Security and Administration

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

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

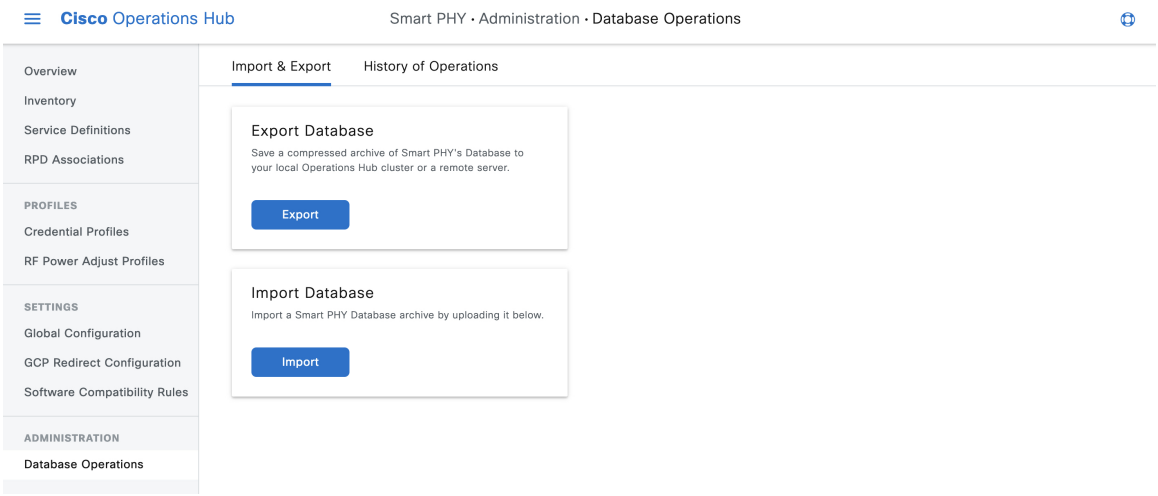
Database Operations

Table 1: Feature History

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

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

Figure 1: Database Operations



Exporting Smart PHY Database to Local Computer

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

Use this task to export the database from local filesystem

Procedure

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

The **Import & Export** page appears.

Step 2 Click **Export**.

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

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

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

Step 4 Click **Export**.

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

Exporting Smart PHY Database to Local Operations Hub Cluster

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

Use this task to export the database from local filesystem

Procedure

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

The **Import & Export** page appears.

Step 2 Click **Export**.

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

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

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

Step 4 Click **Export**.

Exporting Database to a Remote Server

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

Procedure

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

The **Import & Export** page appears.

Step 2 Click **Export**.

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

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

Enter the following details for the remote server:

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

Step 4 Click **Export**.

Importing Database

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

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

This procedure imports a database.

Procedure

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

The **Import & Export** page appears.

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

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

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

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

Step 4 Click **Import**.

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

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

Configuring SSH Private Key Profiles

Table 2: Feature History

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

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

Creating SSH Private Key Profiles

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

Note:

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

The RSA PEM Key format example is given below:

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

When private key is passphrase encrypted:

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

Validating SSH Private Key Profiles

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

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

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

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

Editing SSH Private Key Profiles

An SSH private key profile can be edited anytime.

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

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

Deleting SSH Private Key Profiles

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

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

Viewing History of Database Operations

Smart PHY maintains a history of all database Operations.

The history contains the following information:

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

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

Procedure

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

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

You can also perform the following tasks:

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

Customizing Smart PHY Settings

Feature History

Table 3: Feature History

Feature Name	Release Information	Description
I15 Specifications - GCP Redirect Global Configuration	Cisco Smart PHY, Release 24.2	With this release, if an RPD fails to be redirected using Smart PHY's I15 compliant GCP Redirect, then you can configure a redirect of the same RPD with its original pre-I15 redirect behavior.
Aux Core Configuration for RPD	Cisco Smart PHY, Release 22.4	You can use this option to configure additional cores on RPD's DOCSIS Principal Core using TLV 88.1.
Decision Pending IRA	Cisco Smart PHY, Release 22.4	Decision Pending IRA functionality is introduced to handle GCP redirect delays.

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

- Global Configuration
- GCP Redirect Configuration
- Software Compatibility Rules

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

Global Configuration

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

- **Software Compatibility Rules**
  - **Validate Software Compatibility** - When enabled, Smart PHY performs a compatibility check based on the configured Software Compatibility Rules. For more information, see Software Compatibility Rules.
- **Remote PHY Devices**
  - **Program Additional Cores via**

  - **Smart PHY GCP Redirect** - Enable Smart PHY GCP Redirect. For more information, see GCP Redirect Configuration.
  - **DOCSIS Principal Core (TLV 88.1)** - Configure an RPD's DOCSIS Principal Core program additional cores via TLV 88.1. For more information, see Programming Additional Cores.

- **Send Decision Pending IRA Messages** - Enable Decision Pending IRA Messages feature. For more information, see Configuring Decision Pending IRA Message

  .
- **Enable RPD SSD Max Retry** - Configure the maximum number of failed consecutive SSD operations and also configure the duration between the retry attempts. For more information, see Secure Software Download for RPD.
- **GCP Redirect I15 Globally** - When enabled, GCP redirects all RPD's globally. The I15 global toggle overrides the GCP redirect rules. For more information, see I15 Specifications - GCP Redirect Global Configuration.

- **cBR-8 Routers**
- **Configure Static Routes**—For more details, see the Static Routes section.
- **Persist Running Configuration**—When enabled, Smart PHY saves the changes that are made to the cBR-8 router's running configuration.
  - **Configuration Save Interval**—This value determines the interval at which the changes are saved. The default value is 60 minutes and valid range is 1-65535 mins.

Software Compatibility Rules

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

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

Programming Additional Cores

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

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

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

GCP Redirect Configuration

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

Creating I15 GCP Redirect entry

Procedure

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

The **GCP Redirect Configuration** page appears

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

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

Step 4 Click **Add**

I15 GCP-redirect Result Notification

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

I15 GCP Redirect Configuration

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

I15 Specifications - GCP Redirect Global Configuration

Starting with Cisco Smart PHY, Release 24.2, if an RPD fails to be redirected using Smart PHY's I15 compliant GCP Redirect, then you can configure a redirect of the same RPD with its original pre-I15 redirect behavior.

Procedure

Step 1 At the Main Menu, select on **Smart PHY** > > **Global Configuration**.

Step 2 Select the **GCP Redirect I15 Globally** toggle switch to enable this feature.

Configuring Decision Pending IRA Message

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

When large numbers of RPDs boot-up or initialize at the same time, Smart PHY may not be able to process and reply to every incoming GCP Startup Notify message in a timely manner. RPDs with long waits may send multiple Startup Notify messages or even timeout and reboot before Smart PHY is able to reply with a GCP Redirect IRA message.

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

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

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

Static Routes

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

Note

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

Sample of a Cisco Smart PHY-Generated Configuration

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

 cable fiber-node <next available fiber-node>
```

```
downstream Downstream-Cable 9/0/16
upstream Upstream-Cable 9/0/1
downstream sg-channel 0 23 downstream-Cable 9/0/16 rf-channel 0 23
upstream sg-channel 0 3 Upstream-Cable 9/0/1 us-channel 0 3
service-group managed md 0 Cable 9/0/1
service-group profile SG1
```

Creating a Software Conmpatibility Rule

This procedure creates a software compatibility rule.

Procedure

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

The **Software Compatibility Rules** page appears.

Step 2 Click **Create**.

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

Step 3 Enter the following information:

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

Step 4 Click **Add**

DB Inconsistencies Alerting Mechanism

Table 4: Feature History

Feature Name	Release Information	Description
DB Inconsistencies Alerting Mechanism	Cisco Smart PHY, Release 25.2	This feature fixes inconsistent Smart PHY DB tables data using some of the existing Smart PHY and Operations Hub capabilities. In previous Cisco Smart PHY releases, scripts were used to detect inconsistent Smart PHY DB tables data but fixing the inconsistent data was not possible.

Information about DB Inconsistencies Alerting Mechanism

A new page called *DB Inconsistencies Finder* is introduced with this release, which allows you to schedule tasks in advance, which run at the scheduled time. The task can also be triggered instantly when needed.

To access the DB inconsistencies alerting mechanism, at the main menu select **Smart PHY** > **Settings** > **DB Inconsistencies Finder**. The **DB Inconsistencies Finder** page is displayed.

To create a task, click **Create** and populate the following fields:

Table 5: DB Inconsistencies Finder Fields

Field Name	Description
Task Name	Enter a name for the task
Description	Enter a short description for the task
Core IP list	Select the core already listed or create a new core
Start Date	Enter a start date
Start Time	Enter a start time
Frequency	• Daily – Runs every day at the specified time • Weekly – Runs on selected days of the week • Monthly – Runs at a specific date each month

After populating the fields, click **Schedule** to schedule the task.

Task Page Options

After you click the desired task, you have the **Done**, **Run Now** and **Edit** buttons. You also have three dots next to Edit. If you click the three dots, you can see the **Delete**, **Suspend** and **Resume** Buttons.

Table 6: Task Button Actions

Button Name	Description
Done	Close the Task window once you done viewing or editing the page
Run Now	Run the task
Edit	Edit the task
Delete	Delete the task
Suspend	Suspend the task
Resume	Resume the task

Task Operations (Delete, Suspend, and Resume) are available based on task status found on the DB Inconsistencies Finder page:

- When a task is in the running state, then you can Suspend or Delete the task by clicking the **Suspend** or **Delete** buttons respectively.
- When a task is paused, then it you can first move it to the Pausing state and then to the Paused state.
- When a task is in the paused state, then it can be resumed clicking the **Resume** button.
- When a task is in the running state, then you can delete a task by clicking the **Delete** button and then task is moved to the active state.
- When a task is in active / inactive / completed state, then Task Operations are disabled.

Here are the tabs available after you click the desired task:

- **Overview Tab**:

  Displays the general information about the task.

- **Core IP address Tab**:

  The Core IP address page lists all cores mapped to each run. It shows their reconciliation results with status filters Successful, Failed, Partially Successful or Pending. To access the Run History page, click the desired task and select the **Core IP address** tab.

- **Run History Tab**:

  The Run History page of the Task displays the past execution records with their reconciliation status. It highlights whether runs were successful, failed, or partially successful along with inconsistent details. To access the Run History page, click the desired task and select the **Run History** tab.

Configuration For Email Alerts for DB Inconsistencies

Before setting up email alerts in DB inconsistencies, you need to enable the main email notification in the system setting by following these steps:

1. At the main menu, select **Smart PHY** > **System** > **Email Notifications** to view the **Email Notifications** page.
2. Click Edit on the bottom right of the page and select the **Email Notifications** toggle and enable it.
3. Click **Save**.

Once the main email notifications are enabled, you can proceed to enable the DB inconsistency email notification.

Use this global configuration to enable email alerts in DB inconsistency. This configuration enables triggering emails after task execution in the DB Inconsistency finder page. To access the email alert settings for DB inconsistencies, follow these steps:

1. At the main menu, select **Smart PHY** > **Settings** > **Global Configuration** to view the **Global Configuration** page.
2. Select the **Enable Email Settings for DB Inconsistencies** toggle and enable it. This toggle is disabled by default.
3. Enter valid email addresses separated by a comma in the **Email IDs** text box.