSV file.</p> <p>Sample of the CSV file is available when you click this icon.</p>
	Exports the details of RPD assignments to a CSV file.
	Synchronizes RPD states manually by fetching the latest RPD status.
Assign	To assign the chosen Service Definition to all the selected RPDs.
Clear	To clear the core and the service template assignment for a specific RPD name. This option does not clear the mapping between an RPD name and the MAC address.
Details	To get the details of the RPD, such as RPD Summary, RPD State History, and RPD CLI.
Search	Use any filtering option.
	Sets the required columns in the device table.

Following are the field descriptions in the Associate RPDs table:

Field Name	Description
Status	Shows the status of the RPDs.
Provisioned	Shows whether the RPD is provisioned or not.
RPD Name	<p>Name for the RPD.</p> <p>This RPD name is also used in the <code>cable rpd</code> CLI command.</p>
MAC	MAC address of the RPD.
Segmentation	Node segmentation of the RPD: 1x1, 1x2, or 2x2.

Field Name	Description
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.
Principal Core	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.
SSD Profile	Secure Software Download (SSD) profile details for image storage.
Disable Network Delay	The default is value is No . <ul style="list-style-type: none"> • No: Apply the network-delay from service definition to RPD. • Yes: Do not apply the 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>
Principal Core Interface	If the Principal Core is a managed Cisco cBR-8 router, the name of the TenGigabitEthernet DPIC interface is listed in this field. If the Principal Core is an unmanaged Core, the field is empty.
Video Core	Name of the Cisco cBR-8 router, which is the auxiliary CCAP core for the RPD that provides video services.
Video Core Interfaces	List of complete names of the TenGigabitEthernet DPIC interfaces to be used for Video Services.
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.
OOB Core Interface	Complete name of the TenGigabitEthernet DPIC interface to be used for out-of-band 55-1 and NDF/NDR service.
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.
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 (VARP) 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 (<code>upstreamVarpdProfile</code>) and the Second Upstream VARP Profile (<code>secondUpstreamVarpdProfile</code>) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2, on page 42 .

Field Name	Description
Second Upstream VARPDP Profile	OOB 55-1 Upstream VARPDP profile for second logical Downstream/Upstream (DS/US) pairing. If present, this value overrides the value from the Service Definition. The upstream VARPDP profile (upstreamVarpdProfile) and the second upstream VARPDP profile (secondUpstreamVarpdProfile) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2 , on page 42.
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.
Additional Cores	Semicolon separated list of additional cores to which the RPD must connect.
Latitude	Latitude of the RPD (GPS coordinates)
Longitude	Longitude of the RPD (GPS coordinates)
RPD Description	Description for the RPD

Service Definitions

Allows you to add, edit, delete, or assign service templates. Fields that are not marked as optional are mandatory.

The screenshot displays the 'Service Definitions' configuration interface. On the left, a list of service definitions is shown, each with a 'Create New' button and an 'Assigned' count. The main area shows the configuration for the 'SystemTemplate' service definition. The configuration includes various fields such as 'Name', 'Description', 'Event Profile', 'R-DTI Profile', 'Pilot Tone Profile', 'Cable DSG TGs', 'First Logical DS/US Pairing', 'Second Logical DS/US Pairing', 'Service Group Profile', 'Downstream Controller Profile', 'Upstream Controller Profile', 'Enable MAC Domain Splitting', 'Network Delay', 'Out Of Band', 'Downstream VDM ID', and 'Downstream VOM Profile'. The 'Set as Default' checkbox is checked.

Following are the menu options descriptions:

Name	Description
+ Create New	Click this option to create a new service template.

Name	Description
<i>Name of the existing service definition</i>	Click the name of the existing service definition to edit the template.
New Service Definition	Enter the details in each field and click the Save button to create a new service template.
Search	Use this Search text field in upper right-hand corner to filter service definition names.

Global Settings

You can perform the following configurations from the Global Settings window.

- Database Backup
- Global Configuration
- Software Compatibility

Database Backup

You can back up the database to a local server or a remote server.

Overview RPD Assignment Service Definitions **Global Settings**

Database Backup

Server * ⓘ hostname.domain.com

Username * admin

Password *

Directory * /users/name/folder/

Filename (Import Only *) ⓘ smartphy_InstanceName_backup_timestamp.tar.gz

Export Import Reset

Database Backup Status

Operation	Start Time	End Time	Message

The database backup file is a TAR.GZ file with the following naming convention: filename_YYYYMMDD_HHMMSS.tar.gz. For example, aio_backup_20210318_121354.tar.gz. Enter the following details in the **Database Backup** window to back up the database.

Field	Description
Server	The location where you want to save the DB. <ul style="list-style-type: none"> Local backup—Enter localhost. Local backup files are saved to the /var/smartphy/backup directory on the local filesystem. Remote backup—Enter the IP address or the principal coreFQDN of the remote host. For remote backup, the Cisco Smart PHY application uses SFTP to transfer files from Cisco Smart PHY instances.
Username	<ul style="list-style-type: none"> Local backup—Leave the field empty. Remote backup—Enter the username for the remote server access.

Field	Description
Password	<ul style="list-style-type: none"> Local backup—Leave the field empty. Remote backup—Enter the password for the remote server access.
Directory	<ul style="list-style-type: none"> Local backup—Leave the field empty. Remote backup—Enter the file path of the directory in the remote server.
Filename (Import Only)	<p>Used exclusively for importing a database. Imported file must be in the following format: <code>smartphy_InstanceName_backup_timestamp.tar.gz</code></p> <ul style="list-style-type: none"> Local backup: Enter only the filename of the backup file available in the default directory: <code>/data/smartphy/backup</code> Remote backup: Enter the file path (absolute path) of the remote server.
Export	Click the Export button to perform local and remote backup.
Import	Click the Import button to import a DB.

Global Configuration

The **Global Configuration** section under the **Global Settings** menu provides the following options for you to configure on RPDs. Choose the following functions according to your requirement.

- **Configure Static Routes**—If you enable this option, for interfaces with /31 (IPv4 networks) or /127 (IPv6 networks) configured on the DPIC, the Cisco Smart PHY application adds a static route configuration on the Cisco cBR-8 router per RPD.
- **Validate Software Compatibility**—If you enable this option, the Cisco Smart PHY application checks the compatibility between the RPD version and the Cisco cBR-8 router version that is specified in the table.
- **Persist Running Configuration**—If you enable this option, when the Cisco Smart PHY makes a change to the Cisco cBR-8 configuration, the Cisco Smart PHY makes the configuration persistent. This option allows you to make the changes persistent on the Cisco cBR-8 router at a specific interval.

Global Configuration

 Configure Static Routes

 Validate Software Compatibility

 Persist Running Configuration

Config Save Interval: 60

Software Compatibility Selected 1 / Total 1

Search...

<input checked="" type="checkbox"/>	RPD Vendor	RPD Software Version	Router Product Type	Router Software Version
<input checked="" type="checkbox"/>	Arq	v8.6	CBR-8-CCAP-CHASS	17.2.1

Static Route

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 configure the RPDs.

Smart PHY automatically creates a static route for the RPD if the 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
```

Software Compatibility

Allows you to add, edit, or delete the software compatibility matrix. Fields that are not marked as optional are mandatory.

Software Compatibility—This window displays a compatibility matrix for the RPD software versions and the Cisco cBR-8 software versions. The Smart PHY application detects the software incompatibility between an RPD and a Cisco cBR-8 router, and alerts you about the incompatibility. After the alert appears, either manually upgrade the RPD software or associate the RPD with an SSD profile through the Cisco Smart PHY application, which notifies the Cisco cBR-8 for the software upgrade.

Table 2: Field Description for Software Compatibility Matrix

Name	Description
RPD Vendor	Name of the RPD vendor.
RPD Software Version	Software version running on the RPD.

Name	Description
Router Product Type	Product type of the router from the Inventory. Example: CBR-8-CCAP-CHASS
Router Software Version	Software version of the router.

User Management

Administrators can manage users in the Cisco Smart PHY application by using the **Systems > Users & Roles** menu option. For more details, see [Manage Users, on page 51](#).



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



CHAPTER 2

Configure DAA Infrastructure

This section describes how to configure your Distributed Access Architecture (DAA) infrastructure to work with the Cisco Smart PHY application.

- [Configure DHCP](#) , on page 19
- [Configure Cisco cBR-8 for Smart PHY Application](#), on page 19

Configure DHCP

To establish a GCP session with the Cisco Smart PHY application, 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.

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>
```



CHAPTER 3

Access Cisco Smart PHY Application

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

- [Log in Using a Browser, on page 21](#)
- [Bring Up the RPD, on page 22](#)

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. If the system administrator keeps the session idle for a long time, the Cisco Smart PHY application prompts you to re-login.
-

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 23](#).

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 27](#) and [Import Device Information in Bulk, on page 29](#).

Step 4 Create a Service Template.

For more details, see the section [Create a New Service Definition, on page 37](#).

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 33](#).

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.



CHAPTER 4

Configure Credential Profiles

- [Create a New Credential Profile, on page 23](#)
- [Apply Device Credential from Credential Profiles, on page 24](#)
- [Apply a Different Credential Profile to Existing Devices, on page 24](#)
- [Apply Different Credential Profile in Bulk, on page 25](#)
- [Delete a Credential Profile, on page 25](#)

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 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, under the 'Credential Profiles' heading, there is a '+ Create New' button and a list of profiles. The profile 'sil' is selected and highlighted. On the right, the 'Edit Profile' form is visible, showing the following fields and values:

- 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'. The 'Delete' button is highlighted in blue. A vertical ID number '520634' is located on the right side of the form area.



CHAPTER 5

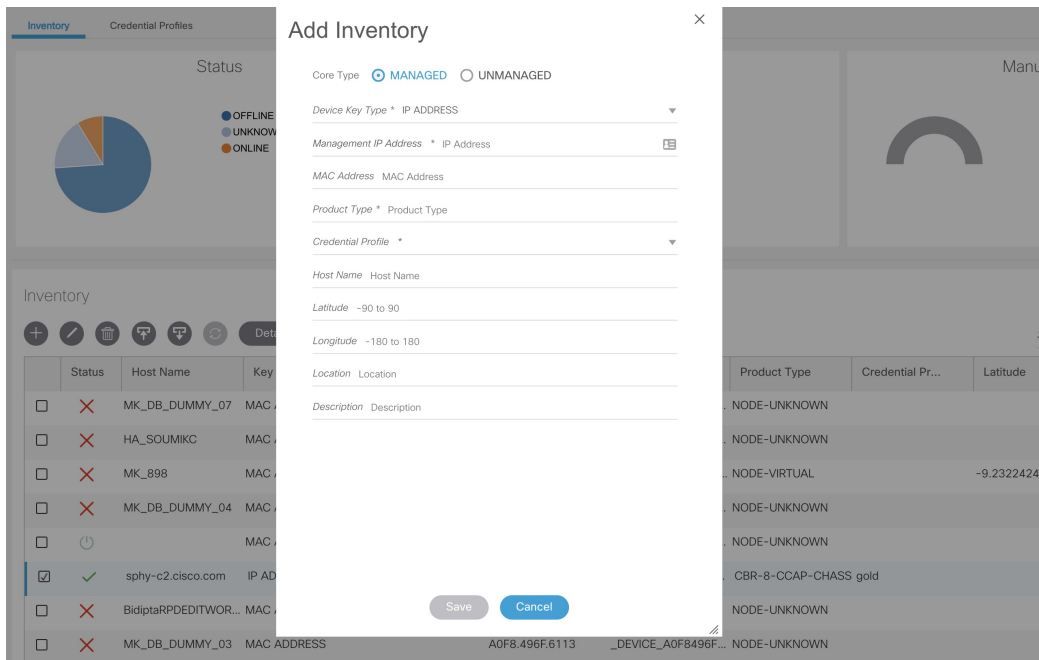
Manage Devices

- [Add Devices through GUI, on page 27](#)
- [Create CSV File for Importing Devices, on page 28](#)
- [Import Device Information in Bulk, on page 29](#)
- [Export Device Information to a CSV File, on page 29](#)
- [Delete a Device from the Inventory, on page 30](#)
- [Fetch SSH Keys from Cisco cBR-8, on page 30](#)
- [Disable Southbound Communication to Cisco cBR-8 Router, on page 31](#)
- [Restricted Cisco Smart PHY Operations, on page 31](#)

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.)



Step 5 Click **Save**.

Step 6 (Optional) Repeat to add more devices.

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

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**.

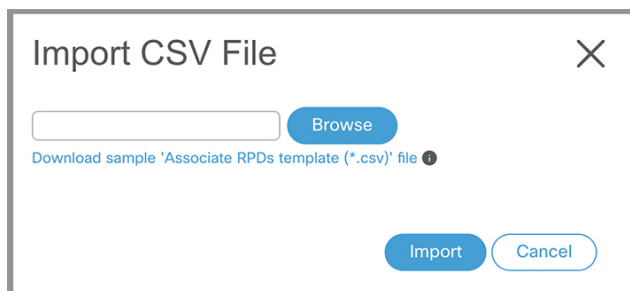
Step 2 Click the import icon (📄).

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.

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 ()

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.

Fetch SSH Keys from Cisco cBR-8

Cisco Smart PHY can fetch new SSH keys either in bulk or by choosing an individual Cisco cBR-8 router using the user interface or API.

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

In the **Inventory** window, choose Cisco cBR-8 routers and click the SSH key icon () . The following pop-up message appears when the fetching process starts:

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

When the fetching process is in progress or the status of the Cisco cBR-8 router is `Unknown`, you cannot do another key fetch.

To view the status of the fetch operation, click the **Details** button.

The following statuses appear for the SSH key fetching process:

- `SSHKEYFETCH_PROGRESS`: When fetching the SSH keys is in progress.
- `ONLINE_WITH_EXCEPTION`: When fetching of SSH keys fails.

When the fetch operation is successful, the status of the router updates to `Online`.

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
```

To fetch the SSH keys for all Cisco cBR-8 routers in the Cisco Smart PHY application, set the `allCore` parameter to `true` in the request message of the

`rpdc-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`

Disable Southbound Communication to Cisco cBR-8 Router


You can enable or disable Cisco Smart PHY southbound communications with a Cisco cBR-8 router or a group of Cisco cBR-8 routers.

Disabling the southbound communications allows the selected Cisco cBR-8 routers to undergo maintenance without interference from Cisco Smart PHY checking for liveness or configuration sync. To set the Cisco cBR-8 router to maintenance mode, choose one or more Cisco cBR-8 routers on the Cisco Smart PHY

Inventory page and click the  icon.

When you disable southbound communication:

- Cisco Smart PHY does not allow you to make any configuration changes through the UI or API to those Cisco cBR-8 routers.
- GCP does not redirect RPDs associated with those Cisco cBR-8 routers.

To resume normal operation, choose an under maintenance Cisco cBR-8 router and click the  icon and confirm it.

Resuming normal operation may take some time, based on your network connectivity, as it checks the state of the router. When this check happens, the router is in the transient state of `NORMALOPS_PROGRESS`. After the check is complete, the state of the router updates to reflect the results: `Online` or `Offline`

You can see the status change by clicking the **Details** button.



Note The version 1 (V1) RPD-pairing REST API is not blocked when the Cisco Smart PHY application disables the southbound communication to a Cisco cBR-8 router by moving the router into maintenance mode. Only the V2 API is blocked.

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 6


Manage RPDs

- [Add and Assign RPDs, on page 33](#)
- [Create a New Service Definition, on page 37](#)
- [Provision RPD for Video Support, on page 41](#)
- [View RPD History, on page 47](#)
- [Manage GCP Redirection, on page 48](#)

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	
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>

Field Name	Description
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	Name for the RPD. This RPD name is also used in the <code>cable rpd</code> CLI command.
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	The default is value is No . <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. Changing this value to <code>yes</code> is service impacting, if the RPD's assigned Service Definition/Template has network-delay configured.
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	
Principal Core	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. 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: <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	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. Leave this field empty if there is no Principal Core or if the principal core is unmanaged.
SSD Profile	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.

Table 3: First and Second Logical DS/US Pairing

Field Name	Description
Downstream Physical Port	Downstream RPD port of the logical pairing. 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.
Base Power (dBmV)	The base channel power for Compact Shelf. Set the base power level. Following is the available ranges for the Base Power : <ul style="list-style-type: none"> • Node RPDs: 20 -22 • Shelf RPDs: 24–61
Tilt Pivot Freq (Hz)	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)	Set the tilt slope. The valid range is 0–8.
Upstream Physical Port	Upstream RPD Port of the logical pairing. May be “0” or “1.” Not applicable to second pairing for 1x1 node segmentation.
DS Data Service Group	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.
US Data 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.

Table 4: 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.

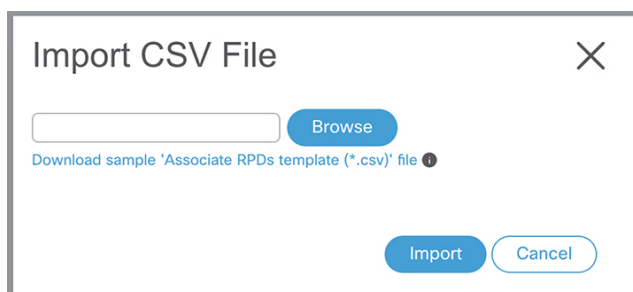
Field Name	Description
Video Service Groups	<p>Video service group (VSG) names. Video is forwarded only in the downstream direction.</p> <p>Not applicable to second pairing for 1x1 or 1x2 node segmentation.</p> <p>Important Cisco Smart PHY does not allow configuring a VSG on a Downstream Port 1 (ds1) 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 5: OOB & Additional Core Configuration

Field Name	Description
OOB Core	<p>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.</p> <p>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.</p>
OOB Core Interface	<p>Complete name of the TenGigabitEthernet DPIC interface to be used for out-of-band 55-1 and NDF/NDR service.</p> <p>Leave this field empty if the OOB 55-1 and NDF/NDR services are not used.</p>
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.
Downstream VOM Profile	OOB 55-1 Downstream VOM profile. If present, this value overrides the value from the Service Definition.
Upstream VARPD ID	OOB 55-1 Upstream Virtual Advanced Return Path Demodulator (VARPD) ID. If present, this value overrides the value from the Service Definition.

Field Name	Description
Upstream VARPDP Profile	OOB 55-1 Upstream VARPDP profile for first logical Downstream/Upstream (DS/US) pairing. If present, this value overrides the value from the Service Definition. The upstream VARPDP profile (upstreamVarpdProfile) and the second upstream VARPDP profile (secondUpstreamVarpdProfile) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2, on page 42 .
Second Upstream VARPDP Profile	OOB 55-1 Upstream VARPDP profile for second logical Downstream/Upstream (DS/US) pairing. If present, this value overrides the value from the Service Definition. The upstream VARPDP profile (upstreamVarpdProfile) and the second upstream VARPDP profile (secondUpstreamVarpdProfile) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2, on page 42 .
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**.



Step 3 Click **Save**.

Step 4 Click **Assign**.

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 6: 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
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
Upstream Controller Profile	Secondary upstream CCAP controller profile.	Yes

Name	Description	Service Affecting Parameter
Enable MAC Domain Splitting	Select the check box to split a MAC domain between two fiber-nodes that share the same downstream controller.	Yes
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, on page 42.</p>	No

Name	Description	Service Affecting Parameter
Second Upstream VARPDP Profile	OOB 55-1 Upstream VARPDP profile for second logical downstream/upstream (DS/US) pairing. The upstream VARPDP profile (<code>upstreamVarpdProfile</code>) and the second upstream VARPDP profile (<code>secondUpstreamVarpdProfile</code>) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2, on page 42 .	No
NDF/NDR		
Pseudowire Name	NDF Narrowband digital forward pseudowire name. Supports up to three pseudowire names and profile ID sets per DS port. NDR Narrowband digital return pseudowire name. Supports up to three pseudowire names and profile ID sets per US port.	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 <code>ntool</code> to convert the XML configuration from the Cisco cBR-8 router to the required XML format.	No

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

Edit Service Definition

You can edit service definition parameters dynamically even when RPDs are associated to those service definitions. You can then apply the changes to one or more RPDs already running that specific service definition.

However, you cannot apply the service definition parameters that lead to a service disruption or `config push error` in the Cisco cBR-8 router to RPDs that are already provisioned. You can save those service definitions in the Cisco Smart PHY application and apply them to new RPD associations.

When RPDs are associated to a service definition, you cannot apply some of the parameters to the existing RPDs, after updating them. For more details, see [Table 6: Service Definition Parameters, on page 38](#). Reconfigure the RPDs if you want to apply the changes. In addition, 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 Details** panel.

Step 1 Choose **RPD Automation > Service Definitions**.

Step 2 Click the service definition which you want to edit and update the required fields.

Step 3 Click **Save** or **Save & Assign**.

Save the changes to the Cisco Smart PHY database and then you can assign it to one or more RPDs running this service definition. The **Save & Assign** button is disabled when the service impacting parameters are updated.

Provision RPD for Video Support

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 the specified Video Auxiliary core. You can configure the OOB core to be either the Principal core or the Video Auxiliary core. 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 and use Cisco cnBR 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

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

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."
}
}

```

Configure Video Service

You can configure video service in Cisco cBR-8 router through 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.

Prerequisite

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

- Manually create the video or virtual service group (VSG) in the Cisco cBR-8 router (Recommended).
Provide a logical name for the VSG. For example: `cable virtual-service-group 18528 downstream-video 1/0/8 profile 101`
- Automatically: 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 details, see the *Cisco Converged Broadband Routers Video Configuration Guide for Cisco IOS XE Bengaluru 17.6.x*.

To add a new video interface, choose Cisco Operations Hub main menu > **Smart PHY** > **RPD Automation**

> **RPD Assignment** and click the  button.

Add RPD

RPD Parameters
 Shelf ⊙

<i>RPD Name</i> * RPD044	<i>Latitude</i> -90 to 90
<i>RPD MAC</i> * a0f8.496f.61e8	<i>Longitude</i> -180 to 180
<i>Node Segmentation</i> * 1x1	<i>RPD Description</i> RPD Description
<i>Service Definition</i> Data_171	<i>Cable DSG TGs</i> 1 to 65535. Separate with ','
<i>Disable Network Delay</i> no	

▼ Data / Principal Core

Principal Core sphy-c2.cisco.com

Principal Core Interface TenGigabitEthernet6/1/0

SSD Profile 1 - ssd_171

First Logical DS/US Pairing

Downstream Physical Port 1

Base Power (dBmV) 25-34

Tilt Pivot Freq (Hz) 0-1218000000

Tilt Slope (dBmV) 0-8

Upstream Physical Port 0

DS Data Service Group

US Data Service Group

Second Logical DS/US Pairing

Downstream Physical Port

Base Power (dBmV) 25-34

Tilt Pivot Freq (Hz) 0-1218000000

Tilt Slope (dBmV) 0-8

Upstream Physical Port

DS Data Service Group

US Data Service Group

▼ Video Configuration

Video Core sphy-c2.cisco.com

Video Core Interfaces TenGigabitEthernet6/1/0

Video Core Interfaces TenGigabitEthernet6/1/1

First Logical DS/US Pairing

Video Service Groups 81501

81501

Video Service Groups 81502

81502

▼ OOB & Additional Core Configuration

OOB Core

OOB Core Interface

Downstream VOM ID 1 to 10

Downstream VOM Profile 1 to 4294967295

Upstream VARP ID 1 to 32

Upstream VARP Profile 1 to 4294967295

Second Upstream VARP Profile 1 to 4294967295

Additional Cores Additional Core

Save
Cancel

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

Configure VSG using API

You can also 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-rdt11",
  "gpslocation": {
    "genericlocation": "",
    "latitude": "",
    "longitude": ""
  },
  "ssdpprofileid": 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
      ]
    }
  ]
}

```

Restrictions and 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.
- Add the video interfaces under port-config also in the assigned-cores. If not, the application shows an error.
- The size of the list of video interfaces and the VSGs must be the same.
- Map a VSG to only one interface. However, you can map it to the same interface in a different port.
- If you configure a video interface without mapping to a VSG, the application ignores the video interface.

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 shows the 'MK_DB_DUMMY_02' configuration window. The left sidebar lists service definitions such as 'SystemTemplate (Default)', 'BidiptaThisIsABigServiceDefina', 'CBR_171', 'CBR_37', 'Copy-OOB171', 'Dummy', 'MD_CBR_171', 'OOB171', and 'Soumik'. The main content area is divided into three sections:

- RPD Summary:** RPD MAC: a0f8.496f.6110
- RPD State History:**
 - 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:**

```
[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 located at the bottom of the configuration window.

Manage GCP Redirection

Cisco Smart PHY application 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. You must enable the I15 GCP-redirect behavior.

Configure I15 GCP Redirect

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

Before configuring I15 GCP Redirect, ensure that your RPDs are compatible with I15 of the Remote PHY specification.

I15 GCP Redirect APIs

Following are the I15 GCP Redirect APIs:

set-redirect-version

The API is used to add GCP redirect version details.

API URL: <https://rpd-service-manager/rpdorch/v2/gcp/set-redirect-version>

Add the following fields in the request payload:

Field Name	Description
redirectVersion	GCP Redirect Version
rpdVendor	RPD Vendor name
rpdVersion	RPD Software Version

In the following example, Cisco Smart PHY searches for an exact match in the RPD vendor value, while evaluating the software version against a regex pattern:

```
{
  "redirectVersion": "I15",
  "rpdVendor": "***Cisco**",
  "rpdVersion": "v9.*"
}
```

remove-redirect-version

The API is used to remove an already configured GCP redirect record from the Cisco Smart PHY application.

API URL: <https://rpd-service-manager/rpdorch/v2/gcp/remove-redirect-version>

Add the following fields in the request payload:

Field Name	Description
rpdVendor	RPD Vendor name
rpdVersion	RPD Software Version

Example:

```
{
  "rpdVendor": "Cisco",
  "rpdVersion": "v9.*"
}
```

query-redirect-version

The API is used to query all GCP-redirect version details from the Cisco Smart PHY application.

API URL: <https://rpd-service-manager/rpdorch/v2/gcp/query-redirect-version>.

This API does not have any parameters.

I15 GCP-redirect Result Notification

The Cisco Smart PHY application displays the result of the `GCP Redirect Notification` in the **Associate RPD Details** panel.

When redirect errors occur, Cisco Smart PHY displays the RPD status as `GcpRedirectError`. The `GcpRedirected` state indicates that the redirect message is processed successfully by the RPD.



CHAPTER 7

Security and Administration

- [Manage Users](#), on page 51
- [Authentication](#), on page 53
- [Customize Login Banner](#), on page 54
- [Database Backup](#), on page 55
- [Renew Kubernetes Client TLS Certificate](#), on page 56

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 Cisco Operations Hub

Step 1 Choose Cisco Operations Hub main menu > **Systems** > **Users & Roles**.

Step 2 Click **Add User**.

The **Add User** pane appears on the right side.

Step 3 Enter the following details:

- **Username:** email ID of the user.
- **Select Role:** Choose the appropriate role for the user. The drop-down list contains three options: Admin, Editor, and Viewer.
- **Password:** Password for the new user.
- **Force password change on next login:** This option is selected by default. New users must change the password after the first login.

Step 4 Click **Add User**.

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
```

Update User Password

Step 1 Click the Cisco Operations Hub main menu and click the username that is displayed at the bottom of the left pane.

The **My Account** page opens.

Step 2 Click **Update Password**.

The **Update Password** pane appears on the right.

Step 3 Update your password and click **Update**.

Edit Users

- Step 1** Choose Cisco Operations Hub main menu > **Systems** > **Users & Roles**.
- Step 2** Select a user and click **Edit User**.
The **Edit User** pane appears on the right side.
- Step 3** You can update the user role and password expiration period.
- Step 4** Click **Save**.
-

Delete a User

- Step 1** Choose Cisco Operations Hub main menu > **Systems** > **Users & Roles**.
- Step 2** Select a user and click **Remove User**.
The **Remove <user>** pop-up window appears.
- Step 3** Click **Remove**.
-

Filter Users

Choose Cisco Operations Hub main menu > **Systems** > **Users & Roles**. Use the **Focus** drop-down list and the **Role** buttons, **Admin**, **Editor**, and **Viewer** to filter the users in the user list based on the password status and user role.

View Session History

- Step 1** Choose Cisco Operations Hub main menu > **Systems** > **Users & Roles**.
- Step 2** Click a user name to open **User Details** pane on the right.
- Step 3** Click the **Sessions History** tab to view the login and logout history of the user.
-

Authentication

The Cisco Smart PHY application is hosted on a Cisco Operations Hub cluster. Cisco Operations Hub provides the following authentication services for Cisco Smart PHY:

- Basic authentication
- LDAP authentication

Switch the authentication method of Cisco Operations Hub from the default Basic authentication to LDAP authentication, and vice versa, through the Cisco Operations Hub main menu > **System** > **Authentication** page. The procedures for switching between the authentication methods are provided in this section.

Switch from Basic Authentication to LDAP Authentication

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



Note Only administrators can access the **Authentication** page.
LDAP support is limited to Microsoft Active Directly (AD) only. Open LDAP is not supported.

- Step 1** Go to the Cisco Operations Hub main menu > **System** > **Authentication** to change the authentication method to LDAP.
Step 2 Enter the following details to configure LDAP.

LDAP Parameters	Description
LDAP Server URL	URL of the LDAP server.
Base Domain Name	Domain name as configured on your LDAP server.
LDAP User Name Domain	Validate the user name against the domain controller.
LDAP Filter	Specify a subset of data items in an LDAP data type.
LDAP Group Attribute	Comma-separated list of LDAP attributes on a group object that can be used in a user member attribute.
LDAP Group Mapping	Map LDAP group to the Cisco Operations Hub role.

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.

Customize Login Banner

An administrator can create and customize a banner for the Cisco Operations Hub login page.

To customize the banner, use the following procedure:

-
- Step 1** On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.
- Step 2** Choose **System > Login Banner Message**.
- Step 3** Enter the message in the text box and click Save.
A maximum of 500 characters are allowed in the banner message text box.
-

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

Local Backup

Local backup files are saved to the `/var/smartphy/backup` directory on the local filesystem.

-
- Step 1** Go to Cisco Operations Hub main menu > **Smart PHY > RPD Automation > Global Settings > Database Backup**.
- Step 2** In the **Server** field, enter **localhost**.
Leave the remaining fields blank (Username, Password, Directory, and Filename).
- Step 3** Click **Export**.
-

Remote Backup

Remote backup files are saved to the remote server at the specified file path.

-
- Step 1** Go to Cisco Operations Hub main menu > **Smart PHY > RPD Automation > Global Settings > Database Backup**.
- Step 2** In the **Server** field, enter the IP address or the `hostname.domain.com` of the remote server.
- Step 3** Enter the user login credentials in the **Username** and **Password** fields.

Step 4 In the **Directory** field, enter the file path on the remote server.
Leave the **Filename (Import Only)** field blank.

Step 5 Click **Export**.

Import Database

You can import local and remote backup files into the Cisco Smart PHY application.

Step 1 Go to Cisco Operations Hub main menu > **Smart PHY** > **RPD Automation** > **Global Settings** > **Database Backup**.

Step 2 In the **Server** field, enter the IP address or the `hostname.domain.com` of the remote server.

Step 3 Enter the following details in the **Filename (Import Only *)** field:

- Local backup: Enter only the filename of the backup file. This backup file is available in the default directory:
`/data/smartyphy/backup`.
In this case, **Username**, **Password**, and **Directory** are disabled.
- Remote backup: Enter the file path (absolute path) of the remote server.

Step 4 Click **Import**.

After importing the DB, Cisco Smart PHY takes a few minutes to synchronize all the database entities. After synchronizing the credential details, Cisco cBR-8 devices appear online in the Cisco Smart PHY application.

After Cisco cBR-8 devices are online, enable the CIN.

Renew Kubernetes Client TLS Certificate

Cisco Smart PHY leverages Kubernetes for container orchestration. During the Cisco Smart PHY cluster deployment, Kubernetes client TLS certificates are created to secure the communication between the Kubernetes API server and kubelets. Kubernetes client TLS certificates are valid for one year.



Caution Renew the Kubernetes client TLS certificates before they expire. Otherwise, the operation and functionality of the Cisco Smart PHY cluster will be impacted.

Administrators can check the current status of the Kubernetes certificates by running the following command in the Linux shell:

```
sudo openssl x509 -enddate -noout -in /data/kubernetes/pki/kubelet-client-current.pem
```

The certificates are valid through the date that is listed in the attribute `notAfter=`.

For more information on renewing the Kubernetes Client TLS Certificate, contact your Cisco Account Team.



CHAPTER 8

Monitor and Troubleshoot

Following are some troubleshooting tips for installing and using the Cisco Smart PHY.

- [Monitor Host Resources, on page 57](#)
- [API Explorer, on page 57](#)
- [Debug RPD SSD on Cisco Smart PHY, on page 57](#)
- [Debug SSD on Cisco cBR-8, on page 61](#)
- [DEPI Latency Measurement in Service Template, on page 62](#)

Monitor Host Resources

Use the Grafana dashboard for monitoring host resources.

Go to Cisco Operations Hub main menu > **Dashboards**.

The **Gallery** page opens. The following two types of dashboards are available:

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

API Explorer

API documentation for the Cisco Smart PHY application and the Cisco Operations Hub are centralised. You can access them from the Cisco Operations Hub main menu > **API Explorer**.

Cisco SmartPHY APIs are categorised into **RPD Service Manager** and **Inventory Management**. You can see these categories under the Cisco Smart PHY API section.

Debug 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.
```

Check 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.

Check 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 pairing 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 `ssidProfileId` 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 pairing table.

The screenshot shows the 'Edit - MK_DB_DUMMY_07' window in the Cisco Smart PHY Application. The window is divided into several sections:

- RPD Parameters:** Includes fields for RPD Name (MK_DB_DUMMY_07), RPD MAC (a0f8.496f.6117), Node Segmentation (2x2), Service Definition (CBR_37), and Disable Network Delay (no).
- Data / Principal Core:** Includes fields for Principal Core (sphy-c2.cisco.com), Principal Core Interface (TenGigabitEthernet6/1/0), SSD Profile (1 - ssd_171), and various pairing options (Downstream Physical Port, Upstream Physical Port, DS Data Service Group, US Data Service Group).
- Video Configuration:** Includes OOB & Additional Core Configuration.

Below the window is a table of RPDs:

S...	P...	RPD Name	MAC	SS...	Se...	Service Definition	Principal Core	Principal Cor...	DS Port	US Port	Base ...	Tilt Pl...
<input type="checkbox"/>	<input checked="" type="checkbox"/>	MK_DB_DUMMY_07	a0f8.496f.6117	1 - ssd_171	2x2	CBR_37	sphy-c2.cisco.com	TenGigabitEthernet6/1/0	0	0		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	MK_DB_DUMMY_01	a0f8.496f.6100	1 - ssd_171	1x1	CBR_171	sphy-c2.cisco.com	TenGigabitEthernet6/1/2	0	0	25	0

4. Verify whether the RPD Details contain the SSD command.



Check 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
ssid 1
rpd-55d1-us-event profile 0
```

Debug 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 ssid status
```

DEPI Latency Measurement in Service Template

If a Service Template is already in use, 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 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, the user can modify the `<delay-val>` for static.

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

If the `network-delay dlm <interval><measure-only>` is configured in the service template, the 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. From the **RPD Assignment** page, click **Edit** for that RPD.
 2. On the **Edit** page, click **Save**.

Check 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 65](#)

Best Practices

System and Cluster Recommendations

On multinode installations, we recommend exporting DB data to a remote server. Do not export the DB data to a local host, because the local host may be any of the three worker nodes.

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>`

Smart PHY Application User Recommendations

Cisco cBR Router

- The Cisco cBR router IP address used in the Cisco Smart PHY application should belong to the interface which the router uses to send SNMP traps.
- Use the following Cisco cBR router command to configure the SNMP trap source: `snmp-server trap-source <interface>`
- We recommend that you should not enter the Cisco cBR-8 hostname in the application. The Cisco Smart PHY application retrieves the hostname, after it connects to the Cisco cBR-8 router. Retrieving the hostname prevents any human errors due to incorrect entries of hostname or the IP address.
- In case of a network outage or loss of connectivity, make sure that the Cisco cBR-8 router is online on the Smart PHY application before modifying the RPD associations.
- Unprovision all RPDs assigned to a Cisco cBR-8 router before deleting the router from the Smart PHY application.

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 will reject all subsequent RPD configurations if there are more than 10 pending RPD transactions in the Cisco cBR-8 router internal queue.
- Any assignment or configuration change to an online RPD will result in the RPD service being interrupted. We recommend that you provision all needed parameters before the RPD is brought Online.