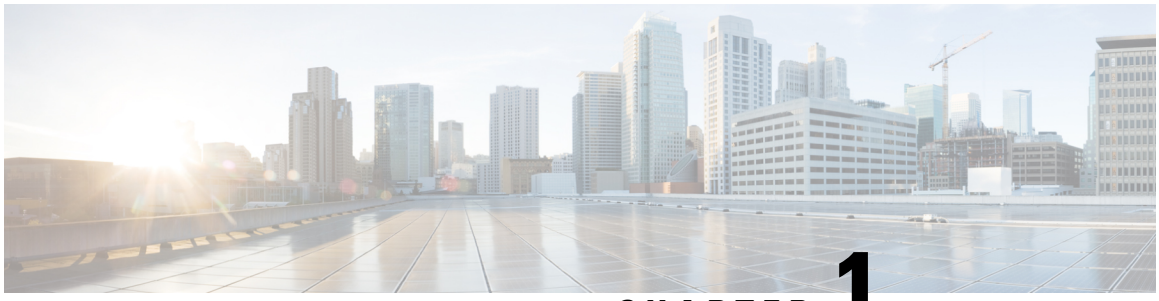
Cisco Smart PHY Application User Guide, Release 3.1.3

First Published: 2020-12-17

Last Modified: 2021-03-03

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

The Cisco Smart PHY application is an integrated package for installing, configuring, monitoring and troubleshooting the Remote-PHY devices (RPD) serviced by the Cisco cBR-8 routers. It enables multiple use cases, including:

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

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

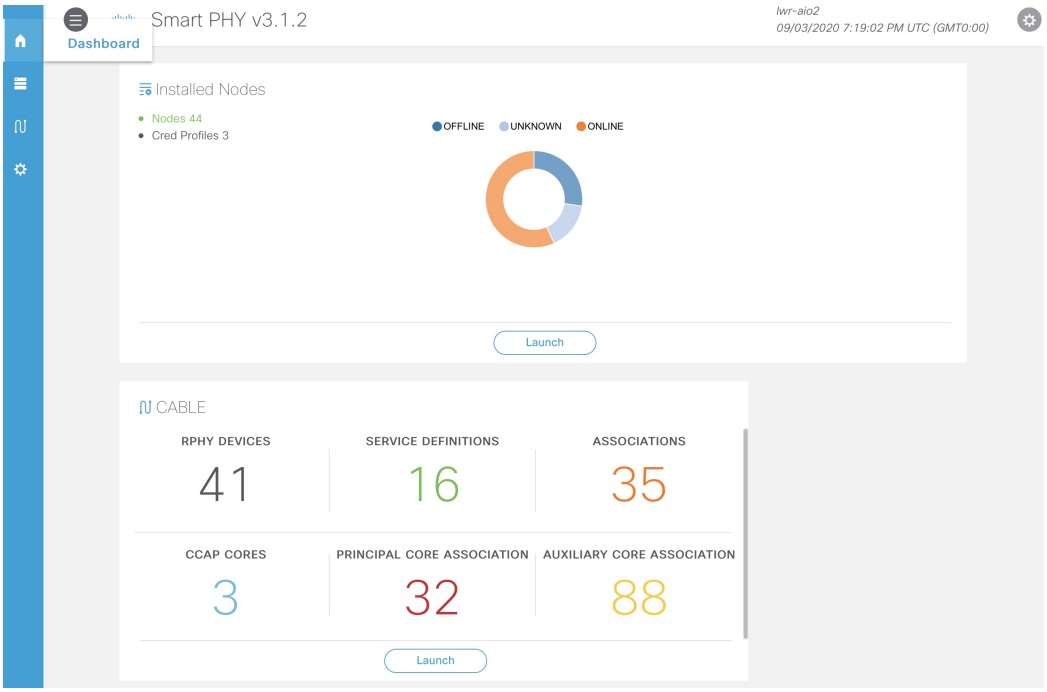
Typically, 200 to 500 RPDs might be connected to a single Cisco CMTS and manual configuration and monitoring could pose a problem.

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.
- RPD Inventory: RPD inventory operations. For example, running inventory reports or searching for RPDs based on specific criteria and so on.

- RPD SW Management: RPD SW version management.
- API Centric Design: Operators have direct programmatic access to Cisco Smart PHY services and functions using open interfaces and tools.

Dashboard



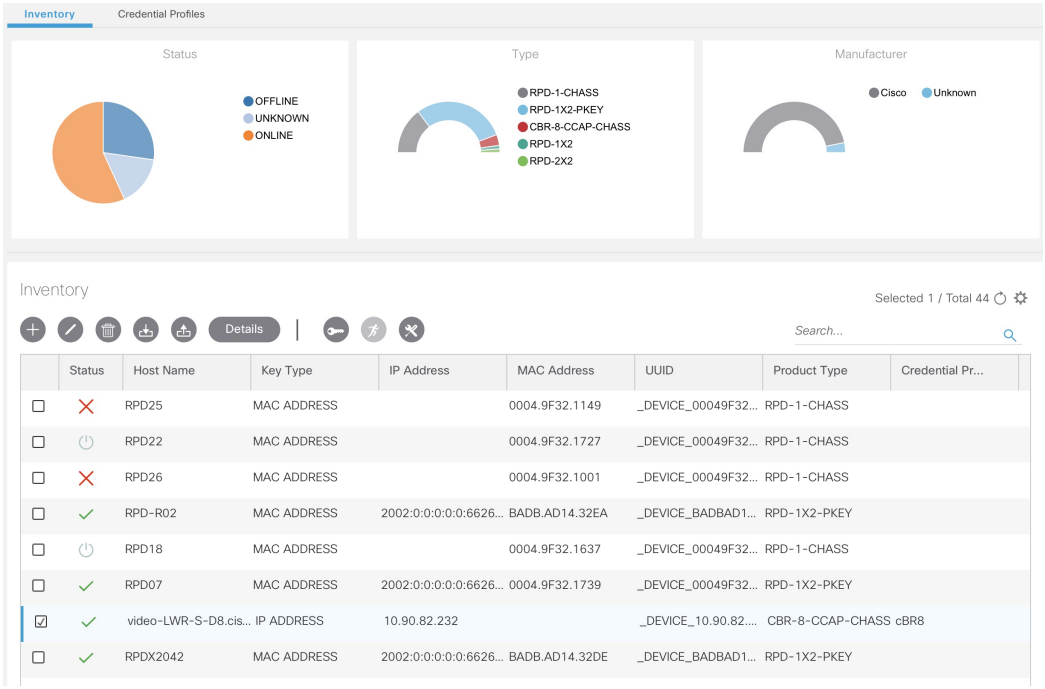
Following are the field descriptions:

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

Name	Description
Cable	Shows the following details in this pane: configured and managed using the **Cable RPD Automation** page. • RPHY Devices • Service Definitions • Associations • CCAP Cores • Prinicipal Core Association • Auxiliary Core Association Click the number to view more details. Click the **Launch** link to go to the **Cable RPD Automation** page.

Inventory

Inventory has two tabs; Inventory and Credential Profiles.



Inventory

The Inventory tab enables you to add, organize, and update information about the network devices. This includes non-Cable devices too and hence the information to be provided is more exhaustive than in the Cable RPD Automation view.

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

Following are the field descriptions for Inventory:

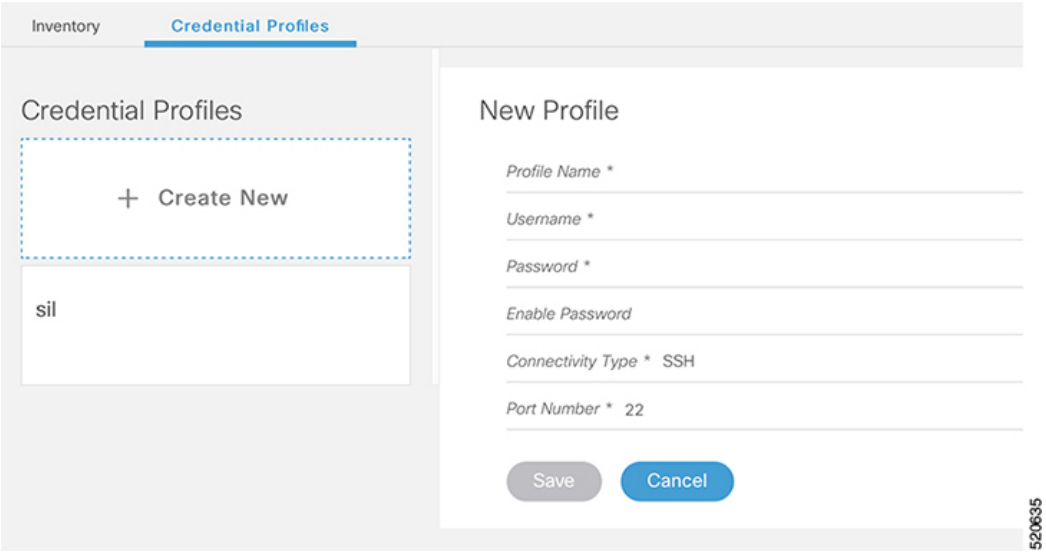
Name	Description
Status	Shows a graphical pie chart of all devices in the network, categorized by status: • ONLINE • OFFLINE • UNKNOWN • SSHKEYFETCH • MAINTENANCE • NORMALOPS_PROGRESS
Host Name	Host name of the device.
Key Type	Two types: • MAC ADDRESS • IP ADDRESS
IP Address	IP address of the device.
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.
	Adds a device to the existing inventory.

Name	Description
	Edits the device information.
	Deletes a device from the inventory.
	Exports device information to a CSV file.
	Imports devices by using a CSV file.
	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.
	Status showing SSH key failure.
	Status shows one of the following states: • 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.

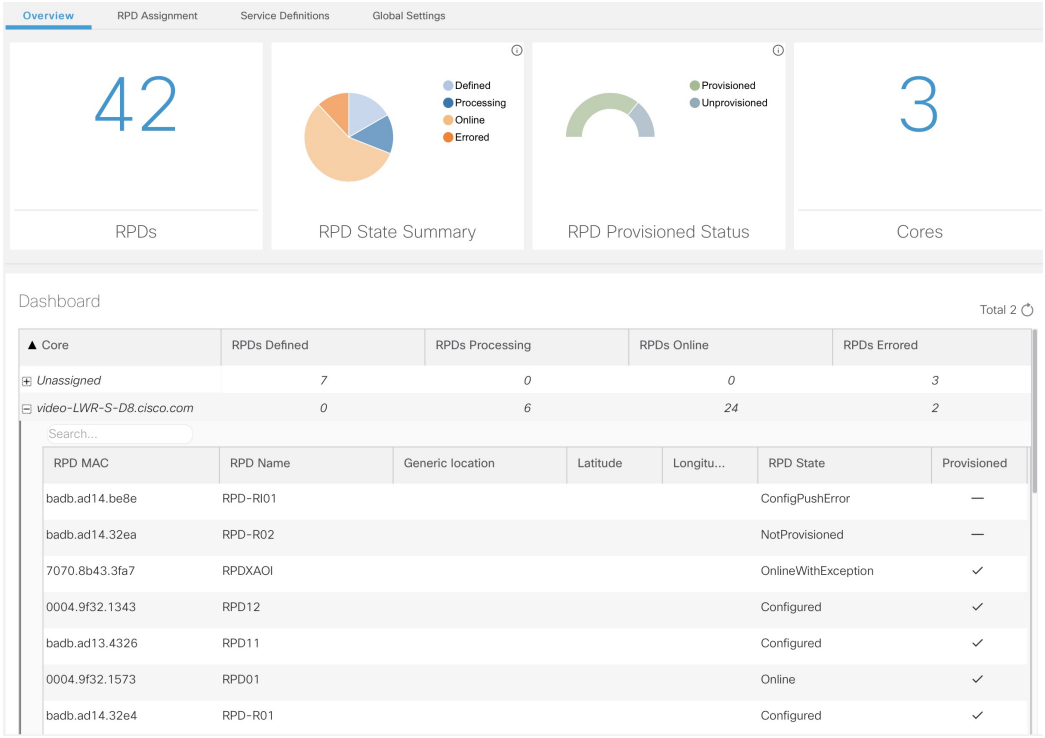
Cable RPD Automation

The Cable 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 Cable 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

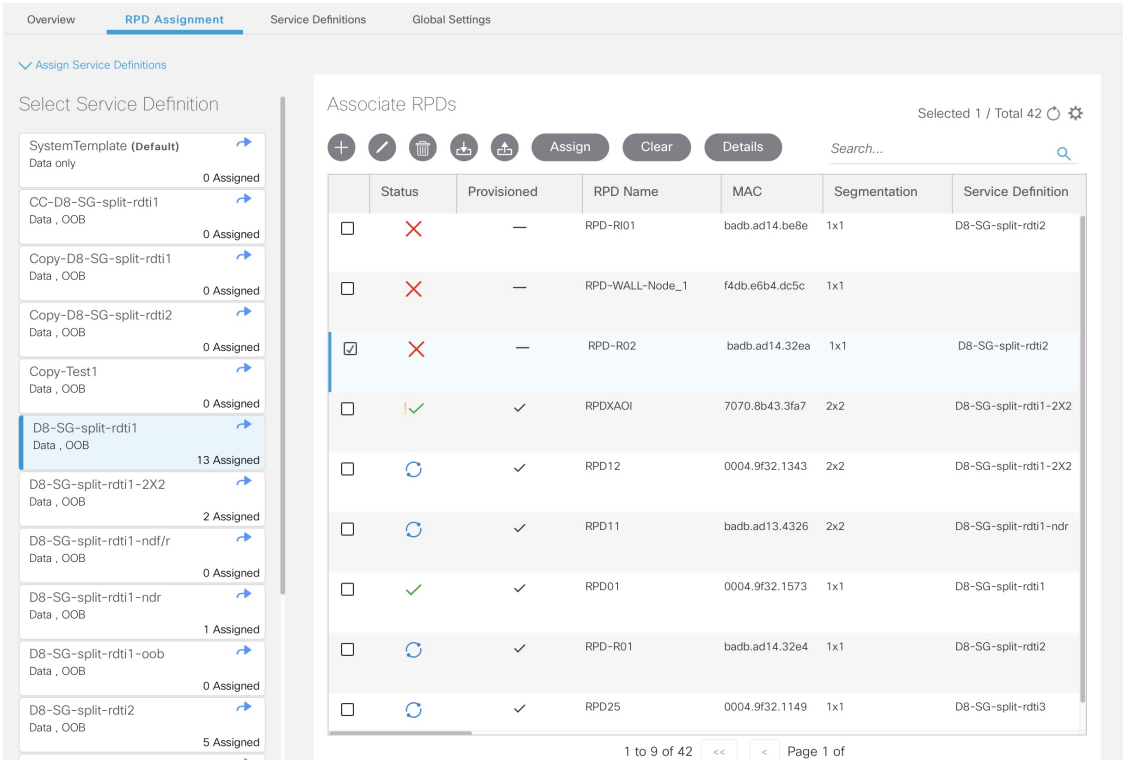
RPD Summary	RPD State	Description
DEFINED	Defined	RPD pairing is defined. However, MAC address is not yet assigned.
DEFINED	Installed	Installed RPD. RPD name, MAC address, and the GPS location are available.
DEFINED	Inventory	Added RPD MAC address to the inventory without the GPS details.
ERRORED	ConfigNotFound	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	Parttial 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.
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: • 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: • RouterVersionIncompatible • StaticRouteNotConfigured
PROCESSING	GcpUp	Received GCP message from the RPD.
WARNING	RouterVersionIncompatible	RPD software version is incompatible with the CCAP core version.

RPD Summary	RPD State	Description
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.



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
	To delete an RPD name and its RPD assignment information. 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. To delete the RPD MAC address, delete it from the main Inventory page. 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.
	Exports the details of RPD assignments to a CSV file.
	Imports the details of RPD assignments using a CSV file. Sample of the CSV file is available when you click this icon.
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:

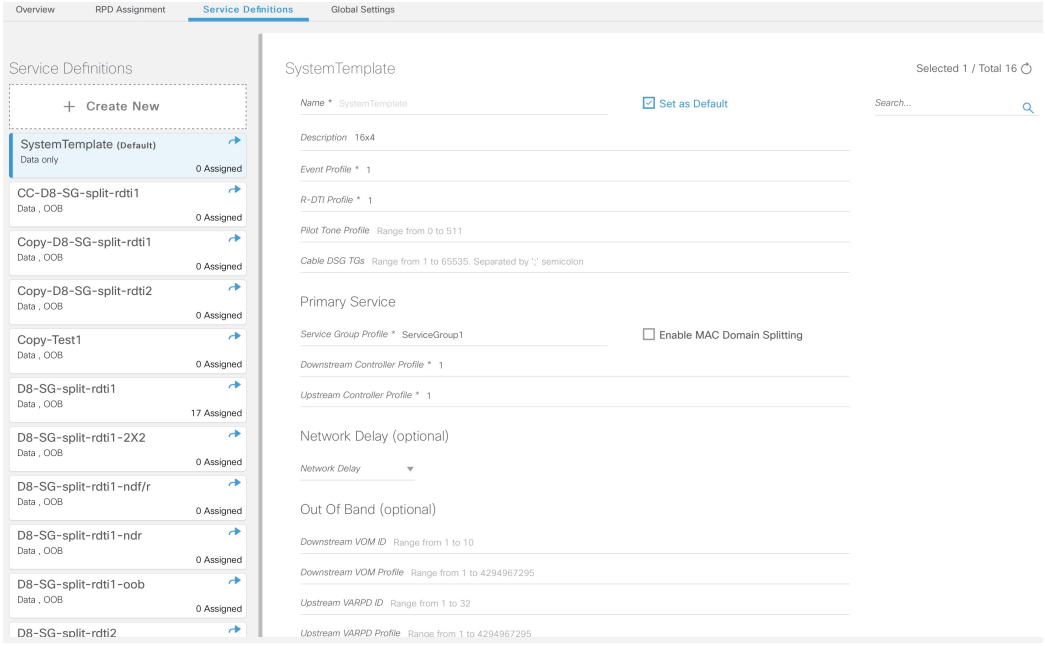
Field Name	Description
Status	Shows the status of the RPDs.
Provisioned	Shows whether the RPD is provisioned or not.
RPD Name	Name for the RPD. This RPD name is also used in the `cable rpd` CLI command.
RPD MAC Address	MAC address of the RPD.
Node Segmentation	Node segmentation of the RPD: 1x1, 1x2,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

Field Name	Description
Principal Core	Name of the Cisco cBR-8 router which is the principal Converged Cable Access Platform (CCAP) Core for the RPD. This core must provide the RPD with data and narrowband digital forward (NDF)/narrowband digital return (NDR) services. This core may also provide the following services: • Out-of-band (OOB) SCTE 55–1 • Video services: If there is no separate auxiliary Video Core Leave this field empty if the RPD has a principal CCAP Core that is not managed by Cisco Smart PHY. An `unmanaged` principal core is a non-cBR-8 principal core such as Cisco cnBR, which is not present in the Cisco SmartPHY inventory and to which it does not push the configuration. In this case, include the `unmanaged` principal core as the first item in the **Additional Cores** list.
SSD Profile	Secure Software Download (SSD) profile details for image storage.
Disable Network Delay	The default is value is **No**. • No: Apply the network-delay from service definition to RPD. • Yes: Do not apply the network-delay from service definition to RPD. Changing this value to `yes` is service impacting, if the RPD's assigned Service Definition/Template has network-delay configured.
Principal Core Interface	Complete name of the TenGigabitEthernet DPIC interface to be used for Data Service. Leave this field empty if there is no Principal Core.
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.
OOB Core	Name of the Cisco cBR-8 router which is the CCAP core for the RPD that provides out-of-band (OOB) SCTE 55–1 service and NDF/NDR services. This field must match either the **Principal Core** or the auxiliary **Video Core**. Leave this field empty if the OOB 55-1 and NDF/NDR services are not used.
OOB Core Interface	Complete name of the TenGigabitEthernet DPIC interface to be used for out-of-band 55-1 and NDF/NDR service. Leave this field empty if the OOB 55-1 and NDF/NDR services are not used.
Downstream VOM ID	OOB 55-1 Downstream Virtual out-of-band Modulator (VOM) Identification (ID). If present, this value overrides the value from the Service Definition.

Field Name	Description
Downstream VOM Profile	OOB 55-1 Downstream VOM profile. If present, this value overrides the value from the Service Definition.
Upstream VARPD ID	OOB 55-1 Upstream Virtual Advanced Return Path Demodulator (VARPD) ID. If present, this value overrides the value from the Service Definition.
Upstream VARPD Profile	OOB 55-1 Upstream VARPD profile for first logical Downstream/Upstream (DS/US) pairing. If present, this value overrides the value from the Service Definition. The Upstream VARPD Profile (upstreamVarpdProfile) and the Second Upstream VARPD Profile (secondUpstreamVarpdProfile) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2, on page 36.
Second Upstream VARPD Profile	OOB 55-1 Upstream VARPD profile for second logical Downstream/Upstream (DS/US) pairing. If present, this value overrides the value from the Service Definition. The upstream VARPD profile (upstreamVarpdProfile) and the second upstream VARPD profile (secondUpstreamVarpdProfile) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2, on page 36.
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. For example, when an SCTE 55-2 OOB auxiliary core is required, additional cores list it here. **Important** If Cisco Smart PHY does not manage the principal CCAP core and if the Principal Core field is empty, you must include the unmanaged principal core as the first item in this list.
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.



Following are the menu options descriptions:

Name	Description
+ Create New	Click this option to create a new service template.
Name of the existing service definition	Click the name of the existing service definition to edit the template.
New Service Definition	Enter the details in each filed 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.

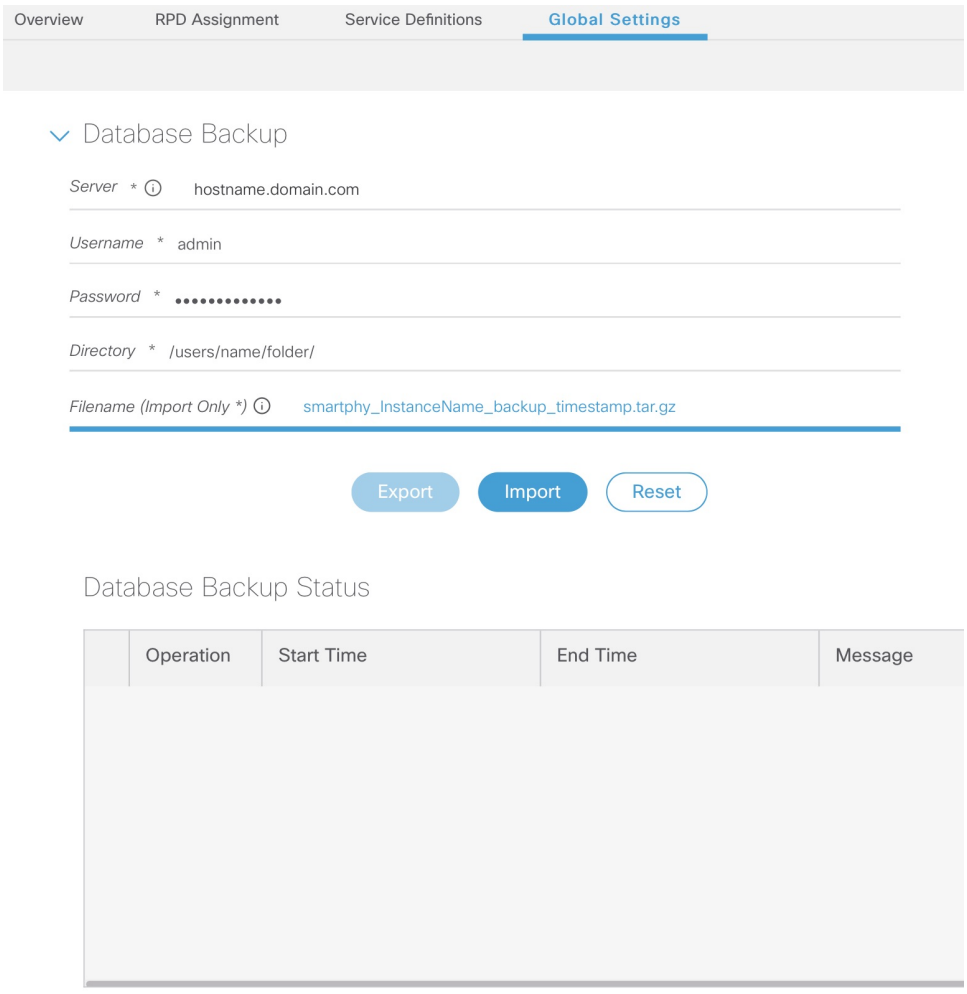
Global Settings

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.



The database backup file is a `TAR.GZ` file with the following naming convention: `smartphy_backup_YYYYHHMM_022639.tar.gz`. Enter the following details in the **Database Backup** window to back up the database.

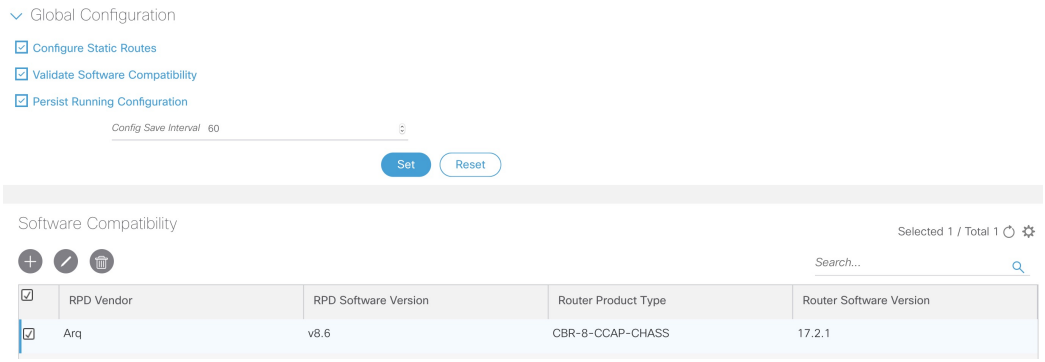
Field	Description
Server	The location where you want to save the DB. • Local backup—Enter **localhost**. Local backup files are saved to the `/var/smartphy/backup` directory on the local filesystem. • Remote backup—Enter the IP address or the `hostname.domain.com`. For remote backup, the Cisco Smart PHY application uses SFTP to transfer files from Cisco Smart PHY instances.
Username	• Local backup—Leave the field empty. • Remote backup—Enter the username for the remote server access.

Field	Description
Password	• Local backup—Leave the field empty. • Remote backup—Enter the password for the remote server access.
Directory	• Local backup—Leave the field empty. • Remote backup—Enter the file path of the directory in the remote server.
Filename (Import Only)	Used exclusively for importing a database. Imported file must be in this format the following format: `smartphy_InstanceName_backup_timestamp.tar.gz` Leave the field empty for both local and remote backup.
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.



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

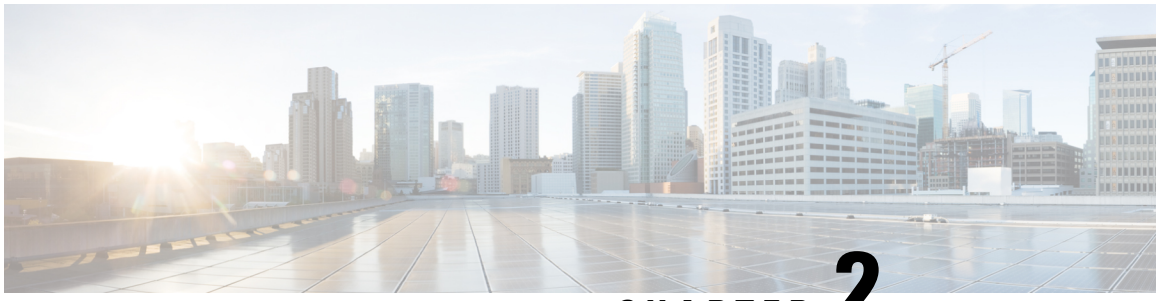
Name	Description
RPD Vendor	Name of the RPD vendor.
RPD Software Version	Software version running on the RPD.
Router Product Type	Product type of the router from the Inventory. Example: CBR-8-CCAP-CHASS

Name	Description
Router Software Version	Software version of the router.

Admin

The **Admin** menu option displays the **User List** window which lists all existing users in the Cisco Smart PHY application.

In this window, you can reset the user passwords by clicking the  . The admin user can reset the passwords of all users. All other users can reset only their own passwords when logged in.



CHAPTER 2

How to Use Cisco Smart PHY

This section describes how to use the Cisco Smart PHY application:

Configure Cisco cBR-8 for Smart PHY Application

Enable Logging

Enable logging to Cisco Smart PHY and set LCHA Traps to Smart PHY to ensure that the Smart PHY state is cBR-8 LCHA aware.

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

Configure Cable Service Profile-Group

Configure the Cable Service Profile-Group on the Cisco cBR-8 router. The following is a sample of how to configure the Service Profile-Group:

Note The number for US bonding groups should be a 2 or 4.

```
cable profile mac-domain test_MD
 cable ip-init dual-stack
 cable privacy accept-self-signed-certificate
 cable privacy skip-validity-period
!
!
cable profile wideband-interface test_WB
 cable downstream attribute-mask 80000001
!
!
cable profile downstream test_DS
 cable rf-bandwidth-percent 20
!
!
cable profile service-group test_SG1
 cable bundle 2
 mac-domain 0 profile test_MD
  downstream sg-channel 0-23 profile test_DS
  upstream 0 sg-channel 0
  upstream 1 sg-channel 1
  upstream 2 sg-channel 2
  upstream 3 sg-channel 3
  upstream 4 sg-channel 4
  upstream 5 sg-channel 5
  us-bonding-group 1
   upstream 0
   upstream 1
   upstream 2
   upstream 3
  us-bonding-group 2
   upstream 2
   upstream 3
   upstream 4
   upstream 5

 wideband-interface 0 profile test_WB
  downstream sg-channel 0-23 rf-bandwidth-percent 20
```

Log In using a Browser

Step 1 In the browser's address bar, enter `https://<fqdn>` or `https://<ip_address>.nip.io`

The access URL is based on the initial cluster configuration.

The Cisco Smart PHY web GUI displays the Login window. When you access Cisco Smart PHY for the first time, some browsers display a warning that the site is untrusted. When this happens, 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.

Step 2 Log in using the password that you provided during the initial installation.

Step 3 To exit the web GUI, close the browser window or click the settings icon in the top right corner and choose Log out.

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://<ip_address>.nip.io`.

Step 2 Create a Credential Profile.

a) Choose **Inventory** > **Credential Profiles**.

b) Enter the following details in the text fields.

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.

c) Click **Save**.

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.

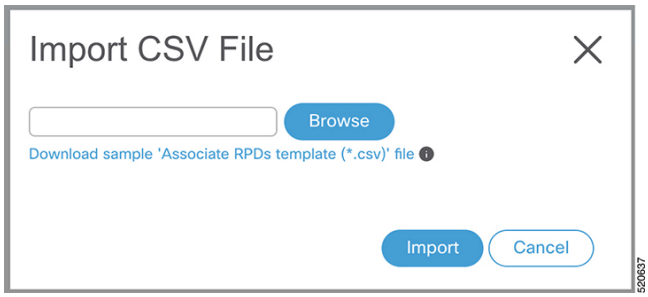
a) Choose **Inventory** > **Inventory**.

b) To import a CSV file, click the icon, choose the 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

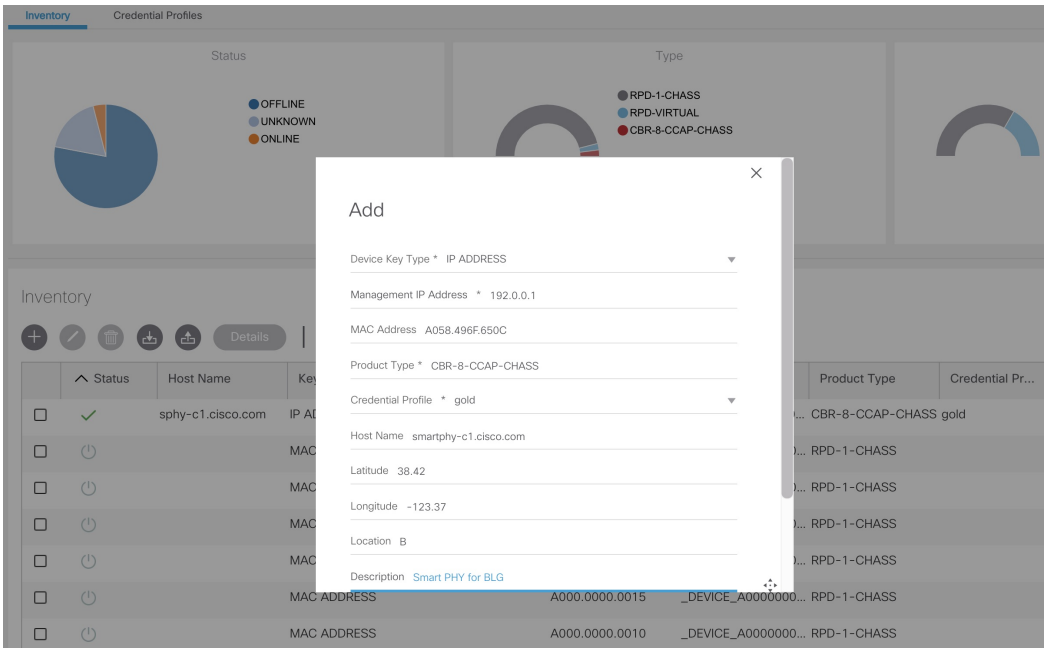


Or

To manually add a device, click the icon and provide the required information and save.

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

- Key Type—IP address
- IP Address—Management IP address on the Cisco cBR-8 router
- Product Type—CBR-8-CCAP-CHASS
- Credential Profile—Specify the credential profile. Devices with the same credentials can use the same credential profile.



Step 4 Configure the Cisco cBR-8 to send syslog 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:

```
logging host <Smart PHY interface connected to the Cisco cBR> transport udp port 8514
```

Enter the IP address of the worker node.

Step 5 Create a Service Template.

Note Fields not marked as optional are mandatory.

a) Choose **Cable RPD Automation** > **Service Definitions**.

b) Specify Profiles as preconfigured on the Cisco cBR-8 router.

Name	Description
Event Profile	RPD Event Profile Set
R-DTI Profile	Remote DOCSIS Timing Interface (R-DTI) Set
Pilot Tone Profile	Pilot tone profile.
Cable DSG TGs	DSG tag IDs.
Primary Service	
Service Group Profile	Pre-existing Cable Service Profile-Group on the Cisco cBR-8
Enable MAC Domain Splitting	Select the check box to split a MAC domain between two fiber-nodes that share the same downstream controller.
Downstream Controller Profile	Primary downstream CCAP controller profile.

Name	Description
Upstream Controller Profile	Primary upstream CCAP controller profile.
Out Of Band	Out-of-band profile parameters.
Network Delay	Network delay has two options: • **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. *Measure only*—Choose to measure network latency between the CCAP core and the RPD. This option is not for updating the cable map advance. You can select this option for a service definition in use, but cannot deselect it. • **Static**—The cable map advance is adjusted by a fixed amount. The valid range is 30–100,000 microseconds. This range is the Converged Interconnect Network (CIN) delay in microseconds. CIN is the network between the CCAP core and RPD. You can change the network-delay range for a service definition in use. For more details, see *DEPI Latency Measurement in the Service Template* section in this document.
Out Of Band	
Downstream VOM ID	OOB 55–1 Downstream Virtual out-of-band Modulator (VOM) identification (ID).
Downstream VOM Profile	OOB 55–1 Downstream VOM profile.
Upstream VARPD ID	OOB 55–1 Upstream Virtual Advanced Return Path Demodulator (VARPD) ID.
Upstream VARPD Profile	OOB 55–1 Upstream VARPD profile for first logical downstream/upstream (DS/US) pairing. The upstream VARPD profile (upstreamVarpdProfile) and the second upstream VARPD profile (secondUpstreamVarpdProfile) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2, on page 36.
Second Upstream VARPD Profile	OOB 55–1 Upstream VARPD profile for second logical downstream/upstream (DS/US) pairing. The upstream VARPD profile (upstreamVarpdProfile) and the second upstream VARPD profile (secondUpstreamVarpdProfile) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2, on page 36.
NDF/NDR	

Name	Description
Pseudowire Name (sic)	**NDF** Narrowband digital forward (NDF) pseudowire name. Up to three pseudowire names, profile ID sets are supported. Values are applied to all downstream ports of the RPD. **NDR** NDR pseudowire name. Up to three pseudowire names, profile ID sets are supported per upstream port.
Profile ID	• NDF—NDF profile ID corresponding to the above NDF pseudowire. • NDR—NDR profile ID corresponding to above NDF pseudowire.
NDR: Port	Upstream port, `Port 0` or `Port 1`, to apply Narrowband Digital Return (NDR) pseudowire name, profile set.
Load Balance	Paste the load balance XML text in the text field. Use the ntool to convert the XML configuration from the Cisco cBR-8 router to the required XML format.

c) Click **Save**.

Step 6 Pair an RPD with the RPD MAC address in the RPD assignment table.

If you are using the Smart PHY application on a mobile device, before you pair an RPD with the MAC address, ensure that you create a table entry for the RPD (`RPD_NAME1`) with the following details: RPD name, description, location, pairing with Cisco cBR-8 router, and service template.

After the initial installation of the RPD, the mobile application scans the RPD, gets an IP address, and contacts the Cisco Smart PHY application for provisioning as RPD_MAC1. You can also pair the `RPD_NAME1` with the `RPD_MAC1` when scanning the RPD using the mobile application.

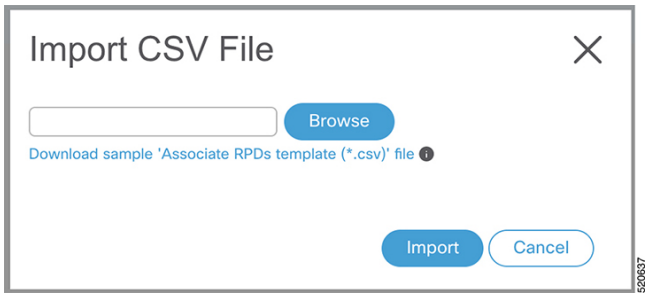
Adding RPD through a Web GUI

Note Fields with an asterisk are mandatory.

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

a) Choose **Cable RPD Automation** > **RPD Assignment**.
b) RPD Assignment can be specified manually or by importing a CSV file.

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



Or

To specify RPD assignment manually, click **Add** or **Edit**.

Field Name	Description
RPD Name	Name for the RPD. This RPD name is also used in the `cable rpd` 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.
Principal Core	Name of the Cisco cBR-8 router which is the principal Converged Cable Access Platform (CCAP) Core for the RPD. This core must provide the RPD with data and narrowband digital forward (NDF)/narrowband digital return (NDR) services. This core may also provide the following services: • Out-of-band (OOB) SCTE 55–1 • Video services: If there is no separate auxiliary Video Core Leave this field empty if the RPD has a principal CCAP Core that is not managed by Cisco Smart PHY. An `unmanaged` principal core is a non-cBR-8 principal core such as Cisco cnBR, which is not present in the Cisco SmartPHY inventory and to which it does not push the configuration. In this case, include the `unmanaged` principal core as the first item in the **Additional Cores** list.
SSD Profile	Secure Software Download (SSD) profile details for image storage.
Disable Network Delay	The default is value is **No**. • No—Apply network delay from service definition to RPD. • Yes—Do not apply network delay from service definition to RPD. Changing this value to `yes` is service impacting, if the RPD's assigned Service Definition/Template has network-delay configured.

Field Name	Description
Principal Core Interface	Complete name of the TenGigabitEthernet DPIC interface to be used for Data Service. Leave this field empty if there is no Principal Core.
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.
OOB Core	Name of the Cisco cBR-8 router which is the CCAP core for the RPD that provides out-of-band (OOB) SCTE 55–1 service and NDF/NDR services. This field must match either the **Principal Core** or the auxiliary **Video Core**. Leave this field empty if the OOB 55-1 and NDF/NDR services are not used.
OOB Core Interface	Complete name of the TenGigabitEthernet DPIC interface to be used for out-of-band 55-1 and NDF/NDR service. Leave this field empty if the OOB 55-1 and NDF/NDR services are not used.
Downstream VOM ID	OOB 55–1 Downstream Virtual out-of-band Modulator (VOM) Identification (ID). If present, this value overrides the value from the Service Definition.
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.
Upstream VARPD Profile	OOB 55–1 Upstream VARPD profile for first logical Downstream/Upstream (DS/US) pairing. If present, this value overrides the value from the Service Definition. The upstream VARPD profile (upstreamVarpdProfile) and the second upstream VARPD profile (secondUpstreamVarpdProfile) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2, on page 36.
Second Upstream VARPD Profile	OOB 55–1 Upstream VARPD profile for second logical Downstream/Upstream (DS/US) pairing. If present, this value overrides the value from the Service Definition. The upstream VARPD profile (upstreamVarpdProfile) and the second upstream VARPD profile (secondUpstreamVarpdProfile) can have the same value. For more details, see Common OOB 55-1 US Profile for Cisco RPD 1x2/2x2, on page 36.
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.

Field Name	Description
Additional Cores	Semi-colon separated list of additional cores to which the RPD must connect. For example, when an SCTE 55-2 OOB auxiliary core is required, additional cores list it here. **Important** If Cisco Smart PHY does not manage the principal CCAP core and if the Principal Core field is empty, you must include the unmanaged principal core as the first item in this list.
Latitude	Latitude of the RPD (GPS coordinates)
Longitude	Longitude of the RPD (GPS coordinates)
RPD Description	Description for the RPD

The description of First and Second Logical DS/US Pairing fields for adding an assignment are as follows:

Field Name	Description
Downstream Physical Port	Downstream RPD Port of the logical pairing. Always “0” for first pairing and not applicable to second pairing for 1x1 or 1x2 node segmentation. May be “0” or “1” for 2x2 node segmentation.
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.

Field Name	Description
Video Service Groups	Video service group (VSG) names. Video only travels in the downstream direction. Not applicable to second pairing for 1x1 or 1x2 node segmentation. **Important** Cisco Smart PHY does not allow configuring a VSG on a Downstream Port 1 (ds1) with `broadcast` keyword through the Cisco cBR-8 CLI. If you try to configure, the CLI shows an error. Cisco Smart PHY maps a VSG to a video interface based on the order of the VSGs and interfaces if a VSG can map to more than one interface: • A VSG can map to more than one video interface if the video interface list includes both ports 0 and 2 or both ports 4 and 6 of one Cisco cBR-8 Series 8x10G Remote PHY Digital Physical Interface Card (CBR-DPIC-8X10G). • Cisco Smart PHY maps the first VSG to a matching Principal Core interface if present; otherwise, it maps the first VSG to the first matching video interface. • Cisco Smart PHY maps second, third, and fourth VSGs to the highest numbered matching video interfaces. Cisco Smart PHY reorders video interfaces and VSGs, so that a video interface that matches the Principal Core interface and the associated VSGs are listed first.

c) 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.

Step 7 In the DHCP server, enter the IPv4 or IPv6 VIP (Virtual IP address) of the CIN network in the **CCAP Core** field for the RPD.

After retrieving the IP address from the DHCP server, the RPDs are redirected to the Cisco Smart PHY application.

When the RPD resets, it gets the new DHCP server attributes and values from the DHCP server and connects to the Cisco Smart PHY application.

To view the details of an RPD such as the RPD Summary, RPD State History, and RPD CLI, select the check box and click the **Details** button.

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 **Inventory** > **Credential Profiles**.

Step 2 Click **Create New**.

Step 3 Enter a profile name and description.

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.

Step 4 Enter the credentials for the profile.

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

Step 5 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 **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 **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 **Inventory** > **Credential Profiles**.

Step 2 Click the profile you want to use. Else, create a new profile.

Step 3 To view device inventory, choose **Inventory** > **Inventory**.

Step 4 Choose which device records to change by including them in the CSV file.

Do one of the following:

- Click the **Export** icon to include all devices.
- Filter the list of devices by entering text in the **Search** field or by filtering on the individual headings, and then click the **Export** icon to include the filtered list of devices.
- Check the check boxes for the device records you want to change, and then click the **Export** icon to include the selected devices.

Step 5 Edit and save the new CSV file. Note: You must save the file opened in MS Excel as a CSV file only.

Step 6 In the Import CSV File dialog box, click **Browse**, select the new CSV file, and click the **Import** icon.

Step 7 In the **Replace Existing Node** dialog box, click **Yes to All**.

Step 8 Click **Save**.

Delete a Device from the Inventory

Step 1 Choose **Inventory** > **Inventory**.

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

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

Step 4 Click delete icon ( ).

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

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

Create CSV File for Importing Devices

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

Step 1 Choose **Inventory** > **Inventory**.

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

You will be prompted to open or save the sample CSV file. Save the CSV file.

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

The mandatory fields are:

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

Export Device Information to a CSV File

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

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

Step 1 Choose **Inventory** > **Inventory**.

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

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

Step 4 Click the export icon ().

Add Devices through GUI

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

Step 1 Choose **Inventory** > **Inventory**.

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

Step 3 Enter the values for the device.

The mandatory fields are:

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

Step 4 Click **Save**.

Step 5 (Optional) Repeat to add more devices.

Import Device Information in Bulk

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

Step 1 Choose **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**.

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

Delete a Credential Profile

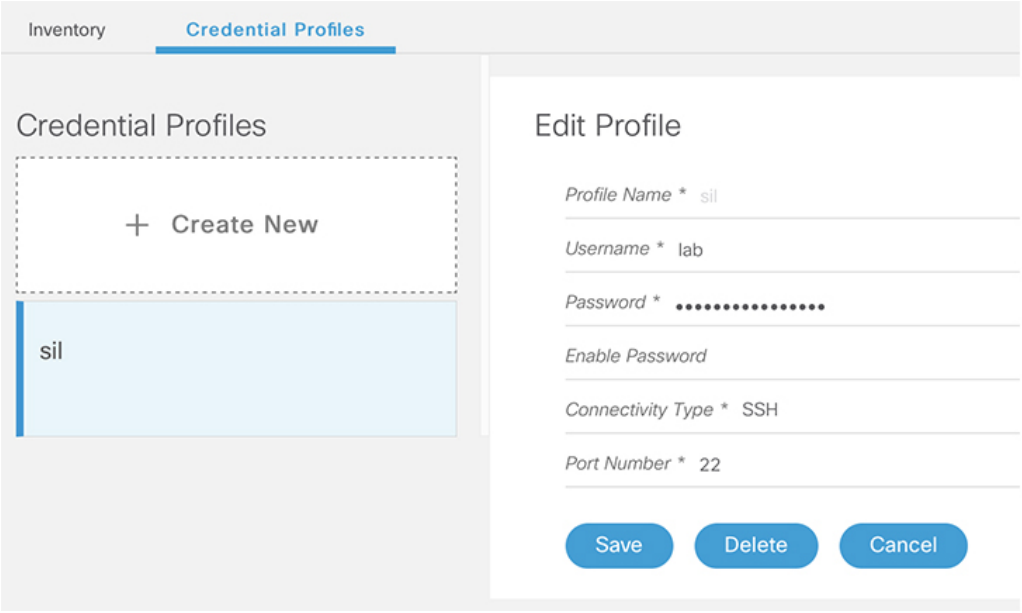
To delete a credential profile from Inventory Manager, disassociate the profile from any devices. Inventory Manager displays an alert if you attempt to delete a credential profile that is associated with devices.

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

1. Choose **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 **Inventory** > **Credential Profiles**.

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



Create a New Service Definition

Step 1 Choose **Cable 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.

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

Specify RPD Assignment

Step 1 Choose **Cable 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.

To upload a CSV file, click **Upload**, select the file and click **Import**.

Step 3 Click **Save**.

Step 4 Click **Assign**.

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.

Note Manually, enter the IPv4 or IPv6 address of the Principal Core CIN interface that is not managed by Cisco Smart PHY as the first entry in the **Additional Cores** field.

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

{
```

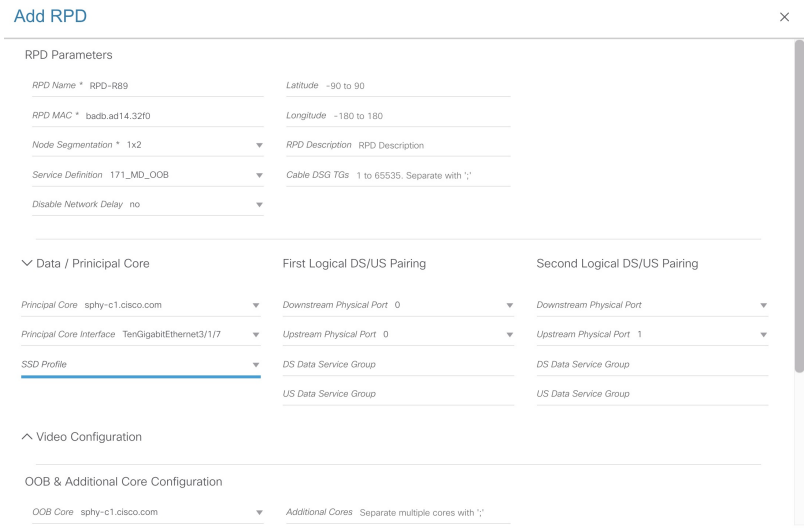
```
  "autoAccept": false,
  "defaultFlag": false,
  "dlmMeasureOnly": false,
  "dsgTunnelGroupIDs": "1",
  "elementsList": [
    {
      "description": "Service profile with 1.5Gbps Data Service. 16x4 DS/US SG channels",
      "downstreamControllerProfile": 0,
      "downstreamVomId": 1,
      "downstreamVomProfile": 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.

To add a new video interface, choose **Cable RPD Automation** > **RPD Assignment** and click the  button.



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-rdti1",
      "gpslocation": {
        "genericlocation": "",
        "latitude": "",
        "longitude": ""
      },
      "ssdprofileid": 1,
      "disablenetworkdelay": false,
      "preconfigure": true,
      "nodesegmentation": "rpd_1x1",
      "additionalcores": [
        "2004:172:30:0:2eab:a4ff:feff:f36c"
      ],
      "assignedcores": [
        {
          "servicetype": "data",
          "mgmtcore": "video-lwr-s-d8.cisco.com",
          "rpdconnectioninterface": "tengigabitethernet9/1/0",
        },
        {
          "servicetype": "video",
          "mgmtcore": "video-lwr-s-d8.cisco.com",
```

```
            "rpdconnectioninterface": "tengigabitethernet9/1/0",
          },
         {
            "servicetype": "video",
            "mgmtcore": "video-lwr-s-d8.cisco.com",
            "rpdconnectioninterface": "tengigabitethernet9/1/6",
          },
          {
            "servicetype": "oob",
            "mgmtcore": "video-lwr-s-d8.cisco.com",
            "rpdconnectioninterface": "tengigabitethernet9/1/0",
          }
        ],
        "portconfigs": [
          {
            "dsport": 0,
            "usport": 0,
            "dsservicegroup": "sg-9-0-0",
            "usservicegroup": "sg-upstream-9-0-0",
            "videoservicegroups": [
              "vsg1",  // Index 0 is read along with video interface index 0
              "vsg2",  // Index 1 is read along with video interface index 1
              "vsg3"  // Index 2 is read along with video interface index 2
            ],
            "videointerfaces":[
              "tengigabitethernet9/1/0", // Index 0 is read along with vsg index 0
              "tengigabitethernet9/1/6", // Index 1 is read along with vsg index 1
              "tengigabitethernet9/1/6" // Index 2 is read along with vsg index 2
             ]
          }
        ]
      }
    ]
}
```

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.

Restrict 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 SSH keys
- Fetch Details
- Import

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

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. You can also disable southbound communications even for offline 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 liveliness or configuration sync.

When you disable southbound communication:

- Cisco Smart PHY does not allow you to make any configuration changes through the user interface 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 connectiovity, as it checks the state of the router. When this check happens, the router is in the transient state of `NORMALOPS_PROGRESS`. After this checking is over, the router becomes online or offline based on result of the checks.

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.

Fetch SSH Keys from Cisco cBR-8

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

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)
```

To view the status of fetching, 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 fetching process is successful, the router becomes online.

The SSH Key icon is enabled only when you choose an online Cisco cBR-8 router.

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

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

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

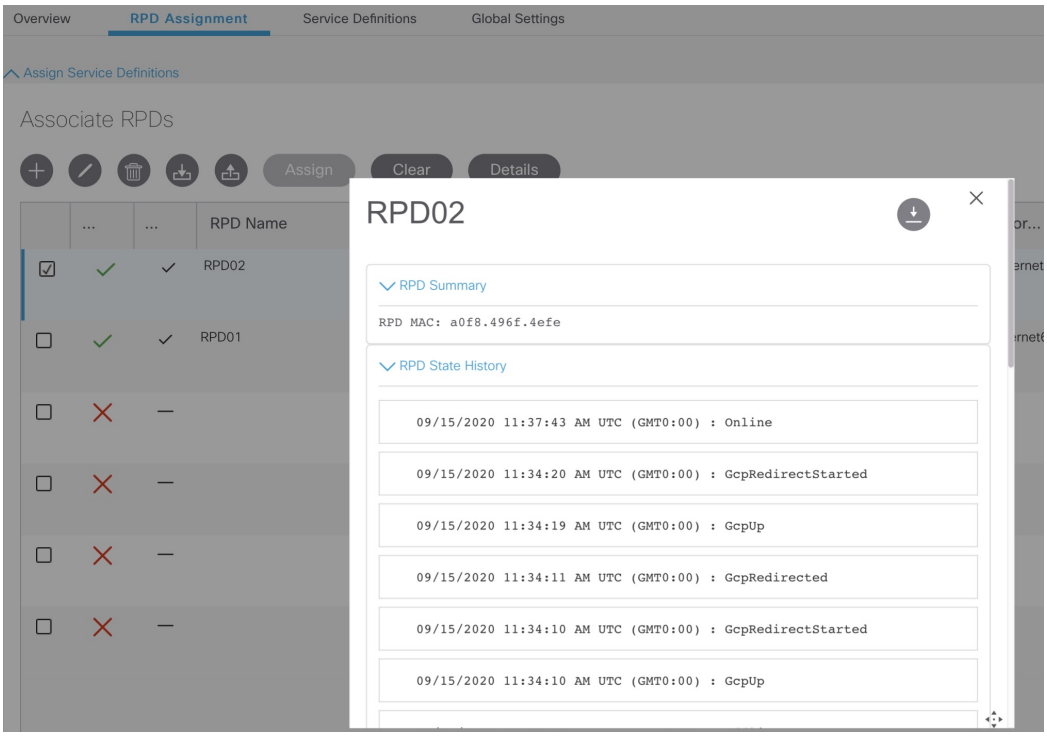
```
inventory-manager/inventory/v1/device/query-device-list
```

View RPD History

Step 1 Choose **Cable 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.



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.

1. Go to **RPD Automation**> **Global Settings** > **Database Backup**.
2. In the Server field enter **localhost**.

Leave the remaining fields blank (Username, Password, Directory, and Filename).

3. Click the **Export** button.

Remote Backup

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

1. Go to **RPD Automation**> **Global Settings** > **Database Backup**.
2. In the Server field enter the IP address or the `hostname.domain.com` of the remote server.

   Enter the user login credentials in the **Username** and **Password** fields.
3. In the **Directory** field, enter the file path on the remote server.

   Leave the **Filename (Import Only)** field blank.
4. Click the **Export** button.

Add Users using Cisco Operations Hub CLI

The Cisco Operations Hub ops-center CLI allows the administrator to create new users.

The Cisco Operations Hub ops-center URL is `https://cli.opshub-data-ops-center.{hostname}/`. The administrator can log into the Cisco Operations Hub ops-center CLI using the `admin` username and its password that is created while installing Cisco Smart PHY application.

```
product opshub# smiuser show-user username admin
User: admin, Group(s): admin api-admin api-editor api-viewer li-admin, Password Expiration
 days: 86
```

Add Users

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: -1
```

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: -1
```

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

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

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

Example:

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

Basic and LDAP Authentication

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

- Basic authentication
- LDAP authentication

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

Switch from Basic Authentication to LDAP Authentication

The Operations Hub `ops-center` CLI allows an administrator to configure LDAP settings for external authentication with AD (Active Directory).

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

Step 1 Access the Operations Hub ops-center by using the following URL:

```
https://cli.opshub-data-ops-center.{Hostname}/
```

Step 2 Log in to the Operations Hub ops-center CLI.

The administrator can log into the Operations Hub ops-center CLI using the `admin` username and its password that is created while deploying the Operations Hub.

Example:

```
product opshub# config t
Entering configuration mode terminal
product opshub(config)# ldap-security ldap-server-url ******
product opshub(config)# ldap-security ldap-username-domain ******.com
product opshub(config)# ldap-security base-dn DC=******,DC=com
product opshub(config)# ldap-security ldap-filter userPrincipalName=%s@******.com
product opshub(config)# ldap-security group-attr memberOf
product opshub(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

Step 3 Configure the mapping between the LDAP groups and the API groups.

Example:

```
product opshub(config)# ldap-security group-mapping ?
Possible completions:
  LDAP group
product opshub(config)# ldap-security group-mapping {ldap group}} ?
Possible completions:
  <NACM group>  admin  api-admin  api-editor  api-viewer
product opshub(config)# ldap-security group-mapping {ldap group}} api-admin
product opshub(config-group-mapping-crdc-docsis/api-admin)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

Switch from LDAP Authentication to Basic Authentication

Remove the LDAP configuration from the Operations Hub ops-center to switch from LDAP authentication to basic authentication.

```
product opshub(config)# no ldap-security
product opshub(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

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.

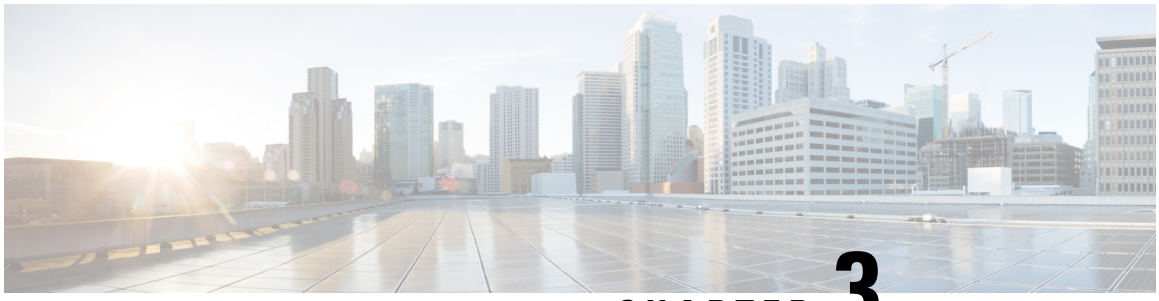
Caution Renew the Kubernetes client TLS certificates before they expire. Otherwise, the operation and functionality of the Cisco Smart PHY cluster will be impacted.

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 3

Monitor and Troubleshoot

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

Monitor Host Resources

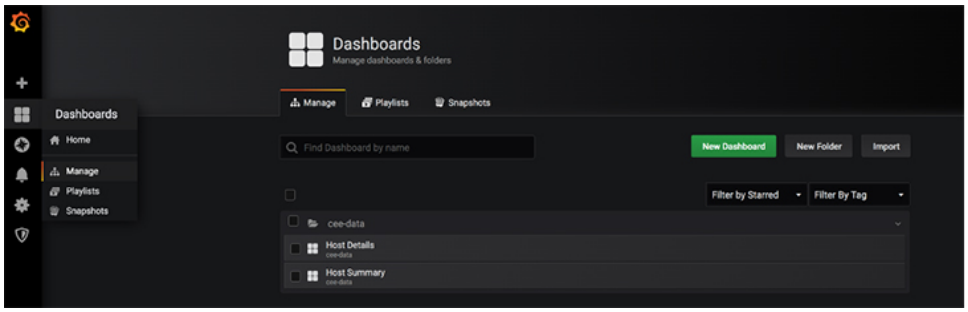
Use the Grafana dashboard for monitoring host resources.

Step 1 Access the Grafana dashboard using the following URL: `https://grafana.<smartphy-ip>.nip.io/` or `https://grafana.<fqdn>/`

Step 2 Log in using the credentials used during the installation.

Step 3 Select **Dashboards** > **Manage**.

Step 4 Click the **cee-data** and then select **Host Details**.



Step 5 To view details of CPU, Memory, or Disk usage, select the **Host** on the top left corner of the screen.

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

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

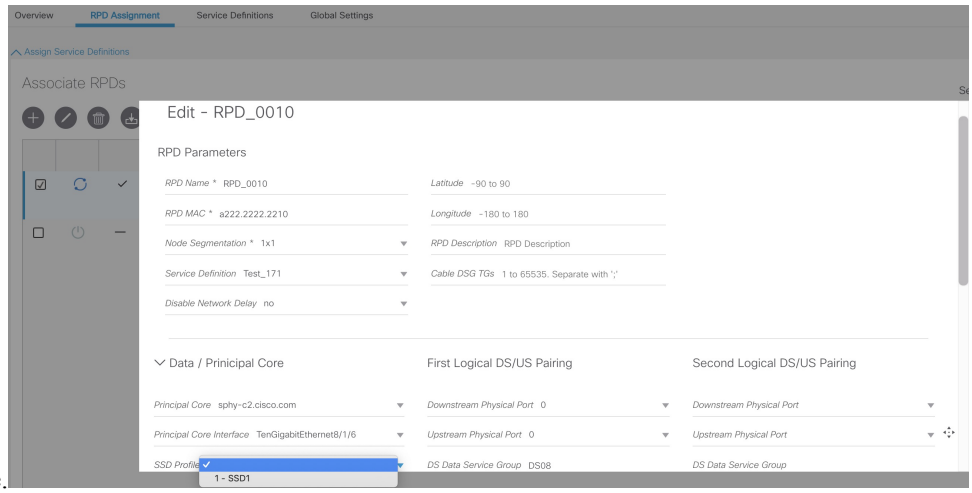
   Output:

   The value of ssdProfileId must be correct.


```
Input:
{
}

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

3. Verify the SSD profile ID and the image name in the **Edit** window of the RPD paring table.



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

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
ssd 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 ssd 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:

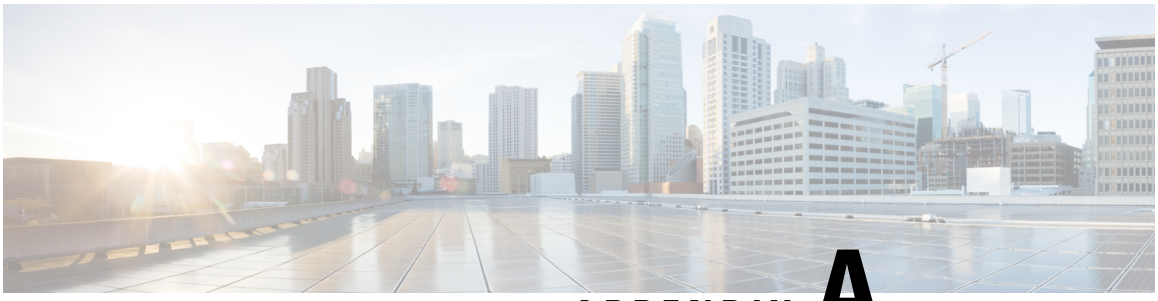
- If the secondary line card is active:
  1. Revert to the primary line card.
  2. Wait until the primary line card is active

- 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

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 Cisoc 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.