



RMS User Guide

CBAC-R4.1.0

September 2024



Radisys Corporation.
Headquarters: Hillsboro, Oregon
8900 NE Walker Rd. Suite 130
Hillsboro, OR 97006
United States
+1.503.615.1100
sales@radisys.com
+1.503.615.1115

© 2024 Radisys Corporation. All rights reserved.

Radisys is a registered trademark of Radisys Corporation. Linux is a registered trademark of Linus Torvalds. All other trademarks, registered trademarks, service marks, and trade names are the property of their respective owners.

Contents

| | |
|---|-----------|
| Preface..... | 15 |
| About this Guide..... | 15 |
| Audience..... | 15 |
| Documentation Map..... | 16 |
| What's New in this Manual..... | 16 |
| Notational Conventions..... | 16 |
| About RMS..... | 18 |
| Browser Requirements..... | 18 |
| Accessing RMS..... | 18 |
| Viewing Timezone..... | 20 |
| Verifying the DB Migration Status..... | 21 |
| RMS Dashboard Page..... | 22 |
| Managing User Accounts..... | 24 |
| Managing User Passwords..... | 24 |
| Managing User Sessions..... | 25 |
| Changing the Password on First Login..... | 26 |
| Resetting the Password..... | 27 |
| Common Operations..... | 27 |
| Customize Columns..... | 28 |
| Show Table Entries..... | 28 |
| Search..... | 28 |
| Editing Resources..... | 28 |
| Viewing Resources..... | 28 |
| Deleting Resources..... | 29 |
| Cloning Resources..... | 29 |
| Using Column Filter..... | 29 |
| Global Search..... | 30 |
| RMS Main Workspaces..... | 31 |
| Fault Icons..... | 34 |
| Workflow for Activating a Service for the Subscriber..... | 36 |
| Configuration Types..... | 36 |
| Create Management Domain Workflow..... | 37 |
| OLT Profiles Workflow..... | 38 |
| OLT Activation Workflow..... | 38 |
| PON Profiles Workflow..... | 39 |

| | |
|--|-----------|
| ONT Activation Workflow..... | 40 |
| Service Activation Workflow..... | 40 |
| Dashboard..... | 42 |
| Tasks..... | 42 |
| Custom Dashboard..... | 42 |
| Widget Descriptions..... | 43 |
| Statistics Charts..... | 44 |
| OLT State Statistics..... | 45 |
| Latest Faults..... | 46 |
| OLT Port State Statistics..... | 47 |
| ONT State Statistics..... | 47 |
| Controller Statistics..... | 48 |
| ME Fault Statistics..... | 48 |
| ME Model Statistics..... | 49 |
| ME Site Statistics..... | 50 |
| ME Make Statistics..... | 50 |
| Alarms Histogram..... | 51 |
| Generating Custom Alarm Histogram..... | 52 |
| Sites Location..... | 53 |
| OLT Location..... | 53 |
| Monitoring Inventory..... | 54 |
| Tasks..... | 54 |
| Field Descriptions..... | 54 |
| OLT Inventory..... | 54 |
| ONT Inventory..... | 58 |
| CPE Inventory..... | 61 |
| Splitter Inventory..... | 63 |
| Card Inventory..... | 63 |
| Rack Inventory..... | 64 |
| SFP Inventory..... | 65 |
| Cable Inventory..... | 66 |
| ONT Card Inventory..... | 66 |
| Exporting Managed Elements..... | 66 |
| Inventory..... | 67 |
| Monitoring OLT..... | 67 |
| Monitoring ONT..... | 156 |
| Monitoring Card Details..... | 171 |
| Monitoring Rack Details..... | 172 |
| Monitoring SFP..... | 175 |

| | |
|---------------------------------------|------------|
| Blacklisted ME..... | 178 |
| Field Descriptions..... | 179 |
| Single Click Provisioning..... | 180 |
| Controller..... | 182 |
| Field Descriptions..... | 183 |
| Monitoring Controller..... | 184 |
| Management Domain..... | 207 |
| Field Descriptions..... | 208 |
| Monitoring Protection..... | 209 |
| Type-B Protection..... | 209 |
| Field Descriptions..... | 209 |
| Type-B Protection Pair Details..... | 210 |
| Ring..... | 214 |
| Field Descriptions..... | 215 |
| Monitoring Services..... | 216 |
| Subscriber Service..... | 216 |
| Field Descriptions..... | 216 |
| Sub Services..... | 216 |
| Historical Statistics..... | 220 |
| Live KPIs..... | 221 |
| Service Queue Statistics..... | 222 |
| Audit Log..... | 222 |
| Exporting Service Inventory List..... | 223 |
| Subscriber..... | 223 |
| Field Descriptions..... | 223 |
| Monitoring Subscriber..... | 224 |
| Services..... | 225 |
| Data Sync Request..... | 226 |
| Audit Log..... | 226 |
| Monitoring Infrastructure..... | 227 |
| Database Statistics..... | 227 |
| Field Descriptions..... | 227 |
| Session..... | 227 |
| Field Descriptions..... | 227 |
| Monitoring Logs..... | 229 |
| Audit Log..... | 229 |
| Fields Descriptions..... | 230 |
| Backup Jobs..... | 231 |

| | |
|--|------------|
| Fields Descriptions..... | 232 |
| Restoring the Backup Configuration File..... | 232 |
| Data Synchronization Request..... | 233 |
| Fields Descriptions..... | 233 |
| Monitoring Reports..... | 235 |
| Field Descriptions..... | 235 |
| Fault Summary Report..... | 236 |
| Performance Summary..... | 237 |
| Monitoring Faults..... | 238 |
| Alarm Severity Levels..... | 238 |
| Tasks..... | 239 |
| Field Descriptions..... | 240 |
| Acknowledging and Clearing Alarms..... | 245 |
| Exporting Fault List..... | 246 |
| Viewing Fault Details..... | 247 |
| Fault Details..... | 247 |
| Monitoring Events..... | 249 |
| Field Descriptions..... | 249 |
| Exporting Events..... | 250 |
| Monitoring Tasks..... | 251 |
| Field Descriptions..... | 251 |
| Monitoring Task Details..... | 252 |
| OLT Software Upgrade..... | 253 |
| Reports..... | 254 |
| EMS Database Backup..... | 255 |
| OLT/Controller Backup..... | 256 |
| OLT/Controller Restore..... | 258 |
| Controller Software Upgrade..... | 259 |
| ONT Firmware Upgrade..... | 260 |
| ONT Bulk Firmware Upgrade..... | 262 |
| OLT Firmware Upgrade..... | 265 |
| Inventory Collection..... | 265 |
| Service Collection..... | 267 |
| Fault Collection..... | 269 |
| Event Collection..... | 270 |
| Audit Log Collection..... | 272 |
| OLT Configuration Update..... | 272 |
| ONT Configuration Update..... | 273 |
| Bulk Port Modification..... | 275 |

| | |
|---|------------|
| Reboot..... | 276 |
| PON Port Migration..... | 277 |
| Banner Update..... | 279 |
| Monitoring Utilities..... | 281 |
| Ping..... | 281 |
| TraceRoute..... | 281 |
| Topology..... | 283 |
| Physical Topology of the OLT..... | 285 |
| Logical Topology of the OLT..... | 286 |
| Legends in the OLT Topology..... | 287 |
| Configuration..... | 289 |
| Site..... | 289 |
| Creating Site Configuration..... | 289 |
| Site Group..... | 290 |
| Creating Site Group Configuration..... | 290 |
| Viewing and Creating Site Sub Groups..... | 291 |
| Site Group Type..... | 292 |
| Field Descriptions..... | 292 |
| Creating Site Group Type Configuration..... | 292 |
| ME Group..... | 293 |
| Creating ME Group Configuration..... | 293 |
| ME Group Member..... | 294 |
| Controller..... | 295 |
| Tasks..... | 295 |
| Field Descriptions..... | 296 |
| Creating Controller Configuration..... | 297 |
| Activating the Controller..... | 305 |
| Deactivating the Controller..... | 306 |
| Replacing the Password..... | 306 |
| Controller Backup and Restore..... | 307 |
| Download Controller Software..... | 309 |
| Upgrade Controller Software..... | 310 |
| Controller Monitored Entity..... | 311 |
| Inventory..... | 313 |
| Tasks..... | 313 |
| OLT..... | 314 |
| ONT..... | 423 |
| CPE..... | 438 |
| Splitter..... | 440 |

| | |
|---------------------------------------|------------|
| BNG..... | 442 |
| CARD..... | 444 |
| Rack..... | 446 |
| SFP..... | 450 |
| Cable..... | 451 |
| Exporting Managed Elements..... | 452 |
| Importing Managed Elements..... | 453 |
| Subscriber..... | 454 |
| Tasks..... | 454 |
| Creating Subscriber..... | 455 |
| Exporting Subscriber Information..... | 456 |
| Service..... | 456 |
| Profiles..... | 473 |
| Alarm Profile..... | 473 |
| Creating Alarm Profile..... | 474 |
| OLT Alarm Profile..... | 475 |
| OLT Port Alarm Profile..... | 482 |
| ONT Alarm Profile..... | 485 |
| LAG Alarm Profile..... | 486 |
| ACE Alarm Profile..... | 488 |
| SFP (NNI) Alarm Profile..... | 489 |
| SFP (PON) Alarm Profile..... | 493 |
| ANI-G Alarm Profile..... | 497 |
| Log Profile..... | 502 |
| Creating Log Profile..... | 503 |
| PPPoE Profile..... | 503 |
| Creating PPPoE Profile..... | 504 |
| PPPoE Over OMCI..... | 505 |
| Device Profile..... | 507 |
| Creating Device Profile..... | 508 |
| OLT Device Profile..... | 508 |
| ONT Device Profile..... | 515 |
| SFP Device Profile..... | 516 |
| CPE Device Profile..... | 518 |
| Splitter Device Profile..... | 519 |
| BNG Device Profile..... | 521 |
| Card Device Profile..... | 522 |
| Rack Device Profile..... | 524 |
| Cable Profile..... | 526 |

| | |
|--------------------------------------|------------|
| Port Configuration..... | 528 |
| Authentication Profile..... | 537 |
| Creating Authentication Profile..... | 537 |
| ACL Profile..... | 538 |
| Creating ACL Profile..... | 538 |
| Deleting ACL Profile..... | 545 |
| ERPS Profile..... | 546 |
| Creating ERPS Profile..... | 546 |
| IP Host Profile..... | 548 |
| Field Descriptions..... | 548 |
| Creating IP Host Profile..... | 549 |
| MEP Profile..... | 550 |
| Creating MEP Profile..... | 550 |
| NTP Profile..... | 553 |
| Creating NTP Profile..... | 553 |
| Circuit ID Format..... | 554 |
| Creating Circuit ID Format..... | 554 |
| Remote ID Profile..... | 557 |
| Creating Remote ID Profile..... | 558 |
| TACACS Profile..... | 559 |
| Creating TACACS Profile..... | 559 |
| Alarm Soak Profile..... | 560 |
| Creating Alarm Soak Profile..... | 561 |
| PON Profiles..... | 563 |
| Bandwidth Profile..... | 563 |
| Field Descriptions..... | 563 |
| Creating Bandwidth Profile..... | 564 |
| Shaper Profile..... | 566 |
| Field Descriptions..... | 566 |
| Creating Shaper Profile..... | 567 |
| MVLAN Profile..... | 568 |
| Creating MVLAN Profile..... | 568 |
| COSQ Profile..... | 570 |
| Creating COSQ Profile..... | 570 |
| VNet Profile..... | 575 |
| VLAN CONTROL..... | 575 |
| Creating VNet Profile..... | 577 |
| IGMP Profile..... | 583 |
| Field Descriptions..... | 583 |

| | |
|--|------------|
| Creating IGMP Profile..... | 584 |
| Policer Profile..... | 586 |
| Creating Policer Profile..... | 587 |
| Storm Control Profile..... | 587 |
| Creating Storm Control Profile..... | 588 |
| Voice Service Profiles..... | 589 |
| POTS Profile..... | 589 |
| Creating POTS Profile..... | 589 |
| SIP Agent Profile..... | 590 |
| Creating SIP Agent Profile..... | 590 |
| SIP User Data Profile..... | 591 |
| Creating SIP User Data Profile..... | 592 |
| Network Dial Plan Profile..... | 593 |
| Creating Network Dial Plan Profile..... | 593 |
| VoIP Service Info Profile..... | 595 |
| Creating VoIP Service Info Profile..... | 595 |
| VoIP Media Info Profile..... | 596 |
| Creating VoIP Media Info Profile..... | 596 |
| RTP Info Profile..... | 598 |
| Creating RTP Info Profile..... | 598 |
| VoIP App Service Profile..... | 599 |
| Creating VoIP Application Service Profile..... | 600 |
| Settings..... | 603 |
| Email Notification..... | 603 |
| Field Descriptions..... | 603 |
| Creating E-Mail Notification..... | 603 |
| Make..... | 605 |
| Field Descriptions..... | 605 |
| Creating Make Configuration..... | 606 |
| Model..... | 608 |
| Field Descriptions..... | 609 |
| Creating Model Configuration..... | 610 |
| Model Version..... | 611 |
| Field Descriptions..... | 611 |
| Creating Model Version Configuration..... | 612 |
| ONT Firmware Information..... | 614 |
| Field Descriptions..... | 614 |
| Creating ONT Firmware Information..... | 614 |
| Alarm Severity..... | 616 |

| | |
|--|------------|
| Field Descriptions..... | 616 |
| Editing Alarm Severity..... | 616 |
| File Storage..... | 617 |
| Field Descriptions..... | 617 |
| Creating File Store Configuration..... | 618 |
| Alarm Suppression..... | 619 |
| Tasks..... | 619 |
| Field Descriptions..... | 619 |
| Creating Alarm Suppression Configuration..... | 620 |
| Editing, Deleting, and Monitoring Alarm Suppression Configuration..... | 622 |
| Others..... | 623 |
| Field Descriptions..... | 623 |
| Filter Expression..... | 629 |
| Field Descriptions..... | 629 |
| Creating Filter Expression..... | 630 |
| Forwarding Policy..... | 631 |
| Field Descriptions..... | 631 |
| Creating Forwarding Policy..... | 631 |
| Logging Configuration..... | 632 |
| Protection..... | 635 |
| Type-B Protection Pair..... | 635 |
| Field Descriptions..... | 636 |
| Creating Type-B Protection Pair..... | 638 |
| Deleting Type-B Protection Pair..... | 640 |
| Manual Switchover..... | 640 |
| Auto Switchover..... | 641 |
| Policy..... | 642 |
| Creating PM Collection Policy..... | 642 |
| Maintenance..... | 644 |
| Field Descriptions..... | 644 |
| Creating Task Configuration..... | 645 |
| Creating Task for Single or Bulk OLT Software Upgrade (ONL or OLT BINS)..... | 647 |
| Creating Task for Report Generation..... | 656 |
| Creating Task for EMS Database Backup..... | 659 |
| Creating Task for Controller or OLT Backup..... | 661 |
| Creating Task for Controller or OLT Restore..... | 667 |
| Creating Task for Single or Bulk Controller Software Upgrade..... | 669 |
| Creating Task for ONT Firmware Upgrade..... | 674 |
| Creating Task for ONT Bulk Firmware Upgrade..... | 681 |

| | |
|--|------------|
| Creating Task for OLT Firmware Upgrade..... | 687 |
| Creating Task for Inventory Collection..... | 689 |
| Creating Task for Service Collection..... | 693 |
| Creating Task for Fault Collection..... | 696 |
| Creating Task for Event Collection..... | 700 |
| Creating Task for Audit Log Collection..... | 705 |
| Creating Task for Bulk Port Modification..... | 710 |
| Creating Task for Configuration Update..... | 716 |
| Creating Task for OLT Reboot..... | 720 |
| Creating Task for PON Port Migration..... | 721 |
| Creating Task for Banner Update..... | 724 |
| Editing and Deleting Task Configuration..... | 728 |
| Automation..... | 730 |
| Bulk Operation..... | 730 |
| Activate, Deactivate, and Reboot ONT..... | 730 |
| Activate and Deactivate UNI Port..... | 735 |
| Activate, Deactivate, and Delete Service..... | 741 |
| Provision New Service..... | 746 |
| Update Service Configuration..... | 755 |
| Single Click Provisioning..... | 761 |
| Field Descriptions..... | 761 |
| Creating Single Click Provisioning..... | 762 |
| Administration..... | 765 |
| Management Domain..... | 765 |
| Creating Management Domain..... | 765 |
| Activating and Deactivating the Management Domain..... | 766 |
| Monitoring Management Domain..... | 766 |
| User..... | 766 |
| Tasks..... | 767 |
| Field Descriptions..... | 767 |
| Creating User Configuration..... | 770 |
| Configuring or Updating Administrator E-Mail ID..... | 773 |
| Viewing Active Sessions for the User..... | 773 |
| Locking and Unlocking the User..... | 774 |
| Activating and Deactivating the Custom User Account..... | 774 |
| Exporting User Accounts..... | 775 |
| User Role..... | 775 |
| Field Descriptions..... | 775 |
| Role Based Access Control..... | 776 |

| | |
|---|------------|
| Field Descriptions..... | 778 |
| Creating Custom User Role Configuration..... | 778 |
| Assigning Access Permissions for User Roles..... | 779 |
| Security Policy..... | 785 |
| Creating Security Policy Configuration..... | 785 |
| Template Builder..... | 787 |
| Tasks..... | 787 |
| Creating OLT Template..... | 788 |
| Creating ONT Template..... | 791 |
| Creating Card Template..... | 792 |
| Creating Rack Template..... | 794 |
| Creating Shelf Template..... | 795 |
| Creating Subscriber Template..... | 796 |
| Creating Subscriber Service Template..... | 798 |
| Creating Controller Template..... | 799 |
| Creating ZTP Template..... | 801 |
| Exporting Template..... | 803 |
| Importing Template..... | 803 |
| Configuration Examples..... | 805 |
| Example: Configuring and Activating HSIA Services for the Subscriber..... | 805 |
| Overview..... | 805 |
| HSIA Service Activation Workflow..... | 805 |
| Verification..... | 829 |
| Example: Configuring Voice Service for Subscriber..... | 830 |
| Overview..... | 830 |
| Voice Service Activation Workflow..... | 830 |
| Verification..... | 836 |
| Example: Voice Service Priority for SIP and RTP Packets..... | 837 |
| Overview..... | 837 |
| SIP and RTP Packets Remarketing Methods..... | 838 |
| Example: Configuring IPTV for Subscriber..... | 847 |
| Overview..... | 847 |
| IPTV Activation Workflow..... | 847 |
| Verification..... | 856 |
| Example: Configuring Whole Home Digital Video Recording..... | 857 |
| Overview..... | 857 |
| WHDVR Activation Workflow..... | 857 |
| WHDVR Configuration..... | 858 |
| Service Activation..... | 865 |

| | |
|--|------------|
| Verification..... | 865 |
| Example: ONT Replacement..... | 866 |
| Overview..... | 866 |
| ONT Replacement Workflow..... | 866 |
| Configuration..... | 867 |
| Verification..... | 869 |
| Example: Movement of ONT..... | 870 |
| Overview..... | 870 |
| ONT Movement Workflow..... | 871 |
| Prerequisites..... | 871 |
| Configuration..... | 871 |
| Verification..... | 872 |
| Example: OLT Pre-Configuration..... | 873 |
| Overview..... | 873 |
| OLT Pre-Configuration Workflow..... | 873 |
| Configuration..... | 874 |
| Verification..... | 884 |
| Example: Pre-Provision of ONT..... | 885 |
| Overview..... | 885 |
| Pre-provisioning Workflow..... | 885 |
| Prerequisites..... | 886 |
| Configuration..... | 886 |
| Verification..... | 890 |
| CBAC-D Upgrade..... | 891 |
| Setup Readiness..... | 891 |
| Prerequisites..... | 892 |
| Pre-Upgrade..... | 896 |
| CBAC-D Upgrade..... | 900 |
| Verifying CBAC-D Upgrade..... | 902 |
| CBAC-D Rollback (PE Window)..... | 904 |
| Verifying CBAC-D Rollback..... | 905 |
| Topology and Recommendation..... | 906 |
| Appendix A: Alarms..... | 907 |
| Appendix B: Events..... | 942 |
| Appendix C: Kubernetes Log Dump Script..... | 960 |

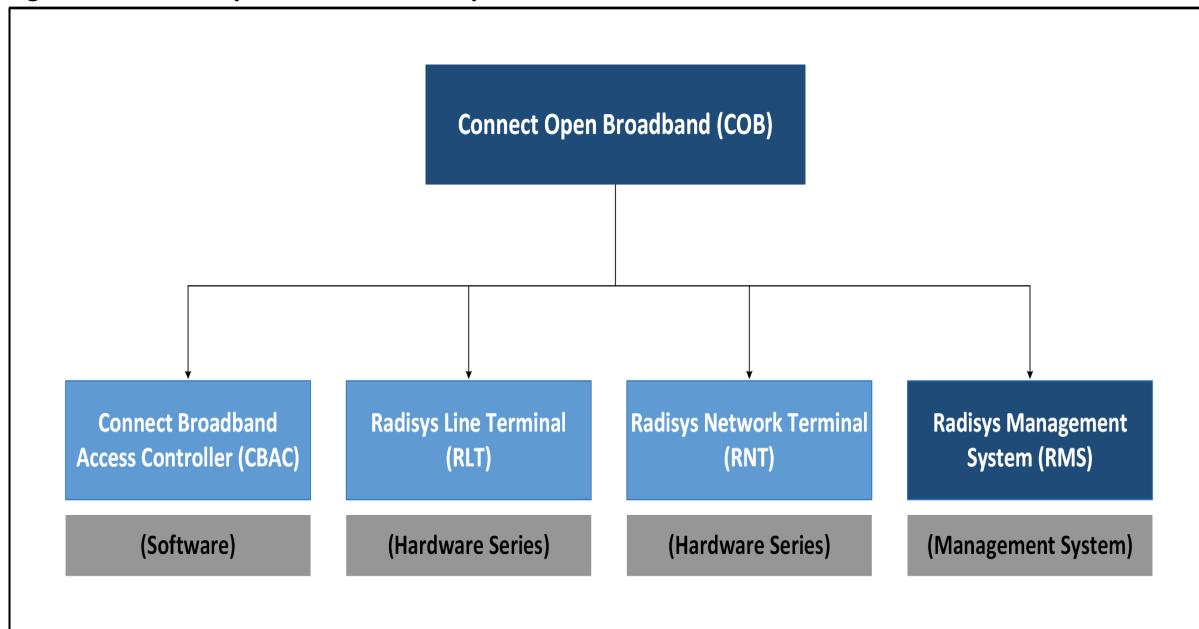
Preface

The Radisys' Connect Open Broadband solution is a software-driven broadband access solution that simplifies the fiber network management with a highly programmable framework based on the open standards and disaggregated architecture.

About this Guide

The following figure illustrates various components of the Connect Open Broadband (COB) solution.

Figure 1. Connect Open Broadband Components



As highlighted in [Figure 1: Connect Open Broadband Components \(on page 15\)](#), this guide provides information about the Radisys Management System (RMS) application. RMS acts as the element management system of the Connect Open Broadband solution and provides a single pane of glass (Web GUI) for service management, subscriber management, device configuration, faults management, and performance metrics.

For more information on the other components and their features refer to the respective documents.



Note: CBAC is the Radisys brand name used for this solution. Internally we reference CBAC as SDPON and you may find instances of SDPON. These two terms refer to the same solution.

Audience

This guide is intended for operators, system administrators, and deployment personnel who configure, monitor, and troubleshoot the RMS resources in a network.

Documentation Map

For more information on the tasks and corresponding documents, refer to the *CBAC Documentation Map*.

What's New in this Manual

The following features are added or updated in this release.

| For Information on... | See in this Manual... |
|---|---|
| OLT and SFPPON monitoring page improvements | ONT List (on page 120) |
| ONT monitor page improvements | Monitoring ONT (on page 156) |
| Controller monitor page improvements | Monitoring Controller (on page 184) |
| CLI sync for LAG, multicast configuration, IP host options profile and MVLAN profile. | CBAC CLI Synchronization with RMS (on page 202) |
| Subscriber and Service monitor page improvements | Monitoring Services (on page 216) |
| Data sync request processing: optimizations and improvements | Data Synchronization Request (on page 233) |
| Enable TACACS for default user roles | <ul style="list-style-type: none">TACACS Profile (on page 559)Creating Controller Configuration (on page 297)Settings (on page 603) |
| Port 80 configuration on ONT from RMS for HTTP access | HTTP Configuration (on page 432) |
| Multiple e-mail ID support for notifications | Settings (on page 603) |

Notational Conventions

This manual uses the following conventions.

| Convention | Meaning |
|-------------------|---|
| BoldText | A keyword. |
| <i>ItalicText</i> | <i>File, function, and utility names.</i> |
| MonoText | Screen text and syntax strings. |

| Convention | Meaning |
|-----------------------|--|
| BoldMonoText | A command to enter. |
| <i>ItalicMonoText</i> | Variable parameters. |
| Brackets [] | Command options. |
| Curly braces { } | A grouped list of parameters. |
| Vertical line | An “OR” in the syntax. Indicates a choice of parameters. |
| Asterisk * | Mandatory fields. |

All numbers are decimal unless otherwise stated.

About RMS

Radisys Management System (RMS) provides an architecture that can manage multiple access platforms. RMS provides a single point of integration for various access platforms, acts as a customer portal for various customer devices, and enables programmable networks.

RMS manages multiple vendor managed elements and controllers connected through the overlay network.

Using the RMS application, you can easily establish CBAC on an overlay network to connect enterprises with multiple offices, branches, school campuses, and so on.

RMS is a collection of microservices and supports the FCAPS (Fault, Configuration, Accounting, Performance, and Security) framework.

Browser Requirements

RMS supports the following version of the Web browser to ensure appropriate functioning of the features.

The following table lists the version of web browser supported in this release.

Table 1. Supported Web Browser

| Web Browser | Supported Version |
|----------------------|--------------------------|
| Google Chrome 64-bit | 76.0.3809.132 or higher. |

Accessing RMS

You can access the URL for the RMS Web GUI through the Web browser. The URL for RMS is *https* or *http://IP Address*, where the *IP Address* denotes the IP address of the RMS deployment server.

Perform the following steps to access the RMS Web GUI.

1. Perform the following steps if you are log in to RMS for the first time. Otherwise, skip to step 4 (*on page 19*).



Note: RMS supports a default username (admin, operator, and viewer) and password. When your administrator creates a default user account, an e-mail is sent to your e-mail address. This e-mail includes the login credentials (username and default password) that you can use to log in to RMS.

2. Log in to RMS using your username and default password.

The **Change Password** window appears. You must change your default password as per the guidelines provided in the following table.

Table 2. Fields on the Change Password Page

| Field | Description |
|----------------------|--|
| Username | Enter your username. |
| Old Password | Enter your old password. |
| New Password | <p>Enter your new password. The new password must fulfill the following requirements.</p> <ul style="list-style-type: none">◦ At least 10 characters◦ At least two lowercase letters (a-z)◦ At least two uppercase letters (A-Z)◦ Combination of lowercase (a-z) and uppercase (A-Z) letters◦ At least one special character (@, !, \$, and %)◦ At least one number (0-9)◦ Must not include the hash (#) symbol◦ Must not be any of the seven previously used passwords◦ Preventing sequences of letters and/or numbers, such as 123 or abc. <p> Note: If the password does not fulfill the above requirement, a pop-up with an appropriate error message is displayed to enter a password based on the requirement.</p> |
| Confirm New Password | Enter your new password again to confirm the password. |

3. Click **Submit**.

You are redirected to the login page to enter the username and new password.

4. Enter your username and new password.

The dashboard page appears as shown in [Figure 4: Dashboard Page \(on page 23\)](#). The main menu bar on the top right and the sub menu of every page allows you to access the different options easily. The top-level menu items are listed in [Table 7: RMS Workspaces \(on page 32\)](#).

Viewing Timezone

You can view the hardened OS timezone through RMS GUI. The time zone is set during the VM/OS installation and must be changed to desired value in the hardened OS. For more information on how to set the OS timezone, refer to the following guides based on the RMS deployment type.

- *Single Node RMS Installation and Upgrade Guide*
- *Multinode RMS Installation and Upgrade Guide*



Note:

- During an upgrade to the latest RMS, the following message is displayed if the database and OS time zones are different. No message is displayed if the database and OS time zones are the same.

```
Do you want to change the Database time zone to system time zone (Options:  
Yes/No, Default: No)
```

- Select **yes** to change the database time zone to system time zone.
- Select **no** to continue with the existing time zone set on database.
- The OS time zone is captured during the fresh installation of the RMS. The following message is displayed.

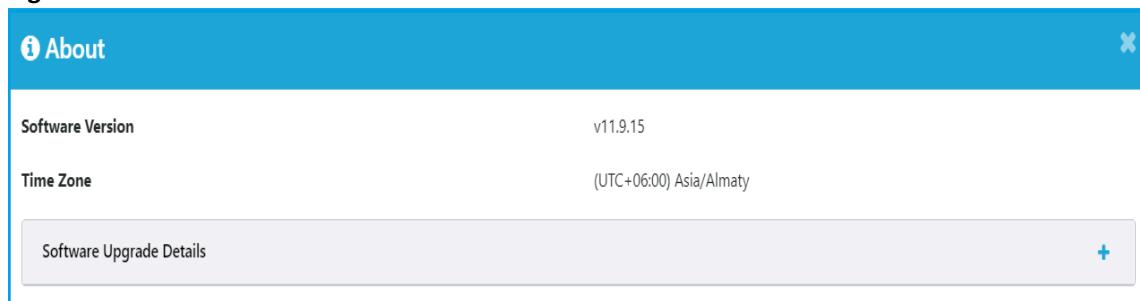
```
Current timezone at OS level is: <os_timezone>  
Do you want to proceed with <os_timezone> timezone (Options:yes/no,  
Default:yes)
```

- Select **yes** to continue with the OS_timezone displayed in the message.
- Select **no** to set the OS_timezone as per your requirement.

Perform the following steps to view the timezone.

1. Click **admin** from the top right corner of the page.
2. Select **About** from the menu. The About page appears.

Figure 2. Timezone



Verifying the DB Migration Status

Database migration is moving data between different types of databases, upgrading to a new database version, or transferring data to another platform or infrastructure.

Perform the following steps to verify the DB migration status.

1. Click **admin** from the top right corner of the page.
2. Select **About** from the menu.
The About page appears.
3. Click the plus icon (+) on the software update details.
The DB Migration Status page appears.

The following table displays the information displayed on the DB migration status page.

Table 3. DB Migration Status

| Field | Description |
|-------------------|---|
| Handler Name | Specifies the handler name including from and to version of the database. For example, V100704ToV110721MigrationHandler |
| Status | Specifies the database migration execution status of the handler. The supported values are. <ul style="list-style-type: none">◦ Success◦ Failure |
| Execution Methods | Specifies the operations executed by the handler. |
| Start Time | Specifies the migration start time of the handler. |

| Field | Description |
|----------|--|
| End Time | Specifies the migration end time of the handler. |

Figure 3. DB Migration

The screenshot shows the 'DB Migration Status' section of the RMS interface. The table has the following data:

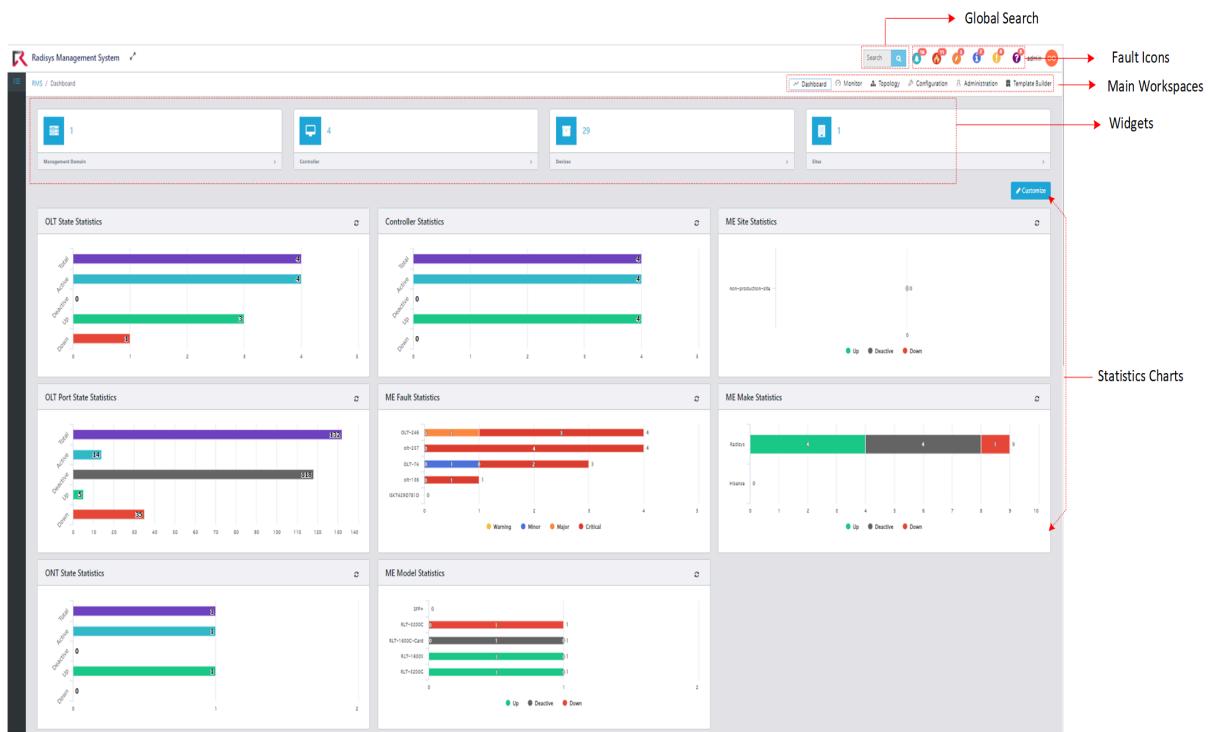
| Handler Name | Status | Executed Methods | Start Time | End Time |
|----------------------------------|---------|---|---------------------------|---------------------------|
| V100704ToV110721MigrationHandler | Success | | Sep 22, 2023, 10:57:33 AM | Sep 22, 2023, 10:57:34 AM |
| V110721ToV110804MigrationHandler | Success | | Sep 22, 2023, 10:57:34 AM | Sep 22, 2023, 10:57:35 AM |
| V110804ToV110818MigrationHandler | Success | [Populate Sfp Technology for Existing SFP], [Change Fault Collection Task Attribute], [Update SubscriberService Role Permissions for all], [Grant Ping Trace Permissions to Viewer], [Deprecate and update AlarmSeverity] | Sep 22, 2023, 10:57:35 AM | Sep 22, 2023, 10:57:36 AM |
| V110818ToV110901MigrationHandler | Success | | Sep 22, 2023, 10:57:36 AM | Sep 22, 2023, 10:57:36 AM |
| V110901ToV110915MigrationHandler | Success | [Migrate ProfileIds and Downstream Fec for Cpon Ports] | Sep 22, 2023, 10:57:36 AM | Sep 22, 2023, 10:57:36 AM |

Showing 1 to 5 of 5 entries

RMS Dashboard Page

The Dashboard is the main landing page for RMS. You can select and access the pages from the dashboard page as described in [Table 4: Dashboard Page Features \(on page 23\)](#).

Figure 4. Dashboard Page



The following table lists the dashboard page features.

Table 4. Dashboard Page Features

| Page | Description |
|-------------------|---|
| Global Search | You can search for RMS resources. For more information, see Global Search (on page 30) . |
| Fault Icons | Provides a list of icons that alert you to the faults reported in RMS. For more information, see Fault Icons (on page 34) . |
| Main Workspaces | The main workspace of RMS is divided by six horizontal tabs immediately following the Banner. For more information, see RMS Main Workspaces (on page 31) . |
| Widgets | Provides information on the management domain, controller, devices, and sites. For more information, see Widget Descriptions (on page 43) . |
| Statistics Charts | Provides statistics information on the managed elements, sites, controllers, management domain, OLT ports, and faults. For more information, see Statistics Charts (on page 44) . |

Managing User Accounts

A user account defines the unique username that is assigned to each user, which is used to log in to RMS. RMS requires that all users have a predefined user account before they log in to RMS.

RMS provides the following criteria for user accounts.

- **Login Notification.** Generates a notification to RMS on successful and unsuccessful login.
- **Unique User ID.** Individual users must be assigned a unique user ID for authentication.
- **User Accounts.** RMS supports default user accounts such as Admin, Operator, and Viewer. For more information about user roles, see [Role Based Access Control \(on page 776\)](#).
- **Account Expiry.** All predefined user accounts and third-party user accounts expire based on the security policy. For more information, see [Security Policy \(on page 785\)](#).
- **Deactivate User Accounts.** Inactive user accounts must be deactivated after the specified number of days configured in the security policy. All accounts that are not being used for a period of 60 days must be temporarily deactivated.
- **Account Lockout.** When a user tries to login with invalid credentials for more than three times, the user account is blocked. For more information, see [Security Policy \(on page 785\)](#).
- **Account Lockout Duration.** Prevents unauthorized users from accessing the RMS application. The default lockout period is 10 minutes. Only the administrator can modify the lockout period value. A user account is unlocked based on the security policy.
- **Log on Error Message.** System generated error messages do not contain any information about login failure and return only as login failed (For example, Access Denied and Invalid Credentials).
- **Concurrent Session.** A single user can open multiple sessions using the same login credentials.
- **Concurrent Access.** Supports concurrent access for multiple IP addresses.

Managing User Passwords

The RMS password management system is interactive and ensures that the login passwords meet the following criteria.

- **Default Passwords.** RMS provides the option to change the default passwords using the initial setup and ensures that weak, blank, or null passwords are not allowed. The default password must be changed after the first login to enhance the security related to login credentials and ensure that the temporary password is not in use. You must change the default system password to a unique password and the password must meet the password complexity policy. For more information, see [Changing the Password on First Login \(on page 26\)](#).
- **Password Complexity.** Passwords must meet the complexity requirements specified in [Table 2: Fields on the Change Password Page \(on page 19\)](#).
- **Password Age.** Passwords cannot be static and must be changed as part of the routine password maintenance policy through password expiration periods (**Password Expiry Days** as configured in the [Creating Security Policy Configuration \(on page 785\)](#)).
- **Password Expiry Notification.**

- RMS sends a password expiry notification e-mail to the users depending upon the **Password Expiry Warning Days** configured in the [Creating Security Policy Configuration \(on page 785\)](#).
- When a password is about to expire, the password expiry notification pop-up message is displayed once the user logs in to the RMS application.
- **Password Expired Scenario.**
 - Once the password expiry warning days has elapsed, the **Password Expired** mail is triggered.
 - When the user tries to log in to the RMS application after the password has expired, the error message is displayed on the login page.
- **Password History.** Password history is enforced to ensure that the users select unique new passwords after a password expires. A user can randomly trigger the update password request anytime to update the password. Password reuse is restricted by maintaining password history of the last seven used passwords for all users.
- **Password Storage.** Passwords of all user accounts are protected using an encryption algorithm and stored in the database as defined in the security policy. A user password is encrypted using the SHA-256 algorithm before storing it in the password file.
- **Change Password.** You can change the password for the predefined users (admin, operator, and viewer).
- **Remote Login.** You can access RMS using the remote super user (root), such as SSH.
- **Local Login.** Disables unauthenticated local console login. Ensures that all local console interfaces require authentication. If the authentication fails, RMS disables the login.
- **Legal Notice Banner.** A legal notice warning banner is displayed when any unauthorized user tries to login to the RMS application.

```
## DO NOT LOGON WITHOUT AUTHORIZATION ## You are attempting to log into a system
owned and operated by RJIL.
If you are not authorized to access this system, please cancel your logon attempt
immediately.
All activities on this system may be monitored. All data residing on this system is a
property of RJIL.
Any unauthorized use, duplication, or disclosure of this device or its contents
and/or the attempt to gain
unauthorized access is strictly prohibited and unlawful and may lead to legal
prosecution.
```

Managing User Sessions

RMS supports session policies in accordance with the policy and guidelines defined in the security policy.

- **Idle Session Timeout.** If a session is unattended after the amount of time specified in the security policy, the session shows the blank screen and suspends the session.

Re-establishment of the session can occur only after the user provides a valid password. The default duration for idle session timeout is 15 minutes.

- **Concurrent Sessions.** A single user can open multiple sessions using the same login credentials. This field is configurable in RMS settings as **Multiple Session Allowed**. An administrator can make this flag as true or false. The number of maximum concurrent sessions can be configured in the security policy. The value ranges from 1 to 512 sessions per user and the default value is 25.

Changing the Password on First Login

To enhance the security related to login credentials, RMS prompts you to change the default password when you login to the RMS application for the first time.



Note: Every user is assigned with a default password for initial login. It is mandatory for the user to change the password after the first login and the password must be unique. For more information on the default password, see [Table 376: User Roles and Access Privileges \(on page 776\)](#).

Perform the following steps to change the default password when you login to RMS for the first time. You must change the password upon first time login and update the password as per the guidelines provided in [Table 5: Fields on the Change Password Page \(on page 26\)](#).

1. Log in to the application using the default login credentials.
2. Click **admin** from the top right corner of the page.
3. Select the Change Password from the menu.

The **Change Password** window appears.

Table 5. Fields on the Change Password Page

| Field | Description |
|--------------|---|
| New Password | <p>Enter your new password.</p> <p>The new password must fulfill the following requirements.</p> <ul style="list-style-type: none">◦ At least 10 characters◦ At least two lowercase letters (a-z)◦ At least two uppercase letters (A-Z)◦ Combination of lowercase (a-z) and uppercase (A-Z) letters◦ At least one special character (@, !, \$, and %)◦ At least one number (0-9)◦ Must not include the hash (#) symbol◦ Must not be any previously used passwords up to password history count and can be configured through security policy configuration (By default-7).◦ Preventing sequences of letters and/or numbers, such as 123 or abc. |

| Field | Description |
|---------|--|
| |  Note: The password strength indicator displays the efficiency of the password that you enter. You cannot proceed to the next step if the password strength indicator shows that the entered password is weak. |
| Confirm | Enter your new password again to confirm it. |

4. Click **Submit**.

The login password is changed, and you are logged out of the system. An e-mail is sent to your registered e-mail address (an e-mail address you used to create the user account) that the password for your RMS account has successfully been changed.

To log in to the application again, you must use your new password. Other sessions logged in with the same username are unaffected until the next login.

Related information

[Changing the Password on First Login \(on page 26\)](#)

Resetting the Password

If you have forgotten your password, you can reset the password from the RMS login page. Perform the following steps to reset the password.

1. Click the **Forgot Password** link on the RMS login page.
2. Enter your valid e-mail address.
3. Click **Submit**.

An email is sent to your registered e-mail address (an e-mail address you used to create the user account) that your RMS account password is reset successfully. The e-mail contains the following information.

- Your e-mail address
 - Default password (This is the password for one time login)
4. Login to the RMS application using the default password.

After a successful login, you must change your password. For more information, see [Changing the Password on First Login \(on page 26\)](#).

Common Operations

The section covers the common operations that can be performed on all the RMS GUI pages.

Customize Columns

A user can customize the number of columns to be displayed on the each resource (OLT, ONT, Site, Alarms Profile, Bandwidth Profile, and so on) landing page. To customize the columns, perform the following.

- Click the  icon on top right corner of the page.
- Check the **Select All** checkbox to dispalys all the columns in a page.
- Select the columns that you want to display on the page. Deselect the table columns that are not required to be displayed on the page.

Show Table Entries

A user can select the number of entries to be displayed on the table for each resource (Blacklisted ME, Controller, Management Domain, Type-B Protection, and so on) on the landing page. To select the table entries, perform the following.

- Select the value from the **Show entries** list. You can select 10, 25, 50, or 100 entries at a time. A maximum of 100 entries can be displayed on the page.

Search

A user can search for any resources (OLT, ONT, Ring, Subscriber, Database Statistics, and so on) using exact search using the  search bar from the landing page. The search results are displayed on the same page. An exact search is case-sensitive and returns records only if the search term or phrase matches exactly.

Editing Resources

A user can edit the parameters configured for resources (OLT, ONT, Site, Site Group, Alarm Profile, Device Profile, Bandwidth Profile, VNet Profile, and so on).

To modify the resource, perform the following steps.

1. Click on the  icon of the resource in the **Action** column that you want to modify.
- The Edit configuration page appears.
2. Modify the parameters as needed.
 3. Click **Save** to save the changes.

A confirmation message appears, indicating the status of the edit operation.

Viewing Resources

A user can view the parameters configured for resources (Policer profile, Storm Control Profile, and so on).

To view the resource, perform the following steps.

1. Click on the  icon of the resource in the **Action** column that you want to view.
2. The view configuration page appears.

Deleting Resources

Before deleting the resource, deactivate the resource and then delete it.

A user can delete the parameters configured for resources (OLT, ONT, Site, Site Group, Alarm Profile, Device Profile, Bandwidth Profile, VNet Profile, and so on).

To delete the resource, perform the following steps.

1. Click on the  icon of the resource in the **Action** column that you want to delete.
2. An alert message appears, asking you to confirm the delete operation.
3. Click **Confirm** to delete the configuration.

A confirmation message appears, indicating the status of the delete operation.

Cloning Resources

A user can clone the parameters configured for resources (OLT, ONT, Site, Site Group, Alarm Profile, Device Profile, Bandwidth Profile, VNet Profile, and so on).

To clone the resource, perform the following steps.

1. Click on the  icon of the resource in the **Action** column that you want to clone.
2. Provide the information for the parameters as needed.
3. Click **Create** to create the clone for the resource.

A confirmation message appears, indicating the status of the clone operation.

Using Column Filter

Filters enable you to quickly find and display the entries that are relevant to your specific needs.

A user can filter the parameters configured for resources (OLT, ONT, Site, Audit Log, Controller, and so on).

To filter the resource, perform the following steps.

1. Click on the  filter icon from the column header of the particular parameter.
2. Select one or multiple check-box to apply the filter.

The selected parameters of the resource are retrieved based on the filter that you have applied. If you want to clear the filter, click **Clear applied filter** from top-right corner of the page.

Global Search

The global search field on the RMS GUI allows you to quickly locate objects within RMS. When you search for an object using global search, RMS displays the search results. In the **Search** box located at the top right of the page, enter the search object. The search results are displayed from the pages that match the specified object.

The search is performed, and the results are displayed based on how the RMS objects are indexed.

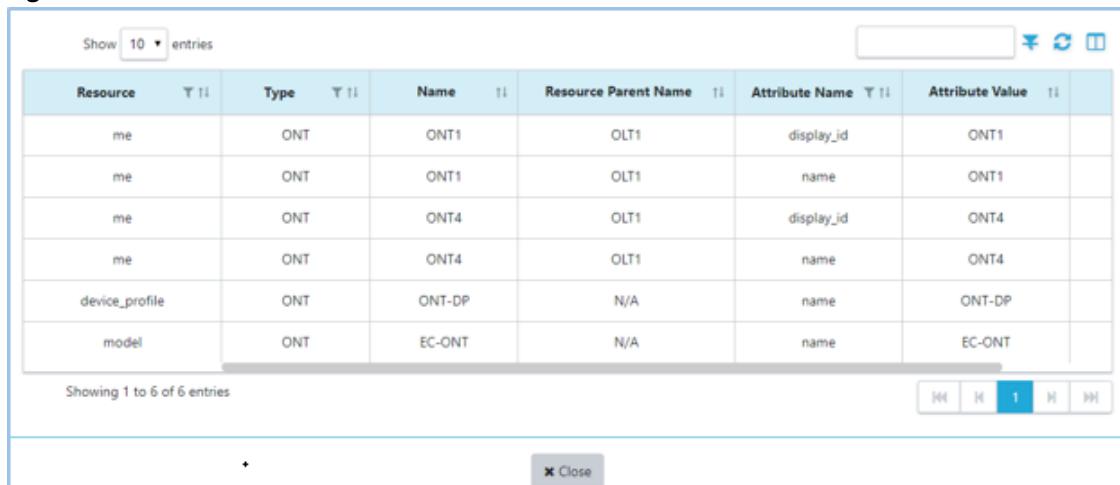
The search is supported for resource such as attribute value.

For example, if you specify the search object as ONT, all pages that include ONT are listed in the search results.

Each search result may provide link to help you navigate to the corresponding object on the **Configuration** and **Monitor** dashboard page.

If none of the objects in RMS match your search criteria, the following error message is displayed: No data available.

Figure 5. Global Search Results



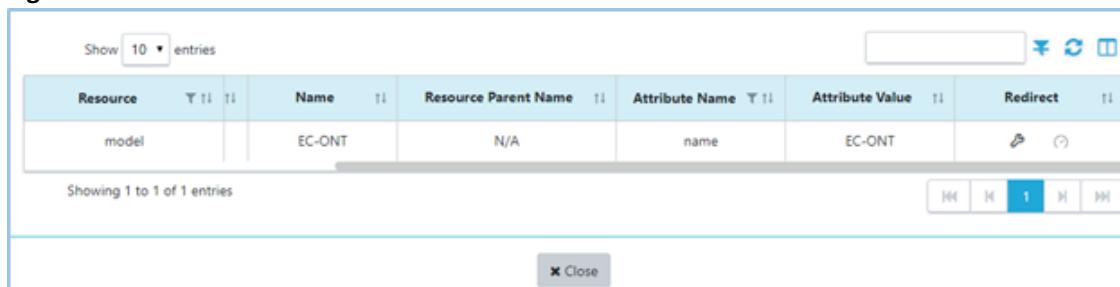
The screenshot shows a table with the following data:

| Resource | Type | Name | Resource Parent Name | Attribute Name | Attribute Value |
|----------------|------|--------|----------------------|----------------|-----------------|
| me | ONT | ONT1 | OLT1 | display_id | ONT1 |
| me | ONT | ONT1 | OLT1 | name | ONT1 |
| me | ONT | ONT4 | OLT1 | display_id | ONT4 |
| me | ONT | ONT4 | OLT1 | name | ONT4 |
| device_profile | ONT | ONT-DP | N/A | name | ONT-DP |
| model | ONT | EC-ONT | N/A | name | EC-ONT |

Showing 1 to 6 of 6 entries

You can search again for categories within the search results using partial or complete keywords. The search results are displayed on the same page. For example, from the ONT search results, you can search for ONT model as EC, the search results appear based on the search criteria as shown in the following figure.

Figure 6. Nested Search Results



The screenshot shows a table with the following data:

| Resource | Name | Resource Parent Name | Attribute Name | Attribute Value | Redirect |
|----------|--------|----------------------|----------------|-----------------|---|
| model | EC-ONT | N/A | name | EC-ONT |   |

Showing 1 to 1 of 1 entries

Field Descriptions

The following table describes the fields on the Search Results page.

Table 6. Search Results

| Field | Description |
|----------------------|---|
| Resource | Specifies the resource entity type. Example: ME |
| Type | Specifies the type of the resource. Example: CARD |
| Name | Specifies the name of the resource. Example: Card-OLT1 |
| Resource Parent Name | Specifies the parent name of the resource. Example: OLT-Slot |
| Attribute Name | Specifies the name of the attribute. Example: display_id |
| Attribute Values | Specifies the attribute value. Example: Card-OLT1 |
| Redirect | Click on the Configuration or Monitor icon to navigate to the corresponding dashboard page. |

Related information

[Global Search \(on page 30\)](#)

RMS Main Workspaces

In RMS, the different tasks that you can perform are categorized into workspaces.

When you log in to the RMS application, the Dashboard page appears by default and displays the following workspaces on the top right-hand side of the page.

- Dashboard
- Monitor
- Topology
- Configuration
- Administration
- Template Builder

When you click each workspace, the corresponding menu appears on the left-hand side of the RMS application and the tasks that you can perform in each workspace. Each workspace and its accessible functions are described later in this document.

You can expand any menu by clicking on its name. When you click on a menu, the next level of tasks for that menu are displayed, some items on the second level may contain further subtasks.

You can expand the task tree by clicking the right arrow (>) button and collapse the menu by clicking the left arrow (<) button from the bottom of the page. The design of the task tree enables you to navigate across the different RMS workspaces and tasks.

The following figure shows the RMS workspaces.

Figure 7. RMS Workspaces



The following table describes the workspaces of RMS.

Table 7. RMS Workspaces

| Workspace Name | Description |
|------------------|--|
| Dashboard | <ul style="list-style-type: none">Graphical widgets for management domain, controller, devices, and sites.View the statistics charts of the OLT, ONT, controller, management domain, Managed Element (ME) fault, ME model, ME make, and ME site.View Alarms histogram, sites location, and OLT location.View information about the sites plotted on the world map. <p>For more information, see Dashboard (on page 42).</p> |
| Monitor | <ul style="list-style-type: none">Monitor managed elements (OLT, ONT, CPE, Splitter, Card, Rack, SFP, Cable, and ONT card), blacklisted MEs, controller, management domains. For more information, see Inventory (on page 54).Monitor type-B protection and ERPS rings. For more information, see Protection (on page 149).Monitor subscriber services and subscribers. For more information, see Services (on page 124).Monitor database statistics, and sessions. For more information, see Infrastructure (on page 227).Monitor audit logs, backup logs, data synchronization requests, and microservice logs. For more information, see Logs (on page 118).Monitor reports. For more information, see Reports (on page 254).Monitor and download faults and events. For more information, see Faults (on page 115) and Events (on page 117).Monitor tasks. For more information, see Tasks (on page 251). |

Table 7. RMS Workspaces (continued)

| Workspace Name | Description |
|----------------------|---|
| Topology | View the physical and logical topology of the OLT. For more information, see Topology (on page 283) . |
| Configuration | <ul style="list-style-type: none"> • Create and manage subscribers, site, site group, site group type, ME group, controller, and inventory (OLT, ONT, SFP, CPE, Splitter, BNG, Card, Rack, and Cable), and configuring local profile. For more information, see Configuration (on page 289). • Create and manage various profiles such as alarm profile, log profile, PPPoE profile, device profile, authentication profile, ACL profile, ERPS profile, MEP profile, NTP profile, Circuit ID format, and TACACS profile. For more information, see Profiles (on page 133). • Create and manage PON profiles such as bandwidth profile, shaper profile, MVLAN profile, multicast group, Class of Service Queues (CoSQ) profile, packet queue, VNet profile, IGMP profile, policer profile, and storm control profile. For more information, see PON Profiles (on page 563). • Create and manage pots profile, IP host profile, SIP agent profile, SIP user data profile, network dial plan profile, VoIP service information profile, VoIP media information profile, RTP information profile, and VoIP application service profile. For more information, see Voice Service (on page 589) Profiles (on page 133). • Create and manage email notification, make, model, model version, ONT firmware information, alarm severity, file storage, alarm suppression, settings, filter expression, and forwarding policy. For more information, see Settings (on page 603). • Create and manage type-B protection pair. For more information, see Protection (on page 149). • Create and manage PM collection policy. For more information, see Policy (on page 642). • Create tasks for the following. <ul style="list-style-type: none"> ◦ OLT software upgrade ◦ Reports generation, ◦ EMS database backup ◦ OLT and controller backup ◦ Controller software upgrade ◦ ONT firmware upgrade ◦ ONT bulk firmware upgrade ◦ OLT firmware upgrade ◦ Inventory collection |

Table 7. RMS Workspaces (continued)

| Workspace Name | Description |
|-------------------------|--|
| | <ul style="list-style-type: none"> ◦ Service collection ◦ Fault collection ◦ Event collection ◦ Configuration update ◦ Bulk Port Modification ◦ OLT reboot ◦ Subscriber service management ◦ Banner update <p>For more information, see Maintenance (on page 644).</p> |
| Administration | <p>Create and manage management domain, user, user role, and security policy.</p> <p>For more information, see Administration (on page 765).</p> |
| Template Builder | <p>Create, manage, import, and export templates for the following resources.</p> <ul style="list-style-type: none"> • OLT • ONT • CARD • RACK • SHELF • SUBSCRIBER • SUBSCRIBER SERVICE • CONTROLLER • Zero Touch Provisioning (ZTP) <p>For more information, see Template Builder (on page 787).</p> |

Fault Icons

The fault icons on the top of the GUI provide the following type of faults raised in RMS.

- Acknowledged/Unacknowledged
- Critical
- Major
- Minor
- Warning
- Indeterminate

For information about alarm severity levels, see [Alarm Severity Levels \(on page 238\)](#).

The following figure shows the faults icons.

Figure 8. Fault Icons



The following table provides the description of fault icons.

Table 8. Fault Icons

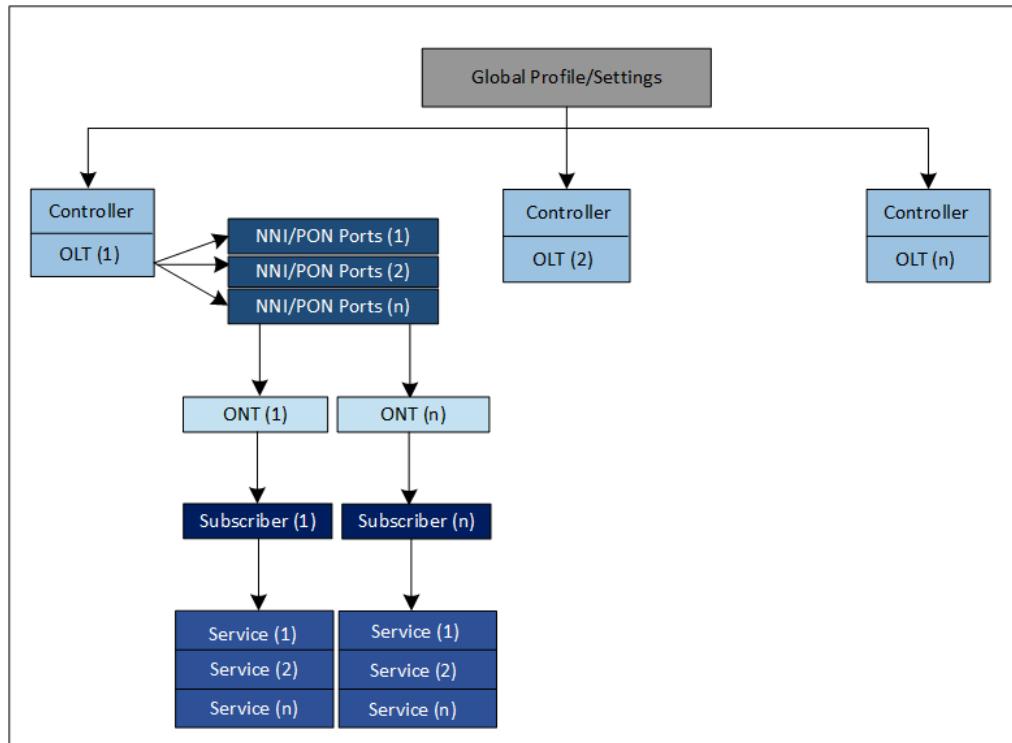
| Fault Icon | Type | Description |
|------------|---------------------------------|--|
| | Acknowledged and Unacknowledged | <p>Displays the current number of acknowledged and unacknowledged faults that exist in RMS.</p> <p>When an alarm is acknowledged, the acknowledged fault count is increased and the unacknowledged faults count is decreased.</p> <p>Click on the icon to view more information about the acknowledged and unacknowledged fault and the alarm histogram.</p> <p>For more information, see Alarm (on page 115) and Alarms Histogram (on page 51).</p> |
| | Critical | <p>Displays the number of critical faults raised in RMS.</p> <p>Click on the icon to view more information about the critical faults and the alarm histogram.</p> <p>For more information, see Alarm (on page 115) and Alarms Histogram (on page 51).</p> |
| | Major | <p>Displays the number of major faults raised in RMS.</p> <p>Click on the icon to view more information about major faults and the alarm histogram.</p> <p>For more information, see Alarm (on page 115) and Alarms Histogram (on page 51).</p> |
| | Minor | <p>Displays the number of minor faults raised in RMS.</p> <p>Click on the icon to view more information about minor faults and the alarm histogram.</p> <p>For more information, see Alarm (on page 115) and Alarms Histogram (on page 51).</p> |
| | Warning | <p>Displays the number of warning faults raised in RMS.</p> <p>Click on the icon to view more information about warning faults and the alarm histogram.</p> <p>For more information, see Alarm (on page 115) and Alarms Histogram (on page 51).</p> |
| | Indeterminate | Displays the number of indeterminate faults raised in RMS. |

Table 8. Fault Icons (continued)

| Fault Icon | Type | Description |
|------------|------|--|
| | | Click on the icon to view more information about indeterminate faults and the alarm histogram. For more information, see Alarm (on page 115) and Alarms Histogram (on page 51) . |

Workflow for Activating a Service for the Subscriber

The following diagram illustrates the workflow for activating a service for the subscriber.

Figure 9. Service Activation Workflow

Configuration Types

The following tables describes the type of configuration.

Table 9. Configuration Types

| Configuration Type | Description |
|--------------------------------|--|
| System Level Configuration | Specifies the global configuration applicable for multiple OLTs and performed before the service deployment. |
| Subscriber Level Configuration | Specifies the configuration that are required for each subscriber. |

Table 9. Configuration Types (continued)

| Configuration Type | Description |
|-----------------------------|--|
| Service Level Configuration | Specifies the configuration that are required for each service for a subscriber. |

Create Management Domain Workflow

The following table explains the workflow for creating management domain.

Table 10. Create Management Domain Workflow

| Steps | Tasks | For More Information, See | Configuration Level |
|--|---|---|---------------------|
| Create Management Domain: One time configuration for multiple OLTs. | | | |
| 1 | (Optional) Create management domain  Note: By default, RMS provides a default management domain as "DEFAULT_MANAGEMENT_DOMAIN". However, the user is allowed to create another management domain if required. | Creating Management Domain (on page 765) | System |
| 2 | Create controller | Creating Controller Configuration (on page 297) | System |
| 3 | Activate controller | Activating the Controller (on page 305) | System |
| 4 | Create "Make" of OLT, ONT, CARD, and Rack  Note: If the default OLT device profile does not exist in the RMS, then you must create a make for the OLT. | Creating Make Configuration (on page 606) | System |
| 5 | Create model of OLT, ONT, CARD, and Rack | Creating Model Configuration (on page 610) | System |

Table 10. Create Management Domain Workflow (continued)

| Steps | Tasks | For More Information, See | Configuration Level |
|-------|--|---|---------------------|
| |  Note: If the default OLT device profile does not exist in the RMS, then you must create a model for the OLT. | | |
| 6 | Create device profile of OLT, CARD, RACK, and ONT  Note: For ONT, creating make, model, and ONT device profile configuration is optional. | Creating OLT Device Profile (on page 509) | System |

OLT Profiles Workflow

The following table explains the workflow for creating OLT profiles.

Table 11. OLT Profiles Workflow

| Steps | Tasks | For More Information, See | Configuration Level |
|---|---|--|---------------------|
| Create OLT Profiles: One time configuration for multiple OLTs. | | | |
| 1 | Create alarm profile for OLT and ONT (Optional) | Alarm Profile (on page 473) | System |
| 2 | Create log profile (Optional) | Creating Log Profile (on page 503) | System |
| 3 | Create circuit ID | Creating Circuit ID Format (on page 554) | System |

OLT Activation Workflow

The following table explains the workflow for OLT creation and activation.

Table 12. OLT Activation Workflow

| Steps | Tasks | For More Information, See | Configuration Level |
|---|-------|---------------------------|---------------------|
| Create and Activate OLT: Repeat this configuration for each OLT. | | | |

Table 12. OLT Activation Workflow (continued)

| Steps | Tasks | For More Information, See | Configuration Level |
|-------|--|---|---------------------|
| 1 | (Optional) Create Inventory for Rack, Shelf, and Slot.  Note: This is an optional and can be skipped if not required. | Creating Rack Configuration (on page 446) | System |
| 2 | Create OLT and assign shelf to the OLT Add the following global profile to the OLT. <ul style="list-style-type: none">• Log profile• OLT alarm profile | Creating OLT Configuration (on page 318) | System |
| 3 | Create card and assign the slot and device profile to the card | CARD (on page 444) | System |
| 4 | Associate the card with the slot or OLT and port | CARD (on page 444) | System |
| 5 | Activate the OLT | Activating and Deactivating the OLT (on page 324) | System |
| 6 | Activate the port | Activating the PON and NNI Port (on page 380) | System |

PON Profiles Workflow

The following table explains the workflow for creating PON profiles.

Table 13. PON Profiles Workflow

| Steps | Tasks | For More Information, See | Configuration Level |
|--|--------------------------|--|---------------------|
| Create PON Profiles: Can be customized for each subscriber. | | | |
| 1 | Create bandwidth profile | Creating Bandwidth Profile (on page 564) | System |
| 2 | Create shaper profile | Creating Shaper Profile (on page 567) | System |
| 3 | Create multicast group. | Creating Multicast Group (on page 568) | System |

Table 13. PON Profiles Workflow (continued)

| Steps | Tasks | For More Information, See | Configuration Level |
|-------|--|--|---------------------|
| |  Note: This is applicable only for the multicast service. | | |
| 4 | Create multicast VLAN (MVLAN) profile  Note: This is applicable only for the multicast service. | Creating MVLAN Profile (on page 568) | System |
| 5 | Create Class of Service Queue (CoSQ) profile | Creating COSQ Profile (on page 570) | System |
| 6 | Create Virtual Network (VNet) profile | Creating VNet Profile (on page 577) | System |

ONT Activation Workflow

The following table explains the workflow for ONT creation and activation.

Table 14. ONT Activation Workflow

| Steps | Tasks | For More Information, See | Configuration Level |
|---|--|--|---------------------|
| Create and Activate ONT: Repeat this configuration for each ONT. | | | |
| 1 | Create ONT alarm profile Create ONT | Creating ONT Configuration (on page 427) | Subscriber |
| 2 | Activate ONT | Activating the ONT (on page 431) | Subscriber |

Service Activation Workflow

The following table explains the workflow for creating subscriber, service, and activating service for the subscriber.

Table 15. Service Activation Workflow

| Steps | Tasks | For More Information, See | Configuration Level |
|---|-------|---------------------------|---------------------|
| Create Subscriber: Repeat this configuration for each subscriber | | | |

Table 15. Service Activation Workflow (continued)

| Steps | Tasks | For More Information, See | Configuration Level |
|--|---|---|---------------------|
| 1 | Create subscriber | Creating Subscriber (on page 455) | Subscriber |
| Create Service: Repeat this configuration for each subscriber | | | |
| 2 | Create and associate the following global profiles to the service. <ul style="list-style-type: none"> • MVLAN Profile • Vnet Profile (global) or Vnet Config (service) • Bandwidth Profile • Shaper Profile • CoSQ Profile | Creating MVLAN Profile (on page 568) Creating VNet Profile (on page 577) Creating Bandwidth Profile (on page 564) Creating Shaper Profile (on page 567) Creating COSQ Profile (on page 570) | Subscriber |
| 3 | Create service | Creating Service (on page 459) | Service |
| 4 | Activate the service | Activating and Deactivating the Service for the Subscriber (on page 467) | Service |

Related information

[Example: Configuring and Activating HSIA Services for the Subscriber \(on page 805\)](#)

[Example: Configuring Voice Service for Subscriber \(on page 830\)](#)

[Example: Voice Service Priority for SIP and RTP Packets \(on page 837\)](#)

[Example: Configuring IPTV for Subscriber \(on page 847\)](#)

[Example: Configuring Whole Home Digital Video Recording \(on page 857\)](#)

Dashboard

RMS provides a dashboard, which is the default landing page after successful login. Whenever you log in to the RMS application, the first thing you see is a user-configurable dashboard that offers you a customized view of the RMS resources through widgets and statistics charts.

Tasks

You can perform the following tasks from this page.

- Use the widgets to view the number of management domains, controllers, devices, and sites that are created.
- View the statistics of the OLT, ONT, management domain, controller, ME make, ME model, managed element faults, and managed element sites.
- View the alarm histogram based on periodicity. You can also hide alarms from the particular severity.
- View the geographic location of various sites.
- Customize the dashboard configuration.
 - To add a chart to the Dashboard, click the **Customize** option and select the chart to be displayed on the Dashboard page.
 - To remove a chart from the Dashboard, click the **Customize** option and uncheck the box.
- To refresh a charts data, click the **Refresh** button in its title bar.

Custom Dashboard

You can create a custom dashboard to view a group of statistics charts that meet a particular requirement. The user-configurable dashboard offers you a customized view of resources through statistics charts.

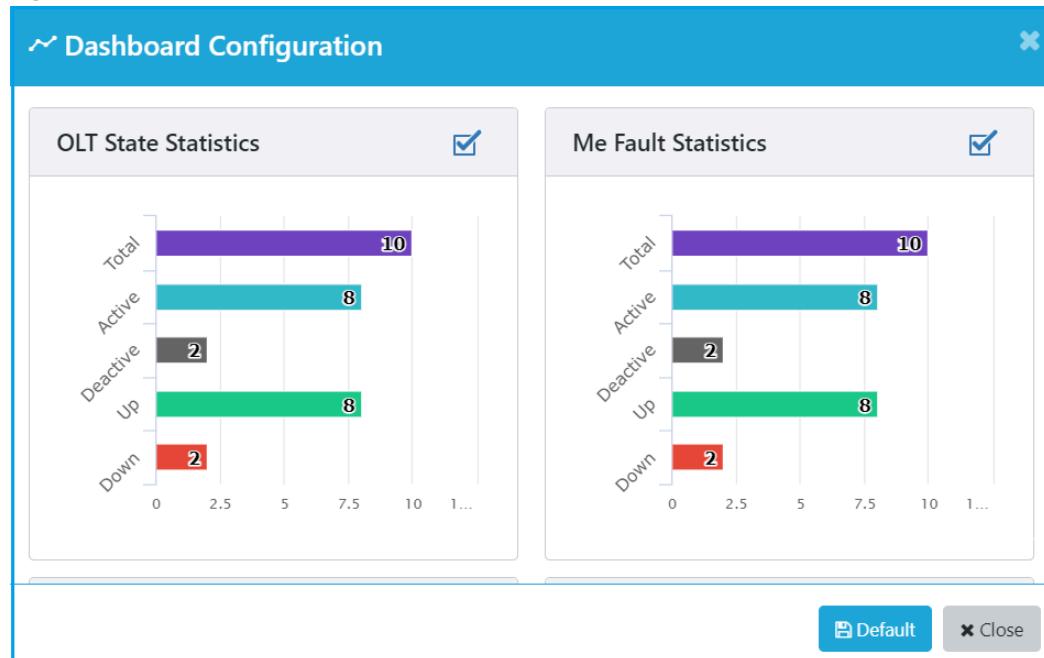
After successful creation of the custom dashboard, the new dashboard is displayed in the Dashboard tab and listed in the **Dashboard** page.

Perform the following steps to create a custom dashboard page.

1. Click the **Customize** option.
2. Select the statistics charts that you want to display on the custom dashboard page.
3. Click **Close**.

The dashboard automatically adjusts the placement of the charts to dynamically fit on your browser window without changing the order.

Figure 10. Custom Dashboard

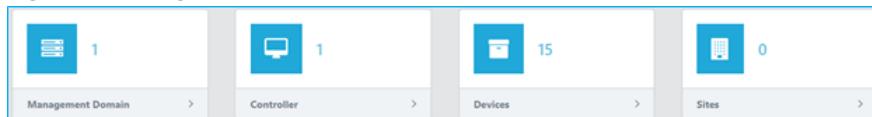


Widget Descriptions

The following figure shows the widgets on the Dashboard page.

- Management Domain
- Controller
- Devices
- Sites

Figure 11. Widgets



The following table describes the widgets on the dashboard page.

Table 16. Widgets on the Dashboard

| Widget | Description |
|-------------------|---|
| Management Domain | Specifies the total number of management domains that are created. Click on the Management Domain link or right arrow to view the list of management domains and its associated information. |

Table 16. Widgets on the Dashboard (continued)

| Widget | Description |
|------------|--|
| Controller | Specifies the total number of controllers that are created. Click on the Controller link or right arrow to view the list of controllers and its associated information. |
| Devices | Specifies the total number of devices that are configured in the system. Devices include OLT, ONT, SFP, Card, Rack, CPE, splitter, cable, BNG, and ONT card. Click on the Devices link or right arrow to view the list of devices and its associated information. |
| Sites | Specifies the total number of sites that are created. Click on the Sites link or right arrow to view the list of sites and its associated information. |

Statistics Charts

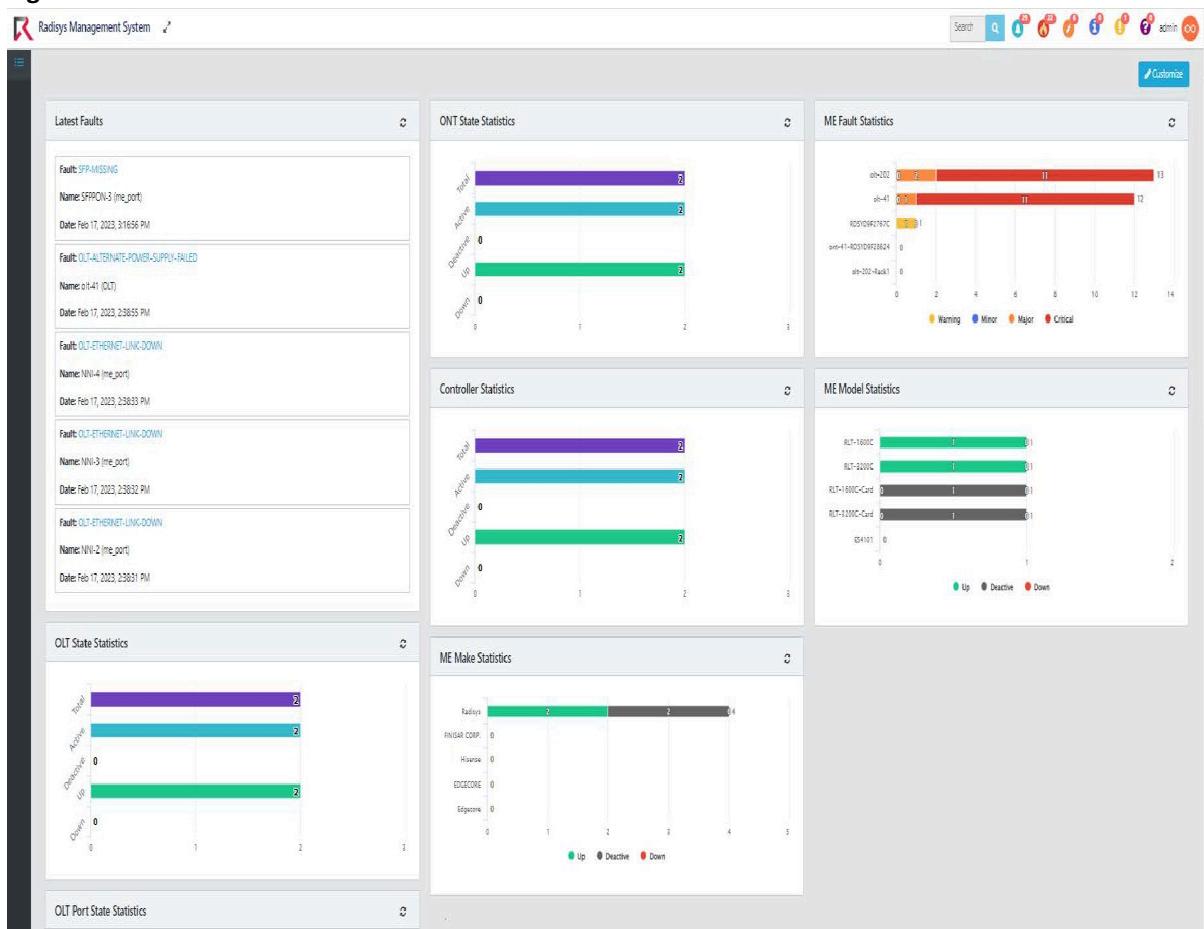
The Dashboard provides a variety of status and statistics information related to the OLT, ONT, controller, site, OLT port, and management domain, ME site, latest faults, ME model, ME make, and ME site.

The dashboard is user-configurable and allows customization to view the statistics information of the following RMS resources.

- OLT State Statistics
- ME Fault Statistics
- ONT State Statistics
- Controller Statistics
- ME Model Statistics
- ME Site Statistics
- ME Make Statistics
- Latest Faults
- OLT Port State Statistics
- Alarm Histogram
- ME OLT Location Statistics

The following figure shows the above statistics charts on the Dashboard page. The information displayed in each chart is read-only.

Figure 12. Statistics Charts

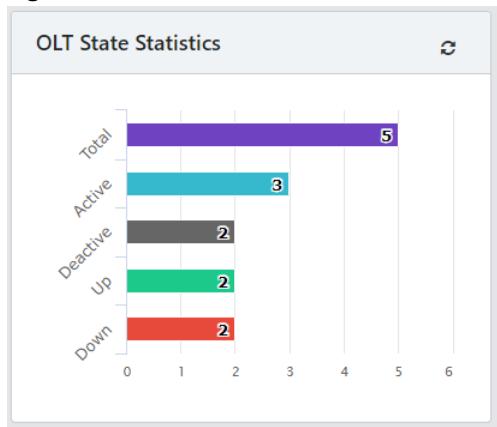


OLT State Statistics

Specifies the statistics of the OLT state. The possible statuses are.

- Down**. Shows the number of OLTs that are down.
- Up**. Shows the number of OLTs that are up.
- Deactivate**. Shows the number of OLTs that are deactivated.
- Active**. Shows the number of OLTs that are activated.
- Total**. Shows the total number of OLTs.

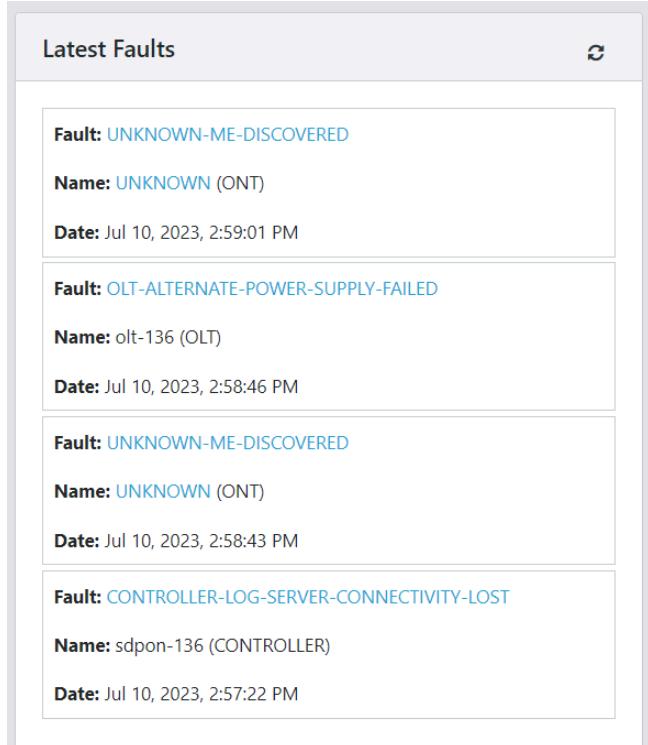
Click on the colored bars to view the corresponding OLT details. For more information, see [OLT Inventory \(on page 54\)](#).

Figure 13. OLT State Statistics

Latest Faults

Specifies the top five latest open faults reported by the system. The chart describes the following information.

- **Fault.** Specifies the name of the fault, for example, HIGH-FAN-SPEED. Click on the fault name to view more details of the fault. For more information, see [Viewing Fault Details \(on page 247\)](#).
- **Name.** Specifies the name of the resource for which the alarm was raised, for example, OLT.
- **Date.** Specifies the date and time when the alarm was reported.

Figure 14. Latest Faults

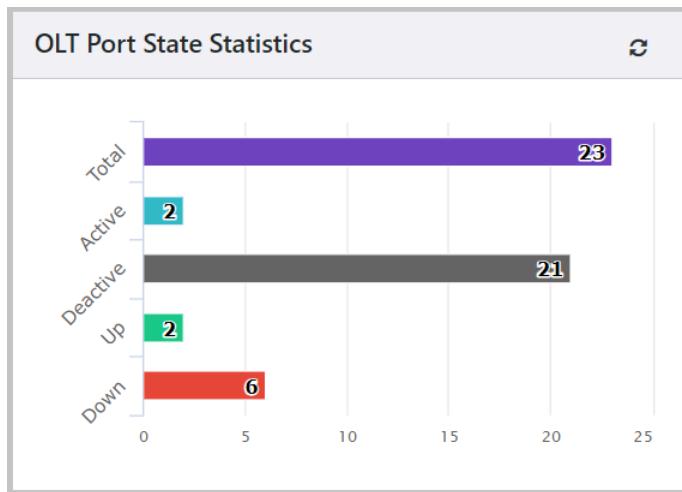
OLT Port State Statistics

Specifies the statistics of the OLT port. The possible statuses are.

- **Down**. Shows the number of ports that are down.
- **Up**. Shows the number of ports that are up.
- **Deactive**. Shows the number of ports that are deactivated.
- **Active**. Shows the number of ports that are activated.
- **Total**. Shows the total number of ports.

Click on the colored bars to view the corresponding port details. For more information, see [Viewing PON and NNI Ports \(on page 372\)](#).

Figure 15. OLT Port State Statistics



ONT State Statistics

Specifies the statistics of the ONT. The possible statuses are.

- **Down**. Shows the number of ONTs that are down.
- **Up**. Shows the number of ONTs that are up.
- **Deactive**. Shows the number of ONTs that are deactivated.
- **Active**. Shows the number of ONTs that are activated.
- **Total**. Shows the total number of ONTs.

Click on the colored bars to view the corresponding ONT details. For more information, see [ONT Inventory \(on page 58\)](#).

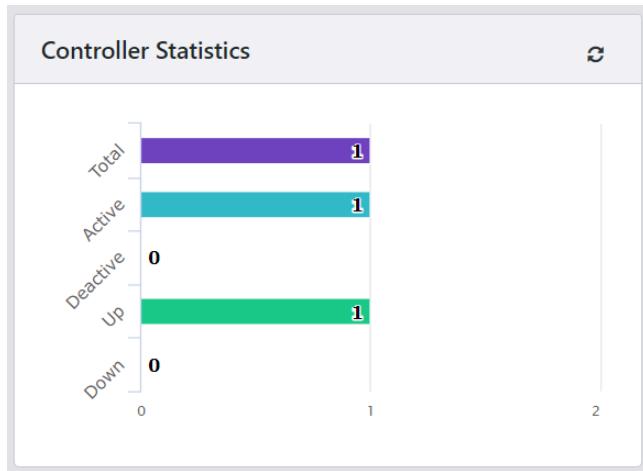
Figure 16. ONT State Statistics

Controller Statistics

Specifies the statistics of the controller. The possible statuses are.

- **Down**. Shows the number of controllers that are down.
- **Up**. Shows the number of controllers that are up.
- **Deactive**. Shows the number of controllers that are deactivated.
- **Active**. Shows the number of controllers that are activated.
- **Total**. Shows the total number of controllers.

Click on the colored bars to view the corresponding controller details. For more information, see [Controller \(on page 182\)](#).

Figure 17. Controller Statistics

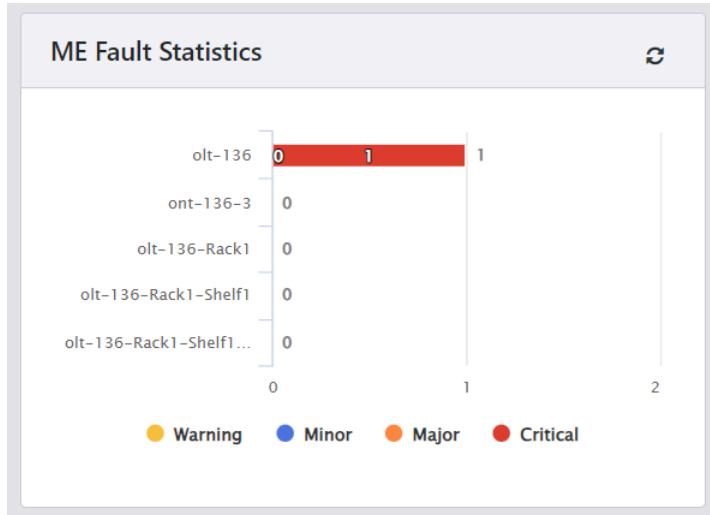
ME Fault Statistics

Specifies the top five managed elements that have open faults. The faults are categorized based on the following severity levels. The possible statuses are.

- **Warning.** Shows the number of warning alarms reported for managed elements such as OLT, ONT, rack, shelf, and SFP.
- **Critical.** Shows the number of critical alarms reported for managed elements such as OLT, ONT, rack, shelf, and SFP.
- **Major.** Shows the number of major alarms reported for managed elements such as OLT, ONT, rack, shelf, and SFP.
- **Minor.** Shows the number of minor alarms reported for managed elements such as OLT, ONT, rack, shelf, and SFP.

Click on the colored bars to view the faults. For more information, see [Alarm \(on page 115\)](#).

Figure 18. ME Fault Statistics



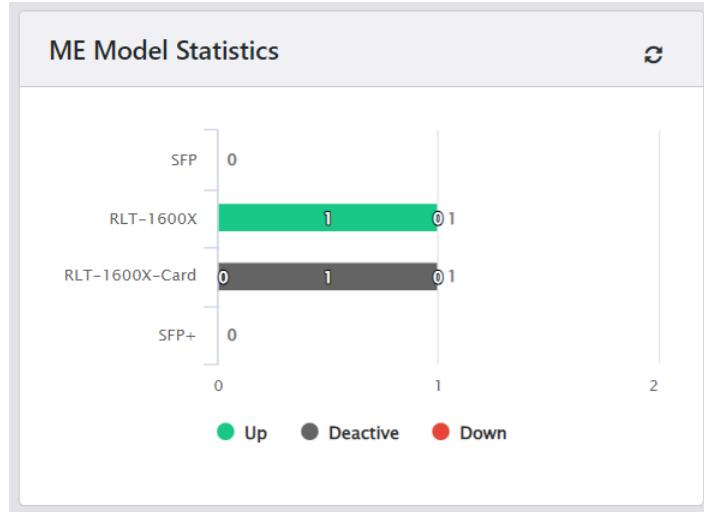
ME Model Statistics

Specifies the statistics of top five models that have the maximum number of associated managed elements. The possible statuses are.

- **Down.** Shows the names of the managed element models that are down.
- **Up.** Shows the names of the managed element models that are up.
- **Deactive.** Shows the names of the managed elements that are deactivated.

For more information, see [Monitoring Inventory \(on page 54\)](#).

Figure 19. ME Model Statistics



ME Site Statistics

Specifies the statistics of the top five sites that have a maximum number of associated managed elements. The possible statuses are.

- **Down.** Shows the total number of sites that are down.
- **Up.** Shows the total number of sites that are up.
- **Deactivate.** Shows the total number of sites that are deactivated.

Figure 20. ME Site Statistics



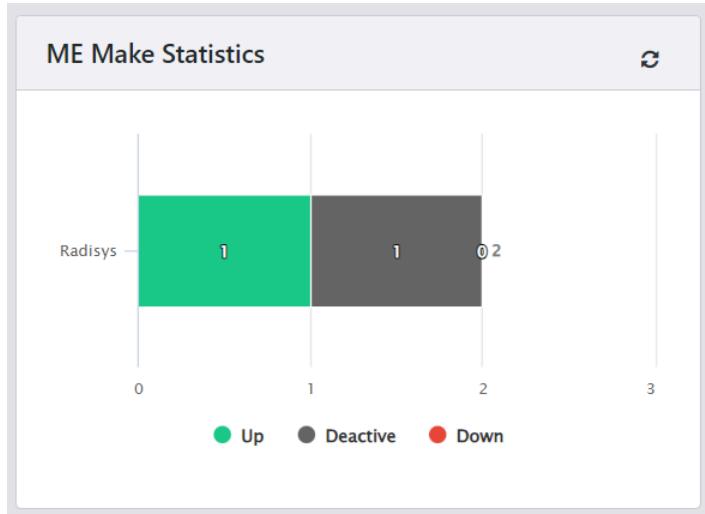
ME Make Statistics

Specifies the statistics of the top five makes with the maximum number of associated managed elements. The possible statuses are.

- **Down.** Shows the number of managed elements of a particular make that are down.
- **Up.** Shows the number of managed elements of a particular make that are up.
- **Deactivate.** Shows the number of managed elements of a particular make that are deactivated.

For information, see [Monitoring Inventory \(on page 54\)](#).

Figure 21. ME Make Statistics



Alarms Histogram

The alarm summary report is a standardized report generated in RMS. The report shows a graphical summary of the alarms that have occurred within a specified period of time. The alarm summary report contains a series of colored bars that provide insight into the trends of alarms in the network.

The alarm histogram displays the alarms with the following severity levels.

- **Critical**
- **Major**
- **Minor**
- **Warning**

You can mouse over the colored bar to view the number of alarms generated for each severity level.

You can generate alarm histogram at an hourly or daily interval. You can also generate alarm histogram for every 1 hour, 3 hours, 6 hours, 12 hours, 24 hours, and 7 days.

Alarms in the "Alarms histogram" are color-coded by severity.

- **Red.** Critical Alarms
- **Orange.** Major Alarms
- **Blue.** Minor Alarms
- **Yellow.** Warning Alarms

Generating Custom Alarm Histogram

RMS allows you to generate a custom alarm histogram.

Perform the following steps to generate a custom alarm histogram.

1. Click **Custom**.

The Date Range window is displayed.

2. Specify the duration (today, yesterday, last 7 days, last 30 days, this month, last month, and custom range) for which the report is generated. When you select the custom option, you must specify the From and To date (in MM/DD/YYYY and HH:MM:SS format respectively).

3. Click **Apply**.

The Alarm Histogram is generated on the Dashboard page. If you want to clear the settings, click **Clear**.

To refresh the alarms, click **Refresh** from the top-right corner of the page.

The following figure shows the alarm histogram.

Figure 22. Alarm Histogram



The above diagram shows the graphical representation of critical, major, minor, and warning alarms that are raised in RMS. The X-axis indicates the date and time when the alarm was reported by RMS, and the Y-axis indicates the number of alarms reported for the particular severity level.

Hover over the status bar to view the number of faults raised for each severity level. You can also hide alarms with a particular severity.

To hide an alarm for a particular severity, click on the particular severity.

The Alarm Histogram appears without the alarms from the selected severity in the status bar.

For example, when you click on **Critical**, the critical alarm status bar is removed from the graph and the Alarm Histogram appears without the “critical alarms” status bar, as shown in the below figure.

The following diagram shows that the critical alarms status bar (red color) is hidden.

Figure 23. Alarm Histogram Chart



Sites Location

RMS allows you to view the information about the sites plotted on the world map. For each site, you can see the list of devices associated with the site. You can also view the geographic location (longitude and latitude) of the devices.

- **View sites and devices.** You can view the sites and their location. Click on each site to view the number of devices associated with each site.
- **Zoom in and out of the page.** Click the zoom in (+) and zoom out (–) icons to zoom in and out of the page.



Note: For the sites to appear on the map, you must configure the latitude and longitude on the site.

OLT Location

RMS allows you to view the information about the OLTs plotted on sites on the world map. For each site, you can see the list of OLTs associated with the site. You can also view the geographic location (longitude and latitude) of the OLT devices.

- **View OLTs and Sites.** You can view the OLTs and their site locations. Click on each site to view the number of devices associated with each site.
- **Zoom in and out of the page.** Click the zoom in (+) and zoom out (–) icons to zoom in and out of the page.

Monitoring Inventory

To access this page, click **Monitor** from the top right corner of the page and select **Inventory** from the left-hand side of the menu.

Tasks

You can perform the following tasks from this page.

- View the physical topology of the OLT and ONT. See [Physical Topology of the OLT \(on page 285\)](#).
- View the logical topology of the OLT and ONT. See [Logical Topology of the OLT \(on page 286\)](#).
- View the configuration details of the OLT, ONT, CPE, splitter, card, rack, SFP, cable, and ONT card. See [Configuration \(on page 289\)](#).
- Export managed elements (OLT, ONT, CPE, splitter, CARD, rack, SFP, cable, and ONT CARD) as a CSV file from RMS to your local computer. See [Exporting Managed Elements \(on page 66\)](#).
- A pattern search using partial or complete keywords is supported for the following fields on the OLT inventory page.
 - Name (NEID)
- View the device configuration by clicking on the three dots icon () > **Configuration** option, which corresponds to the device, such as OLT, ONT, CPE, Splitter, Card, Rack, SFP, Cable, and ONT Card.

Field Descriptions

You can view the field description of the following inventory on this page.

- [OLT Inventory \(on page 54\)](#)
- [ONT Inventory \(on page 58\)](#)
- [CPE Inventory \(on page 61\)](#)
- [Splitter Inventory \(on page 63\)](#)
- [Card Inventory \(on page 63\)](#)
- [Rack Inventory \(on page 64\)](#)
- [SFP Inventory \(on page 65\)](#)
- [Cable Inventory \(on page 66\)](#)
- [ONT Card Inventory \(on page 66\)](#)

OLT Inventory

The following table describes the fields on the OLT page.

Table 17. OLT Inventory

| Field | Description |
|-------------------|--|
| Name | <p>Specifies the name of the OLT.</p> <p>Click on the OLT name to monitor the OLT. For more information, see Monitoring OLT (on page 67).</p> |
| Fault State | <p>Specifies the highest severity fault present on the OLT. The supported states are.</p> <ul style="list-style-type: none"> • WARNING • CRITICAL • MAJOR • MINOR • NO FAULT <p>For more information about the severity supported by RMS, see Alarm Severity Levels (on page 238).</p> |
| Admin State | <p>Specifies the admin state of the OLT.</p> <ul style="list-style-type: none"> • Green. Indicates that the OLT is ACTIVE. • Red. Indicates that the OLT is INACTIVE. |
| Operational State | <p>Specifies the operational state of the OLT.</p> <ul style="list-style-type: none"> • Green. Indicates that the OLT is UP. • Red. Indicates that the OLT is DOWN. |
| ZTP Status | <p>Specifies the ZTP status of the OLT.</p> <p>Example: INITIATED</p> |
| Make | <p>Specifies the vendor name who manufactures the OLT.</p> <p>Example: Radisys</p> |
| Model | <p>Specifies the model name of the OLT.</p> <p>Example: RLT-3200C</p> |
| Display ID | Specifies the display ID of the OLT. |
| Total ONT | Specifies the number of ONTs that are associated with the OLT. |
| Up ONT | Specifies the total number of ONTs associated with the OLT that are UP. |
| Total Subscriber | Specifies the total number of subscribers provisioned on the OLT. |
| Total Services | Specifies the total number of services that are configured in the OLT. |
| Total Alarms | Specifies the total number of alarms (Critical, Minor, Major, and Warning) raised for the OLT. |

Table 17. OLT Inventory (continued)

| Field | Description |
|--------------------|---|
| Critical Alarms | Specifies the total number of critical alarms raised for the OLT. |
| Major Alarms | Specifies the total number of major alarms raised for the OLT. |
| Warning Alarms | Specifies the total number of warning alarms raised for the OLT. |
| Minor Alarms | Specifies the total number of minor alarms raised for the OLT. |
| Ports | Specifies the number of ports present on the OLT. |
| Active Ports | Specifies the number of ports, associated with the OLT, that are active. |
| Deactive Ports | Specifies the number of ports, associated with the OLT, that are deactive. |
| Up Ports | Specifies the number of ports, associated with the OLT, that are UP. |
| Down Ports | Specifies the number of ports, associated with the OLT, that are DOWN. |
| CPU Utilization | Specifies the CPU utilization of the OLT. |
| Disk Utilization | Specifies the disk utilization of the OLT. |
| Memory Utilization | Specifies the memory utilization of the OLT. |
| Temperature | Specifies the OLT temperature, in degree Celsius. The OLT temperature value must be 90° Celsius. |
| MAC Address | Specifies the MAC address of the OLT. |
| Serial No | Specifies the serial number of the OLT. |
| Management IP | Specifies the management IP address of the OLT. |
| Site | Specifies the site to which the OLT is installed. |
| Device Profile | Specifies the name of the OLT device profile. |
| Management Domain | Specifies the name of the management domain. |
| Controller | Specifies the name of the controller. |
| Rack | Specifies the rack to which the OLT is installed. |
| Slot No. | Specifies the slot number on which the OLT is installed. |
| Alarm Profile | Specifies the alarm profile configured for the OLT. |
| Log Profile | Specifies the log profile of the OLT. |

Table 17. OLT Inventory (continued)

| Field | Description |
|-------------------------------|--|
| Authentication Type | Specifies the authentication type of the OLT. The supported values are as follows: <ul style="list-style-type: none"> • LOCAL • RADIUS |
| Resource State | Specifies the resource state of the OLT. The supported values are as follows: <ul style="list-style-type: none"> • PLANNED • INSTALLED • RETIRED |
| Hardware Version | Specifies the hardware version of the OLT. Example: C3708-32-256 |
| Supervision State | Specifies the supervision state of the OLT. The supported values are as follows: <ul style="list-style-type: none"> • NONE • SUPERVISED |
| Software Version | Specifies the software version of the OLT. Example: ROLT.1.21.125 |
| Backup Status | Specifies the backup status of the OLT. The supported values are. <ul style="list-style-type: none"> • BACKUP-INITIATED • BACKUP-FAILED • BACKUP-SUCCESSFUL |
| Restore Status | Specifies the restore status of the OLT. The supported values are. <ul style="list-style-type: none"> • RESTORE-INITIATED • RESTORE-FAILED • RESTORE-SUCCESSFUL |
| Software Release ETSI version | Specifies the ETSI software version of the OLT. |
| Up Since Time | Specifies the date and time from when the OLT is UP.  Note: If the OLT is added to the network for the first time, it shows the time since it was activated. If the OLT is rebooted, it reflects the time since the reboot. |
| ME Group | Specifies the managed element group to which the OLT belongs to. |

Table 17. OLT Inventory (continued)

| Field | Description |
|-------------------------------|---|
| ONT Firmware Upgrade Status | <p>Specifies the ONT firmware upgrade status on the OLT. The supported values are.</p> <ul style="list-style-type: none"> NOT-DOWNLOADED DOWNLOAD-INITIATED DOWNLOAD-FAILED DOWNLOAD-SUCCESSFUL ACTIVATE-INITIATED ACTIVATION-FAILED ACTIVATE-SUCCESSFUL COMMIT-INITIATED COMMIT-FAILED COMMIT-SUCCESSFUL CANCEL-UPGRADE-INITIATED CANCEL-UPGRADE-SUCCESSFUL CANCEL-UPGRADE-FAILED UPGRADED UPGRADE-FAILED |
| ONT Firmware Version | Specifies the current version of the ONT firmware. |
| ONT Firmware Download Version | Specifies the firmware version of the ONT that was downloaded. |
| Creation Time | Specifies the date and time when the OLT was created. |
| HOTO Status | Specifies the Handover Takeover status of the OLT. |

ONT Inventory

The following table describes the fields on the ONT page.

Table 18. ONT Inventory

| Field | Description |
|-------------|--|
| Name | Specifies the name of the ONT. |
| Fault State | Specifies the highest severity fault present on the ONT. The supported states are. |

Table 18. ONT Inventory (continued)

| Field | Description |
|-------------------|---|
| | <ul style="list-style-type: none"> • WARNING • CRITICAL • MAJOR • MINOR • NO FAULT <p>For more information about the severity supported by RMS, see Alarm Severity Levels (on page 238).</p> |
| Admin State | <p>Specifies the admin state of the ONT. The supported values are as follows.</p> <ul style="list-style-type: none"> • Green. Indicates that the ONT is ACTIVE. • Red. Indicates that the ONT is DEACTIVE. |
| Operational State | <p>Specifies the operational state of the ONT. The supported values are as follows.</p> <ul style="list-style-type: none"> • Green. Indicates that the ONT is UP. • Red. Indicates that the ONT is DOWN. |
| Make | Specifies the vendor name of the ONT. |
| Model | Specifies the model name of the ONT. |
| Display ID | <p>Specifies the display ID of the ONT.</p> <p>Example: rack=1/shelf=1/slot=ETH1/port=1/remote_unit=onu1</p> |
| Subscriber | Specifies the subscriber name configured for the ONT. |
| Serial No | Specifies the serial number of the ONT. |
| Device Profile | Specifies the name of the ONT device profile. |
| Management Domain | Specifies the name of the management domain. |
| Controller | Specifies the name of the controller. |
| Alarm Profile | Specifies the alarm profile configured for the ONT. |
| OLT | Specifies the OLT name to which the ONT is connected. |
| Connectivity Mode | <p>Specifies the connectivity model that must be used for the services on the ONU.</p> <p>The supported values are.</p> <ul style="list-style-type: none"> • N:1 bridging • 1:M mapping • 1:P filtering |

Table 18. ONT Inventory (continued)

| Field | Description |
|-----------------------------|--|
| | <ul style="list-style-type: none"> • N:M bridge-mapping • 1:MP map-filtering • N:P bridge-filtering • N:MP bridge-map-filtering <p>The default value must be same as the <i>current_connectivity_mode</i> reported by the ONU.</p> <p>The default value for the residential service is 1:MP map-filtering.</p> |
| Port | Specifies the PON port of the OLT to which ONT is connected. |
| ONT Number | Specifies the ONT number. |
| UNI Port Count | Specifies the number of UNI ports connected to the ONT. |
| ONU Physical Distance | Specifies the physical distance of an ONU (in Km) from the PON port of the OLT. |
| UNI Ports | Specifies the list of UNI ports connected to the ONT. |
| Up Since Time | Specifies the date and time from when the ONT is UP. |
| Registration Id | Specifies the registration ID of the ONT. |
| Equipment Id | Specifies the equipment ID of the ONT. |
| ONT Firmware Upgrade Status | <p>Specifies the ONT firmware upgrade status on the OLT. The supported values are.</p> <ul style="list-style-type: none"> • DOWNLOADED • NOT-DOWNLOADED |
| ONT Firmware Version | Specifies the current version of the ONT firmware. |
| Hardware Version | <p>Specifies the hardware version of the ONT.</p> <p>Example: ES4101</p> |
| Active Firmware Version | <p>Specifies the firmware version of the active ONT.</p> <p>Example: 1.0.0.141</p> |
| Standby Firmware Version | <p>Specifies the firmware version of the standby ONT.</p> <p>Example: 1.0.0.140</p> |
| Me Group | Specifies the managed element group to which the ONT belongs to. |
| Upstream FEC | Specifies whether Forward Error Correction (FEC) is enabled in the upstream traffic. |
| Rx Power (in dBm) | Specifies the current measurement of the optical received power level. |

Table 18. ONT Inventory (continued)

| Field | Description |
|--------------------------|---|
| MAC Ageing time | Specifies the maximum time an ONT can hold a MAC entry in the MAC table when there is no data received from the device. |
| MAC Limit | Specifies the MAC learning depth attribute of the ME MAC bridge service profile on the ONU. |
| Planned Firmware Version | Specifies the expected firmware version of the ONT when the ONT is discovered. |
| DBA Type | Selects the DBA type to be used for ONTs that are created for the ONUs for services. The supported values are. <ul style="list-style-type: none"> NSR SR The default value is NSR. If ONU does not support the value SR, CBAC defaults to the value NSR internally. The user can see the supported DBA type modes in ONU Monitoring capability. |
| Supported DBA Type | Specifies the DBA types which are supported by ONU. The supported values are. <ul style="list-style-type: none"> NSR SR The default value is NSR. |
| Auto Upgrade | Specifies whether the ONU is upgraded with the firmware version mentioned in the ONT Firmware Version Table when the CBAC detects that the firmware version does not match the version mentioned in the table. The supported values are. <ul style="list-style-type: none"> True. Initiates the auto upgrade if the ONT firmware version mentioned in the RMS is not matching the version mentioned in the CBAC. False. Auto upgrade is disabled if you select the false filed. |
| Creation Time | Specifies the date and time when the ONT was created. |

CPE Inventory

The following table describes the fields on the CPE page.

Table 19. CPE Inventory

| Field | Description |
|-------------------|--|
| Name | Specifies the name of the CPE. |
| Fault State | <p>Specifies the highest severity fault present on the CPE. The supported states are:</p> <ul style="list-style-type: none"> • WARNING • CRITICAL • MAJOR • MINOR • No Fault <p>For more information about the severity supported by RMS, see Alarm Severity Levels (on page 238).</p> |
| Admin State | <p>Specifies the admin state of the CPE.</p> <ul style="list-style-type: none"> • Green. Indicates that the admin state of the CPE is enabled. • Red. Indicates that the admin state of the CPE is disabled. |
| Operational State | <p>Specifies the operational state of the CPE.</p> <ul style="list-style-type: none"> • Green. Indicates that the operational state of the CPE is UP. • Red. Indicates that the operational state of the CPE is DOWN. |
| Make | Specifies the vendor name of the CPE. |
| Model | Specifies the model name of the CPE. |
| Display ID | Specifies the display ID of the CPE. |
| MAC Address | Specifies the MAC address of the CPE. |
| Serial No | Specifies the serial number of the CPE. |
| Management IP | Specifies the management IP address of the CPE. |
| Site | Specifies the site name on which the CPE is installed. |
| Device Profile | Specifies the name of the CPE device profile. |
| Management Domain | Specifies the name of the management domain. |
| Controller | Specifies the name of the controller. |
| Alarm Profile | Specifies the alarm profile configured for the CPE. |
| Log Profile | Specifies the log profile of the CPE. |
| ZTP Template | Specifies the ZTP template configured for the CPE. |

Table 19. CPE Inventory (continued)

| Field | Description |
|---------------------|--|
| Server | Specifies the server. |
| Authentication Type | Specifies the authentication type of the CPE. The supported values are as follows. <ul style="list-style-type: none"> • LOCAL • RADIUS |
| Creation Time | Specifies the date and time when the CPE was created. |

Splitter Inventory

The following table describes the fields on the Splitter page.

Table 20. Splitter Inventory

| Field | Description |
|-------------------|--|
| Name | Specifies the name of the splitter. |
| Display ID | Specifies the display ID of the splitter. |
| Make | Specifies the vendor name of the splitter. |
| Model | Specifies the model name of the splitter. |
| Serial No | Specifies the serial number of the CPE. |
| Device Profile | Specifies the name of the splitter device profile. |
| Management Domain | Specifies the name of the management domain. |
| Creation Time | Specifies the date and time when the splitter was created. |

Card Inventory

The following table describes the fields on the Card page.

Table 21. Card Inventory

| Field | Description |
|-------------|---|
| Name | Specifies the name of the card. |
| Fault State | Specifies the highest severity fault present on the card. The supported states are. |

Table 21. Card Inventory (continued)

| Field | Description |
|-------------------------|---|
| | <ul style="list-style-type: none"> • WARNING • CRITICAL • MAJOR • MINOR • No Fault <p>For more information about the severity supported by RMS, see Alarm Severity Levels (on page 238).</p> |
| Display ID | Specifies the display ID of the card. Example: rack=1/shelf=1/slot=ETH1 |
| Make | Specifies the vendor name of the card. |
| Model | Specifies the model name of the card. |
| Technology Capabilities | Specifies the technology supported by card profile. For example, GPON or XGSPON. The default value is GPON. |
| Serial No | Specifies the serial number of the card. |
| Site | Specifies the name of the site on which the card is installed. |
| OLT | Specifies the name of the OLT. |
| Slot Number | Specifies the slot number on which the OLT is placed. |
| Creation Time | Specifies the date and time when the card was created. |

Rack Inventory

The following table describes the fields on the Rack page.

Table 22. Rack Inventory

| Field | Description |
|------------|--|
| Name | Specifies the name of the rack. |
| Display ID | Specifies the display ID of the rack. |
| Make | Specifies the vendor name of the rack. |
| Model | Specifies the model name of the rack. |

Table 22. Rack Inventory (continued)

| Field | Description |
|----------------|--|
| Serial No | Specifies the serial number of the rack. |
| Site | Specifies the name of the site on which the rack is installed. |
| Device Profile | Specifies the name of the rack device profile. |
| Creation Time | Specifies the date and time when the rack was created. |

SFP Inventory

The following table describes the fields on the SFP page.

Table 23. SFP Inventory

| Field | Description |
|--------------------|--|
| Name | Specifies the name of the SFP. Example: SFP_UTXA7000093 |
| Make | Specifies the vendor name of the SFP. Example: Hisense |
| Model | Specifies the model name of the SFP. |
| Display ID | Specifies the display ID of the SFP. Example: SFP_UTXA7000093 |
| Serial No | Specifies the serial number of the SFP. Example: UTXA7000093 |
| Device Profile | Specifies the name of the SFP device profile. Example: SFP_Hisense_SFP_Profile |
| OLT | Specifies the name of the OLT on which the SFP is associated with. |
| Port | Specifies the OLT port. Example: NNI5 |
| Manufacturing Date | Specifies the manufacturing date of the SFP. Example: 09 JUL 2020 |
| Creation Time | Specifies the date and time when the SFP configuration was created. |
| SFP Missing | Specifies whether SFP is missing or not. Example: SFP module is missing on the port |

Cable Inventory

The following table describes the fields on the Cable page.

Table 24. Cable Inventory

| Field | Description |
|---------------|---|
| Name | Specifies the name of the cable. |
| Make | Specifies the vendor name of the cable. |
| Model | Specifies the model name of the cable. |
| Display Id | Specifies the display ID of the cable. |
| Serial No | Specifies the serial number of the cable. |
| Creation Time | Specifies the date and time when the cable configuration was created. |

ONT Card Inventory

The following table describes the fields on the ONT Card page.

Table 25. ONT Card Inventory

| Field | Description |
|---------------|---|
| Name | Specifies the name of the ONT card. Example: onu1-CARD |
| Make | Specifies the vendor name of the ONT card. |
| Model | Specifies the model name of the ONT card. |
| Display ID | Specifies the display ID of the ONT card. Example: rack=1/shelf=1/slot=ETH1/port=1/remote_unit=onu1/slot=1 |
| Serial No | Specifies the serial number of the ONT card. Example: TWXP1AE36BE7-CARD |
| Creation Time | Specifies the date and time when the ONT card was created. |

Exporting Managed Elements

You can export managed elements (OLT, ONT, CPE, splitter, card, rack, SFP, cable, and ONT card) as a CSV file from RMS to your local computer. The CSV file can be opened or edited using an application such as Microsoft Excel. You can view and analyze the exported managed element information, as needed.

Perform the following steps to export managed elements.

1. Select **Monitor > Inventory > Inventory**.
The Inventory List page appears.
2. Navigate to the respective managed element tab.
3. Select the numbers from the **show entries** list.



Note: The supported values are 10, 25, 50, and 100. It defines the number of managed elements you can export. For example, suppose there are 14 managed elements on the page, and you have selected the value 10 from the **show entries** list. In that case, it exports only 10 managed elements and skips the remaining 4 managed elements. To export all 14 managed elements, you must select the next maximum value (25) from the **show entries** list.

4. Click **Export** to export the details.



Note: You can export a maximum of 100 managed elements through the inventory page. If there are more than 100 managed elements, see [Creating Task for Inventory Collection \(on page 689\)](#) to export all the listed managed elements.

The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file using an application such as Microsoft Excel. Optionally, you can save this file on your computer for later use.

Inventory

RMS provides a detailed summary view to enable the network monitoring team to manage the network effectively. The monitoring framework provides an effective way to monitor the managed elements such as OLT, ONT, CPE, splitter, card, rack, SFP, cable, and ONT card.

Monitoring OLT

RMS monitors information about OLTs, including health status, basic Information, ONU statistics, device view, live Key Performance Indicators (KPIs), historical KPIs, port List (NNI and PON), port KPIs, faults, events, activity log, card list, ONT list, services, ONT alarms, LAG, ACL profile, ELine, and ELAN. You can view the summary of all the OLTs connected in your network.

The OLT health status displays information about alarms and ports associated with that particular OLT, including a total number of alarms (critical, minor, major, and warning) raised for the OLT and total number of ports connected to the OLT with the port status (Active, Inactive, Up, and Down).

The ONU statistics include the total number of ONUs connected to the OLT and the status of each ONU (Up, Down, Active, and Deactive).

You can monitor OLTs using live and historical KPIs such as CPU utilization, disk utilization, fan speed, memory utilization, and temperature. You can also monitor the list of ports connected to the OLT, list of alarms and events, activity logs, cards, ONTs, services, and list of ONT alarms.

The following table covers the OLT monitoring information.

| Monitoring OLT Details | For more information, see |
|---|---|
| Health | Health (on page 69) |
| Basic Information | Basic Information (on page 69) |
| ONU Statistics | ONT Statistics (on page 71) |
| Topology | Topology (on page 71) |
| Ports | Ports (on page 71) |
| Faults | Alarm (on page 115) |
| Events | Events (on page 117) |
| Logs | Logs (on page 118) |
| Card List | Card List (on page 119) |
| ONT List | ONT List (on page 120) |
| Services | Services (on page 124) |
| ONT Alarms | ONT Alarms (on page 125) |
| Device View | Device View (on page 126) |
| OLT Live KPIs | OLT Live KPIs (on page 127) |
| Historical KPIs | Historical KPIs (on page 128) |
| Exporting Ports, Faults, Events, and Logs (OLT) | Exporting Ports, Faults, Events, and Logs (OLT) (on page 133) |
| Profiles | Profiles (on page 133) |
| Network Services | Network Services (on page 135) |
| Protection | Protection (on page 149) |
| MEP Instance | MEP Instance (on page 150) |
| OLT Rack | OLT Rack (on page 151) |
| SFP | SFP (on page 152) |
| DHCP Snooping Details | DHCP Snooping Details (on page 153) |
| Login to the Physical OLT | Login to the Physical OLT (on page 155) |

Details

Perform the following steps to monitor the OLT.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

Health

You can view the health status of the OLT configured on the **Configuration > Inventory > Inventory > OLT > Details** page.

- **Critical.** Shows the number of critical alarms raised.
- **Major.** Shows the number of major alarms raised.
- **Minor.** Shows the number of minor alarms raised.
- **Warning.** Shows the number of warning alarms raised.
- **Active Port.** Shows the number of ports that are activated.
- **Inactive Port.** Shows the number of ports that are deactivated.
- **Up Port.** Shows the number of ports that are up.
- **Down Port.** Shows the number of ports that are down.

Basic Information

You can view the basic information about the OLT configured on the **Configuration > Inventory > Inventory > OLT > Details** page.

- **Name.** Name of the OLT, for example, OLT-1.
- **Type.** Type of the device, for example, OLT.
- **Display ID.** Display ID of the OLT, for example, olt-1.
- **Serial No.** Serial number of the OLT, for example, RSYSD9E36606.
- **MAC.** MAC address of the OLT, for example, a8:2b:b5:36:78:09.
- **IP Address.** Specifies the IP address of the OLT, for example, 172.27.173.135. You can login to the OLT console from RMS, for more information, see [Login to the Physical OLT \(on page 155\)](#).
- **Controller.** Name of the controller. Click the controller name to view details of the controller.
- **Total ONTs (Active and Inactive).** Total number of ONTs (active and inactive) that are connected to the OLT.
- **Total Services.** Total number of services that are associated with the OLT.
- **Site.** Site name to which the OLT belongs to.
- **Reboot Time.** Date and time when the OLT was rebooted.
- **Reboot Reason.** Reason provided while rebooting the OLT.

- **Reset Time.** Specifies the reset time of the OLT.
- **Reset Reason.** Specifies the reset reason of the OLT.
- **Alias Name.** Alias name of the OLT.
- **Configuration Change Time.** Date and time when the OLT configuration was changed.
- **ZTP Status.** ZTP status of the OLT.
- **Fan Inventory.** OLT fan inventory information. Click the eye icon to view the fan inventory information of the OLT.
- **PSU Inventory.** Specifies the list of power supply connection status. Click the eye icon to view the PSU information of the OLT such as name, model, and status.
 - **Name.** Specifies the name of the power supply terminal at the OLT, for example, PIM4328_PSU_A.
 - **Model.** Specifies the model of the power supply unit at the OLT, for example, PIM4328.
 - **Status.** Specifies the power feed status of the OLT. The supported values are PRESENT and NOT-PRESENT.
- **Thermal Sensors.** Specifies the OLT thermal sensor information. Click the eye icon to view the thermal sensor information of the OLT.
- **PSU Threshold Values.** Specifies the OLT PSU threshold values (not configurable by user).
 - **High Voltage Threshold (V).** Specifies the OLT high voltage threshold value in volts (V).
 - **Low Voltage Threshold (V).** Specifies the OLT low voltage threshold value in volts (V).
 - **High Current Threshold (A).** Specifies the OLT high electric current threshold value in amperes (A).
- **Admin State.** Admin state of the OLT, for example, ACTIVE.
- **Operational State.** Operational state of the OLT, for example, UP.
- **Up Since.** Specifies the date and time from when the OLT is UP.



Note: If the OLT is added to the network for the first time, it shows the time since it was activated. If the OLT is rebooted, it reflects the time since the reboot.

- **Management Domain.** Click the management domain name to view the details of the management domain.
- **Model.** Model name of the OLT.
- **Make.** Vendor name of the OLT.
- **Software Version.** Software version of the OLT device, for example, SDPON_BINS_1.3.157
- **Hardware Version.** Hardware version of the OLT device, for example, C3708-32-256.
- **Firmware Version.** Firmware version of the OLT device, BAL.3.10.2.
- **Technology.** PON technology supported on the OLT, for example, XGSPON.
- **Total Subscribers.** Total number of subscribers associated with the OLT.
- **Site Address.** Site address of the OLT where the OLT resides.
- **Last Backup Time.** Date and time when the last OLT backup was taken.
- **ME Group.** Managed element group to which the OLT belongs.
- **Alarm Ports.** Number of alarm ports in the OLT.

- **ONT Firmware Upgrade Status.** Upgrade status of the ONT firmware, for example, NOT-DOWNLOADED.
- **ONT Firmware Download Version.** Download version of the ONT firmware.
- **Anti Theft Status.** Status of anti-theft configuration. For example, DISABLED.
- **Enterprise Number.** Vendor's enterprise number of the OLT.

ONT Statistics

You can view the statistics of the ONT configured on the **Configuration > Inventory > Inventory > OLT > Details** page.

- **Active.** Shows the number of ONTs that are activated.
- **Deactive.** Shows the number of ONTs that are deactivated.
- **Up.** Shows the number of ONTs that are up.
- **Down.** Shows the number of ONTs that are down.
- **Blacklisted.** Shows the number of ONTs that are blacklisted.

Topology

Perform the following steps to view the physical and logical topology of the OLT.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Topology** tab.

You can view the physical and logical topology of the OLT.

For more information on Topology, see [Topology \(on page 283\)](#).

Ports

The ports page contains the list of PON, NNI, and ALARM ports connected to the OLT, detection of faults on the ports, and the reporting of performance KPIs to assess the utilization of the port.

Perform the following steps to monitor the ports

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** tab.

The OLT Details page appears.

4. Click the **Port** tab.

You can view the port details of the OLT.

The following table describes the fields on the Ports Details page.

Table 26. OLT Ports List

| Field | Description |
|------------------------|--|
| Name | Specifies the name of the port. <ul style="list-style-type: none">• NNI• PON• ALARM |
| Type | Specifies the type of the port. Example: PHYSICAL |
| Display ID | Specifies the display ID of the port. Example: card1/port=18 |
| No | Specifies the number of PON ports associated with the OLT. Example: 7 |
| Direction | Specifies the port direction type. The supported values are. <ul style="list-style-type: none">• UNI• NNI• ANY |
| Configured Port Mode | Select the configured port mode from the list. The supported values are. <ul style="list-style-type: none">• Auto• GPON• XGSPON• CPON The default value is Auto. |
| Discovered Port Mode | This field is not configurable. The default value is GPON. |
| Capacity | Specifies the capacity of the port. Example: 10 (Gigabit) |
| Description | Specifies the brief description of the OLT port. |
| LAG | Specifies the LAG name, which is associated with the OLT. |
| PON Encryption Enabled | Specifies the PON encryption. The OLT supports the PON downstream unicast encryption. |

Table 26. OLT Ports List (continued)

| Field | Description |
|--------------------------------------|---|
| PON Encryption Key Interval | Specifies the PON encryption key interval in milliseconds. The default value is 3600000 milliseconds (1 hour). If this field is configured as '0', one-time key exchange is considered. However, for the security, always periodic key exchange is recommended. |
| Fault State | Specifies the fault state of the OLT. The supported values are. <ul style="list-style-type: none"> • WARNING • CRITICAL • MAJOR • MINOR • NO FAULT |
| Admin State | Specifies the admin state of the port. <ul style="list-style-type: none"> • Green. Indicates that the port is active. • Red. Indicates that the port is inactive. |
| Operational State | Specifies the operational state of the port. <ul style="list-style-type: none"> • Green. Indicates that the operational state of the port is up. • Red. Indicates that the operational state of the port is down. |
| Type-B Protection State | Specifies the type-B protection state. |
| Type-B Protection Role | Specifies the type-B protection role. |
| Protection Operational State | Specifies the operational state of the port protection. |
| Splitter Name | Specifies the name of the splitter to which the OLT is connected. |
| SFP Name | Specifies the name of the SFP connected to the OLT. Example: J11948000677 Click the SFP name to view the SFP information. |
| Auto-negotiation | Specifies whether the auto-negotiation is enabled. |
| Periodic Rogue ONT Detection Control | Specifies whether the periodic rogue ONT detection is enabled. The supported values are. <ul style="list-style-type: none"> • ENABLED • DISABLED |

Table 26. OLT Ports List (continued)

| Field | Description |
|---|--|
| Periodic Rogue ONT Detection Measurement Type | Specifies the RSSI measurement window type. The supported values are. <ul style="list-style-type: none"> SILENT-WINDOW. Detects and identifies an ONU that is responding to allocations belonging to another ONT but detects most other types of rogue ONT behavior. CUTOFF-WINDOW. Detects an ONT that stops the laser transmit later than it should, potentially interfering with the next allocation. |
| Alloc Type To Scan | Specifies the Alloc ID type to scan. The supported values are. <ul style="list-style-type: none"> UNUSED. Alloc IDs that are currently not in use (not yet assigned to any ONTs). PREVIOUSLY-USED. Alloc IDs that are used once and cleared. ALL. Scan both unused and previously used Alloc IDs. |
| Periodic Rogue ONT Detection Interval (in Milliseconds) | Specifies the periodic rogue ONU detection procedure initiation interval in milliseconds. |
| Creation Time | Specifies the date and time when the PON port was created. |

Alarms

Perform the following steps to monitor the Alarm port.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the Alarm port name to view the alarm details.

Details of Alarm Port

The following table describes the fields on the Alarm Port List page.

Table 27. Alarm Port Details

| Field | Description |
|--------------------------|--|
| Basic Information | |
| Name | Specifies the name of the Alarm port, for example, ALARM. |
| Type | Specifies the type of the Alarm port, for example, PHYSICAL. |
| Display ID | Specifies the display ID of the port, for example, /rack=1/shelf=1/slot=LT-1/port=ALARM. |
| Port No. | Specifies the port number, for example, 101. |
| Capacity | Specifies the capacity of the port, for example, 1 (Gigabit). |
| Description | Specifies the description of the port. |
| Direction | Specifies the port direction, for example, UNI. |
| OLT | Specifies the OLT name of the Alarm port, for example, olt-185. |
| Admin State | Specifies the admin state of the Alarm port, for example, ACTIVE. |
| Operational State | Specifies the operational state of the Alarm port, for example, UP. |
| Fault State | Specifies the fault state of the Alarm port, for example, NO FAULT. |
| MAC Table Dump | |
| Ovlan | Specifies the outer tag value. |
| Ivlan | Specifies the inner tag value. This field is applicable only for the NNI port. |
| MAC Type | <p>Specifies the MAC type. The supported values are.</p> <ul style="list-style-type: none"> • Static • Dynamic • Relay-Agent IPv4 • Relay-Agent IPv6 • Relay-Agent IPv4, IPv6 • PPPoE-IA • MLD/IGMP Proxy |
| Static | <p>The static MAC is configured or learned based on the MAC learning type. If the traffic goes through the PON in the service, static MAC doesn't age out. The supported values for the MAC learning type are.</p> |

Table 27. Alarm Port Details (continued)

| Field | Description |
|------------------------|---|
| | <ul style="list-style-type: none"> • DHCP • DHCP_ALLOW_RELARN • ARP • ARP_ALLOW_RELARN • PPPoE • DHCP_IP_ANTISPOOFING_NO_MAC • DHCP_IP_ANTISPOOFING_MAC • DHCP_NO_MAC • ARP_NO_MAC <p> Note: In the service configuration with DHCP or DHCP_NO_MAC MAC learning type, service-get reports only the last learned MAC address and IP address. If the service is configured on the VEIP or IPhost port of the ONT, this information indicates the WAN interface of the ONT. Otherwise, it indicates the client device behind the ONU when the service is configured on the PPTP port.</p> <p>For more information on MAC Learning Type, see Table 268: MAC Learning Type (on page 580).</p> |
| Dynamic | A MAC is displayed as dynamic when MAC is learned by the data path of the OLT. |
| Relay-Agent IPv4 | The MAC address is learnt at relay-agent when DHCPv4 cycle is in progress. |
| Relay-Agent IPv6 | The MAC address is learnt at relay-agent when DHCPv6 cycle is in progress. |
| Relay-Agent IPv4, IPv6 | The MAC address is learnt at relay-agent when DHCPv4 and DHCPv6 cycle is in progress. |
| PPPoE-IA | The MAC address is learnt by the PPPoE intermediate agent where the PPPoE session establishment is in progress. |
| MLD/IGMP PROXY | Specifies the MAC address of the multicast router or proxy running on the BNG network learnt at NNI. |
| MAC Address | Specifies the MAC address. |
| Creation time | Specifies the date and time when the MAC dump was created. |
| ELine | Specifies the activity log generated for the Eline configuration. For more information on the field descriptions, see ELine (on page 143) . |

Table 27. Alarm Port Details (continued)

| Field | Description |
|-------|---|
| ELAN | Specifies the activity log generated for the ELAN configuration. For more information on the field descriptions, see ELAN (on page 146) . |
| Ring | Specifies the activity log generated for the ring configuration. For more information on the field descriptions, see Ring (on page 214) . |

Historical KPIs

Perform the following steps to monitor the alarm port.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the Alarm name to view the alarm details.
6. Click the **Historical KPIs** tab.

You can view the historical KPIs of the Alarm.

Alarm Historical KPIs

You can view the graphical view of the alarm KPIs by one day, one week, one month, daily, and hourly. You can also view the alarm KPIs for a particular duration using the **Custom** option.

You can select data packet or control packet from the option for which you want to view the historical information. For data packet you can select the upstream and downstream KPI parameter from the list for which you want to view the historical information.

The graphical view of the alarm historical KPIs information is generated based on the periodic interval and the KPI parameter that you have selected.



Note: If you select one option from the list, the second list dynamically populates the relevant data based on the first option. To view all options in the list, deselect the option in the list.

The following table shows the description of Alarm data packet KPI parameters.

Table 28. Alarm Data Packet Historical KPIs

| Field | Description |
|--------------------------|---|
| Downstream KPIs | |
| Rx Data Rate | Specifies the upstream alarm received data rate. The unit is in bytes per second. |
| Rx Utilization | Specifies the upstream alarm received data utilization. The unit is in percentage. |
| Rx Bytes | Specifies the upstream alarm received in bytes. The unit is in bytes. |
| Rx Unicast Packets | Specifies the upstream alarm received unicast packets. The unit is in packet count. |
| Rx Multicast Packets | Specifies the upstream alarm received multicast packets. The unit is in packet count. |
| Rx Broadcast Packets | Specifies the upstream alarm received broadcast packets. The unit is in packet count. |
| Rx Error Packets | Specifies the upstream alarm received error packets. The unit is in packet count. |
| Rx Fcs Error Packet | Specifies the upstream alarm received FCS error packets. The unit is in packet count. |
| Rx Packets Dropped | Specifies the upstream alarm dropped error packets. The unit is in packet count. |
| Rx FEC Codewords | Specifies the received forward error correction (FEC) codewords. |
| Rx BIP Units | Specifies the received units protected by BIP. |
| Rx BIP Errors | Specifies the received BIP errors. |
| Rx GEM | Specifies the received GEM frames. |
| Rx GEM Dropped | Specifies the received dropped GEM frames dead due disabled GEM port ID. |
| Rx GEM Idle | Specifies the received idle GEM frames. |
| Rx GEM Corrected | Specifies the received GEM frames with a header error control (HEC) error that was corrected. |
| Rx GEM Fragmented Errors | Specifies the received packets dropped due to GEM fragmentation error. |

Table 28. Alarm Data Packet Historical KPIs (continued)

| Field | Description |
|------------------------------|--|
| Rx Dropped Packets Too Short | Specifies the received packets that were dropped due to length being too short. |
| Rx Dropped Packets Too Long | Specifies the received packets that were dropped due to length being too long. |
| Rx Key Errors | Specifies the received packets dropped due to key error. Key error occurs when using an invalid key to decrypt data. |
| Rx Allocations Valid | Specifies the received valid bandwidth allocation bursts. |
| Rx Allocations Invalid | Specifies the received invalid bandwidth allocation, due to incorrect bandwidth map. |
| Rx Allocations Disabled | Specifies the received and discarded bandwidth allocations for disabled AllocID. |
| Rx Ploams | Specifies the received PLOAMs. |
| Rx Ploams Non Idle | Specifies the received non idle PLOAMs. |
| Rx Ploams Dropped | Specifies the received PLOAMs that were dropped, due to full PLOAM queue. |
| Rx Ploams Error | Specifies the received PLOAMs with CRC error. |
| Rx CPU | Specifies the received packets that were forwarded to the CPU queue. |
| Rx OMCI | Specifies the received packets that were forwarded to the OMCI queue. |
| Rx OMCI Packets CRC Errors | Specifies the received OMCI packets with CRC errors. |
| Rx XGTC Headers | Specifies the received valid XGTC headers. |
| Rx XGTC Corrected | Specifies the received corrected XGTC headers. |
| Rx XGTC Uncorrected | Specifies the received uncorrected XGTC headers. |
| Rx Fragment Errors | Specifies the received packets dropped due to fragmentation errors. |
| Upstream KPIs | |
| Tx Bytes | Specifies the downstream alarm transmit. The unit is in bytes. |
| Tx Unicast Packets | Specifies the downstream alarm transmit unicast packets. The unit is in packet count. |

Table 28. Alarm Data Packet Historical KPIs (continued)

| Field | Description |
|-----------------------------|--|
| Tx Multicast Packets | Specifies the downstream alarm transmit multicast packets. The unit is in packet count. |
| Tx Broadcast Packets | Specifies the downstream alarm transmit broadcast packets. The unit is in packet count. |
| Tx Error Packets | Specifies the downstream alarm transmit error packets. The unit is in packet count. |
| Tx Data Rate | Specifies the downstream alarm transmit data rate. The unit is in bytes per second. |
| Tx Utilization | Specifies the downstream alarm transmit data utilization. The unit is in percentage. |
| Tx Ploams | Specifies the upstream PLOAMs. |
| Tx GEM | Specifies the upstream GEM frames. |
| Tx CPU | Specifies the upstream CPU packets. |
| Tx OMCI | Specifies the upstream OMCI packets. |
| Tx CPU OMCI Packets Dropped | Specifies the upstream CPU OMCI packets dropped, due to illegal length. |
| Tx Dropped Illegal Length | Specifies the upstream packets dropped, due to illegal length. |
| Tx Dropped TPID Miss | Specifies the packets received from the NNI dropped due to TPID miss. |
| Tx Dropped VID Miss | Specifies the upstream packets dropped, due to VID miss. |
| Tx Dropped Packets | Specifies the downstream alarm dropped error packets. The unit is in packet count. |

The following table shows the description of alarm control packet KPI parameters.

Table 29. Alarm Control Packet Historical KPIs

| Field | Description |
|--------|---|
| PPPoE | Specifies the historical KPIs for PPPoE control packets. |
| DHCPv4 | Specifies the historical KPIs for DHCPv4 control packets. |
| DHCPv6 | Specifies the historical KPIs for DHCPv6 control packets. |

Exporting Alarm Historical KPIs

You can export the alarm historical KPIs. You can view and analyze the exported KPIs list, as needed.

Perform the following steps to export the alarm KPIs.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name.

The OLT Details page appears.

4. Navigate to the **Port** tab.

Click on the Alarm name to view the alarm details.

5. Click the **Historical KPIs** tab.

You can view the historical KPIs of the Alarm.

6. Click **Export** from the historical KPIs.

The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file in a Microsoft Excel sheet. Optionally, you can save this file on your PC for later use.

The downloaded file contains the attributes based on the KPI parameters that you have selected.

Alarms

Perform the following steps to monitor the alarms.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the Alarm name to view the alarm details.
6. Click the **Alarms** tab.

You can view the list of current alarms and cleared alarms.

For more information on the field descriptions, see [Table 42: Alarm List \(on page 115\)](#).

Events

Perform the following steps to monitor the events of the alarm port.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the Alarm name to view the alarm details.
6. Click the **Events** tab.

You can view the list of events reported for the Alarms.

For more information on the field descriptions, see [Table 43: Events List \(on page 117\)](#).

Activity Log

Perform the following steps to monitor the activity log of the alarm port.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the Alarm name to view the alarm details.
6. Click the **Activity Log** tab.

You can view the activity log generated for the alarms.

For more information on the field descriptions, see [Table 44: Activity Logs \(Tabular View\) \(on page 119\)](#).

PON Port

PON port monitoring involves detection of faults and events on the PON ports and the reporting of performance KPIs to assess the utilization of the PON port.

Perform the following steps to view the PON port details.

1. Select **Monitor > Inventory > Inventory**.
The Inventory List page appears.
2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.
The OLT Details page appears.
4. Click the **Ports** tab.
5. Click on the PON port name (for example, SFPPON-32) to view the PON port details.

Details of PON Port

1. Select **Monitor > Inventory > Inventory**.
The Inventory List page appears.
2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.
The OLT Details page appears.
4. Click the **Ports** tab.
5. Click on the PON port name (for example, SFPPON-32) to view the PON port details.

The following table describes the fields on the PON Details List page.

Table 30. PON Port Details

| Field | Description |
|--------------------------|---|
| Basic Information | |
| Name | Specifies the name of the PON port, for example, SFPPON-31. |
| Type | Specifies the type of the PON port, for example, PHYSICAL. |
| Display ID | Specifies the display ID of the port. For example, /rack=1/shelf=1/slot=LT-1/port=SFPPON-31. |
| Port No. | Specifies the port number. For example, 1. |
| Configured Port Mode | Select the configured port mode from the list. The supported values are. <ul style="list-style-type: none">◦ Auto◦ GPON◦ XGSPON◦ CPON The default value is Auto. |
| Discovered Port Mode | This field is not configurable. The default value is GPON. |

| Field | Description |
|---|--|
| Capacity | Specifies the capacity of the port, for example, 2.5 (Gigabit) |
| Description | Specifies the description about the PON port. |
| Direction | Specifies the port direction, for example, UNI. |
| OLT | Specifies of the PON port of the OLT, for example, olt-185. |
| Admin State | Specifies the admin state of the PON port, for example, ACTIVE. |
| Operational State | Specifies the operational state of the PON port. |
| Fault State | Specifies the fault state of the PON port. |
| PON Encryption Enabled | Specifies if the PON encryption is enabled. |
| PON Encryption Key Exchange Interval | Specifies the PON encryption key exchange interval in milliseconds. The default value is 3600000 milliseconds. |
| Periodic Rogue ONT Detection Control | Specifies the RSSI measurement window type. |
| Periodic Rogue ONT Detection Measurement Type | Specifies that the periodic rogue ONT detection is enabled. |
| Alloc Type To Scan | Specifies the allocation ID type to scan. |
| Periodic Rogue ONT Detection Interval (in Milliseconds) | Specifies the periodic rogue ONU detection procedure initiation interval in milliseconds. |
| MAC Table Dump | |
| Ovlan | Specifies the outer tag value. |
| Ivlan | Specifies the inner tag value. This field is applicable only for the NNI port. |
| MAC Type | <p>Specifies the MAC type. The supported values are.</p> <ul style="list-style-type: none"> ◦ Static ◦ Dynamic ◦ Relay-Agent IPv4 ◦ Relay-Agent IPv6 ◦ Relay-Agent IPv4, IPv6 ◦ PPPoE-IA |

| Field | Description |
|------------------------|--|
| Static | <p>The static MAC is configured or learned based on the MAC learning type. If the traffic goes through the PON in the service, static MAC doesn't age out.</p> <p>The supported values for the MAC learning type are.</p> <ul style="list-style-type: none"> ◦ DHCP. ◦ DHCP_ALLOW_RELEARN. ◦ ARP. ◦ ARP_ALLOW_RELEARN. ◦ PPPoE. ◦ DHCP_IP_ANTISPOOFING_NO_MAC. ◦ DHCP_IP_ANTISPOOFING_MAC. ◦ DHCP_NO_MAC. ◦ ARP_NO_MAC. <p> Note: In the service configuration with DHCP or DHCP_NO_MAC MAC learning type, service-get reports only the last learned MAC address and IP address. If the service is configured on the VEIP or IPhost port of the ONT, this information indicates the WAN interface of the ONT. Otherwise, it indicates the client device behind the ONU when the service is configured on the PPTP port.</p> <p>For more information on MAC Learning Type, see Table 268: MAC Learning Type (on page 580).</p> |
| Dynamic | A MAC is displayed as dynamic when MAC is learned by the data path of the OLT. |
| Relay-Agent IPv4 | The MAC address is learnt at relay-agent when DHCPv4 cycle is in progress. |
| Relay-Agent IPv6 | The MAC address is learnt at relay-agent when DHCPv6 cycle is in progress. |
| Relay-Agent IPv4, IPv6 | The MAC address is learnt at relay-agent when DHCPv4 and DHCPv6 cycle is in progress. |
| PPPoE-IA | The MAC address is learnt by the PPPoE intermediate agent where the PPPoE session establishment is in progress. |
| MAC Address | Specifies the MAC address. |
| Creation time | Specifies the date and time when the MAC dump was created. |

Live KPIs

Perform the following steps to view the Live KPIs details.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.

3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.

5. Click on the PON port name (for example, SFPPON-32) to view the PON port details.

The PON port details page appears.

6. Click the **Live KPIs** tab.

You can view the Live KPIs information of the PON port.

PON Port Live KPIs for Data Packets

You can view the live and historical KPIs of the PON port.

The PON port performance helps to monitor the usage of network, the type of packets transiting the network, and consuming the network resources. You can view the real-time performance data of the PON port.

Live KPIs display the changes of a PON port performance indicator in real time. Generally, the live performance data is used for fault diagnosis.

If the port is configured in CPON port mode, you can select the port technology (GPON or XGSPON) from the list to view the following live KPIs for each tech port.

- GPON live KPIs
- XGSPON live KPIs

The following table shows the description of fields of the OLT PON port live KPIs.

Table 31. PON Port Live KPIs

| Field | Description |
|----------------------|---|
| Rx Data Rate (Mbps) | Specifies the upstream PON port data received rate in Mbps. |
| Rx Utilization (%) | Specifies the received upstream port utilization in percentage. |
| Rx Bytes | Specifies the total number of PON port upstream bytes received. The unit is in bytes. |
| Rx Broadcast Packets | Specifies the total number of PON port upstream broadcast packets received. The unit is in packet count. |

Table 31. PON Port Live KPIs (continued)

| Field | Description |
|-----------------------------|---|
| Rx Error Packets | Specifies the number of PON port upstream packets that shows error while receiving the packets. The unit is in packet count. |
| Rx Multicast Packets | Specifies the total number of PON port upstream multicast packets received. The unit is in packet count. |
| Rx Unicast Packets | Specifies the total number of upstream unicast packets received. The unit is in packet count. |
| Rx Packets Dropped | Specifies the number of PON port upstream packets dropped. The unit is in packet count. |
| Rx Ploams | Specifies the received PLOAMs |
| Rx CPU | Specifies the received packets that were forwarded to the CPU queue. |
| Rx OMCI | Specifies the received packets that were forwarded to the ONT Management Control Interface (OMCI) queue. |
| Rx GEM | Specifies the received GEM frames. |
| Rx Dropped Packets Too Long | Specifies the received packets that were dropped due to length being too long. |
| Rx FCS Error Packets | Specifies the number of Frame Check Sequence (FCS) error packets received. |
| Rx Allocations Valid | Specifies the received valid bandwidth allocation bursts. |
| Rx XGTC Headers | Specifies the received valid XG-PON transmission convergence (XGTC) headers. |
| Tx Dropped Illegal Length | Specifies the upstream packets dropped, due to illegal length. |
| Tx Data Rate (Mbps) | Specifies the downstream PON port data transmit rate in Mbps. |
| Tx Utilization (%) | Specifies the transmitted downstream port utilization in percentage. |
| Tx Bytes | Specifies the total number of PON port downstream bytes transmitted. |
| Tx Broadcast Packets | Specifies the total number of PON port downstream broadcast packets transmitted. |
| Tx Error Packets | Specifies the number of PON port downstream packets that shows error while transmitting the packets. |

Table 31. PON Port Live KPIs (continued)

| Field | Description |
|------------------------------|--|
| Tx Multicast Packets | Specifies the total number of PON port downstream multicast packets transmitted. |
| Tx Unicast Packets | Specifies the total number of downstream unicast packets transmitted. The unit is in packet count. |
| Tx Ploams | Specifies the upstream physical layer operation and managements (PLOAMs). |
| Tx CPU | Specifies the upstream CPU packets. |
| Tx OMCI | Specifies the upstream OMCI packets. |
| Tx GEM | Specifies the upstream GEM frames. |
| Tx CPU OMCI Packets Dropped | Specifies the upstream CPU OMCI packets dropped, due to illegal length. |
| Rx Dropped Packets Too Short | Specifies the received packets that were dropped due to length being too short. |
| Rx Ploams Error | Specifies the received PLOAMs with CRC error. |
| Rx Allocations Invalid | Specifies the received valid bandwidth allocation bursts. |
| Rx XGTC Uncorrected | Specifies the received corrected XGTC headers. |
| Tx Dropped TPID Miss | Specifies the packets received from the PON dropped due to TPID miss. |
| Tx Dropped VID Miss | Specifies the upstream packets dropped, due to VID miss. |
| Tx Dropped Packets | Specifies the downstream PON port dropped error packets. The unit is in packet count. |
| Rx FEC Codewords | Specifies the received forward error correction (FEC) codewords. |
| Rx BIP Units | Specifies the received units (bits in GPON/bytes in XGPON) protected by bit-interleaved parity BIP. |
| Rx BIP Errors | Specifies the received BIP errors. |
| Rx GEM Dropped | Specifies the received dropped GEM frames die to disabled GEM port ID. |
| Rx GEM Idle | Specifies the received idle GEM frames. |
| Rx GEM Fragment Errors | Specifies the received packets dropped due to GEM fragmentation error. |
| Rx Key Errors | Specifies the received packets dropped due to key error. Key error occurs when using an invalid key to decrypt data. |

Table 31. PON Port Live KPIs (continued)

| Field | Description |
|----------------------------|---|
| Rx Fragment Errors | Specifies the received packets dropped due to fragmentation errors. |
| Rx GEM Corrected | Specifies the received GEM frames with a Header Error Control (HEC) error that was corrected. |
| Rx Ploams Dropped | Specifies the received PLOAMs that were dropped, due to PLOAM queue full. |
| Rx OMCI Packets CRC Errors | Specifies the received OMCI packets with CRC errors. |
| Rx Ploams Non Idle | Specifies the received non idle PLOAMs. |
| Rx Allocations Disabled | Specifies the received and discarded bandwidth allocations for disabled AllocID. |
| Rx XGTC Corrected | Specifies the received corrected XGTC headers. |

RMS supports clearing the PON KPI counters on the ONT through the openOMCI interface. To clear the KPI counter, click the **CLEAR KPI** from the top right corner on the page.



Note: You can clear the live KPIs only when the **LIVE KPI** option is ON.

PON Port Live KPIs for Control Packets

The PON port performance helps to monitor the usage of network, the type of packets transiting the network, and the consumption of network resources.

The following table shows the description of fields of the PON port live KPIs control packets.

Table 32. PON Port Live KPIs Control Packets

| Field | Description |
|--------------|---|
| PPPoE | |
| PADI | Specifies the PPPoE initiation packets received. |
| PADO | Specifies the PPPoE offer packets received. |
| PADR | Specifies the PPPoE request packets received. |
| PADS | Specifies the PPPoE session packets received. |
| PADT | Specifies the PPPoE termination packets received. |

Table 32. PON Port Live KPIs Control Packets (continued)

| Field | Description |
|---------------------|--|
| DHCPv4 | |
| Discover | Specifies the DHCP discover packets received. |
| Offer | Specifies the DHCP offer packets received. |
| Request | Specifies the DHCP request packets received. |
| Ack | Specifies the DHCP ack packets received. |
| Release | Specifies the DHCP release packets received. |
| Nak | Specifies the DHCP nak packets received. |
| Decline | Specifies the DHCP decline packets received. |
| Inform | Specifies the DHCP inform packets received. |
| DHCPv6 | |
| Solicit | Specifies the DHCPv6 solicit packets received. |
| Advertise | Specifies the DHCPv6 advertise packets received. |
| Request | Specifies the DHCPv6 request packets received. |
| Reply | Specifies the DHCPv6 reply packets received. |
| Release | Specifies the DHCPv6 release packets received. |
| Renew | Specifies the DHCPv6 renew packets received. |
| Rebind | Specifies the DHCPv6 rebind packets received. |
| Confirm | Specifies the DHCPv6 confirm packets received. |
| Decline | Specifies the DHCPv6 decline packets received. |
| Reconfigure | Specifies the DHCPv6 reconfigure packets received. |
| Information Request | Specifies the DHCPv6 information request packets received. |
| Relay Forward | Specifies the DHCPv6 relay forward packets received. |
| Relay Reply | Specifies the DHCPv6 relay reply packets received. |

Clear PON Port KPIs

You can also clear the port KPIs by using the **Clear KPI Data** option.

RMS supports clearing the live KPI subscription of the PON port and resetting the counters to zero. This enables fresh debugging by resetting the counters to zero and starting to get the live KPIs incrementally. You can clear the KPI counters only when the PON port admin state is ENABLED, and the operational state is UP.

After clearing the live PON port KPIs, CBAC resets the counters to zero and incrementally generates KPIs for towards RMS for debugging.

To clear the PON port KPI counters, click **Clear KPI** option from the right-hand side of the page.



Note: You can clear the live KPIs only when the **LIVE KPI** option is ON.

Historical KPIs

Perform the following steps to view the historical KPIs details.

1. Select **Monitor > Inventory > Inventory**.
The Inventory List page appears.
2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.
The OLT Details page appears.
4. Click the **Ports** tab.
5. Click on the PON port name (for example, SFPPON-32) to view the PON port details.
The PON port details page appears.
6. Click the **historical KPIs** tab.
You can view the historical KPIs information of the PON port.

PON Port Historical KPIs

You can view the graphical view of the PON port KPIs by one day, one week, one month, daily, and hourly. You can also view the PON port KPIs for a particular duration using the **Custom** option.

You can select a data packet or control packet from the option for which you want to view the historical information. For data packets, you can select the upstream and downstream KPI parameter from the list for which you want to view the historical information.

The graphical view of the PON port historical KPIs information is generated based on the periodic interval and the KPI parameter that you have selected.



Note: If you select one option from the list, the second list dynamically populates the relevant data based on the first option. To view all options in the list, deselect the option in the list.

If the port is configured in CPON port mode, you can select the port technology (GPON or XGSPON) from the list to view the following historical KPIs for each tech port.

- GPON historical KPIs
- XGSPON historical KPIs

The following table shows the description of PON port data packet KPI parameters.

Table 33. PON Port Data Packet Historical KPIs

| Field | Description |
|------------------------|---|
| Downstream KPIs | |
| Rx Data Rate | Specifies the upstream PON port received data rate. The unit is in bytes per second. |
| Rx Utilization | Specifies the upstream PON port received data utilization. The unit is in percentage. |
| Rx Bytes | Specifies the upstream PON port received in bytes. The unit is in bytes. |
| Rx Unicast Packets | Specifies the upstream PON port received unicast packets. The unit is in packet count. |
| Rx Multicast Packets | Specifies the upstream PON port received multicast packets. The unit is in packet count. |
| Rx Broadcast Packets | Specifies the upstream PON port received broadcast packets. The unit is in packet count. |
| Rx Error Packets | Specifies the upstream PON port received error packets. The unit is in packet count. |
| Rx Fcs Error Packet | Specifies the upstream PON port received FCS error packets. The unit is in packet count. |
| Rx Packets Dropped | Specifies the upstream PON port dropped error packets. The unit is in packet count. |
| Rx FEC Codewords | Specifies the received forward error correction (FEC) codewords. |
| Rx BIP Units | Specifies the received units (bits in GPON/bytes in XGPON) protected by BIP. |
| Rx BIP Errors | Specifies the received BIP errors. |
| Rx GEM | Specifies the received GEM frames. |
| Rx GEM Dropped | Specifies the received dropped GEM frames dead due disabled GEM port ID. |
| Rx GEM Idle | Specifies the received idle GEM frames. |

Table 33. PON Port Data Packet Historical KPIs (continued)

| Field | Description |
|------------------------------|--|
| Rx GEM Corrected | Specifies the received GEM frames with a header error control (HEC) error that was corrected. |
| Rx GEM Fragmented Errors | Specifies the received packets dropped due to GEM fragmentation error. |
| Rx Dropped Packets Too Short | Specifies the received packets that were dropped due to length being too short. |
| Rx Dropped Packets Too Long | Specifies the received packets that were dropped due to length being too long. |
| Rx Key Errors | Specifies the received packets dropped due to key error. Key error occurs when using an invalid key to decrypt data. |
| Rx Allocations Valid | Specifies the received valid bandwidth allocation bursts. |
| Rx Allocations Invalid | Specifies the received invalid bandwidth allocation, due to incorrect bandwidth map. |
| Rx Allocations Disabled | Specifies the received and discarded bandwidth allocations for disabled AllocID. |
| Rx Ploams | Specifies the received PLOAMs. |
| Rx Ploams Non Idle | Specifies the received non idle PLOAMs. |
| Rx Ploams Dropped | Specifies the received PLOAMs that were dropped, due to full PLOAM queue. |
| Rx Ploams Error | Specifies the received PLOAMs with CRC error. |
| Rx CPU | Specifies the received packets that were forwarded to the CPU queue. |
| Rx OMCI | Specifies the received packets that were forwarded to the OMCI queue. |
| Rx OMCI Packets CRC Errors | Specifies the received OMCI packets with CRC errors. |
| Rx XGTC Headers | Specifies the received valid XGTC headers. |
| Rx XGTC Corrected | Specifies the received corrected XGTC headers. |
| Rx XGTC Uncorrected | Specifies the received uncorrected XGTC headers. |
| Rx Fragment Errors | Specifies the received packets dropped due to fragmentation errors. |
| Upstream KPIs | |

Table 33. PON Port Data Packet Historical KPIs (continued)

| Field | Description |
|-----------------------------|--|
| Tx Bytes | Specifies the downstream PON port transmit. The unit is in bytes. |
| Tx Unicast Packets | Specifies the downstream PON port transmit unicast packets. The unit is in packet count. |
| Tx Multicast Packets | Specifies the downstream PON port transmit multicast packets. The unit is in packet count. |
| Tx Broadcast Packets | Specifies the downstream PON port transmit broadcast packets. The unit is in packet count. |
| Tx Error Packets | Specifies the downstream PON port transmit error packets. The unit is in packet count. |
| Tx Data Rate | Specifies the downstream PON port transmit data rate. The unit is in bytes per second. |
| Tx Utilization | Specifies the downstream PON port transmit data utilization. The unit is in percentage. |
| Tx Ploams | Specifies the upstream PLOAMs. |
| Tx GEM | Specifies the upstream GEM frames. |
| Tx CPU | Specifies the upstream CPU packets. |
| Tx OMCI | Specifies the upstream OMCI packets. |
| Tx CPU OMCI Packets Dropped | Specifies the upstream CPU OMCI packets dropped, due to illegal length. |
| Tx Dropped Illegal Length | Specifies the upstream packets dropped, due to illegal length. |
| Tx Dropped TPID Miss | Specifies the packets received from the NNI dropped due to TPID miss. |
| Tx Dropped VID Miss | Specifies the upstream packets dropped, due to VID miss. |
| Tx Dropped Packets | Specifies the downstream PON port dropped error packets. The unit is in packet count. |

The following table shows the description of PON port control packet KPI parameters.

Table 34. PON Port Control Packet Historical KPIs

| Field | Description |
|--------|---|
| PPPoE | Specifies the historical KPIs for PPPoE control packets. |
| DHCPv4 | Specifies the historical KPIs for DHCPv4 control packets. |
| DHCPv6 | Specifies the historical KPIs for DHCPv6 control packets. |

IGMP Statistics

RMS supports the retrieval, storage, and display of the multicast statistics. The multicast statistics is reported to RMS from CBAC per PON port, per channel, and per subscriber.

If the port is configured in CPON port mode, you can select the port technology (GPON or XGSPON) from the list to view the following IGMP KPIs for each tech port.

- GPON IGMP KPIs
- XGSPON IGMP KPIs

The following table describes the fields on the IGMP Statistics page.

Table 35. IGMP Statistics

| Field | Description |
|------------------------|---|
| IP Address | Specifies the channel IP address. Example: 238.1.1.1 |
| Mvlan | Select the MVLAN profile configuration. Example: Static |
| Select Option | |
| Active Subscribers | Specifies the total number of active subscribers for the specified channel on the specified PON interface. Example: 5 |
| Total Joins Received | Specifies the total number of IGMP Joins received at CBAC for the specified channel on the specified PON interface. Example: 10 |
| Total Queries Received | Specifies the total number of IGMP queries received at CBAC for the specified channel on the specified NNI interface. Example: 5 |
| Total Reports Sent | Specifies the total number of IGMP reports reported by CBAC for the specified channel on the specified PON interface. Example: 5 |

Table 35. IGMP Statistics (continued)

| Field | Description |
|-----------------------|--|
| Specific Queries Sent | Specifies the total number of IGMP Group-Specific Queries sent from CBAC for the specified channel on the specified PON interface. Example: 5 |
| Reports Received | Specifies the total number of IGMP reports received at CBAC for the specified channel on the specified PON interface. Example: 5 |
| Unsuccessful Joins | Specifies the total number of unsuccessful joins. |

Exporting PON Port IGMP Statistics and Historical KPIs

You can export the PON port historical KPIs. You can view and analyze the exported KPIs list, as needed.

Perform the following steps to export the PON port KPIs.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name.

The OLT Details page appears.

4. Navigate to the **Port** tab.
5. Click on the PON port.

The PON Port Details page appears.

6. Click **Export** from the historical KPIs or IGMP statistics frame.

The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file in a Microsoft Excel sheet. Optionally, you can save this file on your PC for later use.

The downloaded file contains the attributes based on the KPI parameters that you have selected.

Alarms

Perform the following steps to view the alarm details.

1. Select **Monitor > Inventory > Inventory**.
- The Inventory List page appears.
2. Click on the **OLT** tab.
 3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the PON port name (for example, SFPPON-32) to view the PON port details.

The PON port details page appears.

6. Click the **Alarms** tab.

You can view the list of current alarms and cleared alarms reported for the PON port.

For more information on the field descriptions, see [Table 42: Alarm List \(on page 115\)](#).

Events

Perform the following steps to view the event details.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.

3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.

5. Click on the PON port name (for example, SFPPON-32) to view the PON port details.

The PON port details page appears.

6. Click the **Events** tab.

You can view the list of events reported for the PON port.

For more information on the field descriptions, see [Table 43: Events List \(on page 117\)](#).

ONT List

Perform the following steps to view the ONT details.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.

3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.

5. Click on the PON port name (for example, SFPPON-32) to view the PON port details.

The PON port details page appears.

6. Click the **ONT List** tab.

You can view the list of ONTs associated with the PON port.

For more information on the field descriptions, see [ONT \(on page 423\)](#).

For more information on the blacklisted ONTs, see [Blacklisted ME \(on page 178\)](#).

Subscribers

Perform the following steps to view the subscriber details.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.

3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.

5. Click on the PON port name (for example, SFPPON-32) to view the PON port details.

The PON port details page appears.

6. Click the **Subscribers** tab.

You can view the list of subscribers associated with the ONT.

For more information on the description of fields on the subscribers page, see [Table 97: Subscriber List \(on page 224\)](#).

Services

Perform the following steps to view the service details.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.

3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.

5. Click on the PON port name (for example, SFPPON-32) to view the PON port details.

The PON port details page appears.

6. Click the **Services** tab.

You can view the list of services associated with the PON port.

For more information on the field descriptions, see [Table 48: Services \(on page 124\)](#).

Activity Log

Perform the following steps to view the activity log details.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.

3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
 5. Click on the PON port name (for example, SFPPON-32) to view the PON port details.
The PON port details page appears.
 6. Click the **Activity Log** tab.
You can view the activity log generated for the PON port.
- For more information on the field descriptions, see [Table 44: Activity Logs \(Tabular View\) \(on page 119\)](#).

NNI Port Details

NNI port monitoring involves detection of faults on the NNI ports and the reporting of performance KPIs to assess the utilization of the NNI port.

Perform the following steps to monitor the NNI port.

1. Select **Monitor > Inventory > Inventory**.
The Inventory List page appears.
2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.
The OLT Details page appears.
4. Click the **Ports** tab.
5. Click on the NNI port name to view the NNI port details.

Details of NNI Port

Perform the following steps to monitor the NNI port.

1. Select **Monitor > Inventory > Inventory**.
The Inventory List page appears.
2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.
The OLT Details page appears.
4. Click the **Ports** tab.
5. Click on the NNI port name to view the NNI port details.

The following table describes the fields on the NNI Ports List page.

Table 36. NNI Port Details

| Field | Description |
|--------------------------|--|
| Basic Information | |
| Name | Specifies the name of the NNI port, for example, NNI-1. |
| Type | Specifies the type of the NNI port, for example, PHYSICAL. |
| Display ID | Specifies the display ID of the port, for example, /rack=1/shelf=1/slot=LT-1/port=NNI-1. |
| Port No. | Specifies the port number, for example, 1. |
| Capacity | Specifies the capacity of the port, for example, 10 (Gigabit). |
| Description | Specifies the description of the port. |
| Direction | Specifies the port direction, for example, UNI. |
| OLT | Specifies the OLT name of the NNI port, for example, olt-185. |
| Admin State | Specifies the admin state of the NNI port, for example, ACTIVE. |
| Operational State | Specifies the operational state of the NNI port, for example, UP. |
| Fault State | Specifies the fault state of the NNI port, for example, CRITICAL. |
| MAC Table Dump | |
| Ovlan | Specifies the outer tag value. |
| Ivlan | Specifies the inner tag value. This field is applicable only for the NNI port. |
| MAC Type | <p>Specifies the MAC type. The supported values are.</p> <ul style="list-style-type: none"> • Static • Dynamic • Relay-Agent IPv4 • Relay-Agent IPv6 • Relay-Agent IPv4, IPv6 • PPPoE-IA • MLD/IGMP Proxy |
| Static | <p>The static MAC is configured or learned based on the MAC learning type. If the traffic goes through the PON in the service, static MAC doesn't age out. The supported values for the MAC learning type are.</p> |

Table 36. NNI Port Details (continued)

| Field | Description |
|------------------------|--|
| | <ul style="list-style-type: none"> • DHCP • DHCP_ALLOW_RELARN • ARP • ARP_ALLOW_RELARN • PPPoE • DHCP_IP_ANTISPOOFING_NO_MAC • DHCP_IP_ANTISPOOFING_MAC • DHCP_NO_MAC • ARP_NO_MAC <p> Note: In the service configuration with DHCP or DHCP_NO_MAC MAC learning type, the service-get reports only the last learned MAC address and IP address. If the service is configured on the VEIP or IPHost port of the ONT, this information indicates the WAN interface of the ONT. Otherwise, it indicates the client device behind the ONU when the service is configured on the PPTP port.</p> <p>For more information about the MAC Learning Type, see Table 268: MAC Learning Type (on page 580).</p> |
| Dynamic | A MAC is displayed as dynamic when MAC is learned by the data path of the OLT. |
| Relay-Agent IPv4 | The MAC address is learnt at relay-agent when DHCPv4 cycle is in progress. |
| Relay-Agent IPv6 | The MAC address is learnt at relay-agent when DHCPv6 cycle is in progress. |
| Relay-Agent IPv4, IPv6 | The MAC address is learnt at relay-agent when DHCPv4 and DHCPv6 cycle is in progress. |
| PPPoE-IA | The MAC address is learnt by the PPPoE intermediate agent where the PPPoE session establishment is in progress. |
| MLD/IGMP PROXY | Specifies the MAC address of the multicast router or proxy running on the BNG network learnt at NNI. |
| MAC Address | Specifies the MAC address. |
| Creation time | Specifies the date and time when the MAC dump was created. |

Live KPIs

Perform the following steps to monitor the Live KPIs.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the NNI port name (for example, NNI-6) to view the PON port details.

The PON port details page appears.

6. Click the **Live KPIs** tab.

You can view the Live KPIs of the NNI port.

NNI Port Live KPIs for Data Packets

The NNI port performance helps to monitor the usage of network, the type of packets transiting the network, and consuming the network resources.

The following table shows the description of fields of the NNI port live KPIs.

Table 37. NNI Port Live KPIs

| Field | Description |
|----------------------|--|
| Rx Data Rate (Mbps) | Specifies the upstream NNI port data received rate in Mbps. |
| Tx Data Rate (Mbps) | Specifies the downstream NNI port data transmit rate in Mbps. |
| Rx Utilization (%) | Specifies the received upstream port utilization in percentage. |
| Tx Utilization (%) | Specifies the transmitted downstream port utilization in percentage. |
| Rx Bytes | Specifies the total number of upstream bytes received. |
| Tx Bytes | Specifies the total number of NNI port downstream bytes transmitted. |
| Rx Broadcast Packets | Specifies the total number of NNI port upstream broadcast packets received. |
| Tx Broadcast Packets | Specifies the total number of NNI port downstream broadcast packets transmitted. |
| Rx Error Packets | Specifies the number of NNI port upstream packets that shows error while receiving the packets. |
| Tx Error Packets | Specifies the number of NNI port downstream packets that shows error while transmitting the packets. |

Table 37. NNI Port Live KPIs (continued)

| Field | Description |
|----------------------|--|
| Rx Multicast Packets | Specifies the total number of NNI port upstream multicast packets received. |
| Tx Multicast Packets | Specifies the total number of NNI port downstream multicast packets transmitted. |
| Rx Unicast Packets | Specifies the total number of upstream unicast packets received. |
| Tx Unicast Packets | Specifies the total number of downstream unicast packets transmitted. |
| Rx FCS Error Packets | Specifies the number of FCS error packets received. |

NNI Port Live KPIs for Control Packets

The NNI port performance helps to monitor the usage of network, the type of packets transiting the network, and consuming the network resources.

The following table shows the description of fields of the NNI port live KPIs control packets.

Table 38. NNI Port Live KPIs Control Packets

| Field | Description |
|---------------|---|
| PPPoE | |
| PADI | Specifies the PPPoE initiation packets received. |
| PADO | Specifies the PPPoE offer packets received. |
| PADR | Specifies the PPPoE request packets received. |
| PADS | Specifies the PPPoE session packets received. |
| PADT | Specifies the PPPoE termination packets received. |
| DHCPv4 | |
| Discover | Specifies the DHCP discover packets received. |
| Offer | Specifies the DHCP offer packets received. |
| Request | Specifies the DHCP request packets received. |
| Ack | Specifies the DHCP ack packets received. |
| Release | Specifies the DHCP release packets received. |
| Nak | Specifies the DHCP nak packets received. |

Table 38. NNI Port Live KPIs Control Packets (continued)

| Field | Description |
|---------------------|--|
| Decline | Specifies the DHCP decline packets received. |
| Inform | Specifies the DHCP inform packets received. |
| DHCPv6 | |
| Solicit | Specifies the DHCPv6 solicit packets received. |
| Advertise | Specifies the DHCPv6 advertise packets received. |
| Request | Specifies the DHCPv6 request packets received. |
| Reply | Specifies the DHCPv6 reply packets received. |
| Release | Specifies the DHCPv6 release packets received. |
| Renew | Specifies the DHCPv6 renew packets received. |
| Rebind | Specifies the DHCPv6 rebind packets received. |
| Confirm | Specifies the DHCPv6 confirm packets received. |
| Decline | Specifies the DHCPv6 decline packets received. |
| Reconfigure | Specifies the DHCPv6 reconfigure packets received. |
| Information Request | Specifies the DHCPv6 information request packets received. |
| Relay Forward | Specifies the DHCPv6 relay forward packets received. |
| Relay Reply | Specifies the DHCPv6 relay reply packets received. |

Historical KPIs

Perform the following steps to monitor the Live KPIs.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the NNI port name (for example, NNI-6) to view the NNI port details.

The NNI port details page appears.

6. Click the **Historical KPIs** tab.

You can view the historical KPIs of the NNI port.

NNI Port Historical KPIs

You can view the graphical view of the NNI port KPIs by one day, one week, one month, daily, and hourly. You can also view the NNI port KPIs for a particular duration using the **Custom** option.

You can select a data packet or control packet from the option for which you want to view the historical information. For data packets, you can select the upstream and downstream KPI parameter from the list for which you want to view the historical information.

The graphical view of the NNI port historical KPIs information is generated based on the periodic interval and the KPI parameter that you have selected.



Note: If you select one option from the list, the second list dynamically populates the relevant data based on the first option. To view all options in the list, deselect the option in the list.

The following table describes the NNI port data packet KPI parameters.

Table 39. NNI Port Data Packet Historical KPIs

| Field | Description |
|------------------------|---|
| Downstream KPIs | |
| Rx Data Rate | Specifies the upstream NNI port received data rate. The unit is in bytes per second. |
| Rx Utilization | Specifies the upstream NNI port received data utilization. The unit is in percentage. |
| Rx Bytes | Specifies the upstream NNI port received in bytes. The unit is in bytes. |
| Rx Unicast Packets | Specifies the upstream NNI port received unicast packets. The unit is in packet count. |
| Rx Multicast Packets | Specifies the upstream NNI port received multicast packets. The unit is in packet count. |
| Rx Broadcast Packets | Specifies the upstream NNI port received broadcast packets. The unit is in packet count. |
| Rx Error Packets | Specifies the upstream NNI port received error packets. The unit is in packet count. |
| Rx Fcs Error Packet | Specifies the upstream NNI port received FCS error packets. The unit is in packet count. |

Table 39. NNI Port Data Packet Historical KPIs (continued)

| Field | Description |
|------------------------------|--|
| Rx Packets Dropped | Specifies the upstream NNI port dropped error packets. The unit is in packet count. |
| Rx FEC Codewords | Specifies the received forward error correction (FEC) codewords. |
| Rx BIP Units | Specifies the received units protected by BIP. |
| Rx BIP Errors | Specifies the received BIP errors. |
| Rx GEM | Specifies the received GEM frames. |
| Rx GEM Dropped | Specifies the received dropped GEM frames dead due disabled GEM port ID. |
| Rx GEM Idle | Specifies the received idle GEM frames. |
| Rx GEM Corrected | Specifies the received GEM frames with a header error control (HEC) error that was corrected. |
| Rx GEM Fragmented Errors | Specifies the received packets dropped due to GEM fragmentation error. |
| Rx Dropped Packets Too Short | Specifies the received packets that were dropped due to length being too short. |
| Rx Dropped Packets Too Long | Specifies the received packets that were dropped due to length being too long. |
| Rx Key Errors | Specifies the received packets dropped due to key error. Key error occurs when using an invalid key to decrypt data. |
| Rx Allocations Valid | Specifies the received valid bandwidth allocation bursts. |
| Rx Allocations Invalid | Specifies the received invalid bandwidth allocation, due to incorrect bandwidth map. |
| Rx Allocations Disabled | Specifies the received and discarded bandwidth allocations for disabled AllocID. |
| Rx Ploams | Specifies the received PLOAMs. |
| Rx Ploams Non Idle | Specifies the received non idle PLOAMs. |
| Rx Ploams Dropped | Specifies the received PLOAMs that were dropped, due to full PLOAM queue. |
| Rx Ploams Error | Specifies the received PLOAMs with CRC error. |
| Rx CPU | Specifies the received packets that were forwarded to the CPU queue. |

Table 39. NNI Port Data Packet Historical KPIs (continued)

| Field | Description |
|-----------------------------|--|
| Rx OMCI | Specifies the received packets that were forwarded to the OMCI queue. |
| Rx OMCI Packets CRC Errors | Specifies the received OMCI packets with CRC errors. |
| Rx XGTC Headers | Specifies the received valid XGTC headers. |
| Rx XGTC Corrected | Specifies the received corrected XGTC headers. |
| Rx XGTC Uncorrected | Specifies the received uncorrected XGTC headers. |
| Rx Fragment Errors | Specifies the received packets dropped due to fragmentation errors. |
| Upstream KPIs | |
| Tx Bytes | Specifies the downstream NNI port transmit. The unit is in bytes. |
| Tx Unicast Packets | Specifies the downstream NNI port transmit unicast packets. The unit is in packet count. |
| Tx Multicast Packets | Specifies the downstream NNI port transmit multicast packets. The unit is in packet count. |
| Tx Broadcast Packets | Specifies the downstream NNI port transmit broadcast packets. The unit is in packet count. |
| Tx Error Packets | Specifies the downstream NNI port transmit error packets. The unit is in packet count. |
| Tx Data Rate | Specifies the downstream NNI port transmit data rate. The unit is in bytes per second. |
| Tx Utilization | Specifies the downstream NNI port transmit data utilization. The unit is in percentage. |
| Tx Ploams | Specifies the upstream PLOAMs. |
| Tx GEM | Specifies the upstream GEM frames. |
| Tx CPU | Specifies the upstream CPU packets. |
| Tx OMCI | Specifies the upstream OMCI packets. |
| Tx CPU OMCI Packets Dropped | Specifies the upstream CPU OMCI packets dropped, due to illegal length. |
| Tx Dropped Illegal Length | Specifies the upstream packets dropped, due to illegal length. |

Table 39. NNI Port Data Packet Historical KPIs (continued)

| Field | Description |
|----------------------|--|
| Tx Dropped TPID Miss | Specifies the packets received from the NNI dropped due to TPID miss. |
| Tx Dropped VID Miss | Specifies the upstream packets dropped, due to VID miss. |
| Tx Dropped Packets | Specifies the downstream NNI port dropped error packets. The unit is in packet count. |

The following table shows the description of NNI port control packet KPI parameters.

Table 40. NNI Port Control Packet Historical KPIs

| Field | Description |
|--------|---|
| PPPoE | Specifies the historical KPIs for PPPoE control packets. |
| DHCPv4 | Specifies the historical KPIs for DHCPv4 control packets. |
| DHCPv6 | Specifies the historical KPIs for DHCPv6 control packets. |

NNI Port Packet Size Based KPIs

The NNI port packet size performance helps to monitor the usage of network, the type of packets transiting the network, and consuming the network resources.

The following table shows the description of the NNI port KPI parameters.

Table 41. NNI Port Packet Size Based KPIs

| Field | Description |
|--------------------------|--|
| Tx Packets 64 Bytes | Specifies the upstream NNI port transmit packets of size 64 bytes. The unit is in packet count. |
| Rx Packets 64 Bytes | Specifies the downstream NNI port received packets of size 64 bytes. The unit is in packet count. |
| Tx Packets 65-127 Byte | Specifies the upstream NNI port transmit packets of size between 65-127 bytes. The unit is in packet count. |
| Rx Packets 65-127 Bytes | Specifies the downstream NNI port received packets of size between 65-127 bytes. The unit is in packet count. |
| Tx Packets 128-255 Bytes | Specifies the upstream NNI port transmit packets of size between 128-255 bytes. |

Table 41. NNI Port Packet Size Based KPIs (continued)

| Field | Description |
|----------------------------|---|
| | The unit is in packet count. |
| Rx Packets 128-255 Bytes | Specifies the downstream NNI port received packets of size between 128-255 bytes. The unit is in packet count. |
| Tx Packets 256-511 Bytes | Specifies the upstream NNI port transmit packets of size between 256-511 bytes. The unit is in packet count. |
| Rx Packets 256-511 Bytes | Specifies the downstream NNI port received packets of size between 256-511 bytes. The unit is in packet count. |
| Tx Packets 512-1023 Byte | Specifies the upstream NNI port transmit packets of size between 512-1023 bytes. The unit is in packet count. |
| Rx Packets 512-1023 Bytes | Specifies the downstream NNI port received packets of size between 512-1023 bytes. The unit is in packet count. |
| Tx Packets 1024-1518 Bytes | Specifies the upstream NNI port transmit packets of size between 1024-1518 bytes. The unit is in packet count. |
| Rx Packets 1024-1518 Bytes | Specifies the downstream NNI port received packets of size between 1024-1518 bytes. The unit is in packet count. |
| Tx Packets 1519-2047 Bytes | Specifies the upstream NNI port transmit packets of size between 1519-2047 bytes. The unit is in packet count. |
| Rx Packets 1519-2047 Bytes | Specifies the downstream NNI port received packets of size between 1519-2047 bytes. The unit is in packet count. |
| Tx Packets 2048-4095 Bytes | Specifies the upstream NNI port received packets of size between 2048-4095 bytes. The unit is in packet count. |
| Rx Packets 2048-4095 Bytes | Specifies the downstream NNI port received packets of size between 2048-4095 bytes. The unit is in packet count. |

Table 41. NNI Port Packet Size Based KPIs (continued)

| Field | Description |
|-----------------------------|--|
| Tx Packets 4096-9216 Bytes | Specifies the upstream NNI port transmit packets of size between 4096-9216 bytes. The unit is in packet count. |
| Rx Packets 4096-9216 Bytes | Specifies the downstream NNI port received packets of size between 4096-9216 bytes. The unit is in packet count. |
| Tx Packets 9217-16383 Bytes | Specifies the upstream NNI port transmit packets of size between 9217-16383 bytes. The unit is in packet count. |
| Rx Packets 9217-16383 Bytes | Specifies the downstream NNI port received packets of size between 9217-16383 bytes. The unit is in packet count. |

Clear NNI Port KPIs

RMS supports clearing the live KPI subscription of the NNI ports and resetting the counters to zero. This enables fresh debugging by resetting the counters to zero and starting to get the live KPIs incrementally. You can clear the KPI counters only when the NNI port admin state is ENABLED, and the operational state is UP.

After clearing the live NNI port KPIs, CBAC resets the counters to zero and incrementally generates KPIs for towards RMS for debugging.

To clear the NNI port KPI counters, click **Clear KPI** option from the right-hand side of the page.



Note: You can clear the live KPIs only when the **LIVE KPI** option is ON.

Exporting NNI Port Historical KPIs

You can export the NNI port historical KPIs. You can view and analyze the exported KPIs list, as needed.

You can export the following KPIs.

- Historical KPIs (Data Packet or Control Packet)
- Historical KPIs (Packet based)
- VLAN Historical KPIs

Perform the following steps to export the NNI port KPIs.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name.

The OLT Details page appears.

4. Navigate to the **Port** tab.
5. Click on the NNI port.

The NNI Port Details page appears.

6. Click **Export** from the historical KPIs page.

The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file in a Microsoft Excel sheet. Optionally, you can save this file on your PC for later use.

The downloaded file contains the attributes based on the KPI parameters that you have selected.

Alarms

Perform the following steps to monitor the alarms.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the NNI port name (for example, NNI-6) to view the PON port details.

The NNI port details page appears.

6. Click the **Alarms** tab.

You can view the list of current and cleared faults reported for the NNI port.

For more information on the field descriptions, see [Table 42: Alarm List \(on page 115\)](#).

Events

Perform the following steps to monitor the events.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the NNI port name (for example, NNI-6) to view the PON port details.

The PON port details page appears.

6. Click the **Events** tab.

You can view the list of events reported for the NNI port.

For more information on the field descriptions, see [Table 43: Events List \(on page 117\)](#).

Activity Log

Perform the following steps to monitor the Activity Log.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the NNI port name (for example, NNI-6) to view the PON port details.

The PON port details page appears.

6. Click the **Activity Log** tab.

You can view the activity log generated for the NNI port.

For more information on the field descriptions, see [Table 44: Activity Logs \(Tabular View\) \(on page 119\)](#).

LAG

Perform the following steps to monitor the LAG.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the NNI port name (for example, NNI-6) to view the PON port details.

The PON port details page appears.

6. Click the **LAG** tab.

You can view the LAG details of the NNI port.

For more information on the field descriptions, see [LAG Details \(on page 135\)](#).

Eline

Perform the following steps to monitor the Eline.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the NNI port name (for example, NNI-6) to view the PON port details.

The PON port details page appears.

6. Click the **Eline** tab.

You can view the the activity log generated for the Eline configuration.

For more information on the field descriptions, see [ELine \(on page 143\)](#).

ELAN

Perform the following steps to monitor the ELAN.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the NNI port name (for example, NNI-6) to view the PON port details.

The PON port details page appears.

6. Click the **ELAN** tab.

You can view the activity log generated for the ELAN configuration.

For more information on the field descriptions, see [ELAN \(on page 146\)](#).

Ring

Perform the following steps to monitor the ring.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click the **Ports** tab.
5. Click on the NNI port name (for example, NNI-6) to view the PON port details.

The PON port details page appears.

6. Click the **Ring** tab.

You can view the activity log generated for the ring configuration.

For more information on the field descriptions, see [Ring \(on page 214\)](#).

Exporting Faults, Events, and Logs (PON or NNI)

You can export the following information associated with the PON or NNI port.

- Events, current and cleared faults reported for the PON or NNI port
- Activity logs generated for the PON or NNI port

Perform the following steps to export the faults, events, and activity logs.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name.
4. Click on the **Port/Faults/Events/Logs** tab.

5. Click **Export**.

The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file in a Microsoft Excel sheet.

Alarm

Perform the following steps to view the list of current and cleared alarms reported for the OLT.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.

3. Click on the OLT name.

The OLT Details page appears.

4. Navigate to the **Alarms** tab.

Enable the **Shorten Row Height** option to shorten the height of table entries.

The following table shows the description of fields on the Alarm List page.

Table 42. Alarm List

| Field | Description |
|--------------------------|---|
| Severity | Specifies the severity (WARNING, MAJOR, MINOR, or CRITICAL) of the alarm. Example: WARNING |
| First Occurrence Time | Specifies the date and time when the fault was raised the first time in a human-readable format, that is, MMM DD,YYYY, HH:MM:SS PM. Example: May 18, 2021, 2:26:53 PM |
| Last Occurrence Time | Specifies the date and time when the fault was raised the last time in a human-readable format, that is, MMM DD,YYYY, HH:MM:SS PM. Example: May 18, 2021, 2:26:53 PM |
| Device Reported Time | Specifies the time and date when the fault was reported by the device in a human-readable format, that is, MMM DD,YYYY, HH:MM:SS PM. Example: Sep 20, 2022, 2:26:53 PM |
| Controller Reported Time | Specifies the time and date when the fault was reported by the controller in a human-readable format, that is, MMM DD,YYYY, HH:MM:SS PM. Example: Sep 20, 2022, 2:26:53 PM |
| Fault | Specifies the name of the alarm. Example: HIGH-TEMPERATURE |

Table 42. Alarm List (continued)

| Field | Description |
|-----------------------|---|
| Site | Specifies the site of the OLT. |
| Parent Site | Specifies the parent site name. |
| Error Code | Specifies the error code of the fault. |
| Controller Alarm Code | Specifies the name of the alarm in the CBAC controller. Example: OLT-HIGH-TEMPERATURE |
| Entity | Specifies the name of the entity for which the alarm is reported. Example: OLT |
| ID | Specifies the type of resource. Example: OLT |
| Type | Specifies the type of resource. The supported values are. <ul style="list-style-type: none"> OLT ONT ME_PORT LAG SERVICE SUBSCRIBER |
| Data | Specifies the payload information about the alarm. Example: <pre>{ "member_ports": ["767f1060-851c-11ec-a109-22bd08c77f08-76-ETHERNET-3"], "CONTROLLER-FAULT": "OLT-ETHERNET-LAG-DOWN" }</pre> |

Purge and Fetch

You must use the purge and fetch alarms only in the following scenarios to remove old entries and get a current snapshot of active alarms from CBAC.

- OLT Replacement
- OLT Redeployment
- RMS restore from the backup file

You can perform **Purge and Fetch** for all active alarms, such as OLT, Ports, ONT, Controller, Service, Subscriber, LAG, and so on. This operation deletes all active alarms at RMS and fetches the active alarms from CBAC and builds at RMS.

Perform the following steps to purge and fetch the current faults.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name.

The OLT Details page appears.

4. Click on the **Alarms > Current**.
5. Click **Alarm Purge and Fetch**.

Alarms related to OLT (OLT, ONT, Port, LAG, Subscriber, Service, and so on) are displayed in the **Current** page. However, the controller alarms associated with the specific OLT are deleted from the purge and fetch and can be viewed in the **Monitor > Controller > Controller Details > Alarms**.

Events

Perform the following steps to monitor the events.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Select the **Events** tab.

You can view the list of events reported for the OLT.

Enable the **Shorten Row Height** option to shorten the height of table entries.

The following table shows the description of fields on the Events List page.

Table 43. Events List

| Field | Description |
|-------------|--|
| Event Code | Specifies the event code. Example: ME-LOGIN-SUCCESS |
| Entity | Specifies the name of the entity. Example: olt-185 |
| Entity ID | Specifies the ID of the entity. Example: olt185 |
| Entity Type | Specifies the type of resource. |

Table 43. Events List (continued)

| Field | Description |
|--------------------------|---|
| | Example: OLT |
| Error Code | Specifies the error code of the event. |
| EMS Reported Time | Specifies the time and date when the event was reported by EMS in a human-readable format, that is, MMM DD,YYYY, HH:MM:SS PM. Example: May 18, 2021, 2:26:53 PM |
| Device Reported Time | Specifies the time and date when the event was reported by the device in a human-readable format, that is, MMM DD,YYYY, HH:MM:SS PM. Example: May 18, 2021, 2:26:53 PM |
| Controller Reported Time | Specifies the time and date when the event was reported by the controller in a human-readable format, that is, MMM DD,YYYY, HH:MM:SS PM. Example: May 18, 2021, 2:26:53 PM |
| Data | Specifies the payload information about the event. Example: <pre>{ "user_ip": "172.27.174.111", "user_name": "admin", "SDPON-EVENT": "OLT-LOGIN-SUCCESS" }</pre> |

Logs

Perform the following steps to monitor the logs.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Select the **Logs** tab.

You can view the following type of logs for the OLT.

- **Activity Logs.** Logs generated for the activities performed on the OLT such as part activation, OLT deactivation, and so on. You can view the activity logs in the following format.
 - **Tabular View.** Represents the data in a tabular format.

The following table shows the description of fields on the Logs page.

Table 44. Activity Logs (Tabular View)

| Field | Description |
|-----------------|--|
| Time | Specifies the date and time when the activity was performed. |
| Activity | Specifies the name of the activity performed on the resource. Example: PORT-ACTIVATED |
| Name | Specifies the name of the entity on which the action was performed. Example: nni5 |
| Triggered By | Specifies the name of the entity that triggered the action. Example: EVENT |
| User Name | Specifies the username of the user who performed the action. Example: admin |
| IP Address | Specifies the IP address of the computer from which the user initiated the task. Example: 172.24.40.191 |
| Event Detail | Click to view the event details. |
| Fault Detail | Click to view the fault details. |
| Additional Info | View additional information about the activity log. |

- **Timeline View.** Represents the data in a graphical view.
- **Audit Logs.** List of logs triggered for the operations performed on the OLT. For more information on the field descriptions, see [Table 102: Audit Log List \(on page 230\)](#).

Card List

Perform the following steps to monitor the card list.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Select the **Card List** tab.

You can view the list of cards associated with the OLT.

The following table shows the description of fields on the Card List page.

Table 45. Card List

| Field | Description |
|-------|---------------------------------|
| Name | Specifies the name of the card. |

Table 45. Card List (continued)

| Field | Description |
|-------------------------|---|
| Type | Specifies the type of the managed element. Example: CARD |
| Display ID | Specifies the display ID of the card. Example: rack=1/shelf=1/slot=LT-1 |
| Row | Specifies the number of rows in the card. Example: 3 |
| Cols | Specifies the number of columns in the card. Example: 23 |
| Severity | Specifies the severity of the card. The supported values are. <ul style="list-style-type: none"> • WARNING • CRITICAL • MAJOR • MINOR • NO FAULT |
| Creation Time | Specifies the date and time when the card was created. |
| Technology Capabilities | Specifies the technology supported by card profile. For example, GPON or XGSPON. The default value is GPON. |

ONT List

Perform the following steps to monitor the ONT list.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Select the **ONT List** tab.

You can view the following type of ONTs.

- **ONT.** Specifies the list of ONTs connected to the OLT. For more information, see [Table 46: ONT \(on page 121\)](#).
- **Blacklisted ONT.** Specifies the list of blacklisted ONTs. For more information, see [Table 47: Blacklisted ONT \(on page 123\)](#).

The following table shows the description of fields on the ONT page.

Table 46. ONT

| Field | Description |
|-------------------|---|
| Name | Specifies the name of the ONT. |
| Fault State | Specifies the highest severity fault present on the ONT. The supported states are. <ul style="list-style-type: none"> • WARNING • CRITICAL • MAJOR • MINOR • NO FAULT |
| Admin State | Specifies the admin state of the ONT. <ul style="list-style-type: none"> • Green. Indicates that the admin state of the ONT is enabled. • Red. Indicates that the admin state of the ONT is disabled. |
| Operational State | Specifies the operational state of the ONT. <ul style="list-style-type: none"> • Green. Indicates that the operational state of the ONT is UP. • Red. Indicates that the operational state of the ONT is DOWN. |
| Make | Specifies the vendor name who manufactures the ONT. |
| Model | Specifies the model name of the ONT. |
| Technology | Specifies the technology used by SFP. |
| Display Id | Specifies display ID of the ONT. |
| Serial No. | Specifies the serial number of the ONT. |
| Serial No. Status | Specifies the status of the ONT. |
| Device Profile | Specifies the name of the ONT device profile. |
| Management Domain | Specifies the name of the management domain. |
| Controller | Specifies the name of the controller. |
| Alarm Profile | Specifies the alarm profile configured for the ONT. |
| OLT | Specifies the OLT name to which the ONT is connected. |
| Port | Specifies the OLT port. |
| Registration Id | Specifies the registration ID of the ONT. |
| Vendor Id | Specifies the vendor ID of the ONT. |

Table 46. ONT (continued)

| Field | Description |
|-------------------------------|--|
| Equipment Id | Specifies the equipment ID of the ONT. |
| Up Since Time | Specifies the date and time from when the ONT is UP. |
| ONT Firmware Upgrade Status | Specifies the ONT firmware upgrade status on the OLT. The supported values are: <ul style="list-style-type: none"> NOT-DOWNLOADED DOWNLOAD-INITIATED DOWNLOAD-FAILED DOWNLOAD-SUCCESSFUL ACTIVATE-INITIATED ACTIVATION-FAILED ACTIVATE-SUCCESSFUL COMMIT-INITIATED COMMIT-FAILED COMMIT-SUCCESSFUL CANCEL-UPGRADE-INITIATED CANCEL-UPGRADE-SUCCESSFUL CANCEL-UPGRADE-FAILED UPGRADED UPGRADE-FAILED |
| ONT Firmware Version | Specifies the current version of the ONT firmware. |
| ONT Firmware Download Version | Specifies the firmware version of the ONT that was downloaded. |
| Hardware Version | Specifies the hardware version of the ONT. |
| Active Firmware Version | Specifies the firmware version of the active ONT. |
| Standby Firmware Version | Specifies the firmware version of the standby ONT. |
| Connectivity Mode | Specifies the connectivity model that must be used for the services on the ONU. |
| ME Group | Specifies the managed element group to which the ONT belongs to. |
| ONT Number | Specifies the ONT number. |
| ONT Physical Distance (in km) | Specifies the physical distance of an ONT from the PON port of the OLT. |

Table 46. ONT (continued)

| Field | Description |
|---------------------------|--|
| Upstream FEC | Specifies whether Forward Error Correction (FEC) is enabled in the upstream traffic. |
| Rx Optical Power (in dBm) | Specifies the current measurement of the optical received power level. |
| MAC Ageing Time | Specifies the maximum time an ONT can hold a MAC entry in the MAC table when there is no data received from the device. |
| MAC Limit | Specifies the MAC learning depth attribute of the ME MAC bridge service profile on the ONU. |
| Planned Firmware Version | Specifies the expected firmware version of the ONT when the ONT is discovered. |
| Auto Upgrade | Specifies whether the ONU is upgraded with the firmware version mentioned in the ONT Firmware Version Table when the CBAC detects that the firmware version does not match the version mentioned in the table. The supported values are. <ul style="list-style-type: none"> • True. Initiates the auto upgrade if the ONT firmware version mentioned in the RMS does not match the version mentioned in the CBAC. • False. Auto upgrade is disabled if you select the false filed. |
| DBA Type | Selects the DBA type to be used for ONTs that are created for the ONUs for services. The supported values are. <ul style="list-style-type: none"> • NSR • SR The default value is NSR. If ONU does not support the value SR, CBAC defaults to the value NSR internally. The user can see the supported DBA type modes in ONU Monitoring capability. |
| Creation Time | Specifies the date and time when the ONT was created. |

The following table shows the description of fields on the blacklisted ONT page.

Table 47. Blacklisted ONT

| Field | Description |
|------------|---|
| Serial No. | Specifies the serial number of the blacklisted ONT. |
| OLT Name | Specifies the name of the OLT. |

Table 47. Blacklisted ONT (continued)

| Field | Description |
|--------------------------|---|
| OLT Serial No. | Specifies the serial number of the OLT. |
| OLT Port | Specifies the OLT port number. |
| Registration Id | Specifies the registration ID of the blacklisted ONT. |
| Vendor Id | Specifies the vendor ID of the blacklisted ONT. |
| Equipment Id | Specifies the equipment ID of the blacklisted ONT. |
| Active Firmware Version | Specifies the firmware version of the active ONT. |
| Standby Firmware Version | Specifies the firmware version of the standby ONT. |
| Creation Time | Specifies the date and time when the blacklisted ONT was created. |

Services

Perform the following steps to monitor the services.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Select the **Services** tab.

You can view the list of subscriber services associated with the OLT.

The following table shows the description of fields on the Services page.

Table 48. Services

| Field | Description |
|-------------------|--|
| Service Name | Specifies the name of the service. |
| Template Name | Specifies the name of the service template. |
| Admin State | Specifies the admin state of the service. <ul style="list-style-type: none"> • Green. Indicates that the admin state of the service is ACTIVE. • Red. Indicates that the admin state of the service is DEACTIVE. |
| Operational State | Specifies the operational state of the service. <ul style="list-style-type: none"> • Green. Indicates that the operational state of the service is UP. • Red. Indicates that the operational state of the service is DOWN. |

Table 48. Services (continued)

| Field | Description |
|-------|---|
| Time | Specifies the date and time when the service was created. |

ONT Alarms

Perform the following steps to monitor the ports.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Select the **ONT Alarms** tab.

You can view the list of alarms reported for the ONT.

The following table shows the description of fields on the ONT Alarms page.

Table 49. ONT Alarms

| Field | Description |
|-----------------------|---|
| Severity | Specifies the severity (WARNING, MAJOR, MINOR, or CRITICAL) of the alarm. Example: MINOR |
| First Occurrence Time | Specifies the date and time when the fault was raised the first time in a human-readable format, that is, MMM DD, YYYY, HH:MM:SS PM. Example: May 18, 2021, 2:26:53 PM |
| Last Occurrence Time | Specifies the date and time when the fault was raised the last time in a human-readable format, that is, MMM DD, YYYY, HH:MM:SS PM. Example: May 18, 2021, 2:26:53 PM |
| Fault Code | Specifies the name of the alarm. Example: UNKNOWN-ME-DISCOVERED |
| Entity | Specifies the name of the entity. Example: ONT |
| Site | Specifies the site of the ONT. |
| Parent Site | Specifies the parent site name. |
| Entity Id | Specifies the ID of the entity. Example: 78c512b7a50efab1415242b7 |
| Type | Specifies the type of resource. Example: ONT |
| Data | Specifies the payload information about the alarm. |

Table 49. ONT Alarms (continued)

Device View

OLT device view is created based on the device profile (the number of slots and the layout type) that you have created for the OLT, for more information, see [Creating OLT Device Profile \(on page 509\)](#).

Perform the following steps to monitor the device view.

1. Select **Monitor > Inventory > Inventory**.
 2. Click on the **OLT** tab and select the applicable OLT.
 3. Click **More > Device View**.

The OLT Device view page appears.

The following figure shows the horizontal view of the 1600C OLT.

Figure 24. OLT Device View 1600C



The following figure shows the horizontal view of the 1600G OLT.

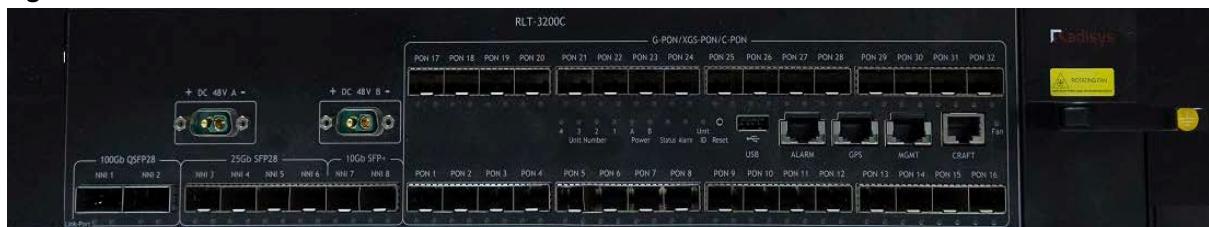
Figure 25. OLT Device View 1600G



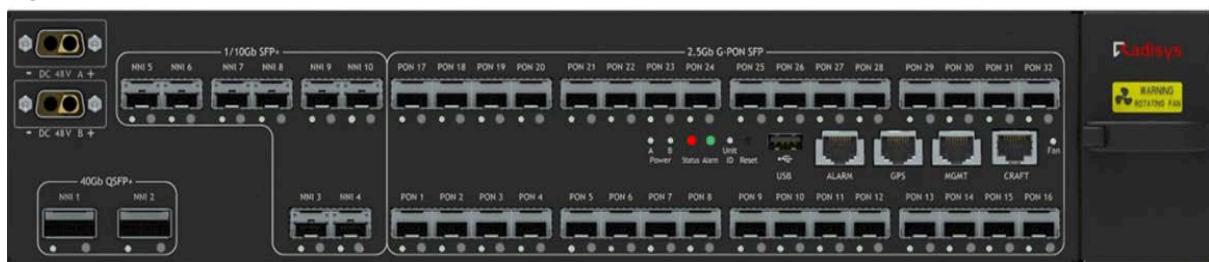
The following figure shows the horizontal view of the 1600X OLT.

Figure 26. OLT Device View 1600X

The following figure shows the horizontal view of the 3200C OLT.

Figure 27. OLT Device View 3200C

The following figure shows the horizontal view of the 3200G OLT.

Figure 28. OLT Device View 3200G

OLT Live KPIs

CBAC reports live KPIs of the OLT to RMS. You can view the real-time performance data of the OLT.

Perform the following steps to view the OLT live KPIs.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Click **More > Live KPI's**.

The OLT Live KPI page appears.

- **CPU Utilization (%)**. Specifies the total CPU utilization of the OLT (in percentage) along with the core CPU utilization. The unit is in percentage.
- **Disk Utilization(%)**. Specifies the total disk utilization of the OLT. The unit is in percentage.
- **Memory Utilization (%)**. Specifies the memory utilization of the OLT. The unit is in percentage.
- **Fan Speed (rpm)**. Specifies the list of OLT fans and each fan's name, fan speed, utilization, model, description, and status.
- **Thermal Sensor (degree)**. Specifies the OLT thermal sensor information.
- **Power Consumption (Watts)**. Specifies the OLT power consumption information.

Live KPI Settings

You can turn on or turn off the retrieval of live KPIs using the **Live KPI ON** or **Live KPI OFF** button.

A **Settings** pop-up icon appears when you mouse over the **Live KPI** option. The following fields are displayed.

- **Time (sec).** Specifies the periodicity of the reporting KPIs based on the interval time. The value ranges from 10 seconds to 3600 seconds.
- **Duration (minutes).** Specifies the duration for which the KPI subscription is valid. The default value is 60 minutes, and the value ranges from 5 minutes to 60 minutes.
- **Counter Type.** Specifies the counter type configuration for the live KPI counters reported for the OLT. The default value is ABSOLUTE.
 - **ABSOLUTE.** Enables the operators to receive the actual KPI values for each refresh interval.
 - **CUMULATIVE.** Enables the operators to receive the KPI values in a cumulative fashion, that is, from the beginning of the subscription (starting from 0).

Historical KPIs

CBAC reports historical KPIs for the OLT side utilization of the PON port. The KPI reporting interval is 15 minutes by default. You can view the OLT performance data within a period. This allows to achieve fast and comprehensive analysis of the OLT performance. You can view the following historical performance data for the OLT.

Perform the following steps to view the OLT historical KPIs.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Click **More > Historical KPI's**.

The OLT Historical KPI page appears.



Note: If you select one option from the list, the second list dynamically populates the relevant data based on the first option. To view all options in the list, deselect the option in the list.

- CPU Utilization
- Disk Utilization
- Memory Utilization
- Thermal Sensor (Degree Celsius)
- Fan Inventory
- IGMP Stats
- Temperature Thresholds
- Bandwidth Profile Ref Count

- Shaper Profile Ref Count
- Power

CPU Utilization

The following figure shows the graphical view of the OLT CPU utilization (%) by one day, one week, one month, hourly, and daily.

You can also view the CPU utilization of the OLT for a particular duration using the **Custom** option.

Disk Utilization

The following figure shows the graphical view of the OLT disk utilization (%) by one day, one week, one month, hourly, and daily.

You can also view the disk utilization of the OLT for a particular duration using the **Custom** option.



Note: You can select a particular partition name from the list to view the disk utilization.

Memory Utilization

The following figure shows the graphical view of the OLT memory utilization (%) by one day, one week, one month, hourly, and daily.

You can also view the memory utilization of the OLT for a particular duration using the **Custom** option.

OLT Thermal Sensor

The following figure shows the graphical view of the thermal sensor by one day, one week, one month, hourly, and daily.

You can also view the information on thermal sensor of the OLT for a particular duration using the **Custom** option.

The following are the supported thermal sensors.

- CPU
- MB_TMP435_1_LOCAL
- MB_TMP435_1_REMOTE_ASSEN
- MB_TMP435_2_LOCAL
- MB_TMP435_2_REMOTE_AIR_INLET
- MB_TMP435_3_LOCAL
- MB_TMP435_3_REMOTE_SWC
- DB_TMP435_1_LOCAL
- DB_TMP435_1_REMOTE_ASSEN
- DB_TMP435_2_LOCAL

- DB_TMP435_2_REMOTE
- TEMP_ASPIRE_CHIP_1
- TEMP_ASPIRE_CHIP_2

Fan Inventory

The following figure shows the graphical view of the fan inventory by one day, one week, one month, hourly, and daily.

You can also view the information on fan inventory of the OLT for a particular duration using the **Custom** option.

The following KPIs are supported for the fan.

- **SPEED.** Specifies the fan speed per fan unit (instance_id) of the OLT. The unit is in RPM (Rotation per minute).
- **UTILIZATION.** Specifies the current fan speed with respect to the maximum fan speed of the OLT. The unit is in percentage.

IGMP Statistics

The following figure shows the graphical view of the IGMP stats by one day, one week, one month, hourly, and daily.

You can also view the information on IGMP stats of the OLT for a particular duration using the **Custom** option.

The following KPIs are supported for the IGMP.

- **Current Num Root Connections.** Specifies the total number of active connections which include static and dynamic connections.
- **Current Num Root Connections No Member.** Specifies the total number of dynamic channels that are in the reserve state.
- **Nums Connects Counter.** Specifies the total number of IGMP new successful joins that are received from the subscriber.
- **Nums Disconnects Counter.** Specifies the total number of IGMP leaves received from the subscriber which includes timer expiry and leaves (normal/ fast leave) that are received from the users.
- **Successful Join Req Counters.** Specifies the joins received from the subscriber and responds to queries.
- **Total Gmq Counters.** Specifies the total number of GMQ (General Membership Queries) counters.
- **Total Gsq Counters.** Specifies the total number of GSQ (Group Specific Queries) counters.
- **Total Gssq Counters.** Specifies the total number of GSSQ (Group and Source Specific Queries) counters.
- **Total igmp msgs Counter.** Specifies the total number of IGMP control messages counter.

Temperature Threshold

The following figure shows the graphical view of the temperature thresholds by one day, one week, one month, hourly, and daily.

You can also view the information on temperature thresholds of the OLT for a particular duration using the **Custom** option.

You can view the threshold values of each thermal sensor. Select any thermal sensor from the drop down provided, and the corresponding threshold value of that sensor is displayed.

The following KPIs are supported for the temperature threshold.

- **Tca Critical.** Specifies the critical threshold, which is configured in the alarm profile for each sensor. The unit is in degree Celsius.
- **Tca Warning.** Specifies the warning threshold, which is configured in the alarm profile for each sensor. The unit is in degree Celsius.
- **Device Shutdown.** Specifies the temperature at which the device is automatically shutdown. The unit is in degree Celsius.
- **Run Fans at full speed.** Specifies the temperature at which the fans run at full speed. The unit is in degree Celsius.

Bandwidth Profile

The following figure shows the graphical view of the bandwidth profile ref count by one day, one week, one month, hourly, and daily.

Reference count specifies the bandwidth profile count associated with the subscriber services.

You can also view the information on bandwidth profile ref count of the OLT for a particular duration using the **Custom** option.

Shaper Profile

The following figure shows the graphical view of the shaper profile ref count by one day, one week, one month, hourly, and daily.

Reference count specifies the shaper profile count associated with the subscriber services.

You can also view the information on shaper profile ref count of the OLT for a particular duration using the **Custom** option.

Power

The following figure shows the graphical view of the power profile by one day, one week, one month, hourly, and daily.

You can also view the information on power of the OLT for a particular duration using the **Custom** option.

The following KPIs are supported for the power.

- **PSU Inventory.** Specifies the list of power supply connection to the OLT. Example: PSU_A, PSU_B, and so on.
- **Current Power Consumption.** Specifies the overall power consumption at the OLT. The unit is in watts.
- **Vin.** Specifies the source input voltage. The unit is in volts.
- **Iout.** Specifies the current drawn at the OLT. The unit is in amps.

OLT Historical KPI Chart Configuration

You can create a custom dashboard to view a group of statistics charts that meet a particular requirement.

Perform the following steps to create a custom dashboard page.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Click **More > Historical KPI's**.
The OLT Historical KPI page appears.
4. Click the **Customize** option.
5. Select the KPI charts that you want to display on your page.
6. Click **Close**.
The dashboard automatically adjusts the placement of the charts to dynamically fit on your browser window without changing the order.

Exporting OLT Historical KPIs

You can export the OLT historical KPIs. You can view and analyze the exported KPIs list, as needed.

Perform the following steps to export the OLT KPIs.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Click **More > Historical KPI's**.
The OLT Historical KPI page appears.
4. Click the **Export** option.
The Export Historical KPIs page appears.
5. Select one or more KPI parameter(s) that you want to export.
6. Select the timeline from the list. The supported values are.
 - 1 Month
 - 1 Week
 - 1 Day
 - Custom
7. Select the aggregation type from the list.

- Daily
 - Hourly
 - 15 Min
8. Click **Export**.
- The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file in a Microsoft Excel sheet. Optionally, you can save this file on your PC for later use.
- The downloaded file contains the attributes based on the KPI parameters that you have selected.

Exporting Ports, Faults, Events, and Logs (OLT)

You can export the following information associated with the OLT.

- PON and NNI ports associated with the OLT.
- Events, current and cleared faults raised for the OLT.
- Activity logs generated for the OLT.

Perform the following steps to export the OLT ports, faults, events, and logs.

1. Select **Monitor > Inventory**.
The Inventory List page appears.
2. Click on the **OLT** tab.
3. Click on the OLT name.
The OLT Details page appears.
4. Click on the Port, Faults, Events, or Logs tab.
5. Click **Export**.
The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file in a Microsoft Excel sheet. Optionally, you can save this file on your PC for later use.

Profiles

Perform the following steps to monitor the OLT profiles.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Click **More > Profiles**.

You can view the following type of profiles associated with the OLT.

- **ACL Profile**. Specifies the list of ACL profiles associated with the OLT. For more information, see [Table 50: ACL Profile \(on page 134\)](#).
- **Storm Profile**. Specifies the list of storm profiles associated with the OLT. For more information, see [Table 51: Storm Profile \(on page 134\)](#).

The following table shows the description of fields on the ACL profile.

Table 50. ACL Profile

| Field | Description |
|----------------|---|
| Name | Specifies the name of the ACL. |
| Type | Specifies the type of ACL configuration. |
| Management ACL | Specifies whether the ACL is management ACL. |
| Status | Specifies the status of the ACL. |
| Stats | Specifies the statistics information about ACL. |
| Time | Specifies the date and time when the ACL was created. |

The following table shows the description of fields on the storm profile.

Table 51. Storm Profile

| Field | Description |
|------------|--|
| Name | Specifies the name of the storm profile. |
| Port Names | Specifies the port name of the storm profile. |
| Status | Specifies the status of the storm profile. |
| Stats | Specifies the statistics information about storm profile. The supported values are. <ul style="list-style-type: none"> • Passed ucast packets • Passed ucast bytes • Passed mcast packets • Passed mcast bytes • Passed bcast packets • Passed bcast bytes • Dropped ucast packets • Dropped ucast bytes • Dropped mcast packets • Dropped mcast bytes • Dropped bcast packets • Dropped bcast bytes |
| Time | Specifies the date and time when the storm profile was created. |

Network Services

Perform the following steps to monitor the network services.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Click **More > Network Services**.

You can monitor the following networks services configured for the OLT.

- LAG
- ELAN
- ELine

LAG Details

LAG monitoring involves the reporting of performance KPIs and MAC dump collection on LAG.

Perform the following steps to view the LAG details.

1. Select **Monitor > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click **More > Network Services**.
5. Click on the LAG name to view the LAG details.

The following table describes the fields on the LAG Details List page.

Table 52. LAG Details

| Field | Description |
|--------------------------|---|
| Basic Information | |
| Name | Specifies the name of the resource (LAG port). Example: lag1 |
| Ports | Specifies the LAG port details associated with the OLT. |
| No | Specifies the number of ports associated with the particular OLT. |
| Reported Time | Specifies the date and time when the KPI was reported. |

Table 52. LAG Details (continued)

| Field | Description |
|---------------------|--|
| IDF | Specifies the indeterminate data file. The KPI counters reported are not reliable as there could be a reboot and clear the counter operations performed on the resource. |
| Tx Data Rate (mbps) | Specifies the upstream LAG port data transmit rate in Mbps. |
| Rx Data Rate (mbps) | Specifies the downstream LAG port data received rate in Mbps. |
| Tx Utilization (%) | Specifies the transmitted upstream port utilization in percentage. |
| Rx Utilization (%) | Specifies the received downstream port utilization in percentage. |
| MTU Size | Specifies the Maximum Transmission Unit (MTU) size. |
| Alarm Profile | Specifies the name of the LAG alarm profile. |
| Admin State | Specifies the admin state of the LAG. The supported states are. <ul style="list-style-type: none"> • ACTIVE. When the LAG configuration is enabled. • INACTIVE. When the LAG configuration is disabled. • UNKNOWN. When the LAG configuration is created. |
| Operational State | Specifies the operational state of the LAG. The supported states are. <ul style="list-style-type: none"> • Green. Indicates that the operational state of the LAG is up. • Red. Indicates that the operational state of the LAG is down. |
| Controller State | Specifies the state of the controller. The supported states are. <ul style="list-style-type: none"> • ADD_IN_PROGRESS • ADDED • ENABLE_IN_PROGRESS • ENABLED • DISABLE_IN_PROGRESS • DISABLED • DELETE_IN_PROGRESS • ADD_FAILED • DELETE_FAILED • ENABLE_FAILED • DISABLE_FAILED • ASSOCIATION_FAILED • DISSOCIATION_FAILED |

Table 52. LAG Details (continued)

| Field | Description |
|---|---|
| Port Name | Specifies the port name. Example: NNI-3 |
| Description | Specifies the description about the PON port. |
| Direction | Specifies the port direction, for example, UNI. |
| OLT | Specifies of the PON port of the OLT, for example, olt-185. |
| Admin State | Specifies the admin state of the PON port, for example, ACTIVE. |
| Operational State | Specifies the operational state of the PON port. |
| Fault State | Specifies the fault state of the PON port. |
| PON Encryption Key Exchange Interval | Specifies the PON encryption key exchange interval in milliseconds. The default value is 3600000 milliseconds. |
| Type-B Protection Pair | Specifies the type-b protection pair for the PON port, for example, pair1. |
| Protection Role | Specifies the protection role of the PON port. The supported values are. <ul style="list-style-type: none"> PRIMARY SECONDARY |
| Periodic Rogue ONT Detection Control | Specifies the RSSI measurement window type. |
| Periodic Rogue ONT Detection Measurement Type | Specifies that the periodic rogue ONT detection is enabled. |
| Alloc Type To Scan | Specifies the allocation ID type to scan. |
| Periodic Rogue ONT Detection Interval (in Milliseconds) | Specifies the periodic rogue ONU detection procedure initiation interval in milliseconds. |
| LAG Port KPIs | <ul style="list-style-type: none"> LAG Port KPIs. Specifies the KPIs reported for the LAG port. For information, see LAG Port KPIs (on page 139). Packet Size based Live KPIs. Specifies the packet size based KPIs reported for the LAG port. For more information, see LAG Port Packet Size Based KPIs (on page 140). You can also clear the KPIs by using the Clear KPI Data option. For more information, see Clear LAG KPIs (on page 142). |
| Show MAC Dump | |

Table 52. LAG Details (continued)

| Field | Description |
|--------------------|--|
| Ovlan | Specifies the outer tag value. |
| Ivlan | Specifies the inner tag value. This field is applicable only for the NNI port. |
| MAC Type | <p>Specifies the MAC type. The supported values are.</p> <ul style="list-style-type: none"> • Static • Dynamic |
| MAC Type (Static) | <p>The static MAC is configured or learned based on the MAC learning type. If the traffic goes through the PON in the service, static MAC doesn't ages out.</p> <p>The supported values for the MAC learning type are.</p> <ul style="list-style-type: none"> • DHCP • DHCP_ALLOW_RELEARN • ARP • ARP_ALLOW_RELEARN • PPPoE • DHCP_IP_ANTISPOOFING_NO_MAC • DHCP_IP_ANTISPOOFING_MAC • DHCP_NO_MAC • ARP_NO_MAC <p> Note: In the service configuration with DHCP or DHCP_NO_MAC MAC learning type, service-get reports only the last learned MAC address and IP address. If the service is configured on the VEIP or IPhost port of the ONT, this information indicates the WAN interface of the ONT. Otherwise, it indicates the client device behind the ONU when the service is configured on the PPTP port.</p> <p>For more information on MAC Learning Type, see Table 268: MAC Learning Type (on page 580).</p> |
| MAC Type (Dynamic) | <p>A MAC is displayed as dynamic for the following reasons.</p> <ul style="list-style-type: none"> • Learned by the data path of the OLT. • Packets that are trapped in the controller. <p>The default timeout duration for dynamic MAC address is five minutes.</p> |

Table 52. LAG Details (continued)

| Field | Description |
|-------------|---|
| |  Note: <ul style="list-style-type: none"> The dynamic MAC address is displayed when the DHCP IP assignment cycle progresses. The static MAC address is displayed when the DHCP cycle is completed. <p>For example, if a DHCP cycle is initiated for IPv4 and IPv6, a dynamic MAC address is displayed for an in-progress DHCP Cycle. In contrast, a static MAC address is displayed for a completed DHCP cycle.</p> |
| MAC Address | Specifies the MAC address of the OLT. |

LAG Port KPIs

You can view the LAG ports associated with the OLT.

The following table shows the description of fields on the LAG port KPIs.

Table 53. LAG Port KPIs

| Field | Description |
|----------------------|--|
| Name | Specifies the name of the LAG port associated with the OLT. |
| Ports | Specifies the LAG port details associated with the OLT. |
| No | Specifies the number of ports associated with the particular OLT. |
| Reported Time | Specifies the date and time when the KPI was reported. |
| IDF | Specifies the indeterminate data file. The KPI counters reported are not reliable as there could be a reboot and clear the counter operations performed on the resource. |
| Tx Data Rate (Mbps) | Specifies the downstream LAG port data transmit rate in Mbps. |
| Rx Data Rate (Mbps) | Specifies the upstream LAG port data received rate in Mbps. |
| Tx Bytes | Specifies the downstream LAG port transmit bytes. |
| Rx Bytes | Specifies the upstream LAG port received bytes. |
| Tx Broadcast Packets | Specifies the downstream LAG port transmit broadcast packets. The unit is in packet count. |

Table 53. LAG Port KPIs (continued)

| Field | Description |
|----------------------|--|
| Rx Broadcast Packet | Specifies the upstream LAG port received broadcast packets. The unit is in packet count. |
| Tx Error Packets | Specifies the number of LAG port downstream packets that shows error while transmitting the packets. |
| Rx Error Packets | Specifies the number of LAG port upstream packets that shows error while receiving the packets. |
| Tx Multicast Packets | Specifies the downstream LAG port transmit multicast packets. The unit is in packet count. |
| Rx Multicast Packets | Specifies the upstream LAG port received multicast packets. The unit is in packet count. |
| Tx Unicast Packets | Specifies the downstream LAG port transmit unicast packets. The unit is in packet count. |
| Rx Unicast Packets | Specifies the upstream LAG port received unicast packets. The unit is in packet count. |
| Tx Utilization (%) | Specifies the transmitted downstream port utilization in percentage. |
| Rx Utilization (%) | Specifies the received upstream port utilization in percentage. |
| Rx Packets Dropped | Specifies the number of LAG port upstream packets dropped. |
| Rx FCS Error Packets | Specifies the number of FCS error packets received. |
| Creation Time | Specifies the date and time when the lag port was created. |

LAG Port Packet Size Based KPIs

The LAG port packet size performance helps to monitor the usage of network, the type of packets transiting the network, and consuming the network resources.

The following table shows the description of the LAG port KPI parameters.

Table 54. LAG Port Packet Size Based KPIs

| Field | Description |
|---------------------|---|
| Tx Packets 64 Bytes | Specifies the upstream LAG port transmit packets of size 64 bytes. The unit is in packet count. |

Table 54. LAG Port Packet Size Based KPIs (continued)

| Field | Description |
|----------------------------|---|
| Rx Packets 64 Bytes | Specifies the downstream LAG port received packets of size 64 bytes. The unit is in packet count. |
| Tx Packets 65-127 Bytes | Specifies the upstream LAG port transmit packets of size between 65-127 bytes. The unit is in packet count. |
| Rx Packets 65-127 Bytes | Specifies the downstream LAG port received packets of size between 65-127 bytes. The unit is in packet count. |
| Tx Packets 128-255 Bytes | Specifies the upstream LAG port transmit packets of size between 128-255 bytes. The unit is in packet count. |
| Rx Packets 128-255 Bytes | Specifies the downstream LAG port received packets of size between 128-255 bytes. The unit is in packet count |
| Tx Packets 256-511 Bytes | Specifies the upstream LAG port transmit packets of size between 256-511 bytes. The unit is in packet count. |
| Rx Packets 256-511 Bytes | Specifies the downstream LAG port received packets of size between 256-511 bytes. The unit is in packet count. |
| Tx Packets 512-1023 Bytes | Specifies the upstream LAG port transmit packets of size between 512-1023 bytes. The unit is in packet count. |
| Rx Packets 512-1023 Bytes | Specifies the downstream LAG port received packets of size between 512-1023 bytes. The unit is in packet count. |
| Tx Packets 1024-1518 Bytes | Specifies the upstream LAG port transmit packets of size between 1024-1518 bytes. The unit is in packet count. |
| Rx Packets 1024-1518 Bytes | Specifies the downstream LAG port received packets of size between 1024-1518 bytes. The unit is in packet count. |
| Tx Packets 1519-2047 Bytes | Specifies the upstream LAG port transmit packets of size between 1519-2047 bytes. |

Table 54. LAG Port Packet Size Based KPIs (continued)

| Field | Description |
|-----------------------------|--|
| | The unit is in packet count. |
| Rx Packets 1519-2047 Bytes | Specifies the downstream LAG port received packets of size between 1519-2047 bytes. The unit is in packet count. |
| Tx Packets 2048-4095 Bytes | Specifies the upstream LAG port received packets of size between 2048-4095 bytes. The unit is in packet count. |
| Rx Packets 2048-4095 Bytes | Specifies the downstream LAG port received packets of size between 2048-4095 bytes. The unit is in packet count. |
| Tx Packets 4096-9216 Bytes | Specifies the upstream LAG port transmit packets of size between 4096-9216 bytes. The unit is in packet count. |
| Rx Packets 4096-9216 Bytes | Specifies the downstream LAG port received packets of size between 4096-9216 bytes. The unit is in packet count. |
| Tx Packets 9217-16383 Bytes | Specifies the upstream LAG port transmit packets of size between 9217-16383 bytes. The unit is in packet count. |
| Rx Packets 9217-16383 Bytes | Specifies the downstream LAG port received packets of size between 9217-16383 bytes. The unit is in packet count. |

Clear LAG KPIs

RMS supports clearing the live KPI subscription of LAG ports and reset the counters to zero. This enables fresh debugging by resetting the counters to zero and start getting the live KPIs incrementally. You can clear the KPI counters only when the LAG port admin state is ENABLED, and the operational state is UP.

After clearing the live LAG KPIs, CBAC resets the counters to zero and incrementally generates KPIs for towards RMS for debugging.

To clear the LAG port KPI counters, click **Clear KPI** option from the right-hand side of the page.



Note: You can clear the live KPIs only when the **LIVE KPI** option is ON.

ELine

You can view the ELine configuration of the OLT.

Perform the following steps to monitor the ELine.

1. Select **Monitor > Inventory**.

The Inventory page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click **More > Network Services**.
5. Click on the **ELine** tab.
6. Click on the ELine name to view the ELine details.

The ELine Details page appears.



Note: Alternatively, you can navigate to **Configuration > Inventory > OLT > ELine** (under Network Services) > **Monitor**.

The following table shows the description of fields on the ELine.

Table 55. ELine

| Field | Description |
|--------------------------|---|
| Basic Information | |
| Name | Specifies the unique name of the ELine. |
| VLAN ID | Specifies the VLAN ID. The supported value ranges from 2 to 4095. |
| Admin State | Specifies the admin state of the ELine. The supported values are. <ul style="list-style-type: none">• ACTIVE• DEACTIVE |
| Port | Specifies the NNI or LAG port. |
| Live KPIs | |
| Downstream | Specifies the downstream traffic on the CPU, PON, and network interface based on the packet. |
| VLAN Packets | Specifies the number of VLAN packets on downstream traffic. |

Table 55. ELine (continued)

| Field | Description |
|-----------------|---|
| VLAN Bytes | Specifies the number of VLAN bytes on downstream traffic. |
| VLAN Data Rate | Specifies the VLAN data rate on downstream traffic. The unit is in Mega bits per second (Mbps). |
| Upstream | Specifies the upstream traffic on the CPU, PON, and network interface based on the packet. |
| VLAN Packets | Specifies the number of VLAN packets on upstream traffic. |
| VLAN Bytes | Specifies the number of VLAN bytes on upstream traffic. |
| VLAN Data Rate | Specifies the VLAN data rate on upstream traffic. The unit is in Mega bits per second (Mbps). |
| Historical KPIs | Specifies the historical KPIs reported for the ELine. For more information, see Historical KPIs (on page 144) . |

Historical KPIs

CBAC reports historical KPIs for the ELine. You can view the following historical performance data for the ELine.



Note:

- If you select one option from the list, the second list dynamically populates the relevant data based on the first option. To view all options in the list, deselect the option in the list.
- The ELine KPIs appear in the list only when the historical data is received from CBAC.

Enabling and Disabling ELine KPI

By default, the ELine KPIs are disabled. Perform the following steps to enable the ELine KPI.

1. Select **Monitor > Inventory**.

The Inventory page appears.

2. Click on the **OLT** tab.

3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click **More > Network Services**.

5. Click on the **ELine** tab.

6. Click on the ELine name to view the ELine details.

The ELine Details page appears.



Note: Alternatively, you can navigate to **Configuration > Inventory > OLT > ELine** (under Network Services) > **Monitor**.

7. Click **Enable KPI**.

Perform the following steps to disable the ELine KPI.

1. Select **Monitor > Inventory**.

The Inventory page appears.

2. Click on the **OLT** tab.

3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click **More > Network Services**.

5. Click on the **ELine** tab.

6. Click on the ELine name to view the ELine details.

The ELine Details page appears.



Note: Alternatively, you can navigate to **Configuration > Inventory > OLT > ELine** (under Network Services) > **Monitor**.

7. Click **Disable KPI**.

ELine LIVE KPI Settings

You can turn on or turn off the retrieval of live KPIs using the **Live KPI ON** or **Live KPI OFF** button. Once the Live KPI button is turned on you can select ports from the list and can view KPI's for that port. Clicking the **LIVE KPI ON** button for subscription automatically starts LIVE KPI for all the ports mentioned under the historical KPI option. For more information, see [Live KPI Settings \(on page 128\)](#).

Clear ELine KPIs

RMS supports to clear the live KPI subscription of ELine and reset the counters to zero. This enables fresh debugging by resetting the counters to zero and start getting the live KPIs incrementally.

After clearing the live ELine KPIs, CBAC resets the counters to zero and incrementally generates KPIs for towards RMS for debugging.

To clear the ELine KPI counters, click **Clear KPI** option from the right-hand side of the page.



Note: You can clear the live KPIs only when the **LIVE KPI** option is ON.

ELAN

You can view the ELAN configuration of the OLT.

Perform the following steps to monitor the ELAN.

1. Select **Monitor > Inventory**.

The Inventory page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click **More > Network Services**.
5. Click on the **ELAN** tab.
6. Click on the ELAN name to view the ELAN details.

The ELAN Details page appears.



Note: Alternatively, you can navigate to **Configuration > Inventory > OLT > ELAN** (under Network Services) > **Monitor**.

The following table shows the description of fields on the ELAN.

Table 56. ELAN

| Field | Description |
|--------------------------|--|
| Basic Information | |
| Name | Specifies the unique name of the ELAN. |
| Parent Name | Specifies the OLT details associate with the ELAN. |
| Ports | Specifies the NNI or LAG port. |
| VLAN ID | Specifies the VLAN ID. The supported value ranges from 2 to 4095. |
| Admin State | Specifies the admin state of the ELAN. The supported values are. <ul style="list-style-type: none">• ACTIVE• DEACTIVE |
| Sub Ports | Specifies the OLT ports that are connected to the subtending OLT. |
| Router Ports | Specifies the OLT ports that are connected to the router. |
| Live KPIs | |

Table 56. ELAN (continued)

| Field | Description |
|-----------------|---|
| Downstream | Specifies the downstream traffic on the CPU, PON, and network interface based on the packet. |
| VLAN Packets | Specifies the number of VLAN packets on downstream traffic. |
| VLAN Bytes | Specifies the number of VLAN bytes on downstream traffic. |
| VLAN Data Rate | Specifies the VLAN data rate on downstream traffic. The unit is in Mega bits per second (Mbps). |
| Upstream | Specifies the upstream traffic on the CPU, PON, and network interface based on the packet. |
| VLAN Packets | Specifies the number of VLAN packets on upstream traffic. |
| VLAN Bytes | Specifies the number of VLAN bytes on upstream traffic. |
| VLAN Data Rate | Specifies the VLAN data rate on upstream traffic. The unit is in Mega bits per second (Mbps). |
| Historical KPIs | Specifies the historical KPIs reported for the eline. For more information, see Historical KPIs (on page 147) . |

Historical KPIs

CBAC reports historical KPIs for the ELAN. You can view the following historical performance data for the ELAN.



Note:

- If you select one option from the list, the second list dynamically populates the relevant data based on the first option. To view all options in the list, deselect the option in the list.
- The ELAN KPIs appear in the list only when the historical data is received from CBAC.

Enabling and Disabling ELAN KPI

Perform the following steps to enable the ELAN KPI.

1. Select **Monitor > Inventory**.

The Inventory page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click **More > Network Services**.
5. Click on the **ELAN** tab.
6. Click on the ELAN name to view the ELAN details.

The ELAN Details page appears.



Note: Alternatively, you can navigate to **Configuration > Inventory > OLT > ELAN** (under Network Services) > **Monitor**.

7. Navigate to **Historical KPI's** and select the NNI port from the list.
8. Click **Enable KPI**.

Perform the following steps to disable the ELAN KPI.

1. Select **Monitor > Inventory**.

The Inventory page appears.

2. Click on the **OLT** tab.
3. Click on the OLT name under the **Name** column.

The OLT Details page appears.

4. Click **More > Network Services**.
5. Click on the **ELAN** tab.
6. Click on the ELAN name to view the ELAN details.

The ELAN Details page appears.



Note: Alternatively, you can navigate to **Configuration > Inventory > OLT > ELAN** (under Network Services) > **Monitor**.

7. Click **Disable KPI**.

ELAN LIVE KPI Settings

You can turn on or turn off the retrieval of live KPIs using the **Live KPI ON** or **Live KPI OFF** button. Once the Live KPI button is turned on you can select ports from the list and can view KPI's for that port. Clicking the **LIVE KPI ON** button for subscription automatically starts LIVE KPI for all the ports mentioned under the historical KPI option. For more information, see [Live KPI Settings \(on page 128\)](#).

Clear ELAN KPIs

RMS supports to clear the live KPI subscription of ELAN and reset the counters to zero. This enables fresh debugging by resetting the counters to zero and start getting the live KPIs incrementally.

After clearing the live ELAN KPIs, CBAC resets the counters to zero and incrementally generates KPIs for towards RMS for debugging.

To clear the ELAN KPI counters, click **Clear KPI** option from the right-hand side of the page.



Note: You can clear the live KPIs only when the **LIVE KPI** option is ON.

Protection

Perform the following steps to view the OLT protection page.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Click **More > Protection**.

You can view the following type of protections.

- **Type-B Protection Pair.** Specifies the list of type-B protection pair. For more information, see [Table 57: Type-B Protection Pair \(on page 149\)](#).
- **Ring.** Specifies the list of rings configured for the OLT. For more information, see [Table 58: Ring \(on page 150\)](#).

The following table shows the description of fields on the type-B protection pair.

Table 57. Type-B Protection Pair

| Field | Description |
|---|---|
| Name | Specifies the unique name of the primary protection pair. |
| Protection Type | Specifies the type of the PON protection. |
| Primary OLT | Specifies the name of the primary OLT. |
| Primary Port | Specifies the primary port of the protection pair. |
| Primary Port Protection State | Specifies the primary port protection state. |
| Primary Port Protection Operational State | Specifies the operational state of the primary PON port in the protection pair. |
| Secondary OLT | Specifies the name of the secondary OLT. |
| Secondary Port | Specifies the name of the secondary port. |
| Secondary Port Protection State | Specifies the secondary port protection state. |
| Secondary Port Protection Operational State | Specifies the secondary port protection operational state. |

Table 57. Type-B Protection Pair (continued)

| Field | Description |
|---------------|---|
| Creation Time | Specifies the date and time when the PON protection pair was created. |

The following table shows the description of fields on the Rings page.

Table 58. Ring

| Field | Description |
|-----------------------|--|
| Name | Specifies the unique name of the rings. |
| Ring ID | Specifies the ring ID. |
| Ring Type | Specifies the ring type. |
| East port | Specifies the ERPS instance east port. |
| West port | Specifies the ERPS instance west port. |
| Configuration Status | Specifies the configuration status of the ring. |
| Config Failure Reason | Specifies the reason for the configuration failure. |
| Creation Time | Specifies the date and time when the ring was created. |

MEP Instance

Perform the following steps to view the details of the MEP instance that was configured for the OLT.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Click **More > MEP Instance**.

The following shows the description of fields on the MEP Instance.

Table 59. MEP Instance

| Field | Description |
|----------------------|--|
| Name | Specifies the name of the MEP instance. |
| MEP Profile Name | Specifies the MEP profile name. |
| Port | Specifies the port type. |
| Configuration Status | Specifies the port configuration status. |

Table 59. MEP Instance (continued)

| Field | Description |
|-----------------------|--|
| Config Failure Reason | Specifies the reason for the configuration failure. |
| Creation Time | Specifies the date and time when the MEP instance was created. |
| LOC State | Specifies the Los of Connection (LOC) state. The supported values are. <ul style="list-style-type: none"> True False |

OLT Rack

Perform the following steps to view the OLT rack information.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Click **More > OLT Rack**.

The following table shows the description of fields on the OLT Rack page.

Table 60. OLT Rack

| Field | Description |
|----------------|--|
| Name | Specifies the name of the rack. Example: olt-185-Rack1 |
| Display ID | Specifies the display ID of the OLT rack. Example: rack=1 |
| Make | Specifies the vendor name of the OLT rack. Example: Radisys |
| Model | Specifies the model name of the OLT rack. Example: RLT-3200G |
| Device Profile | Specifies the device profile of the OLT rack. Example: RLT-3200G-OLT |
| Layout | Specifies the layout of the OLT rack. The supported values are. <ul style="list-style-type: none"> HORIZONTAL VERTICAL |
| Creation Time | Specifies the date and time when the OLT rack instance was created. |

SFP

Perform the following steps to view the SFP optical information for the particular OLT NNI and PON ports.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Click **More > SFP**.

The following table shows the description of fields on the SFP NNI ports. The current, voltage, temperature, Rx power, and Tx power are instantaneous values read from the NNI SFP Erasable Programmable Read-Only Memory (EPROM). The NNI port SPF reports both Tx and Rx power level information.

Table 61. SFP NNI Ports

| Field | Description |
|------------------|--|
| Name | Specifies the name of the port. Example: NNI-8 |
| Serial Number | Specifies the serial number of the SFP. Example: MW1033M |
| Make | Specifies the vendor name of the SFP. Example: FINISAR CORP |
| Current (mA) | Specifies the SFP current in mili ampere. |
| Voltage (Volts) | Specifies the SFP voltage in volts. |
| Temperature (°C) | Specifies the SFP temperature in degree celsius. |
| Rx Power (dBm) | Specifies the received power of the SFP in dBm. |
| Tx Power (dBm) | Specifies the transmit power of the SFP in dBm. |
| Technology | Specifies the technology used by SFP. |

The following table shows the description of fields on the SFP PON ports. The current, voltage, temperature, XGSPON Tx power, and GPON Tx power are instantaneous values read from the PON SFP Erasable Programmable Read-Only Memory (EPROM). The PON port SPF reports only the Tx power level information.

Table 62. SFP PON Ports

| Field | Description |
|-------|---|
| Name | Specifies the name of the port. Example: SFPPON-32 |

Table 62. SFP PON Ports (continued)

| Field | Description |
|-----------------------|---|
| Serial Number | Specifies the serial number of the SFP. Example: UK4AA000042 |
| Make | Specifies the vendor name of the SFP. Example: Hisense |
| Current (mA) | Specifies the SFP current in mili ampere. |
| Voltage (Volts) | Specifies the SFP voltage in volts. |
| Temperature (°C) | Specifies the SFP temperature in degree celsius. |
| XGSPON Tx Power (dBm) | Specifies the transmit power of the SFP in dBm. |
| GPON Tx Power (dBm) | Specifies the transmit power of the SFP in dBm. |
| Technology | Specifies the technology used by SFP. |

DHCP Snooping Details

Perform the following steps to view the DHCP snooping table for all the subscriber services on the OLT.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **OLT** tab and select the applicable OLT.
3. Click **More > DHCP Snooping Details**.

The following table shows the description of fields on the DHCP snooping table details.

Table 63. DHCP Snooping Table

| Field | Description |
|------------------|--|
| PON Port Number | Specifies the PON port ID. Example: SFPPON-1 |
| SVLAN | Specifies the subscriber's S-Tag value. |
| CVLAN | Specifies the subscriber's C-Tag value. |
| UNI VLAN | Specifies the VLAN for UNI port. |
| DHCP IPv4 Status | Specifies the status of IPv4. The supported values are. <ul style="list-style-type: none"> • ASSIGNED • REQUESTED • TIMED-OUT |

Table 63. DHCP Snooping Table (continued)

| Field | Description |
|------------------|--|
| DHCP IPv6 Status | Specifies the status of IPv6. The supported values are. <ul style="list-style-type: none"> ASSIGNED REQUESTED TIMED-OUT |

If you want the DHCP snooping information, click the **Fetch DHCP Information** option.

The following table shows the description of fields on the DHCP information tab.

Table 64. Fetch DHCP Snooping Information

| Field | Description |
|---------------------------|--|
| PON | Specifies the PON port ID. Example: SFPPON-1 |
| ONT | Specifies the ONT name. |
| UNI Port Name | Specifies the UNI port name. |
| SVLAN | Specifies the subscriber's S-Tag value. |
| CVLAN | Specifies the subscriber's C-Tag value. |
| UNI VLAN | Specifies the VLAN for UNI port. |
| Mac Address | Specifies the MAC address. |
| IPv4 Address | Specifies the IPv4 address. |
| Status v4 | Specifies the status of IPv4. The supported values are. <ul style="list-style-type: none"> ASSIGNED REQUESTED TIMED-OUT |
| Remaining Lease Time IPv4 | Specifies the remaining lease time for IPv4. |
| IPv6-IAPD | Specifies a set of IPv6 prefixes that are assigned to a requesting device through an IAPD. |
| IPv6-IANA | Specifies the IPv6 address allocated by DHCP server to the client. |
| Status v6 | Specifies the status of IPv6. The supported values are. |

Table 64. Fetch DHCP Snooping Information (continued)

| Field | Description |
|---------------------------|--|
| | <ul style="list-style-type: none"> ASSIGNED REQUESTED TIMED-OUT |
| Remaining Lease Time IPv6 | Specifies the remaining lease time for IPv6. |

Login to the Physical OLT

From RMS, you can login to the physical OLT using the **T&D Login** option to troubleshoot any issues.



Note: The T&D login is used only by Radisys personnel for troubleshooting. The customer is recommended not to use T&D login for any other reason.

Perform the following steps to login to the physical OLT.

1. Select **Monitor > Inventory > Inventory**.

The Inventory List page appears.

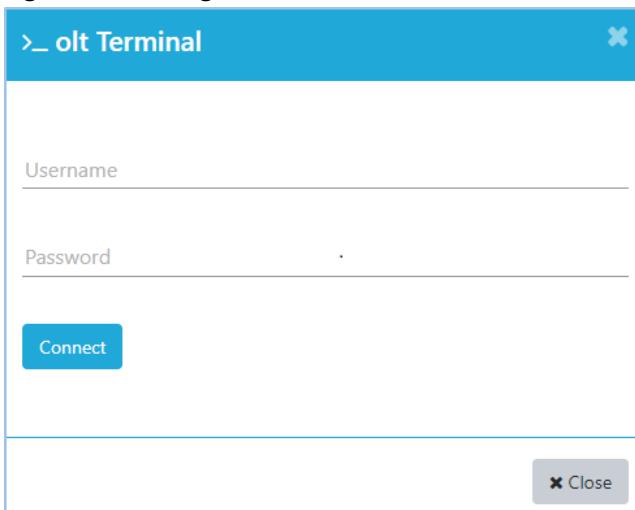
2. Click on the **OLT** tab.
3. Click on the OLT name.

The OLT Details page appears.

4. Click on the CLI prompt icon  , in the **IP Address** field of the OLT basic information.

The OLT terminal appears.

Figure 29. OLT Login



5. Enter a valid username and password.
6. Click **Connect**.

The connection is established, and the OLT console window is displayed.

Monitoring ONT

RMS monitors information about ONTs that include health status, basic information, optical information, current KPIs, list of ports (NNI and PON) associated with the ONT, faults AND events reported for the ONT, activity log, card list, and audit logs.

You can view the summary of all the ONTs connected to your network and monitor the following details of the ONT.

- Health Status
- Basic Information
- Optical Information
- Live KPIs
- Historical KPIs
 - ONT Statistics
 - UNI Port Statistics

Perform the following steps to monitor the ONT details.

1. Select **Monitor > Inventory**.
2. Click on the **ONT** tab.
3. Click on the ONT name under the **Name** column.

The ONT Details page appears.

Health and Basic Information

You can view the health and basic information about the ONT configured on the **Monitor > Inventory > Inventory > ONT > Details** page.

The following table describes the ONT health status information of the ONT.

Table 65. ONT Health Status

| Field | Description |
|--------|--|
| Health | <p>You can view the health status of the ONT based on the following.</p> <ul style="list-style-type: none">• Critical. Shows the number of critical alarms raised.• Major. Shows the number of major alarms raised.• Minor. Shows the number of minor alarms raised.• Warning. Shows the number of warning alarms raised. |

Table 65. ONT Health Status (continued)

| Field | Description |
|-------|--|
| | <ul style="list-style-type: none"> Active Port. Shows the number of ports that are activated. Inactive Port. Shows the number of ports that are deactivated. Up Port. Shows the number of ports that are up. Down Port. Shows the number of ports that are down. |

The following table describes the basic information of the ONT.

Table 66. ONT Basic Information

| Field | Description |
|--------------------------|---|
| Basic Information | |
| Name | Specifies name of the ONT. |
| Type | Specifies type of the device. |
| Display ID | Specifies display ID of the ONT. |
| Serial No. | Specifies serial number of the ONT. |
| Serial No. Status | Specifies ONT status for a particular serial number. |
| IP Address | Specifies IP address of the ONT. |
| Equipment ID | Specifies equipment ID of the ONT. |
| Vendor ID | Specifies manufacturer name of the ONT. |
| Controller | Specifies name of the controller. |
| Subscriber | Specifies name of the subscriber. |
| Splitter | Specifies name of the splitter. |
| Registration ID | Specifies registration ID of the ONT. |
| UNI Ports Count | Specifies number of UNI ports connected to the ONT. |
| UNI Ports | Specifies UNI ports that are connected to the ONT. |
| T-CONT Count | Specifies number of TCONTs connected to the ONT. |
| ME Group | Specifies managed element group to which the ONT belongs. |
| Reboot Time | Specifies reboot time of the ONT. |

Table 66. ONT Basic Information (continued)

| Field | Description |
|-------------------|---|
| Mac Limit | Specifies the MAC learning depth attribute of the ME MAC bridge service profile on the ONU. |
| Mac Ageing Time | Specifies the maximum time an ONT can hold a MAC entry in the MAC table when there is no data received from the device. |
| ONT Type | Specifies the ONT type. The supported values are. <ul style="list-style-type: none"> Bridged. This ONT only reports to PPTP Ethernet UNIs. Devices connected to PPTP Ethernet UNIs get their IP addresses from the network or static IP addresses. Routed. This ONT provides home gateway functionality and reports to the VEIP interface. The PPTP interfaces might be reported, but CBAC ignores them. Hybrid. This ONT reports to both the PPTP Ethernet UNIs and VEIP ports. Services can be provisioned on both PPTP Ethernet UNIs and VEIP ports. |
| Auto Upgrade | Specifies whether the ONU is upgraded with the firmware version mentioned in the ONT Firmware Version Table when the CBAC detects that the firmware version does not match the version mentioned in the table. The supported values are. <ul style="list-style-type: none"> True. Initiates the auto upgrade if the ONT firmware version mentioned in the RMS does not match the version mentioned in the CBAC. False. Auto upgrade is disabled if you select the false field. |
| Technology | Specifies the technology supported by the ONT. The supported values are. <ul style="list-style-type: none"> GPON XGSPON |
| Alias Name | Specifies alias name of the ONT. |
| Admin State | Specifies admin state of the ONT. |
| Operational State | Specifies operational state of the ONT. |
| Up Since | Specifies time from when the ONT is up. |
| Management Domain | Specifies name of the management domain. |
| Model | Specifies model name of the ONT. |
| Make | Specifies vendor name of the ONT. |

Table 66. ONT Basic Information (continued)

| Field | Description |
|--------------------------|--|
| Active Firmware Version | Specifies the firmware version of the active ONT. |
| Standby Firmware Version | Specifies the firmware version of the standby ONT. |
| Planned Firmware Version | Specifies the expected firmware version of the ONT when the ONT is discovered. |
| Active Partition Status | Specifies the ONT active partition status. The supported values are. <ul style="list-style-type: none"> • Proper state • Improper state |
| Standby Partition Status | Specifies the ONT standby partition status. The supported values are. <ul style="list-style-type: none"> • Proper state • Improper state |
| Splitter Port | Specifies name of the splitter port. |
| OLT Name | Specifies name of the OLT. |
| OLT Port Name | Specifies name of the OLT port. |
| ONT Number | Specifies the ONT number. |
| Hardware Version | Specifies hardware version of the OLT. |
| Upstream FEC | Specifies whether Forward Error Correction (FEC) is enabled in the upstream traffic. |
| Reboot Reason | Specifies reboot reason of the ONT. |
| DBA Type | Selects the DBA type to be used for ONTs that are created for the ONUs for services. The supported values are. <ul style="list-style-type: none"> • NSR • SR The default value is NSR. |
| Supported DBA Type | Specifies the DBA types which are supported by ONU. The supported values are. <ul style="list-style-type: none"> • NSR • SR The default value is NSR. |

Optical Information

You can view the optical information about the ONT configured on the **Monitor > Inventory > Inventory > ONT > Details** page.

Sometimes, when you troubleshoot the ONTs, you need to check the optical information of the ONT.

RMS retrieves the current and default threshold values of the optical information from the ONT. If the ONT ID is valid and the ONT is ENABLED and UP, the CBAC sends the optical Information to RMS.

The following table shows the description of optical parameters of the ONT.

Table 67. ONT Optical Information–Parameters

| Parameter | Description |
|---------------|---|
| Response Time | Specifies the actual ONT response time recorded by the ONT. The unit is in ns (nanosecond). The value ranges from 34000 to 36000 ns. The value 0: null, function is supported. |
| Tx Power | Specifies the current measurement of the optical transmit power level. The unit is in dBm (decibels relative to one milliwatt). The value ranges from 0.5 to +5 dBm. |
| Rx Power | Specifies the current measurement of the optical received power level. The unit is in dBm (decibels relative to one milliwatt). The value ranges from -4 to -32dBm. |
| Voltage | Specifies the voltage of the ONT. The unit is in mV (milli-volts). The value ranges from 1000 to 3300mV. |
| Bias Current | Specifies the bias current of the ONT. The unit is in mA (milli-amps). The value ranges from 0 to 25mA. |
| Temperature | Specifies the temperature of the ONT. The unit is in degree. |

Firmware Details

You can view the firmware details about the ONT configured on the **Monitor > Inventory > Inventory > ONT > Details** page.

The following table shows the description of firmware details.

Table 68. Firmware Details

| Parameter | Description |
|------------------|--|
| Version | Specifies the current version of the ONT firmware. Example, 7.0.1b15-0.6 |
| Download Version | Specifies the firmware version of the ONT that was downloaded. |
| Upgrade Status | Specifies the ONT firmware upgrade status on the OLT. The supported values are. <ul style="list-style-type: none"> • DOWNLOADED • NOT-DOWNLOADED • DOWNLOAD-ON-ONT-SUCCESSFUL • DOWNLOAD-ON-ONT-FAILURE • ACTIVATE-COMMIT-SUCCESSFUL • ACTIVATE-COMMIT-FAILURE |

RSSI Management Information

You can view the RSSI management information about the ONT configured on the **Monitor > Inventory > Inventory > ONT > Details** page.

CBAC and OLT perform the Received Signal Strength Indicator (RSSI) measurement of an active ONT at the OLT PON port side. This on-demand RSSI measures the received power of an ONT, which is required for field debugging to understand the PON conditions and optical fiber plant communication losses for an ONT.

The following table shows the description of ONT statistics parameters.

Table 69. RSSI Management Information

| Field | Description |
|----------|---|
| TX Power | Specifies a transmitter optical power of the OLT for the downstream transmissions. The unit is in dBm. |
| Rx Power | Specifies the receiver optical power measured on the OLT for the ONT upstream transmissions. The unit is in dBm. |
| OLT | Specifies the OLT from which the RSSI measurement for the ONT is performed. This is useful for the type-B protection scenario. |

Table 69. RSSI Management Information (continued)

| Field | Description |
|----------|--|
| PON PORT | Specifies the PON Port from which the RSSI measurement for the ONT is performed. This is useful for the type-B protection scenario. |

ONT Live KPIs

You can view the ONT live KPIs about the ONT configured on the **Monitor > Inventory > Inventory > ONT > Live KPIs** page.

The ONTs report the KPIs periodically towards CBAC on the OpenOMCI interface. CBAC reports the ONT KPIs to RMS. The KPIs are reported for the ONT only if the ONTs admin state is ACTIVE and the operational state is UP. The KPI reporting interval is five minutes by default.

The following table shows the description of ONT KPI parameters.

Table 70. ONT KPIs

| Field | Description |
|----------------------|--|
| UNI Port | Specifies the UNI port. |
| RX Packets | Specifies the count of GEM frames received correctly on the monitored GEM port. A correctly received GEM frame is the one that does not contain any incorrect errors and has a valid header error check. The unit is in packet count. |
| TX Packets | Specifies the count of GEM frames transmitted on the monitored GEM port. The unit is in packet count. |
| TX Bytes | Specifies the count of user payload bytes received on the monitored GPON Encapsulation Method (GEM) port. The unit is in bytes. |
| RX Bytes | Specifies the count of user payload bytes transmitted on the monitored GEM port. The unit is in bytes. |
| MCAST RX Packets | Specifies the count of the received multicast packets. The unit is in packet count. |
| MCAST TX Packets | Specifies the count of the transmitted multicast packets. The unit is in packet count. |
| RX FCS Error Packets | Specifies the count of the packets received with FCS errors. The unit is in packet count. |

Table 70. ONT KPIs (continued)

| Field | Description |
|------------------|---|
| TX Drop Events | Specifies the total number of events in which the upstream packets were dropped due to a lack of resources. This is not necessarily the number of packets dropped; it is the number of times the event was detected. The unit is in packet count. |
| RX Drop Events | Specifies the total number of events in which the downstream packets were dropped due to a lack of resources. This is not necessarily the number of packets dropped; it is the number of times the event was detected. The unit is in packet count. |
| BCAST RX Packets | Specifies the count of the upstream broadcast packets. The unit is in packet count. |
| BCAST TX Packets | Specifies the count of the downstream broadcast packets. The unit is in packet count. |

Clear ONT KPIs

You can clear the ONT KPIs configured on the **Monitor > Inventory > Inventory > ONT > Live KPIs** page.

RMS supports clearing the live KPI subscription ONT and reset the counters to zero. This enables fresh debugging by resetting the counters to zero and start getting the live KPIs incrementally. You can clear the KPI counters only when the OLT admin state is ENABLED and the operational state is UP.

After clearing the live ONT KPIs, CBAC resets the counters to zero and incrementally generates KPIs for towards RMS for debugging.

To clear the ONT KPI counters, click the **Clear KPI** option from the right-hand side of the page.



Note: You can clear the live KPIs only when the **LIVE KPI** option is ON.

Historical KPIs

You can view the historical KPIs about the ONT configured on the **Monitor > Inventory > Inventory > ONT > Historical KPI** page.

You can view the following historical KPIs of the ONT.

- ONT Statistics
- UNI Port Statistics



Note: If you select one option from the list, the second list dynamically populates the relevant data based on the first option. To view all options in the list, deselect the option in the list.

ONT Statistics

You can view the graphical view of the ONT statistics information by one day, one week, one month, daily, and hourly.

You can also view the statistics information of the ONT for a particular duration using the **Custom** option.

You must select the KPI parameter from the list for which you want to view the statistical information.

The supported KPIs are.

- RX BIP Errors
- RX Optical Power
- TX Optical Power
- Voltage
- Temperature
- ONT Response Time
- Bias Current
- Upstream/Downstream Stats

The following table shows the description of ONT statistics parameters.

Table 71. ONT Statistics Information

| Field | Description |
|-------------------|--|
| RX BIP Errors | Specifies the count of bit errors in the received downstream FS frames as measured using BIP-32. If FEC is supported in the downstream direction, the BIP-32 count applies to the downstream FS frame after the FEC correction applied and the FEC parity bytes are removed. |
| RX Optical Power | Specifies the current measurement of optical received power level. The unit is in dBm (decibels relative to one milliwatt). The value ranges from -4 to -32 dBm. |
| TX Optical Power | Specifies the current measurement of optical transmit power level. The unit is in dBm (decibels relative to one milliwatt). The value ranges from 0.5 to +5 dBm. |
| Voltage | Specifies the voltage on ONT. The unit is in mV (milli-volts). The value ranges from 1000 to 3300 mV. |
| Temperature | Specifies temperature of the ONT. The unit is in degree Celsius. |
| ONT Response Time | Specifies the actual ONT response time recorded by ONT. The unit is in nanosecond (ns). |

Table 71. ONT Statistics Information (continued)

| Field | Description |
|---------------------------|---|
| | Value 0: null, function is not supported. The value ranges from 34000 to 36000 ns. |
| Bias Current | Specifies the bias current on ONT. The unit is in mA (milli-amps). The value ranges from 0 to 25 mA. |
| Upstream/Downstream Stats | Specifies the statistical information about the following. <ul style="list-style-type: none"> Upstream Ber. Specifies the upstream BIP (Bit Interleaved Parity) errors. Downstream Ber. Specifies the downstream BIP (Bit Interleaved Parity) errors. Upstream Ucast Byte. Specifies the count of upstream unicast bytes. The unit is in bytes. Downstream Ucast Byte. Specifies the count of downstream unicast bytes. The unit is in bytes. Upstream Throughput. Specifies the upstream throughput. The unit is in Mbps. Downstream Throughput. Specifies the downstream throughput. The unit is in Mbps. |

The graphical view of the ONT statistics is generated based on the KPI parameter and the periodic interval type that you have selected.

UNI Port Statistics

You can view the UNI port statistics about the ONT configured on the **Monitor > Inventory > Inventory > ONT > Historical KPI** page.

You can view the graphical view of the UNI port statistics information by one month, one week, one day, daily, and hourly.

You can also view the statistics information UNI for a particular duration using the **Custom** option.

You can select both upstream and downstream packet KPI parameter from the list for which you want to view the statistics information.

The UNI port upstream KPI parameters are.

- RX Packets
- RX Drop Events
- BCAST RX Packets
- RX Bytes

- MCAST RX Packets
- RX FCS Packet Errors

The UNI port downstream KPI parameters are.

- TX Packets
- TX Drop Events
- BCAST TX Packets
- MCAST TX Packets

For description about the KPI parameters, see [Table 70: ONT KPIs \(on page 162\)](#).

The graphical view of the UNI port statistics is generated based on the KPI upstream parameter or downstream parameter, and the periodic interval type that you have selected.

You can also view the details of the following.

- **Ports.** View the list of UNI ports connected to the ONT.
- **Faults.** Displays the list of current and cleared faults reported for the ONT.
- **Events.** Displays the list of events reported for the ONT.
- **Card List.** View the card list. For more information, see [Monitoring Card Details \(on page 171\)](#).
- **Activity Log.** View the activity logs generated for the ONT.
- **Audit Log.** List of logs triggered for the operations performed on ONT. For more information on the field descriptions, see [Table 102: Audit Log List \(on page 230\)](#).

UNI Port Details

UNI port monitoring involves detection of faults and events on the UNI ports and the reporting of performance KPIs to assess the utilization of the UNI port.

Perform the following steps to view the UNI port details.

1. Select **Monitor > Inventory**.

The Inventory List page appears.

2. Click on the **ONT** tab.
3. Click on the ONT name under the **Name** column.

The ONT Details page appears.

4. Click the **Ports** tab.
5. Click on the UNI port name to view the UNI port details.

The following table describes the fields on the UNI Port List page.

Table 72. UNI Port Details

| Field | Description |
|--------------------------|--|
| Basic Information | |
| Name | Specifies the name of the UNI port, for example, ONT2-PON6-PPTP-ETHERNET-1. |
| Type | Specifies the type of the UNI port, for example, PHYSICAL. |
| Display ID | Specifies the display ID of the port. For example, /rack=1/shelf=1/slot=LT-1/port=SFPPON-6/remote_unit=2/port=1 |
| Port No. | Specifies the port number, for example, 1. |
| Capacity | Specifies the capacity of the port, for example, 2.5 (Gigabit) |
| Description | Specifies the description about the UNI port. |
| Direction | Specifies the port direction, for example, UNI. |
| ONT | Specifies the UNI port of the ONT, for example, ONT2-PON6. |
| Admin State | Specifies the admin state of the UNI port, for example, ACTIVE. |
| Operational State | Specifies the operational state of the UNI port. |
| Fault State | Specifies the fault state of the UNI port. |
| UNI Port Type | Specifies the UNI port type, for example, PPTP-ETHERNET. |
| Technology | Specifies the technology used. |
| Faults | Specifies the list of current and cleared faults reported for the UNI port. For more information on the field descriptions, see Table 42: Alarm List (on page 115) . |
| Events | Specifies the list of events reported for the UNI port. For more information on the field descriptions, see Table 43: Events List (on page 117) . |
| Activity Log | Specifies the activity log generated for the UNI port. For more information on the field descriptions, see Table 44: Activity Logs (Tabular View) (on page 119) . |
| Show MAC Dump | |
| Ovlan | Specifies the outer tag value. |
| MAC Type | Specifies the MAC type. |

Table 72. UNI Port Details (continued)

| Field | Description |
|--------------------|--|
| | <p>The supported values are.</p> <ul style="list-style-type: none"> • Static • Dynamic |
| MAC Type (Static) | <p>The static MAC is configured or learned based on the MAC learning type. If the traffic goes through the PON in the service, static MAC does not age out.</p> <p>The supported values for the MAC learning type are.</p> <ul style="list-style-type: none"> • DHCP • DHCP_ALLOW_RELEARN • ARP • ARP_ALLOW_RELEARN • PPPoE • DHCP_IP_ANTISPOOFING_NO_MAC • DHCP_IP_ANTISPOOFING_MAC • DHCP_NO_MAC • ARP_NO_MAC <p> Note: In the service configuration with DHCP or DHCP_NO_MAC MAC learning type, service-get reports only the last learned MAC address and IP address. If the service is configured on the VEIP or IPhost port of the ONT, this information indicates the WAN interface of the ONT. Otherwise, it indicates the client device behind the ONU when the service is configured on the PPTP port.</p> <p>For more information on MAC Learning Type, see Table 268: MAC Learning Type (on page 580).</p> |
| MAC Type (Dynamic) | <p>A MAC is displayed as dynamic for the following reasons.</p> <ul style="list-style-type: none"> • Learned by the data path of the OLT. • Packets that are trapped in the controller. <p>The default timeout duration for dynamic MAC address is five minutes.</p> <p> Note:</p> |

Table 72. UNI Port Details (continued)

| Field | Description |
|---------------|--|
| |  • The dynamic MAC address is displayed when the DHCP IP assignment cycle progresses. • The static MAC address is displayed when the DHCP cycle is completed. For example, if a DHCP cycle is initiated for IPv4 and IPv6, a dynamic MAC address is displayed for an in-progress DHCP cycle. In contrast, a static MAC address is displayed for a completed DHCP cycle. |
| MAC Address | Specifies the MAC address. |
| Creation Time | Specifies the date and time when the MAC dump was created. |

Alarms

Perform the following steps to view the ONT Alarm details.

1. Select **Monitor > Inventory**.

The Inventory List page appears.

2. Click on the **ONT** tab.
3. Click on the ONT name under the **Name** column.

The ONT Details page appears.

4. Click the **Alarms** tab.

You can view the list of alarms.

For more information on the fields of ONT alarms, see [Table 49: ONT Alarms \(on page 125\)](#).

Events

Perform the following steps to view the event details.

1. Select **Monitor > Inventory**.

The Inventory List page appears.

2. Click on the **ONT** tab.
3. Click on the ONT name under the **Name** column.

The ONT Details page appears.

4. Click the **Events** tab.

You can view the list of events reported for ONT.

For more information on the list of events, see [Table 43: Events List \(on page 117\)](#).

Logs

Perform the following steps to view the log details.

1. Select **Monitor > Inventory**.

The Inventory List page appears.

2. Click on the **ONT** tab.
3. Click on the ONT name under the **Name** column.

The ONT Details page appears.

4. Click the **Logs** tab.

You can view the following type of logs for the ONT.

- **Activity Logs.** Logs generated for the activities performed on the ONT such as part activation, ONT deactivation, and so on. For more information on the field descriptions, see [Table 44: Activity Logs \(Tabular View\) \(on page 119\)](#).
- **Audit Logs.** List of logs triggered for the operations performed on the ONT. For more information on the field descriptions, see [Table 102: Audit Log List \(on page 230\)](#).

Card List

Perform the following steps to view the card list details.

1. Select **Monitor > Inventory**.

The Inventory List page appears.

2. Click on the **ONT** tab.
3. Click on the ONT name under the **Name** column.

The ONT Details page appears.

4. Click the **Card List** tab.

You can view the list of cards associated with the ONT.

For more information on the description of fields on the Card List page, see [Table 45: Card List \(on page 119\)](#).

Subscribers

Perform the following steps to view the subscriber details.

1. Select **Monitor > Inventory**.

The Inventory List page appears.

2. Click on the **ONT** tab.
3. Click on the ONT name under the **Name** column.

The ONT Details page appears.

4. Click the **Subscribers** tab.

You can view the list of subscribers associated with the ONT.

For more information on the description of fields on the subscribers page, see [Table 97: Subscriber List \(on page 224\)](#).

Monitoring Card Details

You can monitor the following details of the card.

- Basic Information
- Device View
- Port List (PON and NNI)
- Audit Log

Perform the following steps to monitor the card details.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **CARD** tab.
3. Click on the card name under the **Name** column.

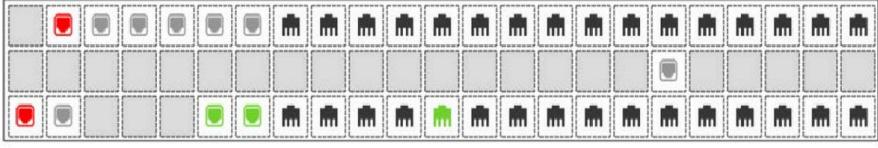
The Card Details page appears.

The following table describes the basic information.

Table 73. Card Basic Information

| Field | Description |
|--------------------------|--|
| Basic Information | |
| Name | Specifies the name of the card. |
| Make | Specifies the vendor name of the card. |
| Model | Specifies the model name of the card. |

Table 73. Card Basic Information (continued)

| Field | Description |
|-------------|--|
| | Example: Radisys-1RU-ETH-AnyPON |
| OLT | Specifies the OLT details associate with the card. |
| Fault State | <p>Specifies the highest severity fault present on the card. The supported states are.</p> <ul style="list-style-type: none"> • WARNING • CRITICAL • MAJOR • MINOR • No Fault <p>For more information about the severity supported by RMS, see Alarm Severity Levels (on page 238).</p> |
| Serial No | Specifies the serial number of the card. |
| Site Name | Specifies the site name of the card. |
| Slot | <p>Specifies the slot name in the rack.</p> <p>Example: olt-Rack1-Shelf1-ETH1</p> |
| Device View | <p>Figure 30. Card View</p>  |
| Port List | You can view the details of the PON and NNI ports configured. For more information, see PON Port (on page 82) and NNI Port Details (on page 99) . |
| Audit Log | Specifies the list of logs triggered for the operations performed on card. For more information on the field descriptions, see Table 102: Audit Log List (on page 230) . |

Monitoring Rack Details

You can monitor the following details of the rack.

- Basic Information
- Device View
- Shelf Details

Perform the following steps to monitor the rack details.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **RACK** tab.
3. Click on the rack name under the **Name** column.

The RACK Details page appears.

The following table describes the basic information of rack.

Table 74. RACK Basic Information

| Field | Description |
|--------------------------|--|
| Basic Information | |
| Name | Specifies the name of the rack. |
| Make | Specifies the vendor name of the rack. |
| Model | Specifies the model name of the rack. |
| Total Shelf | Specifies the total number of shelves available in the rack. |
| Site Name | Specifies the site name where the rack is installed. |
| Serial No | Specifies the serial number of the shelf. |
| Holder State | Specifies the holder state of the rack. The supported states are. <ul style="list-style-type: none">• EMPTY• INSTALLED AND EXPECTED• EXPECTED AND NOT INSTALLED• INSTALLED AND NOT EXPECTED• MISMATCH INSTALLED AND EXPECTED• UNAVAILABLE• UNKNOWN |
| Resource State | Specifies the resource state of the rack. The supported states are. <ul style="list-style-type: none">• PLANNED• INSTALLED• RETIRED |

Table 74. RACK Basic Information (continued)

| Field | Description |
|--------------------------|---|
| Device View | <p>Figure 31. Rack View</p>  |
| Name | Specifies the name of the rack. |
| OLT Name | Specifies the name of OLT installed in the rack shelf. |
| Type | Specifies the type of device, for example, rack. |
| Display ID | Specifies the display ID of the rack. |
| Total Slots | Specifies the number of slots available in the rack. |
| Layout | Specifies the layout (horizontal or vertical) of the rack. |
| Admin. State | Specifies the admin state (ACTIVE or DEACTIVE) of the card ports. |
| Op. State | Specifies the operational state (UP or DOWN) of the card ports. |
| Shelf | |
| Name | Specifies the name of the shelf. |
| Display ID | Specifies the display ID of the shelf. |
| Holder State | Specifies the holder state of the shelf. Example: INSTALLED_AND_EXPECTED |
| Resource State | Specifies the resource state of the shelf. Example: INSTALLED |
| Creation Time | Specifies the date and time when the shelf was created. |
| Shelf Details | Click on the shelf name to view information about shelf. |
| Basic Information | |
| Name | Specifies the name of the shelf, for example, shelf1. |
| Display ID | Specifies the Display ID of the shelf, for example, s1. |
| OLT Name | Specifies name of the OLT placed in the shelf. |
| Shelf No. | Specifies the shelf number, for example, 1. |

Table 74. RACK Basic Information (continued)

| Field | Description |
|--------------------|--|
| Total Slots | Specifies the number of slots on the shelf, for example, 2. |
| Type | Specifies the type of the shelf. |
| MTOSI Type | Specifies Multi-Technology Operations Systems Interface (MTOSI) type. The supported values are: <ul style="list-style-type: none"> • OT_OS • OT_MANAGEMENT_DOMAIN • OT_MANAGED_ELEMENT • OT_TOPOLOGICAL_LINK • OT_SUBNETWORK_CONNECTION • OT_PHYSICAL_TERMINATION_POINT • OT_EQUIPMENT HOLDER • OT_EQUIPMENT |
| Holder Type | Specifies the holder type. |
| Creation Time | Specifies the date and time when the shelf was created. |
| Status Information | <ul style="list-style-type: none"> • Holder State. Specifies the holder state of the shelf, for example, INSTALLED_AND_EXPECTED. • Resource State. Specifies the resource state of the shelf, for example, INSTALLED. |
| Audit Log | Specifies the list of tasks triggered on rack. For more information on the field descriptions, see Table 102: Audit Log List (on page 230) . |

Monitoring SFP

RMS retrieves the Inventory configuration for Field Replaceable Units (FRUs), which has the SFP information of PON ports per ME. The OLT reports the SFP for each PON port after the OLT activation.

CBAC collects the SFP inventory information for each PON port of the OLT and sends the PORT-SFP-INVENTORY event towards RMS.

RMS supports the retention of historical KPIs for the NNI SFP module.



Note: When the SFP device is plugged out from the OLT, the corresponding SFP device information is removed from the **Monitor** page.

Perform the following steps to monitor the SFP details.

1. Select **Monitor > Inventory > Inventory**.
2. Click on the **SFP** tab.
3. Click on the SFP name under the **Name** column.

The SFP details page appears.

The following table describes the basic information of SFP.

Table 75. SFP Basic Information

| Field | Description |
|--------------------------|--|
| Basic Information | |
| Name | Specifies the name of the SFP. Example: SFP_UVS2BBX |
| Make | Specifies the vendor name of the SFP. Example: FINISAR CORP |
| Model | Specifies the model name of the SFP. |
| Display ID | Specifies the display ID of the SFP. |
| Serial No. | Specifies the serial number of the SFP. Example: UVS2BBX |
| Revision No. | Specifies the revision number of the SFP. |
| OLT | Specifies the name of the OLT to which the SFP is associated with. Example: olt-185 |
| SFP | Specifies if the OLT detects that an SFP module is missing on the port during the port activation or when the SFP module is removed. The supported values are. <ul style="list-style-type: none"> • Missing • Present |
| SFP Technology | Specifies the technology used by SFP. The supported values are. <ul style="list-style-type: none"> • GPON • XGSPON |
| GPON Nominal Bitrate | Specifies the nominal bit rate of the GPON SFP. The nominal bit rate is specified in units of 100 Megabits per second, which is rounded off to the nearest 100 Megabits per second. The bit rate includes those bits necessary to encode |

Table 75. SFP Basic Information (continued)

| Field | Description |
|-------------------------------|--|
| | and delimit the signal as well as those bits carrying data information. Example: 10.3 |
| GPON Signal Range | Specifies the signal range of the GPON SFP. Example: 20 |
| GPON Transmitter Wavelength | Specifies the transmitter wavelength of the GPON SFP. Example: 850 |
| XGSPON Nominal Bitrate | Specifies the nominal bit rate of the XGSPON SFP. The nominal bit rate is specified in units of 100 Megabits per second, which is rounded off to the nearest 100 Megabits per second. The bit rate includes those bits necessary to encode and delimit the signal as well as those bits carrying data information. |
| XGSPON Signal Range | Specifies the signal range of the XGSPON SFP. |
| XGSPON Transmitter Wavelength | Specifies the transmitter wavelength of the XGSPON SFP. |
| Part Number | Specifies the part number of the SFP. Example: FTLX8574D3BCL |
| Manufacturing Date | Specifies the manufacturing date of the SFP. Example: 09 JUL 2020 |
| OLT Port | Specifies the OLT port. Example: card1-NNI-4 |
| SFP Optical Information | <p>You can view the SFP optical information generated for the SFP.</p> <ul style="list-style-type: none"> • Current (mA) • Voltage (Volts) • Temperature (degree) • TX Power (dBm) • RX Power (dBm) • Technology <p> Note:</p> |

Table 75. SFP Basic Information (continued)

| Field | Description |
|----------------------|--|
| |  <ul style="list-style-type: none"> • If the PON port is configured in CPON port mode, GPON and XGSPON live SFP KPIs are displayed by default. • Click the Refresh button to view the latest SFP optical information data. |
| Historical KPIs |  <p>Note: If the PON port is configured in CPON port mode, you can select GPON or XGSPON port technology from the list to view the historical SFP KPIs.</p> |
| Current (mA) | Displays the graphical view of the current (mA) of the SFP. You can retrieve this information by hourly, daily, and weekly. |
| Temperature (degree) | Displays the graphical view of the SFP temperature. You can retrieve this information by hourly and daily. |
| TX Power (dBm) | Displays the graphical view of the transmit power of the SFP. You can retrieve this information by hourly and daily. |
| RX Power (dBm) | Displays the graphical view of the received power of the SFP. You can retrieve this information by hourly and daily. |
| Voltage (volts) | Displays the graphical view of the SFP voltage. You can retrieve this information by hourly and daily. |

Blacklisted ME

To access this page, click **Monitor** from the top right corner of the page and select **Inventory > Blacklisted ME** from the left-hand side of the menu.

RMS monitors the blacklisted ONTs and the OLTs to which the blacklisted ONTs are connected. Once the blacklisted ONT is discovered, RMS deactivates the ONT and reports an alarm.

When RMS reports an UNKNOWN-ONT-DISCOVERED alarm and if the ONT serial number is not present in the RMS database, RMS adds the ONT to the blacklisted MEs list. You can view the blacklisted ONT in the OLT topology, which is connected to the PON port. When the user adds the ONT to RMS, RMS clears the same ONT from the blacklist.

RMS supports for reporting the **Active Firmware Version** and **Standby Firmware Version** for the blacklisted ONT discovered on the PON port.

Field Descriptions

The following table describes the fields on the Blacklisted ME page.

Table 76. Blacklisted MEs

| Field | Description |
|-------------------------------|--|
| ONT | |
| Serial No. | Specifies the serial number of the ONT. |
| OLT Name | Specifies the name of the OLT associated with the ONT. |
| OLT Serial Number | Specifies the serial number of the OLT associated with the ONT. |
| Technology | Specifies the technology supported by ONT. |
| Supported Connectivity Models | <p>Specifies the supported connectivity model that must be used for the services on the ONU.</p> <p>The supported values are.</p> <ul style="list-style-type: none"> • N:1 bridging • 1:M mapping • 1:P filtering • N:M bridge-mapping • 1:MP map-filtering • N:P bridge-filtering • N:MP bridge-map-filtering <p>The default value must be same as the Supported Connectivity Models reported by the ONU.</p> <p>The default value for the residential service is 1:MP map-filtering.</p> |
| Current Connectivity Models | <p>Specifies the current connectivity model that must be used for the services on the ONU.</p> <p>The supported values are.</p> <ul style="list-style-type: none"> • N:1 bridging • 1:M mapping • 1:P filtering • N:M bridge-mapping • 1:MP map-filtering • N:P bridge-filtering • N:MP bridge-map-filtering |

Table 76. Blacklisted MEs (continued)

| Field | Description |
|--------------------------|---|
| | The default value must be same as the Current Connectivity Models reported by the ONU. The default value for the residential service is 1:MP map-filtering. |
| OLT Port | Specifies the port name of the OLT associated with the ONT. |
| Registration Id | Specifies the registration ID of ONT. The registration ID must contain only alphanumeric characters and length must be 72 alphanumeric characters. |
| Vendor Id | Specifies the vendor ID of the ONT. Example: RDSY |
| Equipment Id | Specifies the equipment ID of the ONT. Example: ES6005 |
| UNI Ports | Specifies the list of UNI ports connected to the ONT. |
| UNI Port Count | Specifies the number of UNI ports connected to the ONT. |
| Creation Time | Specifies the date and time when the blacklisted ONT was created. |
| Active Firmware Version | Specifies the firmware version of the active ONT. |
| Standby Firmware Version | Specifies the firmware version of the standby ONT. |
| OLT | |
| Serial Number | Specifies the serial number of the OLT. |
| Make | Specifies the vendor name who manufactured the OLT. |
| Model | Specifies the model name of the OLT. |
| MAC Address | Specifies the MAC address of the OLT. Example: 28:b9:d9:e2:6f:5e |
| Creation Time | Specifies the date and time when the blacklisted OLT was created. |

Single Click Provisioning

You can directly create an ONT, subscriber, and service using single click provisioning.

Perform the following steps to provision the ONT using single click.

1. Select **Monitor > Inventory > Blacklisted ME**.
2. Click on the **ONT** tab.

A list of blacklisted ONTs are displayed.

3. Navigate to the applicable ONT.
4. Click on the three dots icon (⋮) and select **Single Click Provisioning**.

Figure 32. Single Click Provisioning

| Serial No. | OLT Name | OLT Serial No. | Technology | Supported Connectivity Models | Current Connectivity Models | OLT Port | Registration Id | Vendor |
|--------------|----------|----------------|------------|---|-----------------------------|----------|--------------------------|---|
| ISKT4285D740 | vs4 | RSYSD9E47D89 | gpon | N:1 bridging, 1:M mapping, 1:P filtering ... Read more | 1:MP map-filtering | SFPON-1 | 0xONU7478762002806211405 |  Single Click Provisioning |
| ISKT4285D730 | vs4 | RSYSD9E47D89 | gpon | N:1 bridging, 1:M mapping, 1:P filtering ... Read more | 1:MP map-filtering | SFPON-1 | 0xONU4539589599778027461 | ISKT  |
| ISKT4285D720 | vs4 | RSYSD9E47D89 | gpon | N:1 bridging, 1:M mapping, 1:P filtering ... Read more | 1:MP map-filtering | SFPON-1 | 0xONU546185760471285372 | ISKT  |

5. Click **Activate** under the **Action** Column.

Figure 33. Activate ONT

| Single Click Provisioning | | | | | | | | |
|--|---------------|------------------|----------|----------------|----------|--------------------------|--------|--------|
| You can select any blacklisted ONT from the list below to quickly create subscribers and activate them | | | | | | | | |
| ONT Serial No. | ONT Vendor Id | ONT Equipment Id | OLT Name | OLT Serial No. | OLT Port | Action | Search | Filter |
| ISKT4285D740 | ISKT | G64_10 | vs4 | RSYSD9E47D89 | SFPON-1 | Activate | | |
| Showing 1 to 1 of 1 entries | | | | | | | | |

6. Select the **Service Template** from the list to active services for the ONT and verify the other details.

Figure 34. ONT Service Template

The screenshot shows a 'Single Click Provisioning' interface. At the top, there are two dropdown menus: 'Blacklisted ME's Serial Number' (set to 'ISKT4285D740') and 'Blacklisted ME's Equipment ID' (set to 'G64_10'). Below these are fields for 'Connected OLT's Configuration': 'OLT Name' (set to 'vs4') and 'OLT Serial Number' (set to 'RSYSD9E47D89'). Further down, 'OLT PON Port' is set to 'SFPPON-1'. A section titled 'Select a template from below to activate services for the ONT' contains a dropdown menu 'Service Template *' (set to 'Select'). Below this, a note says 'Configure the prefix that will be used for configuring the ONT, subscribers and their services. By default the blacklisted ONT's serial number will be used.' Another note states 'This is introduced to shorten the time required to create an ONT, subscribers and activate the services.' A 'Prefix word to be used' field contains 'RSYSD9E47D89'. At the bottom are 'Cancel' and 'Activate' buttons.

7. Click **Activate.**

A success message is displayed with ONT, subscriber, and service detail.

Figure 35. Success Message

The screenshot shows a 'Single Click Provisioning' interface with a success message. The message states: 'Successfully activated services for the blacklisted ME with serial number ISKT4285D730, below are the details.' Below this, it lists the activated components: 'ONT' (set to 'RSYSD9E47D89_ISKT4285D730'), 'Subscriber' (set to 'RSYSD9E47D89_ISKT4285D730_Subscriber'), and 'Services' (set to 'RSYSD9E47D89_ISKT4285D730_Service_1'). At the bottom is a 'Close' button.

Controller

To access this page, click **Monitor** from the top right corner of the page and then select **Inventory > Controller** from the left-hand side of the menu.

You can monitor the controller information. The information includes the following.

- List of OLTs, ONTs, and CPEs associated with the controller.
- List of faults and events generated for the controller.
- List of resynchronization and data synchronization request.
- List of audit logs generated for the controller.

Field Descriptions

The following table describes the fields on the Controller List page.

Table 77. Controller List

| Field | Description |
|-------------------|--|
| Name | Specifies the name of the controller. Example: CBAC |
| Admin State | Specifies the admin state of the controller. Example: ACTIVE |
| Operational State | Specifies the operational state of the controller. <ul style="list-style-type: none">• Up. Shows that the controller is operationally up.• Down. Shows that the controller is operationally down. |
| Rest | Specifies the state of the REST server. <ul style="list-style-type: none">• Up. Shows that the REST server is operationally up.• Down. Shows that the REST server is operationally down. |
| Kafka | Specifies the state of the Kafka message bus. <ul style="list-style-type: none">• Up. Shows that the Kafka is operationally up.• Down. Shows that the Kafka is operationally down. |
| Adaptor | Specifies the name of the adaptor. Example: SDPON |
| Management Domain | Specifies the name of the management domain. Example: RMS |
| Kafka Host | Specifies the IP address of the Kafka. Example: 172.27.173.134 |
| Kafka Port | Specifies the port number of the Kafka. Example: 30000 |
| Kafka User Name | Specifies the Kafka user name. Example: ams |
| Kafka Alarm Topic | Specifies the CBAC alarm topic to listen and receive faults. Example: EMSFAULT |

Table 77. Controller List (continued)

| Field | Description |
|--------------------------|--|
| Kafka Notification Topic | Specifies the CBAC notification topic to listen and receive notifications. Example: EMSNOTIFICATION |
| Kafka KPI topic | Specifies the CBAC KPI topic to listen and receive KPIs. Example: EMSKPINOTIFICATION |
| REST Base URL | Specifies the base URL of the REST server. Example: <a href="https://<IP>:31082/sdpon/v1">https://<IP>:31082/sdpon/v1 |
| REST User Name | Specifies the valid REST server username. |
| REST Super User Name | Specifies the valid REST server super username. |
| Mode | Specifies the mode of controller. Example: DISTRIBUTED |
| Backup Status | Specifies the controller configuration backup status. The supported values are. <ul style="list-style-type: none"> • BACKUP-INITIATED • BACKUP-FAILED • BACKUP-SUCCESSFUL |
| Restore Status | Specifies the controller configuration restore status. The supported values are. <ul style="list-style-type: none"> • RESTORE-INITIATED • RESTORE-FAILED • RESTORE-SUCCESSFUL |
| Upgrade Status | Specifies the upgrade status of the controller. The supported values are. <ul style="list-style-type: none"> • UPGRADE-INITIATED • UPGRADE-FAILED • UPGRADE-SUCCESSFUL |
| Version | Specifies the version of the controller. |
| Creation Time | Specifies the date and time when the controller was created. |

Monitoring Controller

You can monitor the following details of the controller.

- Basic Details
- Topology

- Reconciliation
- Troubleshooting
- Device List
- Fault List
- Events List
- Resync Requests
- Data Sync Requests
- Audit Log

Perform the following steps to monitor the controller details.

1. Select **Monitor > Inventory > Controller**.

The **Controller List** page opens.

2. Click on the controller name under the **Name** column.

The Controller Details page appears.

The following table describes the basic information.

Table 78. Controller Information

| Field | Description |
|--------------------------|--|
| Name | Specifies the name of the controller. |
| Admin State | Specifies the admin state of the controller. |
| Kafka Host | Specifies the IP address of the Kafka. |
| Kafka Port | Specifies the port number of the Kafka. |
| Kafka User Name | Specifies the Kafka username. |
| Kafka Alarm Topic | Specifies the CBAC alarm topic to listen and receive faults. |
| Kafka Notification Topic | Specifies the CBAC notification topic to listen and receive notifications. |
| Kafka KPI Topic | Specifies the CBAC KPI topic to listen and receive KPIs. |
| Kafka Current KPI Topic | Specifies the current KPI topics. |
| SDPON Version | Specifies the SDPON version. |
| CBAC Release Version | Specifies the release version of the CBAC. Example: CBAC-R4.1.0 |
| Monitoring Endpoint Port | Specifies the port number of the monitored entity. Example: 30014 |

Table 78. Controller Information (continued)

| Field | Description |
|------------------------|---|
| Monitoring Endpoint IP | Specifies the monitoring REST server IP address, which is running on the RMS server or an external server. Example: <code>http://<host-ip>:<monitoring-rest-servernodeport></code> Where, Host IP is the system IP where monitoring PODs (Grafana, Prometheus, and monitoring REST server) are running. This PODs can either run with RMS PODs or as a separate entity. |
| Operational State | Specifies the operational state of the controller. |
| REST | Specifies the operational state of the REST server. |
| Kafka | Specifies the operational state of the Kafka message bus. |
| Adaptor | Specifies the name of the adaptor. The default value is SDPON. |
| Management Domain | Specifies the name of the management domain. |
| REST Base URL | Specifies the IP address of the REST server. Example: <code>https://<IP>:31082/sdpon/v1</code> |
| Last Backup Time | Date and time when the last controller backup was taken. |
| Mode | Specifies the controller mode type. Example: DISTRIBUTED |
| Upgrade Status | Specifies the upgrade status of the controller. Example: UPGRADE-SUCCESSFUL |
| CBAC Build Version | Specifies the build version of the CBAC. Example: 1.21.114 |
| Grafana Port | Specifies the IP address of Grafana. |
| Grafana IP | Specifies the port number of Grafana. |

You can also monitor the following.

- Devices (OLT, ONT, and CPE) associated with controller. See [Monitoring OLT \(on page 67\)](#) and [Monitoring ONT \(on page 156\)](#).
- Alarms reported for controller. For more information, see [Alarm \(on page 115\)](#).
- Events reported for controller. For more information, see [Table 43: Events List \(on page 117\)](#).
- Resynchronization Request.
- Data Synchronization Request. See [Data Synchronization Request \(on page 233\)](#).
- Audit Logs. See [Audit Log \(on page 229\)](#).

Controller Topology

Perform the following steps to view the physical and logical topology of the controller.

1. Select **Monitor > Inventory > Controller**.

The **Controller List** page opens.

2. Click on the controller name under the **Name** column.

The Controller Details page appears.

3. Click on the **Topology** tab.

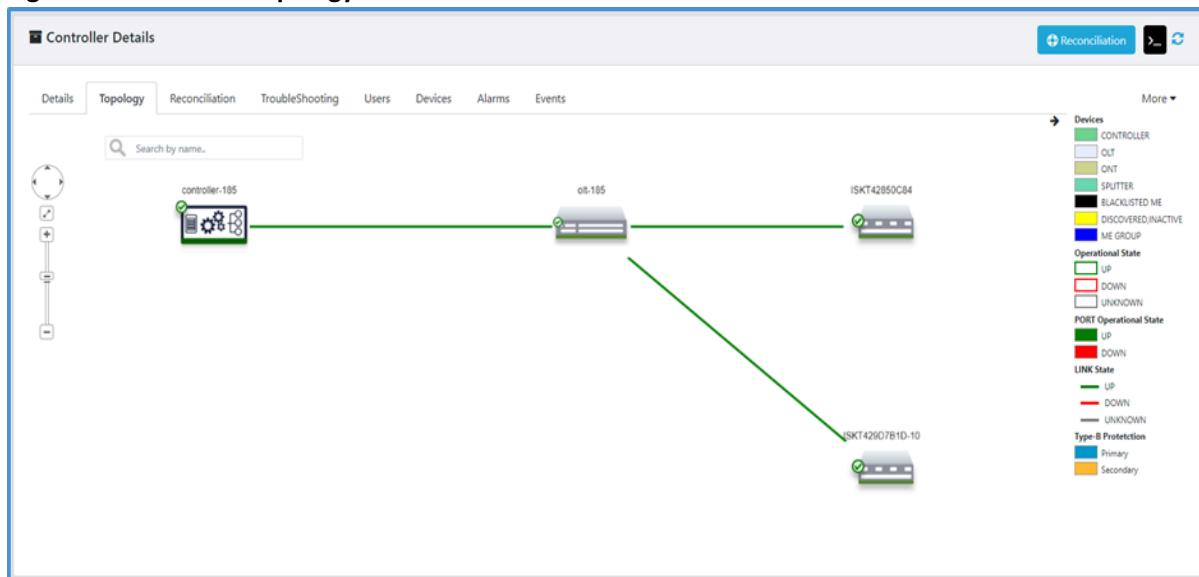
You can view the physical and logical topology of the controller.

The following figure shows the topology of the controller. This topology shows how the controller is connected to the devices (OLT and ONT).

You can perform the following tasks from the controller topology page.

- Click the zoom slider to zoom in and zoom out to the topology.
- Reposition the topology view (left, right, up, or down) by clicking the respective arrow button.
- You can search for various elements of your network infrastructure.

Figure 36. Controller Topology



Reconciliation



Note: During reconciliation if there is a version mismatch between CBAC and RMS, it is recommended to resolve the conflicts for new features added by RMS (in higher version) only after upgrading CBAC to the latest version.

Perform the following steps to monitor the reconciliation.

1. Select **Monitor > Inventory > Controller**.

The **Controller List** page opens.

2. Click on the controller name under the **Name** column.

The Controller Details page appears.

3. Click on the **Reconciliation** tab.

You can view the reconciliation details of the controller.

Reconciliation is a two-step procedure.

1. Reconcile resources between RMS and CBAC.
2. Resolve the reconciled resources.

Sometimes, when you perform any operation (add, edit, or delete) on the resource from CBAC, the respective operation does not reflect in RMS, leading to a configuration mismatch between CBAC and RMS.

RMS supports the reconciliation of resources between RMS and CBAC and ensures that the operations performed on RMS reflect on CBAC. This feature is triggered only when the “Operational State” of the controller is UP and resolves the configuration mismatch between RMS and CBAC.

After successfully restoring a backed-up DB, resources managed from RMS and CBAC must be synchronized. To ensure the same, RMS supports a reconciliation procedure. CBAC enables REST APIs for RMS to fetch/GET all the resources present on CBAC. The following status is marked after fetching all the resources from RMS to CBAC.

- **Pending:** Resource exists on RMS and does not exist on CBAC.
- **Conflict:** Resource exists on RMS and CBAC with conflict (only on the parameters present in PATCH/PUT).
- **Orphan:** Resource does not exist on RMS and exists on CBAC.
- **Failures:** RMS fails in creation of resources on CBAC.



Note:

- If the OLT is in pending state, the network services (E-LINE, E-LAN, ACL profile, ERPS instances, rings, and MEP instances) and service profiles (bandwidth, CoSQ, shaper, VNet, MVLAN, SIP agent, and network dial plan) are reconciled automatically.
- If the OLT is in pending state and if the OLT is referring to the local profiles (alarm, log, NTP, TACACS, and alarm soak), it is recommended to follow the below steps
 - Dissociate local profiles in the OLT
 - Create OLT
 - Create local profiles
 - Associate local profiles to the OLT



- If the admin state of the resource is CONFLICT, the user needs to synchronize the RMS resource state with the CBAC resource from the **Configuration > Inventory** page.
- OLT name can be updated only when it is in a **DEACTIVE** state. If the OLT is in a **Conflict** state with a name mismatch, the user must deactivate the OLT and perform the update and reconciliation.
- After the OLT backup, the global profiles must not be removed if there are any type-B dual-homing (cross-shelf) configurations.

Reconciliation Sequence

The following is the sequence in which RMS reconciles resources with CBAC.

1. Controller Settings (CBAC, Security, and IGMP)
2. Global profiles are categorized into service and non-service profiles.
 - a. Non-Service Profiles (Silent Reconciliation)
For example: ACE profile, ACL profile, LAG alarm profile, ERPS profile, MEP profile, ME alarm profile, log profile, NTP profile, SFP alarm profile, policer profile, storm control profile, ANI-G alarm profile, and IP-Host options profile.
 - b. Service Profiles
For example: MVLAN profile, VNET profile, bandwidth profile, shaper Profile, CoSQ profile, SIP agent profile, network dial plan profile, POTS Profile, and IGMP Profile.
3. OLT
4. Ports
 - a. NNI Ports
 - b. Alarm Ports
 - c. PON Ports
5. Network Services
 - a. LAG
 - b. ERPS Ring
 - c. ELINE and ELAN
 - d. ACL
 - e. MEP Instance
 - f. ERPS Instance
6. Type-B Pairs
7. ONU and UNI Ports (Only explicit ports)
8. Subscriber
9. Services

Reconciliation of Associations

This section explains the association of reconciled resources.

ACL Profiles. Synchronizethe ACL profile association by retrieving all the associated ACL profiles from CBAC (retrieve all ACL profiles of OLT) and reconciling them with the associated ACL profiles in RMS.

Storm Control Profile. Synchronize the storm profile association by retrieving all the associated storm profiles from CBAC (retrieve all storm profiles of OLT) and reconciling themwith the associated ACL profiles in RMS.

RMS Handling of Silent Reconciliation Failures

Global profiles (non-service profiles) are silently reconciled by RMS using GET from CBAC. When silent reconciliations fail (500 Internal processing errors or timeout failures), RMS lists the failures in a separate tab in the GUI.



Note:

- The average time to synchronize RMS and CBAC is 6 to 7 minutes.
- Reconciliation of resources follows the order of reconciliation as mentioned in the [Reconciliation Sequence \(on page 189\)](#).

Resolution of Reconciled Resources

This section explains the resolution of reconciled resources.

RMS Handling of Silent Resolution Failure

RMS silently resolves global profiles (non-service profiles) to CBAC for the following scenarios.

- **Creation Failure:** RMS fails in creating resources on CBAC (pending scenario) if any HTTP response code other than **200 OK**, **201 created**, or **timeout** is observed. RMS lists these failures in a separate tab in the GUI.
 - **Update Failure:** RMS fails in updating resources on CBAC (conflict scenario) if any HTTP response code other than **200 OK** or **timeout** is observed. RMS lists these failures in a separate tab in the GUI.
1. **PENDING**– RMS creates the resource on the controller.
 - a. If the parent resource is PENDING, do not reconcile the child resources. Upon creation, attempt the children resources creation.
 - b. RMS needs to ensure the admin state of a resource on CBAC is the same as that on RMS.
 2. **CONFLICT**– RMS provides the option to PUT/PATCH the resource on a controller.

- a. ADMIN state to be reconciled – OLT, ONT, services, and so on.
 - If the conflict is only on the admin state – Disable the **Modify** button. The users can activate/deactivate by moving to configuration.
 - If conflict is in the admin state and other fields, the user triggers modify for this resource, then activate/deactivate by moving to configuration.
 - b. Network service objects state (ENABLED/DISABLED) – ELine, ELAN, LAG, and so on to be reconciled.
 - c. The resources controller does not support PATCH/PUT is marked as ORPHAN as RMS has no way to resolve the conflict. RMS displays the reason for putting this resource in the ORPHAN state.
 - d. For PON port, the port must be **Disabled** for modifying the following fields.
 - Port Mode
 - GPON Downstream FEC
 - XGSPON Downstream FEC
 - Enable PON Encryption
 - PON Encryption Key Interval
3. **ORPHAN:** RMS provides the option to DELETE (force_delete) the resource from SDPON.
 - a. SDPON deletes the children upon receiving force_delete of the parent resource. Force delete on CBAC ensures deletion of child resources.
 - Subscriber – Ensure the deletion of subscriber and services associated with the subscriber.
 - ONU – Ensure the deletion of ONU and all UNI Ports associated with the ONU.
 - OLT – Ensure the deletion of OLT and all the ports (PON, NNI, and Alarm Ports) associated with the OLT.

A user can resolve reconciled resources from the reconciliation tab, and the user needs to ensure the order for the resolution of resources (pending and orphan resources).

Resolution Order for Pending Resources

- The following is the resolution order of the pending reconciled resources.
1. Service Profiles
 2. OLT
 3. Ports
 - a. NNI Ports
 - b. Alarm Ports
 4. Network Services
 - a. LAG
 - b. ERPS Ring
 - c. ELINE and ELAN
 - d. ACL

- e. MEP Instance
 - f. ERPS Instance
5. Resolve PON Ports
 6. Type-B Pairs
 7. ONU and UNI Ports (Only explicit ports)
 8. Subscriber
 9. Services



Note: Controller settings (CBAC, security, IGMP) and non-service profiles are autoresolved by RMS.

Resolution Order for Orphan Resources

The following is the resolution order of the orphan reconciled resources.

1. Service Profiles
2. Services
3. Subscriber
4. UNI Ports (Explicit)
5. ONU
6. Type-B Pairs
7. N/W Services
 - a. ERPS Instance
 - b. MEP Instance
 - c. ACL
 - d. ELAN, and ELine
 - e. ERPS Ring
 - f. LAG
8. Ports
 - a. PON Ports
 - b. Alarm Ports
 - c. NNI Ports
9. OLT

Resolution of Associations

The following is the resolution order of the associated reconciled resources.

ACL and Storm Profile

If associated ACL and storm profiles are available under the **Pending** tab at RMS level. Disassociate and associate the ACL and storm profiles to the OLT. For more information, see [Associate the ACL Profile to the OLT \(on page 392\)](#) and [Associate the Storm Profiles to the OLT \(on page 325\)](#).



Note: These ACL and storm profiles are silently reconciled and added at CBAC-D.

ACL Profile

For an orphan ACL profile, if it is associated with OLT, the user must disassociate the profile from the OLT. The PATCH on ACL profiles is not supported.

Storm Control Profile

For an orphan storm control profile, if it is associated with OLT, the user can disassociate the profile from the OLT. The delete option is not provided. PATCH on storm control profile is not supported.

Reconciliation Procedure

Perform the following steps for reconciliation.

1. Silent reconciliation of non-service profiles with CBAC.
 - a. Push what is there in RMS to CBAC.
 - b. Get all the profiles from RMS and synchronize on CBAC.
2. Reconcile OLTs
 - a. Pending
 - Do not reconcile child resources.
 - When resolving the conflict, create child resources automatically.

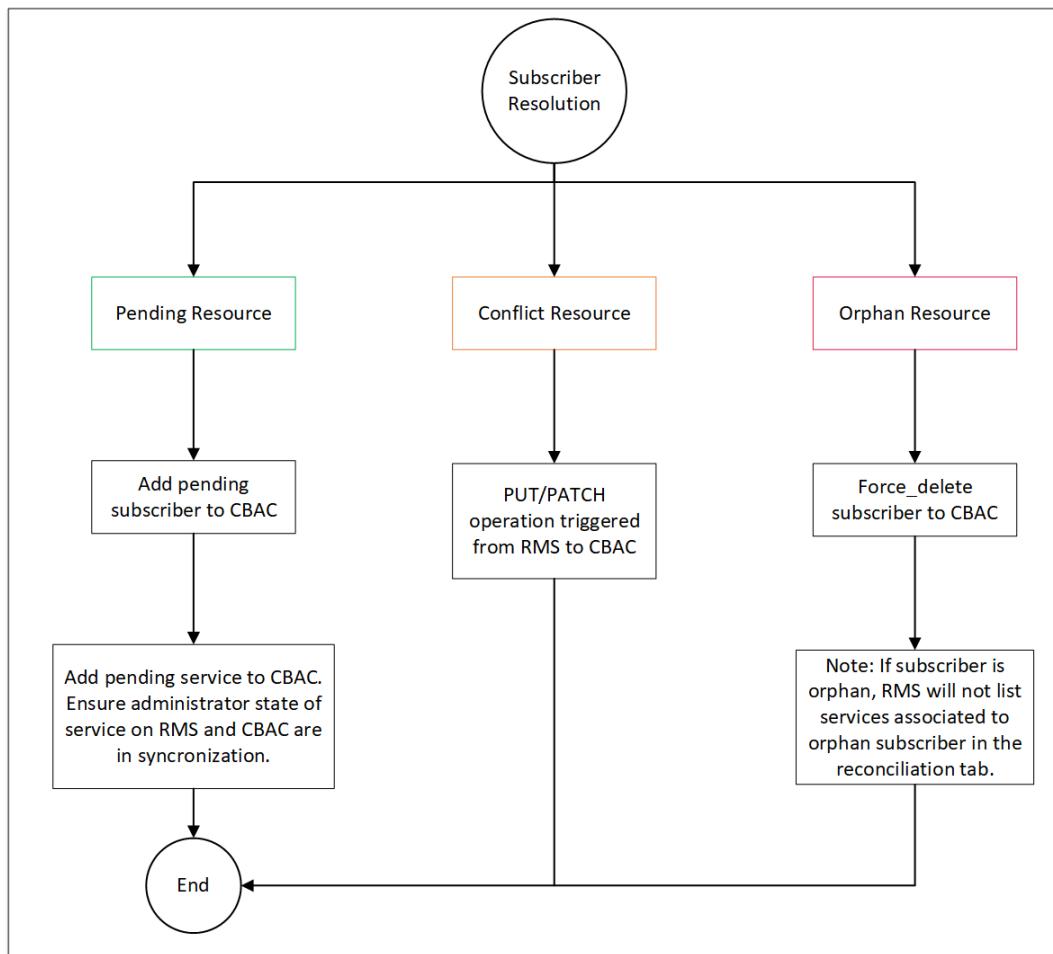
Example:

- OLT – OLT, ports (NNI and alarm), network services, PON port, Type-B pairs, service profiles, ONU, UNI, subscriber, and services.
 - PON port – PON Port, ONU, UNI, subscriber, and services.
 - ONU – ONU and UNI
 - Subscriber – Subscriber and Services
- b. Conflict/In Sync/Orphan
 - Follow the order for the resolution of pending reconciled resources. To view the resolution order, refer to the [Resolution Order for Pending Resources \(on page 191\)](#).
 - Follow the order for the resolution of orphan reconciled resources. To view the resolution order, refer to the [Resolution Order for Orphan Resources \(on page 192\)](#).

Workflow for Subscriber Resolution

The following diagram explains the workflow for the subscriber resolution.

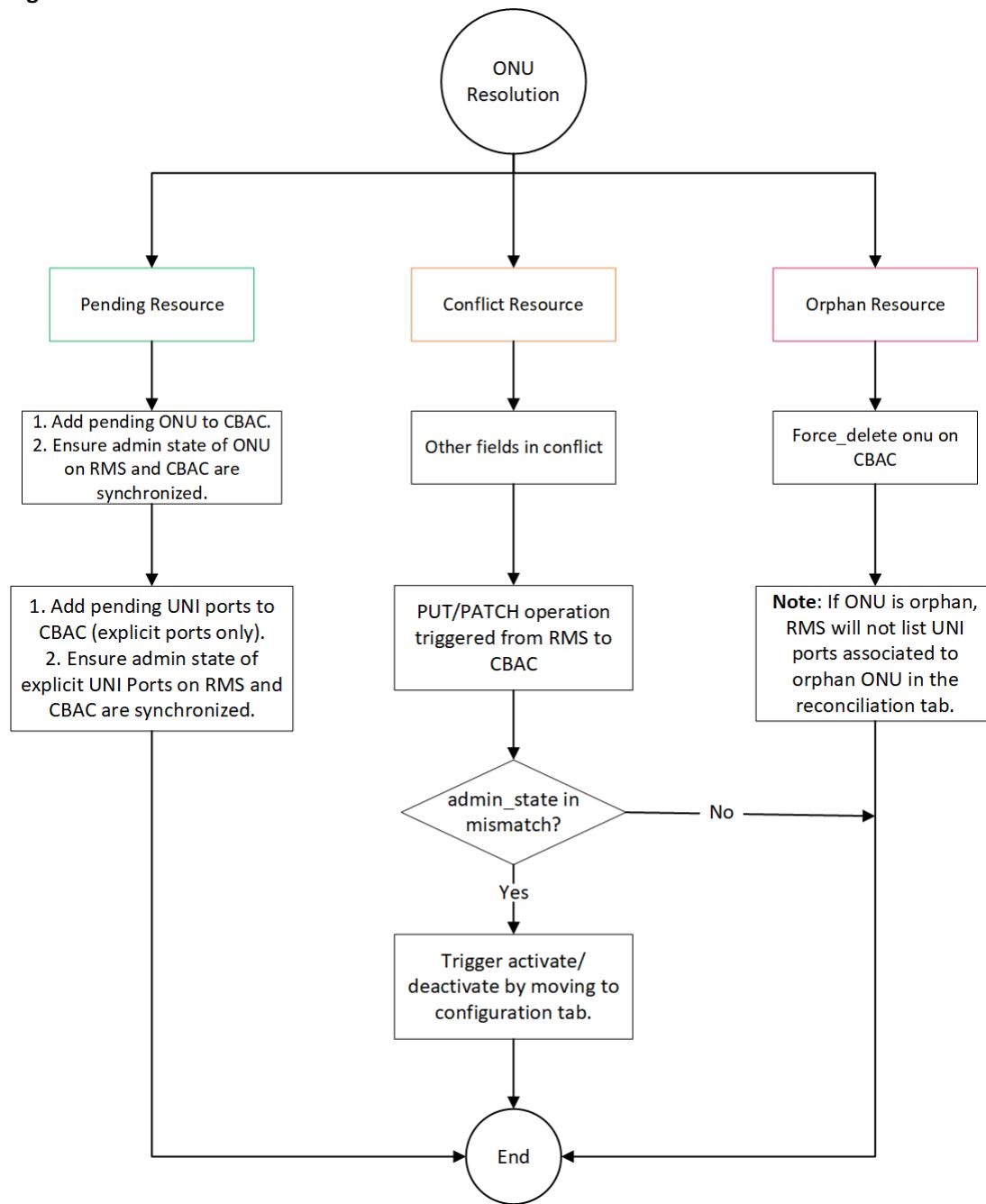
Figure 37. Subscriber Resolution



Workflow for ONU Resolution

The following diagram explains the workflow for the ONU resolution.

Figure 38. ONU Resolution



Perform the following steps for reconciliation operation.

1. Select **Monitor > Inventory > Controller**.

The Controller List page appears.

2. Click on the controller name from the **Name** column.

The Controller details page appears.

3. Click the **Reconciliation** tab and then click the **Reconciliation** icon from the top right corner of the page.

When you click the **Reconciliation** icon, the RMS sends the GET-ALL request to retrieve all resources (For example, retrieve all bandwidth profiles, VNet profiles, MVLAN profiles, and so on) from CBAC.

When the request from RMS is accepted, CBAC sends all the resources that were configured in CBAC and the RMS reconciliation page lists the resources that are retrieved from CBAC.

The CBAC microservices supports the “Action” (create or delete) procedures from RMS when the previous “Action” procedure is in progress, for example,

- When the activate resource is in progress, the deactivate procedure is supported.
- When the deactivated resource is in progress, the activate procedure is supported.

The CBAC microservices allows the "Action" procedure irrespective of whether the resource is reachable or not. The request is buffered and executed when the resource is reachable.

Resources present in CBAC, but not in RMS. The supported action for this type of resource is Delete.

The following table describes the fields on the orphan tab of the Reconciliation page.

Table 79. Reconciliation Orphan

| Field | Description |
|-------------------|---|
| STATUS | Specifies reconciliation status of controller. The supported values are. <ul style="list-style-type: none">• NOT-INITIATED• INITIATED• COMPLETED• FAILED |
| Resource Name | Specifies the name of the resource. Example: service1 |
| Resource Type | Specifies the type of the resource. Example: subscriber_service |
| Resource Sub Type | Specifies the sub type of the resource. |
| Parent Name | Specifies the parent name of the resource. Example: sub2 |
| Action Status | Specifies the action status of the operation performed for the resource. The supported values are. <ul style="list-style-type: none">• SUCCESS• FAILURE |
| Comment | Specifies the comment for the controller. |
| Actions | Specifies the action that you can perform for the resource. The supported action is. |

Table 79. Reconciliation Orphan (continued)

| Field | Description |
|-------|--|
| | <ul style="list-style-type: none"> Delete. You can delete the resource whose resource state is ORPHAN. The resource is deleted from RMS. |

Resources present at RMS and CBAC but have a few differences. You can compare the configuration between RMS and CBAC and resolve the conflict by accepting the latest configuration. The supported action for this type of resource is Modify.

The following table describes the fields on the conflict tab of the Reconciliation page.

Table 80. Reconciliation Conflict

| Field | Description |
|-------------------|--|
| STATUS | Specifies reconciliation status of controller. The supported values are. <ul style="list-style-type: none"> NOT-INITIATED INITIATED COMPLETED FAILED |
| Resource Name | Specifies the name of the resource. Example: service1 |
| Resource Type | Specifies the type of the resource. Example: subscriber_service |
| Resource Sub Type | Specifies the sub type of the resource. |
| Parent Name | Specifies the parent name of the resource. Example: sub2 |
| Action Status | Specifies the action status of the operation performed for the resource. The supported values are. <ul style="list-style-type: none"> SUCCESS FAILURE |
| Comment | Specifies the comment for the controller. |
| Actions | Specifies the action that you can perform for the resource. The supported action is. <ul style="list-style-type: none"> Modify. You can modify the configuration whose resource state is CONFLICT. |

Resources present in RMS, but not in CBAC. The supported action for this type of resource is Create.

The following table describes the fields on the pending tab of the Reconciliation page.

Table 81. Reconciliation Pending

| Field | Description |
|-------------------|---|
| STATUS | Specifies reconciliation status of controller. The supported values are. <ul style="list-style-type: none"> • NOT-INITIATED • INITIATED • COMPLETED • FAILED |
| Resource Name | Specifies the name of the resource. Example: service1 |
| Resource Type | Specifies the type of the resource. Example: subscriber_service |
| Resource Sub Type | Specifies the sub type of the resource. |
| Parent Name | Specifies the parent name of the resource. Example: sub2 |
| Action Status | Specifies the action status of the operation performed for the resource. The supported values are. <ul style="list-style-type: none"> • SUCCESS • FAILURE |
| Actions | Specifies the action that you can perform for the resource. The supported action is. <ul style="list-style-type: none"> • Create. You can create a resource whose resource state is PENDING. The resource is created in CBAC. |

RMS fails to create resources on CBAC.

The following table describes the fields on the failures tab of the Reconciliation page.

Table 82. Reconciliation Failures

| Field | Description |
|--------|---|
| STATUS | Specifies the reconciliation status of the controller. The supported values are. <ul style="list-style-type: none"> • NOT-INITIATED • INITIATED |

Table 82. Reconciliation Failures (continued)

| Field | Description |
|-------------------------------|---|
| | <ul style="list-style-type: none"> COMPLETED FAILED |
| Resource Name | Specifies the name of the resource. Example: service1 |
| Resource Type | Specifies the type of the resource. Example: subscriber_service |
| Resource Sub Type | Specifies the sub type of the resource. |
| Resource State | Specifies the state of the resource. |
| Reconciliation Failure Reason | Specifies the failure reason for the resource. |

Troubleshooting

You can perform the following troubleshooting tasks from the controller page.

- [Ping \(on page 199\)](#)
- [Traceroute \(on page 200\)](#)

Ping

You can ping controller to check whether it is reachable from RMS. If the ping is successful, it indicates the controller is reachable from RMS.

Perform the following steps to ping from the RMS.

1. Select **Monitor > Inventory > Controller**.

The Controller List page appears.

2. Click on the controller name from the **Name** column.

The Controller details page appears.

3. Click the **TroubleShooting** tab and then click the **Ping** tab.
4. Complete the configuration according to the guidelines provided in the following table.

Table 83. Ping

| Field | Description |
|------------|---|
| IP Address | Specifies the controller IP address in IPv4 or IPv6 format. You cannot edit this field. |

| Field | Description |
|---------------------------|---|
| Overall Timeout (Seconds) | Specifies the duration after which ping execution command stops. The supported value ranges from 4 to 25. The default value is 4. |

5. Click **Execute**.

A Result page appears, indicating the ping details.

Traceroute

A traceroute is a tool to trace the path of an IP packet as it traverses routers between a source and a destination.

Perform the following steps to traceroute from the RMS.

1. Select **Monitor > Inventory > Controller**.

The Controller List page appears.

2. Click on the controller name from the **Name** column.

The Controller details page appears.

3. Click the **TroubleShooting** tab and then click the **Traceroute** tab.

4. Complete the configuration according to the guidelines provided in the following table.

Table 84. Traceroute

| Field | Description |
|-----------------------------------|---|
| IP Address | Specifies the controller IP address in IPv4 or IPv6 format. You cannot edit this field. |
| Maximum Hops | Specifies the maximum number of hops after which the traceroute command stops. The supported value ranges from 3 to 30. The default value is 10. The overall timeout of a traceroute command can be defined as Maximum Hops * Timeout per try per hop * Number of tries per hop . For example, If the maximum hop is 5, timeout per try per hop is 10 seconds, and number of tries per hop is 3. The overall timeout can be calculated as $5*10*3$. |
| Timeout per try per hop (seconds) | Specifies the timeout per try for each hop. The overall timeout for each hop can be defined as Timeout per try per hop * Number of tries per hop . The supported value ranges from 1 to 10. The default value is 3. |

| Field | Description |
|-------------------------------|---|
| Number of tries per hop | Specifies the number of tries attempted for each hop in case of failure. The supported value ranges from 1 to 3. The default value is 3. |
| Enable domain name resolution | Select this checkbox to view DNS name of the hop IP. By default, this field is not selected.  Note: The command execution time can be reduced if you disable this field. |
| Protocol | Specifies the supported protocol for tracing the path to the destination IP. The supported values are. ◦ UDP ◦ ICMP The default value is UDP. |

5. Click **Execute**.

A Result page appears, indicating the traceroute details.

Users

Perform the following steps to view the users of the controller .

1. Select **Monitor > Inventory > Controller**.

The **Controller List** page opens.

2. Click on the controller name under the **Name** column.

The Controller Details page appears.

3. Click on the **Users** tab.

You can view the users of the controller.

The following table shows the information of the controller users.

Table 85. Controller Users Information

| Fields | Description |
|----------|--|
| Username | Specifies the username of the user who has initiated the task. |

Table 85. Controller Users Information (continued)

| Fields | Description |
|---------------|--|
| Type | Specifies the type of the user. |
| Account State | Specifies the state of the user account. |
| Creation Time | Specifies the date and time when the user was created. |

Login to the CBAC CLI

From RMS, you can log in to the CBAC CLI through SSH to troubleshoot any issues.

- ## 1. Select **Monitor > Inventory > Controller**.

The Controller List page appears.

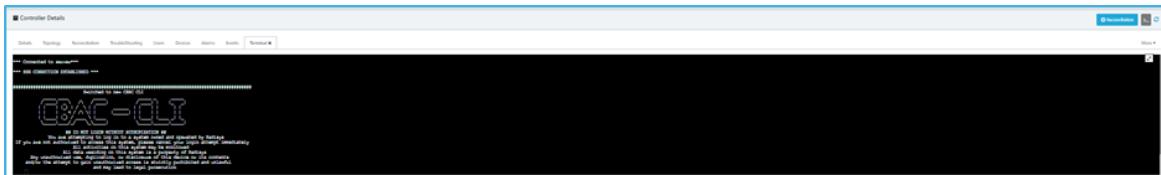
2. Click on the controller name from the **Name** column.

The Controller details page appears.

3. Click the right arrow button from the right side of the page.

The CBAC CLI console window appears.

Figure 39. CBAC CLI Console Window



CBAC CLI Synchronization with RMS

Any configuration changes (created, updated, or deleted) made from the CBAC CLI are synchronized to RMS. CBAC CLI synchronization events are generated to synchronize the configuration from the CBAC CLI with RMS through the CLI SYNC notification events. The synchronization events are published to the Kafka message bus on a specific topic (EMSCLISYNCNOTIFICATION) and delivered to RMS.

The CBAC CLI synchronization mode is enabled by default, which means that RMS is connected to CBAC. However, it can be disabled for customers working only with CLI without RMS.

The CBAC CLI synchronization with RMS is enabled for the following resources.

Table 86. Supported Operations for the Resources

| Resources | Supported Operations for the Resources |
|---------------------|---|
| Managed Element | <ul style="list-style-type: none">• Add OLT• Update OLT• Delete• Reboot• Activate• Deactivate• OLT download software• OLT activate software• OLT commit software• OLT rollback software• OLT activate firmware• ONT firmware download on OLT• ONT firmware download on ONTs• ONT firmware activate commit |
| Ports (PON and NNI) | <ul style="list-style-type: none">• Activate• Deactivate• Live-KPI-subscribe• Live-KPI-unsubscribe |
| Profiles | <ul style="list-style-type: none">• Log profile<ul style="list-style-type: none">◦ Add◦ Update◦ Delete• ERPS profile<ul style="list-style-type: none">◦ Add◦ Update◦ Delete• MEP profile<ul style="list-style-type: none">◦ Add◦ Update◦ Delete• Storm profile• NTP profile• Alarm profile |

Table 86. Supported Operations for the Resources (continued)

| Resources | Supported Operations for the Resources |
|--------------|--|
| | <ul style="list-style-type: none"> ◦ Port alarm profile ◦ SFP alarm profile ◦ ONT ANI-G alarm profile ◦ ME alarm profile ◦ LAG alarm profile <ul style="list-style-type: none"> ▪ Add ▪ Update ▪ Delete <p> Note:</p> <ul style="list-style-type: none"> ◦ Local profiles are supported at the OLT level. when the local profiles are created from the CBAC CLI they are synchronized with RMS. ◦ SFP alarm profile and port alarm profile must be configured explicitly on the secondary OLTs PON port in case of Type-B protection. |
| PON Profiles | <ul style="list-style-type: none"> • CoSQ Profile <ul style="list-style-type: none"> ◦ Add ◦ Update ◦ Delete • Storm control profile <ul style="list-style-type: none"> ◦ Associate ◦ Dissociate • MVLAN profile <ul style="list-style-type: none"> ◦ Add ◦ Update ◦ Delete • VNet profile <ul style="list-style-type: none"> ◦ Add ◦ Update ◦ Delete • Shaper profile |

Table 86. Supported Operations for the Resources (continued)

| Resources | Supported Operations for the Resources |
|------------------|--|
| | <ul style="list-style-type: none">◦ Add◦ Update◦ Delete• Bandwidth profile<ul style="list-style-type: none">◦ Add◦ Update◦ Delete• Policer Profile<ul style="list-style-type: none">◦ Add◦ Update◦ Delete• IP host options profile<ul style="list-style-type: none">◦ Add◦ Update◦ Delete |
| Network services | <ul style="list-style-type: none">• LAG<ul style="list-style-type: none">◦ Add◦ Update◦ Delete◦ LAG member port add◦ LAG member port delete• ERPS Instance<ul style="list-style-type: none">◦ Add◦ Update◦ Delete• MEP Instance<ul style="list-style-type: none">◦ Add◦ Update◦ Delete• E-Line<ul style="list-style-type: none">◦ Add◦ Delete• ELAN |

Table 86. Supported Operations for the Resources (continued)

| Resources | Supported Operations for the Resources |
|-------------------------|--|
| | <ul style="list-style-type: none"> ◦ Add ◦ Update ◦ Delete • Ring <ul style="list-style-type: none"> ◦ Add ◦ Update ◦ Delete • Subscriber <ul style="list-style-type: none"> ◦ Add ◦ Update ◦ Delete • Service <ul style="list-style-type: none"> ◦ Add ◦ Update ◦ Delete ◦ Activate ◦ Deactivate ◦ Live-KPI-subscribe ◦ Live-KPI-unsubscribe <p> Note: For other resources, only the GET command is visible to the users.</p> |
| Multicast Configuration | <ul style="list-style-type: none"> • Add • Update • Delete |
| Others | <ul style="list-style-type: none"> • CBAC backup config • CBAC restore config • CBAC upgrade software • Security settings update • Clear Alarms |

When the CBAC CLI synchronization is enabled, the following conditions are applicable.

- The global profiles for the resources are not allowed to be configured from the CBAC CLI.
- The resource configurations are name-based, and the ID is not configurable. CBAC generates the ID.

The following table provides the list of resources and supported operations from the CBAC CLI synchronization with RMS.

When a resource is created, updated, or deleted from the CBAC CLI, a notification is sent to RMS with the configuration data. RMS consumes this notification to create, update, or delete the configuration in RMS DB. Therefore, the resource created, updated, or deleted from the CBAC CLI is synchronized with RMS.

When a resource created from the CBAC CLI is synchronized with RMS, it can be updated or deleted from RMS.



Note:

- Any profile added from the CLI Sync is a local profile for the OLT.
- The default local users are created based on the *enable_default_local_users* flag during deployment.

The following are the default users.

- cliadmin
- clioperator
- cliviewer

Default local users cannot perform operations on the global users.

- When the controller is disabled at RMS, CBAC blocks any configuration from the CLI SYNC mode. By default, the controller state at CBAC is in enabled to support the backward compatibility.
- When the resources are created from RMS, the CBAC CLI does not send any notification to RMS.
- For the CBAC CLI synchronization-enabled resources, an update of the name field and space in the name is not allowed. However, if the resource name was created with a space and the update is supported for the resource, it must continue to work post-upgrade to support backward compatibility.

For more information on supported alarms and notifications, refer to the ***CBAC Alarms and Events*** guide.

Management Domain

To access this page, click **Monitor** from the top right corner of the page and select **Inventory > Management Domain** from the left-hand side of the menu.

You can monitor the status of the management domain such as REST server, Kafka, and Mongo database.

Field Descriptions

The following table describes the fields on the Management Domain List page.

Table 87. Management Domain List

| Field | Description |
|---------------|--|
| Name | Specifies the name of the management domain. |
| Creation Time | Specifies the date and time when the management domain was created. Example: Jun 23, 2020, 4:56:31 PM |

Monitoring Protection

The RMS monitoring framework provides an effective way of monitoring the type-B protection pair and the ERPS rings.

Type-B Protection

To access this page, click **Monitor** from the top right corner of the page and select **Protection > Type-B Protection** from the left-hand side of the menu.

CBAC and the OLT monitor the status of both primary and secondary PON ports for the PON MAC status, SFP module presence, and PON cable connectivity. CBAC and OLT report the operational state and trigger the auto switchover when the active PON port goes DOWN.

When the primary port goes DOWN, and the secondary port is already DOWN, CBAC sends the TYPE-B-PROTECTION-SWITCHOVER-FAILED alarm to RMS.

When the secondary port becomes UP, and the primary port is still DOWN, the switchover operation is re-initiated automatically, and all the ONUs are discovered, ranged, and activated again. The Alloc IDs, GEM ports, and flows are created automatically, and the subscriber flows resume for each ONU.

Field Descriptions

The following table describes the fields on the Type-B Protection Pair List page.

Table 88. Type B-Protection Pair List

| Field | Description |
|-------------------------------|---|
| Name | Specifies the unique name of the primary protection pair. |
| Primary Port | Specifies the name of the primary PON port. |
| Protection Type | Specifies the protection type. The supported types are. <ul style="list-style-type: none">SINGLE_SHELFCROSS_SHELF |
| Primary OLT | Specifies the name of the primary OLT. Example: OLT-185 |
| Primary Port Protection State | Specifies the state of the primary PON port in the protection pair. The supported values are. <ul style="list-style-type: none">ACTIVE-WORKINGACTIVE-STANDBYINACTIVE |

Table 88. Type B-Protection Pair List (continued)

| Field | Description |
|---|---|
| Primary Port Protection Operational State | Specifies the operational state of the primary PON port in the protection pair. |
| Secondary OLT | Specifies the name of the secondary OLT. Example: OLT-158 |
| Secondary Port | Specifies the name of the secondary port. |
| Secondary Port Protection State | Specifies the state of the secondary PON port in the protection pair. The supported values are. <ul style="list-style-type: none"> • ACTIVE-WORKING • ACTIVE-STANDBY • INACTIVE |
| Secondary Port Protection Operational State | Specifies the operational state of the secondary PON port in the protection pair. |
| Creation Time | Specifies the date and time when the type-B protection pair was created. |

Type-B Protection Pair Details

RMS monitors information about type-b protection pairs that include basic information, device information, activity log, event details, fault details, data sync request, and audit log.

Perform the following steps to monitor the type-b protection pair.

1. Select **Monitor > Protection > Type-B Protection**.
2. Click on the Type-B Protection Pair under the **Name** column.

The protection pair page appears with the following.

- Basic Information
- Device Information

Basic Information

You can view the basic information about the protection pair configured on the monitor page.

The following table describes the fields on the Type-B Protection Pair List page.

Table 89. Basic Information

| Field | Description |
|-----------------|---|
| Protection Type | Specifies the protection type. The supported types are. <ul style="list-style-type: none"> • SINGLE_SHELF • CROSS_SHELF |
| Creation Time | Specifies the date and time when the type-B protection pair was created. |

Device Information

You can view the device information about the protection pair configured on the monitor page.

The following table describes the fields on the Type-B Protection Pair List page.

Table 90. Device Information

| Field | Description |
|---|---|
| Primary OLT | Specifies the name of the primary OLT. Example: olt1 |
| Primary Port Name | Specifies the name of the primary PON port. |
| Primary Port Protection State | Specifies the state of the primary PON port in the protection pair. Example: ACTIVE-WORKING |
| Primary Port Protection Operational State | Specifies the operational state of the primary PON port. Example: ActiveUp, and ActiveDown |
| Secondary OLT | Specifies the name of the secondary OLT. Example: olt1 |
| Secondary Port Name | Specifies the name of the secondary port. |
| Secondary Port Protection State | Specifies the state of the secondary PON port in the protection pair. Example: ACTIVE-STANDBY |
| Secondary Port Protection Operational State | Specifies the operational state of the secondary PON port. Example: InactiveUp, and InactiveDown |

Event Details

You can view the event details about the protection pair configured on the monitor page.

Perform the following steps to view the event details of the type-b protection pair.

1. Select **Monitor > Protection > Type-B Protection**.
2. Click on the Type-B Protection Pair under the **Name** column.

The Type-B Protection-<pair name> page appears.

3. Click on the **Activity Log** tab.
4. Click on the **View Event Details** icon under the **Event Detail** column.

The following table describes the fields on the event details page.

Table 91. Event Details Information

| Field | Description |
|--------------------------|--|
| Event | Specifies the name of the event. Example: TYPE-B-PROTECTION-SWITCHOVER-SUCCESSFUL |
| Entity | Specifies the name of the entity. |
| Entity ID | Specifies the ID of the entity. |
| Entity Type | Specifies the entity type. Example: TYPE_B_PROTECTION |
| Parent Name | Specifies the parent name of the event. |
| Error Code | Specifies the error code of the event. |
| Reported Time | Specifies the time and date when the event was reported in a human-readable format, that is, MMM DD,YYYY, HH:MM:SS AM/PM. Example: Mar 10, 2022, 2:26:53 PM |
| Device Reported Time | Specifies the time and date when the event was reported by the device in a human-readable format, that is, MMM DD,YYYY, HH:MM:SS AM/PM. Example: Mar 10, 2022, 9:51:21 AM |
| Controller Reported Time | Specifies the time and date when the event was reported by the controller in a human-readable format, that is, MMM DD,YYYY, HH:MM:SS AM/PM. Example: Mar 10, 2022, 9:51:21 AM |
| Description | Specifies the description of the event. Example: Type-B Protection Switchover Successful |
| Data | Specifies the payload information about the event. <pre>{ "active_olt_id": "6881ab51-64da-11ed-9636-c2a601c624c1-69", "switchover": "auto-switchover", "standby_port_id": "689a1551-64da-11ed-9636-c2a601c624c1-85-PON-12", }</pre> |

Table 91. Event Details Information (continued)

| Field | Description |
|-------|--|
| | <pre> "standby_olt_id": "6881ab51-64da-11ed-9636-c2a601c624c1- 69", "active_port_protection_operational_state": "ActiveDown", "SDPON-EVENT": "TYPE-B-PROTECTION-SWITCHOVERSUCCESSFUL", "standby_port_protection_operational_state": "InactiveDown", "active_port_id": "c14f3630-a004-11ec-92d8-8220892a02a3- 6-PON-5" } </pre> |

Fault Details

You can view the fault details about the protection pair configured on the monitor page.

Perform the following steps to view the fault details of the type-b protection pair.

1. Select **Monitor > Protection > Type-B Protection**.
2. Click on the Type-B Protection Pair under the **Name** column.

The Type-B Protection-<pair name> page appears.

3. Click on the **Activity Log** tab.
4. Click on the **View Fault Details** icon under the **Fault Detail** column.

The following table describes the fields on the event details page.

Table 92. Fault Details Information

| Field | Description |
|--------------------------|--|
| Basic Information | |
| Severity | Specifies the severity of the fault. The supported values are. <ul style="list-style-type: none"> • WARNING • MAJOR • MINOR • CRITICAL |
| Time | Specifies the time and date when the fault was raised. |
| Fault Code | Specifies the fault code. Example: TYPE-B-PROTECTION-NOT-AVAILABLE |
| Entity | Specifies the name of the entity. |

Table 92. Fault Details Information (continued)

| Field | Description |
|----------------------------|--|
| Type | Specifies the type of the resource. Example: TYPE_B_PROTECTION |
| ID | Specifies the display ID of the resource. |
| Data | Specifies the data related to the fault. <pre>{ "CONTROLLER-FAULT": "TYPE-B-PROTECTION-NOT-AVAILABLE", "reason": "One of the protected port is down", "olt_id": "22c7a5c0-66fa-11ed-a948-f25dad5679a3-96", "port_id": "331a4450-66fa-11ed-a948-f25dad5679a3-84-PON-1" }</pre> |
| Acknowledge Details | |
| Acknowledge | Specifies whether the fault is acknowledged. The supported values are. <ul style="list-style-type: none"> Yes No |
| Ack Time | Specifies the time and date when the fault was acknowledged. |
| Comment | Displays the comment entered when the fault was acknowledged. |
| Clear Details | |
| Clear Status | Specifies if the fault is cleared or not. The supported values are, <ul style="list-style-type: none"> Y N |
| Clear Time | Specifies the time and date when the fault was cleared in human readable format, that is, MMM DD,YYYY, HH:MM:SS AM/PM. Example: Mar 10, 2022, 9:51:21 AM |
| Type | Specifies how the fault was cleared. <ul style="list-style-type: none"> Manual. An operator cleared the alarm manually. Auto. The alarm was cleared by CBAC automatically. |
| Comment | Displays the comment entered when the fault was cleared. |

Ring

To access this page, click **Monitor** from the top right corner of the page and select **Protection > Ring** from the left-hand side of the menu.

A ring is formed when you create an ERPS instance. A ring is formed on OLT by associating two NNI ports to the ERPS instance.

You can configure the ring ID in the range of 1 to 239 for each ERP instance. The ring ID used in the R-APS message transmission function determines the value of the last octet value of the MAC destination address field of the R-APS protocol data units (PDUs), which is generated by the ERPS protocol on a particular RING node.

The ring ID is also used by the validity check function to discard any R-APS PDUs received by the ERPS protocol on a particular ring node with a non-matching ring ID.

When you configure the ring ID, the following rules must apply.

- All ERPS ring nodes in a ring must be identified by a unique (ring ID and Control[R-APS] VID) pair.
- For a ring, all Instances must be assigned a different value of the control VLAN ID on the same underlying physical ring.
- Across the rings, the ERPS instances can be assigned the same control VLAN ID.

Field Descriptions

The following table describes the fields on the Ring page.

Table 93. Ring

| Field | Description |
|---------------|--|
| Name | Specifies the name of the ring. |
| Ring id | Specifies the ring ID. |
| East Port | Specifies the east port of the ring. |
| West Port | Specifies the west port of the ring. |
| Creation Time | Specifies the date and time when the ring was created. |

Monitoring Services

The RMS monitoring framework provides an effective way of monitoring the subscriber services and the subscriber information.

Subscriber Service

To access this page, click **Monitor** from the top right corner of the page and select **Services > Subscriber Service** from the left-hand side of the menu.

Use this page to view the list of main and sub-services activated for the subscribers. You can monitor the service information, KPIs generated for the service, IGMP channels, IGMP valid and invalid packets, and the devices and ports associated with the service. You can also view the audit log information about the subscriber services.

Field Descriptions

The following table describes the fields on the Service List page.

Table 94. Service List

| Field | Description |
|-------------------|--|
| Name | Specifies the name of the service. |
| Subscriber Name | Specifies the name of the subscriber. |
| Admin State | Specifies the admin state of the service, whether the service is enabled or disabled for the subscriber. |
| Operational State | Specifies the operational state of the service, whether the service is UP or DOWN. |
| ONT Name | Specifies the name of the ONT. |
| OLT Name | Specifies the OLT name. |
| OLT Port Name | Specifies the OLT port. |
| Creation Time | Specifies the date and time when the subscriber service was created. |

Sub Services

Perform the following steps to monitor the sub services of the subscriber.

1. Select **Monitor > Services > Subscriber Service**.
2. Click on the service name on the **Name** column.

The Subscriber Service details page appears.

3. Click on the **Sub Services** tab.

The Subscriber Service Sub Services page appears.

The following table describes the Sub Services information.

Table 95. Sub Services Details

| Field | Description |
|--------------------------|--|
| Sub Services | |
| Service Name | Specifies the name of the sub service. Example: HSIA |
| IPv6 IAPD | Specifies the IPv6 IAPD address. |
| Allocated Time IPv6 IAPD | Specifies the epoch time stamp at which the IPv6 address is allocated. |
| Lease Time IPv6 IAPD | Specifies the lease time of the allocated IPv6 IAPD address in seconds. |
| Allocated Time IPv6 | Specifies the time to allocate IPv6 address. |
| Lease Time IPv6 (in sec) | Specifies the time to lease IPv6 address. |
| Operational Status | Specifies the operational state of the sub service. <ul style="list-style-type: none">• Green. Indicates that the operational state of the service is UP.• Red. Indicates that the operational state of the service is DOWN. |
| Line Status | Specifies the following line status details of the sub service. <ul style="list-style-type: none">• Voip Codec Used• Voip Voice Server Status• Voip Port Session Type• Voip Call1 Packet Period• Voip Call2 Packet Period• Voip Call1 Dest Addr• Voip Call2 Dest Addr• Voip Line Status• Emergency Call Status |
| IPv4 Address | Specifies the IPv4 address of the subscriber service. |
| Allocated Time IPv4 | Specifies the time to allocate IPv4 address. |

Table 95. Sub Services Details (continued)

| Field | Description |
|--------------------------|---|
| Lease Time IPv4 (in sec) | Specifies the time to lease IPv4 address. |
| IPv6 Address | Specifies the IPv6 address of the subscriber service. |
| CPE IP Type | <p>Specifies the type of Customer Premises Equipment (CPE) IP. The supported values are.</p> <ul style="list-style-type: none"> • IPv4 • IPv6 • NONE <p>The default value is NONE.</p> |
| CPE IP Subnet Mask | <p>Specifies the subnet mask for the CPE IP address. This field is mandatory when the CPE IP type is IPv4 or IPv6.</p> <p>Example:</p> <p>IP subnet mask for IPv4: 255.255.255.255</p> <p>IP subnet mask for IPv6: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff</p> |
| CPE IP Address | <p>Specifies the IP address of CPE/CE router device connected to the particular UNI port for the enterprise (Bridged Mode) solution.</p> <p>The length is 4 bytes. A standard valid IP range is supported.</p> <p>This field can take IPv4 or IPv6 address based on the value provided in the CPE IP type field.</p> <p>This field is mandatory when the CPE IP type is IPv4 or IPv6.</p> <p>Example: 1.1.1.1 or 2001:db8:3333:4444:5555:6666:7777:8888</p> |
| UNI Port Name | Specifies the UNI port name. Example: ONT1-PPTP-ETHERNET-1 |
| UNI Port Number | Specifies the UNI port number. |
| UNI Port Type | Specifies the UNI port type. Example: PPTP-ETHERNET |
| SVLAN | Specifies the subscriber's S-Tag value. |
| CVLAN | Specifies the subscriber's C-Tag value. |
| UNI VLAN | Specifies the VLAN for UNI port. |
| Vnet Profile | Specifies the Vnet profile. |
| Learnt CPE MAC | Specifies the MAC address of the CPE connected to the particular UNI port. Example: 00:10:94:00:02:0 |

Table 95. Sub Services Details (continued)

| Field | Description |
|------------------------------|---|
| MVLAN Profile | Specifies the MVLAN profile. |
| AES Encryption | Select whether the AES encryption is supported for the service. <ul style="list-style-type: none"> True. Supports AES encryption. False. Does not support AES encryption. |
| Circuit ID | Specifies the circuit ID. |
| Remote ID Type | Specifies the type of remote ID. The supported values are. <ul style="list-style-type: none"> MAC_Address Custom <p>This field is applicable only when the MAC Learning Type is set to DHCP, PPPoE, or PPPoE-IA. Otherwise, this field is ignored.</p> |
| Remote ID | Specifies the remote ID. |
| Encapsulation | Specifies the type of access protocol used to establish the access link. The supported values are. <ul style="list-style-type: none"> IPoE PPPoE PPPoE-IA |
| VLAN Control | Specifies the VLAN tagging supported at the ONU and OLT. The supported values are. <ul style="list-style-type: none"> ONU_CVLAN_OLT_SVLAN OLT_CVLAN_OLT_SVLAN ONU_CVLAN OLT_SVLAN ONU_CVLAN_ONU_SVLAN NONE <p>The default value is ONU_CVLAN_OLT_SVLAN.</p> |
| ONT Ethertype Classification | Specifies the upstream traffic that needs to be classified based on the Ether type. The supported values are. <ul style="list-style-type: none"> ENABLED DISABLED |
| MAC Learning Type | Select the type of method to be used to learn the device MAC address. For more information on MAC Learning Type, see Table 268: MAC Learning Type (on page 580) . |

Table 95. Sub Services Details (continued)

| Field | Description |
|------------------------------|--|
| Upstream Bandwidth Profile | Specifies the upstream bandwidth profile. Example: bw-1 |
| Upstream Shaper Profile | Specifies the upstream shaper profile. |
| Upstream CoSQ Profile | Specifies the upstream cosq profile. Example: cosq-1 |
| Downstream Bandwidth Profile | Specifies the downstream bandwidth profile |
| Downstream Shaper Profile | Specifies the downstream shaper profile. Example: sp-1 |
| Downstream CoSQ Profile | Specifies the downstream cosq profile. Example: cosq-1 |

Historical Statistics

Perform the following steps to monitor the historical statistics of the subscriber service.

1. Select **Monitor > Services > Subscriber Service**.
2. Click on the service name in the **Name** column.

The Subscriber Service details page appears.

3. Click on the **Historical Statistics** tab.

The Subscriber Service historical statistics page appears.

You can view the graphical view of the historical statistics (data packet and control packet) information by one month, one week, one day, daily, and hourly.

You can also view the statistics information for a particular duration using the **Custom** option.

You can select both **Select IP Address** and **Select Option** parameter for data packet from the list for which you want to view the statistics information.

The select option parameters are.

- **Specific Queries Sent.** Specifies the number of group-specific queries sent.
- **IGMP V2 Reports Received.** Specifies the number of IGMPv2 reports received.
- **IGMP V3 Reports Received.** Specifies the number of IGMPv3 reports received.
- **Unsuccessful Joins.** Specifies the number of joins that were not honored by CBAC due to various reasons.

- **MLD V1 Reports Received.** Specifies the number of MLDv1 reports received.
- **MLD V2 Reports Received.** Specifies the number of MLDv2 reports received.
- **Mvlan.** Specifies the multicast profile for the subscriber.

Live KPIs

Perform the following steps to monitor the Live KPIs of the subscriber service.

1. Select **Monitor > Services > Subscriber Service**.
2. Click on the service name on the **Name** column.

The Subscriber Service details page appears.

3. Click on the **Live KPIs** tab.

The Subscriber Service Live KPIs page appears.

You can view the live KPIs of the subscriber service based on the selected service name.

The following table shows the description of field of the subscriber service live KPIs.

Table 96. Live KPI

| Field | Description |
|----------------------------|---|
| Service Name | Specifies the name of the service. |
| OLT Stats COSQ Profile ID | Specifies the ID of the CoSQ profile. |
| OLT Stats Tx Packets | Specifies the count of frames transmitted on the monitored GEM Port on the OLT. The unit is in packet count. |
| OLT Stats Rx Packets | Specifies the count of frames received on the monitored GEM Port on the OLT. The unit is in packet count. |
| OLT Stats Tx Bytes | Specifies the count of user payload bytes transmitted on the queue, based on the GEM ports of the queue on the OLT. The unit is in bytes. |
| OLT Stats Rx Bytes | Specifies the count of user payload bytes received on the queue, based on the GEM ports of the queue on the OLT. The unit is in bytes. |
| ONT Stats COSQ Profile ID | Specifies the name of the upstream CoSQ profile. |
| ONT Stats Tx GEM Frames | Specifies the count of GEM frames transmitted on the monitored GEM Port on the OLT. The unit is in packet count. |
| ONT Stats Rx GEM Frames | Specifies the count of GEM frames received on the monitored GEM Port on the ONT. The unit is in packet count. |
| ONT Stats Tx Payload Bytes | Specifies the count of user GEM payload bytes transmitted on the queue, based on the GEM ports of the queue on the ONT. The unit is in bytes. |

Table 96. Live KPI (continued)

| Field | Description |
|----------------------------|--|
| ONT Stats Rx Payload Bytes | Specifies the count of user GEM payload bytes received on the queue, based on the GEM ports of the queue on the ONT. The unit is in bytes. |

Service Queue Statistics

Perform the following steps to monitor the Service Queue Statistics of the subscriber service.

1. Select **Monitor > Services > Subscriber Service**.
 2. Click on the service name on the **Name** column.
- The Subscriber Service details page appears.
3. Click on the **Service Queue Statistics** tab.

The Subscriber Service, Service Queue Statistics page appears.

You can view the graphical view of the service queue statistics information by one month, one week, one day, daily, and hourly.

You can also view the statistics information for a particular duration using the **Custom** option.

You can select both **Select Service Name** and **Select Option** parameter from the list for which you want to view the statistics information.

The select option parameters are.

- OLT Stats Tx Packet
- OLT Stats Rx Packets
- OLT Stats Tx Bytes
- OLT Stats Rx Bytes
- ONT Stats Tx GEM Frames
- ONT Stats Rx GEM Frames
- ONT Stats Tx Payload Bytes
- ONT Stats Rx Payload Bytes

Audit Log

Perform the following steps to monitor the Audit Logs of the subscriber.

1. Select **Monitor > Services > Subscriber Service**.
2. Click on the service name in the **Name** column.

The Subscriber Service details page appears.

3. Click on the **Audit Log** tab.

The Subscriber Service Audit Log page appears.

You can view the actions performed on the subscriber services. For more information about the field descriptions, see [Audit Log \(on page 229\)](#).

Exporting Service Inventory List

You can export the service inventory list as a CSV file that can be opened or edited using an application such as Microsoft Excel. You can view and analyze the exported service list, as needed. The service list contains the following attributes.

- Service ID/Name
- VLAN details
- MAC details for the service
- Bandwidth profile
- Shaper profile
- COSQ profile
- Mapping with OLT/PON/ONT and so on
- Service up timestamp
- Service down timestamp

Perform the following steps to export service inventory list.

1. Select **Monitor > Services > Subscriber Service**.

The Subscriber Service List page appears.

2. Click **Export** to export the details.

The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file in a Microsoft Excel sheet. Optionally, you can save this file on your PC for later use.

Subscriber

To access this page, click **Monitor** from the top right corner of the page and select **Service > Subscriber** from the left-hand side of the menu.

You can monitor the list of subscribers and the basic and service information of the subscriber.

Field Descriptions

The following table describes the fields on the Subscriber List page.

Table 97. Subscriber List

| Field | Description |
|---------------|--|
| Name | Specifies the name of the subscriber. |
| Display ID | Specifies the display ID of the subscriber. |
| Latitude | Specifies the latitude of the subscriber location. |
| Longitude | Specifies the longitude of the subscriber location. |
| Address | Specifies the address of the subscriber. |
| ONU | Specifies the name of the ONU. |
| Creation Time | Specifies the date and time when the subscriber was created. |

Monitoring Subscriber

You can monitor the following details of the subscriber.

- Basic Information
- Service

Perform the following steps to monitor the subscriber.

1. Select **Monitor > Services > Subscriber**.

The Subscriber List page appears.

2. Click on the subscriber name in the **Name** column.

The Subscriber Details page appears.

The following table describes the basic information.

Table 98. Subscriber Details

| Field | Description |
|--------------------------|---|
| Basic Information | |
| Subscriber Name | Specifies the name of the subscriber. |
| Address | Specifies the address of the subscriber. |
| ONU | Specifies the name of the ONU. |
| Latitude | Specifies the latitude of the subscriber location. |
| Longitude | Specifies the longitude of the subscriber location. |

Table 98. Subscriber Details (continued)

| Field | Description |
|---------------------|--|
| Display ID | Specifies the display ID of the subscriber. |
| Total Service | Specifies the total number of services for the subscriber. |
| Total Up Services | Specifies the total number of services that are up. |
| Total Down Services | Specifies the total number of services that are down. |
| Creation Time | Specifies the date and time when the subscriber was created. |

Services

Perform the following steps to monitor the services of the subscriber.

1. Select **Monitor > Services > Subscriber**.

The Subscriber List page appears.

2. Click on the subscriber name on the **Name** column.

The Subscriber Details page appears.

3. Click on the **Services** tab.

The Subscriber Services page appears.

The following table describes the services information of the subscriber.

Table 99. Services

| Field | Description |
|-------------------|--|
| Services | |
| Name | Specifies the name of the service. |
| Admin State | Specifies the admin state of the service, whether the service is enabled or disabled for the subscriber. |
| Operational State | Specifies the operational state of the service, whether the service is UP or DOWN. |
| ONT Name | Specifies the name of the ONT. |
| OLT Name | Specifies the OLT name. |
| OLT Port Name | Specifies the OLT port. |

Table 99. Services (continued)

| Field | Description |
|---------------|--|
| Creation Time | Specifies the date and time when the subscriber service was created. |

Data Sync Request

Perform the following steps to monitor the Data Sync Request of the subscriber.

1. Select **Monitor > Services > Subscriber**.

The Subscriber List page appears.

2. Click on the subscriber name on the **Name** column.

The Subscriber Details page appears.

3. Click on the **Data Sync Request** tab.

The Subscriber Data Sync Request page appears.

For more information on fields on the Data Sync Request page, see [Table 104: Data Sync Request List \(on page 233\)](#).

Audit Log

Perform the following steps to monitor the Audit Log of the subscriber.

1. Select **Monitor > Services > Subscriber**.

The Subscriber List page appears.

2. Click on the subscriber name on the **Name** column.

The Subscriber Details page appears.

3. Click on the **Audit Log** tab.

The Subscriber Audit Log page appears.

You can view the actions performed on the subscriber services. For more information about the field descriptions, see [Audit Log \(on page 229\)](#).

Monitoring Infrastructure

The RMS monitoring framework provides an effective way of monitoring the database statistics, RMS microservices, and user sessions.

Database Statistics

To access this page, click **Monitor** from the top right corner of the page and select **Infrastructure > Database** from the left-hand side of the menu.

Use this page to view statistics information about the database.

Field Descriptions

The following table describes the fields on the Database Statistics List page.

Table 100. Database Statistics List

| Field | Description |
|--------------------------|---|
| Name | Specifies the name of the database. Example: DB_ADMIN |
| No of Collections | Specifies the number of collections in a specific database. Example: 2 |
| No of Objects | Specifies the number of objects in a collection. Example: 7 |
| Storage Size (Megabytes) | Specifies the storage size of the database in bytes. Example: 8192.0 |

Session

To access this page, click **Monitor** from the top right corner of the page and select **Infrastructure > Session** from the left-hand side of the menu.

You can view the list of users who are logged in to the system along with their IP addresses and when they are logged in. They can selectively choose to kill some of the sessions, if required.

Field Descriptions

The following table describes the fields on the Session List page.

Table 101. Session List

| Field | Description |
|-------------------|--|
| User Name | Specifies the username of the user who initiated the session. Example: admin |
| User Type | Specifies the user type. The supported types are. <ul style="list-style-type: none">• System User• Deployment User Example: SYSTEM_USER |
| Client IP Address | Specifies the IP address of the client from which the user has logged in. Example: 172.24.56.55 |
| Creation Time | Specifies the date and time when the session was created. Example: Jun 24, 2020, 3:37:35 PM |
| Action | Specifies the action to be performed on the session. The supported action is. <ul style="list-style-type: none">• Delete |

Monitoring Logs

The RMS monitoring framework provides an effective way of monitoring the audit logs, backup jobs, data synchronization requests, and microservice logs.

Audit Log

To access this page, click **Monitor** from the top right corner of the page and then select **Log > Audit Log** from the left-hand side of the menu.

RMS supports audit logs according to the policy and guidelines defined in the security policy.

Audit logs are generated for login activity and tasks initiated (by users) from RMS. Audit log entries usually include details about user-initiated tasks, such as username, user ID of the user who initiated a task, date and time of execution, resource ID, resource type, resource name, IP address, parent name of the resource, resource action, the status of the task, and request data (Job ID, subscriber ID, and service name).

Audit logs are visible to administrators only and not to operators and viewers. An administrator can permit the operator and viewer to view audit logs according to the requirement.

Administrators can use audit logs to review events; for example, to identify which user accounts are associated with an event, to determine the chronological sequence of events, that is, what happened before and during an event, and so on.

Administrators can sort and filter audit logs; for example, administrators can use audit log filtering to track the user accounts that were added on a specific date, track configuration changes across a particular resource type, and view actions that were performed on specific resources.

RMS enables system logging to capture the following information.

- Operations and maintenance activities performed by the users on files, user accounts, and configuration settings
- System failures, system events, and faults that are related to disk, fan, power supply, CPU, or memory boards
- Unauthorized user attempts to files and commands

Following types of logs are captured.

- Management of accounts and access rights
- Command logs and systems log
- Modification of security rules
- Transactional logs without any sensitive details
- Database modification and object creation/deletion/update

Audit and security logs generated by the OLT and CBAC instances are streamed to the centralized log server and the same are relayed to the Centralized Log Management System (CLMS). RMS security and

audit logs from the RMS node are directly streamed to the CLMS. Both the security and audit logs must clearly distinguish the instance such as RMS, OLT, or CBAC instance along with the following mandatory parameters.

- Source IP address
- Username
- Timestamp
- Command name
- Command execution status (success or failure)
- Timezone information

**Note:**

- All the above parameters must be in a single log line. The log line delimiter is LF (ASCII 10) character.
- Source IP address is provided in the OLT OS log.
- All the operations performed through the external interface (GUI) are visible in audit logs. If the operation is performed through the OSS interface, only the operations performed by the user are visible in the audit logs. For example, configure.

Fields Descriptions

The following table describes the fields on the Audit Log List page.

Table 102. Audit Log List

| Field | Description |
|-----------------|--|
| User Name | Specifies the username of the user who has initiated the task. |
| User Id | Specifies the user id. |
| Time | Specifies the date and time at which the execution of the task was attempted. Example: May 5, 2020, 2:30:47 PM |
| Resource Id | Specifies the resource ID of the job associated with the task. Example: 076304b0-33ad-11ea-a379-0242b6dc8ce0-90 |
| Resource Name | Specifies the name of the resource. |
| Resource Type | Specifies the name of the resource from which the user initiated the task. For example, login, role, make, model, me_template, me_port, and so on. |
| Resource Action | Specifies the type of action performed on the resource. The supported actions are. |

Table 102. Audit Log List (continued)

| Field | Description |
|--------------|---|
| | <ul style="list-style-type: none"> • ACTIVATE • ADD • CHANGE_PASSWORD • DEACTIVATE • ENABLE • LOGIN • LOGOUT • MODIFY • RECONCILE • REPLACE |
| IP Address | <p>Specifies the IP address of the computer from which the user initiated the task.</p> <p>Example: 172.24.40.191</p> |
| Parent Name | <p>Specifies the parent resource of the entity on which the task is performed.</p> <p>Example: OLT</p> |
| Status | <p>Specifies the status of the task that triggered the audit log:</p> <ul style="list-style-type: none"> • SUCCESS. Indicates that the job has completed successfully. • FAILED. Indicates that the job has failed and is terminated. |
| Request Data | <p>Displays the payload information with which the request is attempted.</p> <p>Example:</p> <pre>{ "id": "b95dfe70-6b76-11eb-87d4-3e88bfe2b017-83", "password": "xxxxxxxxxx", "user_name": "admin", "confirm_password": "xxxxxxxxxx", "old_password": "xxxxxxxxxx" }</pre> |

Backup Jobs

To access this page, click **Monitor** from the top right corner of the page and select **Log > Backup Job** from the left-hand side of the menu.

A job refers to a backup job, which enables you to automatically backup configuration information for OLT, controller, and RMS database (Mongo DB). You can also restore the backed-up configuration from this page.

A backup job is created when you take a backup of the following.

- OLT configuration
- Controller configuration
- RMS database configuration

Fields Descriptions

The following table describes the fields on the Backup Job List page.

Table 103. Backup Job List

| Field | Description |
|-----------------|---|
| Name | Specifies the name of the backup job. Example: 2020-07-02_09_35_45_673 |
| Status | Specifies the status of the backup job. <ul style="list-style-type: none">• SUCCESS. The backup job is completed successfully.• FAILURE. The backup job is failed. |
| Task Name | Specifies the name of the task that was created to perform this operation. Example: Database-backup |
| File Size (Mb) | Specifies the size of the backup configuration file in Mb. |
| File Store Name | Specifies the name of the file storage. Example: MPServer |
| Creation Time | Specifies when the backup job was created. |
| Description | Specifies the description of the backup job. |

Restoring the Backup Configuration File

There are two ways to restore the backup configuration file.

- After the initial deployment
- After the successful creation of the RMS database (Mongo DB) backup

When you perform the database backup operation, a backup job is created, if the backup operation is successful.



Note:



- Do not perform any action which results into configuration or database change during backup and restore operation.
- After restoring the RMS database backup, you must delete the bulk tasks that remain incomplete (Tasks in SCHEDULED, CREATED, and RUNNING state) to ensure the system's efficiency and accuracy. See the [Editing and Deleting Task Configuration \(on page 728\)](#).

Data Synchronization Request

To access this page, click **Monitor** from the top right corner of the page and select **Log > Data Sync Request** from the left-hand side of the menu.

Whenever you update the RMS resources (alarm profile, log profile, RADIUS profile, CoSQ profile, MVLAN profile, shaper profile, bandwidth profile, and VNet profile), RMS synchronizes the data with the target resource, such as a controller.

You can synchronize the requested resources with the controller by creating a data sync request.



Note: All the failed data synchronization requests are retried after a regular interval in a sequence. If there is any issue, update the resource on RMS and the synchronization request gets passed when retried. Also, if a controller is down and comes up later, all the data synchronization requests are retried on a controller.

Fields Descriptions

The following table describes the fields on the Data Sync Request List page.

Table 104. Data Sync Request List

| Field | Description |
|-------------|---|
| Time | Specifies the time when the request was created. |
| Entity Type | Specifies the type of resource. Example: bandwidth_profile |
| Entity ID | Specifies the ID of the resource. Example: c93840b0-6ac5-11ea-9659-d28b0fd8e0f0-81 |
| Entity Name | Specifies the resource name. Example: MVLAN |
| Target Name | Specifies the name of the destination. For example, a controller name to which the request was sent. Example: Edgecore |
| Target Type | Specifies the name of the resource. |

Table 104. Data Sync Request List (continued)

| Field | Description |
|-----------|---|
| | Example: Controller |
| Operation | Specifies the operation (ADD, MODIFY, DELETE, and so on). Example: ADD |
| Status | Specifies the status of the request. For the failed requests, hover on the icon to see the error message. The supported status are. <ul style="list-style-type: none">• SUCCESS• FAILED• INVALID• PENDING• ON-HOLD <p> Note:</p> <ul style="list-style-type: none">• The user can click the RESYNC button to change the status from ON-HOLD to PENDING only for requests with an ON-HOLD status.• The RESYNC button is displayed only for ON-HOLD status requests. |
| Action | Specifies the action that can be performed on the request. The supported action is Delete. |

Monitoring Reports

To access this page, click **Monitor** from the top right corner and select **Reports** from the left-hand side of the menu.

The RMS monitoring framework provides an effective way to view and download the following types of reports.

- Fault Summary
- Performance Summary

You can also email the report to the recipient.

RMS supports generating a standardized fault report. You can also create customized fault reports based on operator requests.

You must create a task for generating reports and the reports are generated based on the report type that you have selected while creating the task. For more information, see [Creating Task for Report Generation \(on page 656\)](#).

Field Descriptions

The following table describes the fields on the Reports List page.

Table 105. Reports List

| Field | Description |
|------------------|--|
| Report Name | Specifies the name of the report. |
| Status | Specifies whether the report generation is scheduled immediately or for a later date and time. The status of the report generation are. <ul style="list-style-type: none">• CREATED• SCHEDULED• COMPLETED |
| Execution Result | Specifies the execution result of the report. The supported values are. <ul style="list-style-type: none">• SUCCESS. The report generation is successful.• FAILED. The report generation is failed. |
| Creation Time | Specifies the date and time when the report generation task was created. |
| Execution Time | Specifies the date and time when the report was generated. |
| Schedule Time | Specifies the date and time when the report generation is scheduled. |
| Description | Specifies the description about the report. |

Table 105. Reports List (continued)

| Field | Description |
|--------------|--|
| Download | Click on the download icon to download the fault summary or fault detailed summary report. The report is downloaded and appears at the bottom of the page. |
| View | Click to view the PDF preview of the report. |
| Email Report | Enter the e-mail address of the recipient to send the report. Example: xyz@domain.com |

Fault Summary Report

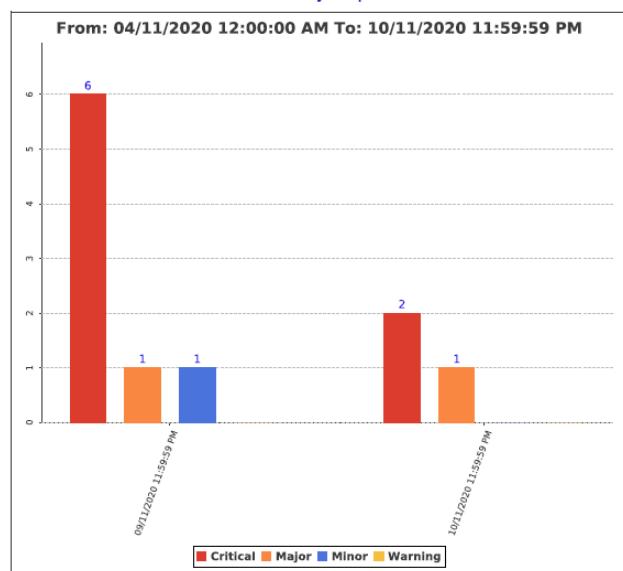
A fault summary report is a standardized report generated in RMS. It shows a graphical summary of alarms (by severity level) that occurred within a specified period. The fault summary report contains a series of four colored status bars as follows.

- **Red.** Critical Alarms
- **Orange.** Major Alarms
- **Blue.** Minor Alarms
- **Yellow.** Warning Alarms

You can also generate daily, weekly, last 7 days, last 30 days, this month, and last month fault summary reports.

The following figure shows the fault summary report generated in RMS.

Figure 40. Fault Summary
Fault Summary Report



Performance Summary

You can generate a performance summary report for the OLT, and the report can be generated for one or more OLTs in the network at the same time. This report contains the following KPIs information about the OLT.

- **CPU Utilization.** Specifies the CPU utilization of the OLT in percentage.
- **Memory Utilization.** Specifies the memory utilization of the OLT in percentage.
- **Disk Utilization.** Specifies the disk utilization of the OLT in percentage.
- **Temperature.** Specifies the temperature of the OLT in Milli Celsius.
- **Time.** When the KPI is reported to RMS from CBAC.

The following figure shows the performance summary report for the OLT.

Figure 41. Device Performance Summary

| From: 04/11/2020 12:00:00 AM To: 10/11/2020 11:59:59 PM | | | | | |
|---|------------------------|----------------------|-----------------------------|------------------------|--|
| Management Domain: md223 | | | | | |
| Name: OLT1 | | | | | |
| ID: e3ae7d80-1f45-11eb-983f-06601aa31bba-89 | | | | | |
| CPU Utilization (%) | Memory Utilization (%) | Disk Utilization (%) | Temperature (Milli Celsius) | Time | |
| 12.88 | 21.86 | 9.47 | 38 | 06/11/2020 05:29:43 AM | |
| 14.57 | 24.69 | 10.15 | 36 | 07/11/2020 05:29:59 AM | |
| 18.66 | 26.64 | 10.62 | 37 | 08/11/2020 05:29:46 AM | |
| 16.95 | 28.45 | 10.61 | 37 | 09/11/2020 05:29:50 AM | |
| 16.73 | 29.55 | 11.03 | 37 | 10/11/2020 05:29:38 AM | |

If the threshold value (CPU, memory, disk, and temperature) of the OLT reaches the maximum threshold value configured in RMS, then the particular threshold value is highlighted in red color and this helps the operators to troubleshoot the issues.

Monitoring Faults

To access this page, click **Monitor** from the top right corner of the page and select **Faults** from the left-hand side of the menu.

The RMS monitoring framework provides an effective way to monitor the faults reported in RMS. This helps the network monitoring team to quickly review the alarms and perform the recovery actions to clear the alarms.

Fault is an indication of an abnormal condition detected by RMS. Faults report issues identified in the network that may cause disruption or impact the quality of the service provided to the subscribers.

Faults are published to the Kafka message bus on a specific topic (EMSFault) and delivered to RMS. The severity field of the fault determines whether the published notification is a fault or an event. If the severity is CRITICAL, WARNING, MAJOR, or MINOR, then the notification is a fault.

You can view the following types of faults using this page.

- Current
- Acknowledged
- Unacknowledged
- Cleared

The fault list is refreshed automatically at the specified interval.

You can also view the alarm histogram of all the alarms. See [Alarms Histogram \(on page 51\)](#).

To view the list of faults generated by RMS, see [Appendix A: Alarms \(on page 907\)](#).

Alarm Severity Levels

Once an alarm is active, it has one of the following states.

- **WARNING, MINOR, MAJOR, or CRITICAL.** Alarms that are current and not yet resolved.
- **INDETERMINATE.** Alarms severity level cannot be determined.
- **CLEARED.** Alarms that are resolved and returned to normal operation.

The following table lists the severity level of alarms.

Table 106. Severity of Faults

| Severity Level | Description |
|----------------|---|
| WARNING | Indicates the detection of a potential or impending service affecting fault before any significant effects. You must take the required action to diagnose |

Table 106. Severity of Faults (continued)

| Severity Level | Description |
|----------------|--|
| | (if necessary) and correct the problem to prevent any serious service affecting fault. |
| MINOR | Indicates the existence of a non-service affecting fault condition and a corrective action is required to prevent serious (for example, service affecting) fault. This severity needs to be reported when the detected alarm condition is not currently degrading the capacity of the managed element. |
| MAJOR | This severity level indicates a service affecting condition and urgent corrective action is required. Report this severity when there is a severe degradation in the capability of the managed element and its full capability must be restored. |
| CRITICAL | Indicates a presence of service affecting condition for which an immediate corrective action is required. This severity is reported when a managed element is completely out of service and its capability must be restored. |
| CLEARED | Indicates the clearing of previously reported alarm. This alarm clears all alarms for the managed element with the same alarm type and cause. The clearing of previously reported alarm need not be reported. |

Alarms in the alarm table are color-coded by severity as follows.

- **Red.** Critical Alarms
- **Amber or Orange.** Major Alarms
- **Blue.** Minor Alarms
- **Yellow.** Warning Alarms

Tasks

You can perform the following tasks on this page.

- Generate alarms histogram on an hourly or daily interval. You can also generate alarm histogram every 1 hour, 3 hours, 6 hours, 12 hours, 24 hours, and 7 days.
- View the graphical representation of all the alarms. See [Alarms Histogram \(on page 51\)](#).
- Export fault list. See [Exporting Fault List \(on page 246\)](#).
- View fault details. See [Viewing Fault Details \(on page 247\)](#).
- Acknowledge and clear faults. See [Acknowledging and Clearing Alarms \(on page 245\)](#).
- A pattern search using partial or complete keywords is supported for the following fields on the current and cleared fault page.
 - Fault
- You can filter the faults based on the following fields.

- OLT
 - Site
 - Type
 - Controller
 - Severity
- Click the **AUTO REFRESH** option to refresh the fault list automatically for every 30 seconds. By default, the auto refresh option is OFF.
 - Enable the **Shorten Row Height** option to shorten the height of table entries.

Field Descriptions

The following table shows the description of fields on the Fault List-Current page.

Table 107. Fault List-Current

| Field | Description |
|----------------------|--|
| Severity | <p>Specifies the severity level of an alarm. The severity levels are.</p> <ul style="list-style-type: none">• WARNING• MAJOR• MINOR• CRITICAL <p> Note: The severity of the alarm is color-coded as follows.</p> <ul style="list-style-type: none">• Critical > Red• Major > Amber or Orange• Minor > Blue• Warning > Yellow |
| Fault | <p>Specifies the name of the fault.</p> <p>Example: UNKNOWN-ME-DISCOVERED</p> |
| Entity | <p>Specifies the name of the entity.</p> |
| Entity ID | <p>The ID of the entity causing this fault.</p> <p>Example:de2d6f50b6be485e21370b6b</p> |
| Type | <p>Specifies the type of the resource such as OLT, ONT, ME_PORT, SUBSCRIBER and so on.</p> <p>Example: ONT</p> |
| Last Occurrence Time | <p>Specifies the date and time when the fault was raised the last time.</p> |

Table 107. Fault List—Current (continued)

| Field | Description |
|--------------------------|---|
| Device Reported Time | Specifies the date and time when the fault was reported to the managed element. |
| Controller Reported Time | Specifies the date and time when the fault was reported to the CBAC controller. |
| OLT | Specifies the OLT name on which the fault was raised. You can also filter the OLT column to display all the alarms related to the OLT (OLT, NNI, SFP, ONT, UNI, Services, and so on). |
| Site | Specifies the site name on which the fault was raised. You can also filter the Site column to display all the alarms related to the site (OLT, NNI, SFP, ONT, UNI, Services, and so on). |
| Error Code | Specifies the error code of the fault. |
| Data | Click on the icon to view the details about an alarm. |
| Service Affecting | Specifies whether the fault affects the service. The supported values are. <ul style="list-style-type: none"> • SA_SERVICE_AFFECTING • SA_NON_SERVICE_AFFECTING • SA_UNKNOWN |
| Probable Cause | Specifies the detailed information about the alarm. This description provides more information about the probable cause or the condition that caused the alarm. Example: OLT discovers an unknown ONT. |
| Proposed Repair Action | Specifies the proposed recovery action for the fault. |



Note: Click on the three dots icon () to acknowledge or clear the reported alarm. See [Acknowledging and Clearing Alarms \(on page 245\)](#).

The following table shows the description of fields on the Fault List—Acknowledged page.

Table 108. Fault List—Acknowledged

| Field | Description |
|----------|---|
| Severity | Specifies the severity level of an alarm. The severity levels are. <ul style="list-style-type: none"> • WARNING • MAJOR |

Table 108. Fault List—Acknowledged (continued)

| Field | Description |
|--------------------------|---|
| | <ul style="list-style-type: none"> MINOR CRITICAL |
| Fault | Specifies the name of the fault. Example: SFP-MISSING |
| Entity | Specifies the name of the entity. Example: NNI-1 |
| Entity ID | Specifies the ID of the entity. Example: Card-OLT1/port=1 |
| Type | Specifies the type of entity. Example: me_port |
| Last Occurrence Time | Specifies the date and time when the fault was raised the last time. Example: Apr 29, 2020, 12:00:02 AM |
| Device Reported Time | Specifies the date and time when the fault was reported to the managed element. |
| Controller Reported Time | Specifies the date and time when the fault was reported to the CBAC controller. |
| OLT | Specifies the OLT name on which the fault was raised. You can also filter the OLT column to display all the alarms related to the OLT (OLT, NNI, SFP, ONT, UNI, Services, and so on). |
| Site | Specifies the site name on which the fault was raised and acknowledged. You can also filter the Site column to display all the alarms related to the site (OLT, NNI, SFP, ONT, UNI, Services, and so on). |
| Parent Site | Specifies the site of the parent. You can also filter the Parent Site column to display all the alarms related to the parent site (OLT, NNI, SFP, ONT, UNI, Services, and so on). |
| Error Code | Specifies the error code of the fault. |
| Ack Time | Specifies the date and time when the fault was acknowledged. |
| Data | Click on the icon to view the details about an alarm. |
| Service Affecting | Specifies whether the fault affects the service. The supported values are. <ul style="list-style-type: none"> SA_SERVICE_AFFECTING SA_NO_SERVICE_AFFECTING |

Table 108. Fault List—Acknowledged (continued)

| Field | Description |
|------------------------|---|
| Probable Cause | Specifies the detailed information about the alarm. This description provides more information about the probable cause or the condition that caused the alarm. Example: OLT detects that the SFP module is missing on the port. |
| Proposed Repair Action | Specifies the proposed recovery action for the fault. Example: Check the SFP module presence. |

The following table shows the description of fields on the Fault List-Unacknowledged page.

Table 109. Fault List—Unacknowledged

| Field | Description |
|--------------------------|---|
| Severity | Specifies the severity level of an alarm. The severity levels are. <ul style="list-style-type: none"> • WARNING • MAJOR • MINOR • CRITICAL |
| Fault | Specifies the name of the fault. |
| Entity | Specifies the name of the entity. |
| Entity ID | Specifies the display ID of the entity. |
| Type | Specifies the type of the resource. |
| Last Occurrence Time | Specifies the date and time when the fault was raised the last time. |
| Device Reported Time | Specifies the date and time when the fault was reported to the managed element. |
| Controller Reported Time | Specifies the date and time when the fault was reported to the CBAC controller. |
| OLT | Specifies the OLT name on which the fault was raised and unacknowledged. You can also filter the OLT column to display all the alarms related to the OLT (OLT, NNI, SFP, ONT, UNI, Services, and so on). |
| Site | Specifies the site name on which the fault was raised and unacknowledged. You can also filter the Site column to display all the alarms related to the site (OLT, NNI, SFP, ONT, UNI, Services, and so on). |

Table 109. Fault List—Unacknowledged (continued)

| Field | Description |
|------------------------|---|
| Parent Site | Specifies the site of the parent. You can also filter the Parent Site column to display all the alarms related to the parent site (OLT, NNI, SFP, ONT, UNI, Services, and so on). |
| Error Code | Specifies the error code of the fault. |
| Data | Click on the icon to view the details about an alarm. |
| Service Affecting | Specifies whether the fault affects the service. The supported values are. <ul style="list-style-type: none"> • SA_SERVICE_AFFECTING • SA_NO_SERVICE_AFFECTING |
| Probable Cause | Specifies the detailed information about the alarm. This description provides more information about the probable cause or the condition that caused the alarm. |
| Proposed Repair Action | Specifies the proposed recovery action for the fault. |



Note: Click on the three dots icon () to acknowledge or clear the reported alarm. See [Acknowledging and Clearing Alarms \(on page 245\)](#).

The following table shows the description of fields on the Fault List-Cleared page.

Table 110. Fault List—Cleared

| Field | Description |
|----------------------|--|
| Severity | Specifies the severity level of an alarm. The severity levels are. <ul style="list-style-type: none"> • WARNING • MAJOR • MINOR • CRITICAL |
| Fault | Specifies the name of the fault. |
| Entity | Specifies the name of the entity. |
| Entity ID | Specifies the ID of the entity. |
| Type | Specifies the type of the resource. |
| Last Occurrence Time | Specifies the date and time when the fault was raised the last time. |

Table 110. Fault List—Cleared (continued)

| Field | Description |
|--------------------------|---|
| Device Reported Time | Specifies the date and time when the fault was reported to the managed element. |
| Controller Reported Time | Specifies the date and time when the fault was reported to the CBAC controller. |
| OLT | Specifies the OLT name on which the fault was cleared. You can also filter the OLT column to display all the alarms related to the OLT (OLT, NNI, SFP, ONT, UNI, Services, and so on). |
| Site | Specifies the site name on which the fault was cleared. You can also filter the Site column to display all the alarms related to the site (OLT, NNI, SFP, ONT, UNI, Services, and so on). |
| Parent Site | Specifies the site of the parent. You can also filter the Parent Site column to display all the alarms related to the parent site (OLT, NNI, SFP, ONT, UNI, Services, and so on). |
| Error Code | Specifies the error code of the fault. |
| Clear Time | Specifies the date and time when the alarm was cleared. |
| Data | Click on the icon to view the details about an alarm. |
| Service Affecting | Specifies whether the fault affects the service. The supported values are. <ul style="list-style-type: none"> • SA_SERVICE_AFFECTING • SA_NO_SERVICE_AFFECTING |
| Probable Cause | Specifies the detailed information about the alarm. This description provides more information about the probable cause or the condition that caused the alarm. |
| Proposed Repair Action | Specifies the proposed recovery action for the fault. |

Acknowledging and Clearing Alarms

You can use **Acknowledge** option to acknowledge that the alarm is known and is being addressed.



Note: Acknowledging an alarm does not change the severity of the alarm and the alarm count for the particular severity. For example, if there are ten critical alarms and if you acknowledge one of them, the acknowledged alarm count increases by one and the unacknowledged alarm count decreases by one.

Perform the following steps to acknowledge an alarm.

1. Click **Monitor > Fault**.

The Fault List (Current, Acknowledged, Unacknowledged, and Cleared) page appears.

2. Select **Current** or **Unacknowledged** tab.
3. Click on the three dots icon (⋮) and select the **Acknowledge** option.
4. Enter the comments. The maximum length is 256 characters.
5. Click **Submit**.

A confirmation message appears indicating that the alarm is acknowledged successfully.

The system can clear the alarm when the state changes again or an administrator can clear it manually, which indicates that the condition is now resolved.

You can use the **Clear** option to clear or remove the alarm. You can clear both acknowledged and unacknowledged alarm. Once an alarm is cleared, it just disappears from the table, with the indication that the alarm has been cleared. Once cleared, you cannot restore an alarm.

Perform the following steps to clear an alarm.

1. Select **Monitor > Fault**.

The Fault List (Current, Acknowledged, Unacknowledged, and Cleared) page appears.

2. Select **Current, Acknowledged**, or **Unacknowledged** tab.
3. Click on the three dots icon (⋮) and select the **Acknowledge** option.
4. Enter the comments. The maximum length is 256 characters.
5. Click **Submit**.

A confirmation message appears indicating that the alarm is cleared successfully.

Exporting Fault List

You can export the fault list (current, acknowledged, unacknowledged, and cleared) as a CSV file that can be opened or edited using an application such as Microsoft Excel. You can view and analyze the exported fault list, as needed.

Perform the following steps to export fault list.

1. Select **Monitor > Fault**.

The Fault List page appears.

2. Click **Export** to export the details.

The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file in a Microsoft Excel sheet. Optionally, you can save this file on your PC for later use.

Viewing Fault Details

You can view the fault details for the particular fault. This fault details help the user to identify the resource on which the fault is raised. It also provides the acknowledgment and cleared details of the fault.

Perform the following steps to view the details of a fault.

1. Select **Monitor > Fault**.

The Fault List page appears.

2. Click on the fault name.

The Fault Details page appears.

Fault Details

The following table describes the fields on the Fault Details page.

Table 111. Fault Details

| Field | Description |
|-------------------------------|---|
| Fault | |
| Severity | Specifies the severity (WARNING, MAJOR, MINOR, or CRITICAL) of the fault. |
| Time | Specifies the date and time when the fault was raised. |
| Fault Code | Specifies the fault code. |
| Entity | Specifies the name of the entity. |
| ID | Specifies the display ID of the resource. |
| Type | Specifies the type of the resource. |
| Error Code | Specifies the error code of the fault. |
| Data | Specifies the data related to the fault. |
| Acknowledgment Details | |
| Acknowledged | Specifies whether the fault is acknowledged. The supported values are. <ul style="list-style-type: none">• Yes• No |
| Ack Time | Specifies the date and time when the fault was acknowledged. |

Table 111. Fault Details (continued)

| Field | Description |
|----------------------|--|
| Comment | Specifies the comment entered while acknowledging the fault. |
| Clear Details | |
| Clear Status | Specifies whether the fault is cleared. The supported values are. <ul style="list-style-type: none">• Yes• No |
| Clear Time | Specifies the date and time when the alarm was cleared. |
| Comment | Specifies the comment entered while clearing the fault. |
| Type | Specifies how the fault was cleared. <ul style="list-style-type: none">• Manual. The alarm was cleared manually by an operator.• Auto. The alarm was cleared by CBAC automatically. |

Monitoring Events

To access this page, click **Monitor** from the top right corner of the page and select **Events** from the left-hand side of the menu.

Events provide information to the operators about the significant operations performed on the hardware and software components of the CBAC.

Events are published to the Kafka message bus on a specific topic (EMS NOTIFICATION) and delivered to RMS. The severity field of the event determines whether the published event is a notification or an alarm. If the severity is 'INFO', then the notification is an event.

The event list is refreshed automatically at the specified interval.

To view the list of events generated by RMS, see [Appendix B: Events \(on page 942\)](#).

Field Descriptions

The following table describes the fields on the Events page.

Table 112. Events

| Field | Description |
|--------------------------|---|
| Event Code | Specifies the name of the event. Example: ME-LOGIN-SUCCESS |
| Entity | Specifies the name of the resource. Example: olt1 |
| Entity Id | Specifies the display ID of the entity. Example: olt1 |
| Entity Type | Specifies the type of the resource. Example: olt1 |
| Parent Name | Specifies the parent name of the entity. Example: Shelf |
| Error Code | Specifies the error code of the event. |
| Reported Time | Specifies the time and date when the event was reported to RMS. |
| Device Reported Time | Specifies the time and date when the event was reported by the device. |
| Controller Reported Time | Specifies the time and date when the event was reported by the controller. |
| Description | Specifies the description about an event. Example: User login successful |

Table 112. Events (continued)

| Field | Description |
|-------|--|
| Data | <p>Specifies the payload information about the event.</p> <p>Example:</p> <pre>{ "user_ip": "172.24.56.90", "user_name": "admin", "SDPON-EVENT": "OLT-LOGIN-SUCCESS" }</pre> |

Exporting Events

You can export the event list as a CSV file that can be opened or edited using an application such as Microsoft Excel. You can view and analyze the exported event list, as needed.

Perform the following steps to export the event list.

1. Select **Monitor > Event**.

The Event List page appears.

2. Click **Export** to export the details.

The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file in a Microsoft Excel sheet. Optionally, you can save this file on your PC for later use.

Monitoring Tasks

To access this page, click **Monitor** from the top right corner of the page and select **Task** from the left-hand side of the menu.

The RMS monitoring framework provides an effective way to monitor the tasks that are created to perform the following operations.

- OLT Software Upgrade
- Reports (Faults, Events, and performance summary)
- EMS Database Backup (Mongo DB)
- OLT or Controller Backup
- Restore OLT and Controller
- Controller Software Upgrade
- ONT Firmware Upgrade
- ONT Bulk Firmware Upgrade
- OLT Firmware Upgrade
- Inventory Collection
- Service Collection
- Fault Collection
- Event Collection
- Audit Log Collection
- Configuration Update (Single and Bulk OLT)
- Bulk Port Modification
- Reboot
- PON Port Migration
- Banner Update

Field Descriptions

The following table describes the fields on the Task List page.

Table 113. Task List

| Field | Description |
|-------|--|
| Name | Specifies the name of the task. Example: Database-backup |
| Type | Specifies the type of the task that you have created. The following tasks are supported. |

Table 113. Task List (continued)

| Field | Description |
|-------------|---|
| | <ul style="list-style-type: none"> Reports OLT Software Upgrade Database Backup Backup Restore Controller Software Upgrade ONT Firmware Upgrade Inventory Collection |
| Status | <p>Specifies the status of the task. The supported values are.</p> <ul style="list-style-type: none"> SCHEDULED. The task is scheduled for later execution. CREATED. The task is created. RUNNING. The task is created and running. COMPLETED. The task execution is completed. |
| Description | Specifies the description about the task. |
| Created At | <p>Specifies the date and time when the task was created.</p> <p>Example: Jul 2, 2020, 3:03:08 PM</p> |
| Time Policy | <p>Specifies the whether the report is scheduled for immediate execution or for a later date and time.</p> <p>Example: IMMEDIATE</p> |
| Executed At | <p>Specifies the date and time when the task was executed.</p> <p>Example: Jul 2, 2020, 3:05:45 PM</p> |

Monitoring Task Details

You can monitor the tasks created for the following operations.

- OLT Software Upgrade. See [OLT Software Upgrade \(on page 253\)](#).
- Reports (Fault summary and performance summary). See [Reports \(on page 254\)](#).
- EMS Database Backup (Mongo DB). See [EMS Database Backup \(on page 255\)](#).
- OLT or Controller Backup. See [OLT/Controller Backup \(on page 256\)](#).
- Restore OLT and Controller. See [OLT/Controller Restore \(on page 258\)](#).
- Controller Software Upgrade. See [Controller Software Upgrade \(on page 259\)](#).
- ONT Firmware Upgrade. See [ONT Firmware Upgrade \(on page 260\)](#).
- ONT Bulk Firmware Upgrade. See [ONT Bulk Firmware Upgrade \(on page 262\)](#).

- OLT Firmware Upgrade. See [OLT Firmware Upgrade \(on page 265\)](#).
- Inventory Collection. See [Inventory Collection \(on page 265\)](#).
- Service Collection. See [Service Collection \(on page 267\)](#).
- Fault Collection. See [Fault Collection \(on page 269\)](#).
- Event Collection. See [Event Collection \(on page 270\)](#).
- Audit Log Collection. See [Audit Log Collection \(on page 272\)](#).
- OLT Configuration Update (Single and Bulk OLT). See [OLT Configuration Update \(on page 272\)](#).
- ONT Configuration Update. See [ONT Configuration Update \(on page 273\)](#).
- Bulk Port Modification. See [Bulk Port Modification \(on page 275\)](#).
- Reboot. See [Reboot \(on page 276\)](#).
- PON Port Migration. See [PON Port Migration \(on page 277\)](#).
- Banner Update. See [Table 133: Banner Update Task Details \(on page 279\)](#).

You can monitor the following details of the task.

- Basic Task Information
- Device Details List

Perform the following steps to monitor the task details.

1. Click on the **Monitor > Task** tab.
2. Click on the task name under the **Name** column.

The Task Details page appears.

OLT Software Upgrade

The following table describes the basic information about the OLT software upgrade task.

Table 114. OLT Software Upgrade Task

| Field | Description |
|-------------------------------|--|
| Basic Task Information | |
| Name | Specifies the name of the task. Example: OLT |
| Type | Specifies the type of the task. Example: SOFTWARE-UPGRADE |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. Example: CREATED |
| Creation Time | Specifies the date and time when the task was created. |

Table 114. OLT Software Upgrade Task (continued)

| Field | Description |
|----------------------------|---|
| Time Policy | Specifies whether the report is scheduled for immediate execution or for a later date and time. Example: IMMEDIATE |
| Device Details List | |
| Device Name | Specifies the name of the device. |
| Current Version | Specifies the current version of the software. |
| Version to be Upgraded | Specifies the new software version to which the OLT needs to be upgraded. |
| Task Execution Status | Specifies the execution status of the task. |
| Status | Specifies the status of the task. Example: CREATED |
| Remarks | Displays any remark. |
| Creation Time | Specifies the date and time when the task was created. |

Reports

The following table describes the basic information about report task. For more information, see [Monitoring Reports \(on page 235\)](#).

Table 115. Report Summary

| Field | Description |
|-------------------------------|--|
| Basic Task Information | |
| Name | Specifies the name of the task. Example: Fault summary report |
| Type | Specifies the type of the task. Example: REPORTS |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. Example: COMPLETED |
| Creation Time | Specifies the date and time when the task was created. |
| Execution Time | Specifies the date and time when the task was executed. |

Table 115. Report Summary (continued)

| Field | Description |
|------------------------------|---|
| EXECUTION TIME POLICY | |
| Immediate | Select this option if you want to generate the report immediately. |
| Schedule | <p>Select this option if you want to schedule the report generation for a later date and time. You can select daily, weekly, or monthly.</p> <ul style="list-style-type: none"> • Daily. If you have selected the option as Daily, select the time when the report needs to be generated. • Weekly. If you have selected the option as Weekly, you must select the day (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday) from the Select Day list and then select the time from the Select Time list. • Monthly. If you have selected the option as Monthly, you must select the date (From 1 to 31, or Last Day of the Month) from the Select Date list and then select the time from the Select Time list. • One Time. If you have selected the option as One Time, you need to set a specific date and time for the task. By default, the Start Time field displays the current date and time. To select a different date and time, choose the desired date and set the exact time using the time picker. |

EMS Database Backup

The following table describes the basic information about the database backup task.

Table 116. EMS Database Backup Task Details

| Field | Description |
|-------------------------------|--|
| Basic Task Information | |
| Name | Specifies the name of the database. Example: RMS |
| Type | Specifies the type of the task. Example: EMS-BACKUP |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. Example: CREATED |
| Creation Time | Specifies the date and time when the task was created. |

Table 116. EMS Database Backup Task Details (continued)

| Field | Description |
|------------------------------|--|
| File Store | Select the file storage location where you want to store the fault collection report. |
| File Store Path | Specifies the file store location. |
| EXECUTION TIME POLICY | |
| Immediate | Select this option if you want to generate the report immediately. |
| Schedule | <p>Select this option if you want to schedule the report generation for a later date and time. You can select daily, weekly, or monthly.</p> <ul style="list-style-type: none"> Daily. If you have selected the option as Daily, select the time when the report needs to be generated. Weekly. If you have selected the option as Weekly, you must select the day (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday) from the Select Day list and then select the time from the Select Time list. Monthly. If you have selected the option as Monthly, you must select the date (From 1 to 31, or Last Day of the Month) from the Select Date list and then select the time from the Select Time list. |

The following figure shows the EMS database backup, which contains the detailed information about the task.

Figure 42. EMS Database Backup

The screenshot shows a software interface for managing database backups. At the top, there's a header with a 'Task Details' icon and a 'Close' button. Below the header, there are two main sections: 'Basic Task Information' and 'Execution Details'.

Basic Task Information:

| | |
|-------------|----------------------------|
| Name | EMS-DB |
| Type | DB-BACKUP |
| Description | Creating Backup for EMS DB |
| Status | COMPLETED |

Execution Details:

| | |
|-----------------|--------------------------|
| Time Policy | IMMEDIATE |
| Creation Time | Oct 26, 2023, 4:40:33 PM |
| Execution Time | Oct 26, 2023, 5:00:23 PM |
| File Store | test |
| File Store Path | /home/sdponmp/vibhuti |

OLT/Controller Backup

The following table describes the basic information about the OLT or controller backup task.

Table 117. OLT or Controller Backup Task Information

| Field | Description |
|-------|---------------------------------|
| Name | Specifies the name of the task. |

Table 117. OLT or Controller Backup Task Information (continued)

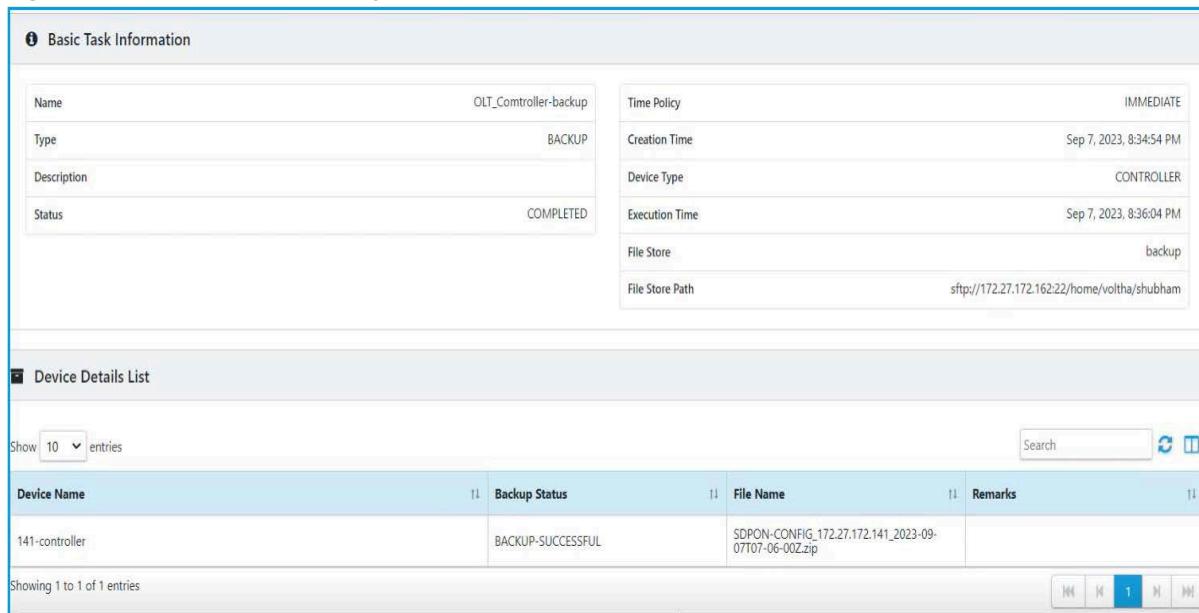
| Field | Description |
|------------------------------|--|
| | Example: Backup_Controller |
| Type | Specifies the type of the task. Example: OLT or Controller Backup |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. |
| Time Policy | Specifies the time policy. |
| Creation Time | Specifies the date and time when the task was created. |
| Path | Specifies the SFTP sever location where the OLT or controller backup configuration is stored. |
| Schedule Time | Specifies the time when the backup operation is scheduled. |
| Device Type | Specifies device type for which the backup operation task is created. Example: Controller or OLT |
| Execution Time | Specifies the date and time when the backup operation was executed.  Note: This field appears when the backup task is executed successfully for the first time. |
| File Name | Specifies the name of the backed-up configuration file.  Note: This field appears when the backup task is executed successfully for the first time. |
| Device Details List | |
| Device Name | Specifies the device name of the OLT or controller. |
| Backup Status | Specifies the backup status of the OLT or controller. |
| File Name | Specifies the file name of the OLT or controller. |
| Remarks | Displays any remark. |
| EXECUTION TIME POLICY | |
| Immediate | Select this option if you want to generate the report immediately. |

Table 117. OLT or Controller Backup Task Information (continued)

| Field | Description |
|----------|--|
| Schedule | <p>Select this option if you want to schedule the report generation for a later date and time. You can select daily, weekly, or monthly.</p> <ul style="list-style-type: none"> Daily. If you have selected the option as Daily, select the time when the report needs to be generated. Weekly. If you have selected the option as Weekly, you must select the day (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday) from the Select Day list and then select the time from the Select Time list. Monthly. If you have selected the option as Monthly, you must select the date (From 1 to 31, or Last Day of the Month) from the Select Date list and then select the time from the Select Time list. |

The following figure shows the EMS database backup, which contains the detailed information about the task.

Figure 43. OLT/Controller Backup



The screenshot displays the EMS database backup interface. The top section, 'Basic Task Information', shows the following details:

| | | | |
|-------------|-----------------------|-----------------|--|
| Name | OLT_Controller-backup | Time Policy | IMMEDIATE |
| Type | BACKUP | Creation Time | Sep 7, 2023, 8:34:54 PM |
| Description | | Device Type | CONTROLLER |
| Status | COMPLETED | Execution Time | Sep 7, 2023, 8:36:04 PM |
| | | File Store | backup |
| | | File Store Path | sftp://172.27.172.162:22/home/voltha/shubham |

The bottom section, 'Device Details List', shows a table with the following data:

| Device Name | Backup Status | File Name | Remarks |
|----------------|-------------------|--|---------|
| 141-controller | BACKUP-SUCCESSFUL | SDPON-CONFIG_172.27.172.141_2023-09-07T07-06-00Z.zip | |

Showing 1 to 1 of 1 entries

OLT/Controller Restore

The following table describes the basic information about the OLT or controller restore task.

Table 118. Task Information—OLT or Controller Restore

| Field | Description |
|-------------------------------|-------------|
| Basic Task Information | |

Table 118. Task Information—OLT or Controller Restore (continued)

| Field | Description |
|---------------------|---|
| Name | Specifies the name of the task. Example: Restore_Controller |
| Type | Specifies the type of the task. Example: RESTORE |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. Example: COMPLETED |
| Time Policy | Specifies the time policy whether the restore operation is performed immediately or on the scheduled time. Example: IMMEDIATE |
| Creation Time | Specifies the date and time when the task was created. |
| Device Details List | You can view the following details of the device. <ul style="list-style-type: none"> Device Name Restore status of the device File Name Remarks |
| File Store | Select the file storage from the drop-down. |
| File Store Path | Specifies the file store location. |
| Execution Time | Specifies the date and time when the controller restore has happened. |

Controller Software Upgrade

The following table describes the basic information about the controller software upgrade task.

Table 119. Task Information—Controller Software Upgrade

| Field | Description |
|--|---|
| Basic Task Information -OLT or Controller | |
| Name | Specifies the name of the task. Example: Controller Software Upgrade |
| Type | Specifies the type of the task. Example: CONTROLLER-SW-UPGRADE |

Table 119. Task Information—Controller Software Upgrade (continued)

| Field | Description |
|---------------------|--|
| Description | Specifies description of the task. |
| Status | Specifies the status of the task. |
| Creation Time | Specifies the date and time when the task was created. |
| Schedule Time | Specifies the date and time when the report was executed. |
| Device Details List | <p>You can view the following details of the device.</p> <ul style="list-style-type: none"> • Device Name • Current version of the device • Version to which the device needs to be upgraded • Status of the device • Remarks |

ONT Firmware Upgrade

The following table describes the basic information about the ONT firmware upgrade task.

Table 120. ONT Firmware Upgrade Task Details

| Field | Description |
|--------------------------------|---|
| Basic Information | |
| Name | Specifies the name of the task. Example: ONT Firmware Upgrade |
| Type | Specifies the type of the task. Example: ONT_FIRMWARE_UPGRADE |
| Description | Specifies description of the task. |
| Status | Specifies the status of the task. The supported values are. <ul style="list-style-type: none"> • CREATED • RUNNING • COMPLETED |
| Creation Time | Specifies the date and time when the ONT firmware task was created. |
| Device Type | Specifies the device type. |
| Download on OLT Execution Type | Specifies the option to download the ONT firmware on the OLT. |

Table 120. ONT Firmware Upgrade Task Details (continued)

| Field | Description |
|---|---|
| | <p>The supported values are.</p> <ul style="list-style-type: none"> • Immediate. Select this option to perform the ONT firmware download operations immediately. • Timing. Select this option to specify the date and time when you want to download the ONT firmware. |
| Download on ONT Execution Type | <p>Specifies the option to download the ONT firmware on the ONT. The supported values are.</p> <ul style="list-style-type: none"> • Immediate. Select this option to perform the ONT firmware download operations immediately. • Timing. Select this option to specify the date and time when you want to download the ONT firmware. |
| Enable Auto Commit | Specifies if the auto commit is enabled or not. |
| Activate and Commit on ONT Execution Type | <p>Specifies the option to auto-activate and commit the new ONT firmware after the ONT reboot.</p> <p>The supported values are.</p> <ul style="list-style-type: none"> • Immediate. Select this option to perform the auto-activate and commit operations immediately after the ONT reboot. • Timing. Select this option to specify the date and time when you want to auto-activate and commit the ONT firmware. |
| OLT List | |
| Device Name | Specifies the name of the OLT device. |
| ONT Firmware Version (Upgrade From) | Specifies the ONT firmware version before the ONT upgrade. Example: 1.0.0.161 |
| ONT Firmware Version (Upgrade To) | Specifies the ONT firmware version after the ONT upgrade. Example: 1.0.0.164 |
| Task Status | Specifies the ONT firmware download status. Example: DOWNLOAD-ON-OLT-SUCCESS |
| Remarks | Displays any remarks. |
| ONT List | |
| Device Name | Specifies the name of the ONT device. |
| ONT Firmware Version (Upgrade From) | Specifies ONT firmware version before the ONT upgrade. Example: 1.0.0.161 |

Table 120. ONT Firmware Upgrade Task Details (continued)

| Field | Description |
|-----------------------------------|---|
| ONT Firmware Version (Upgrade To) | Specifies ONT firmware version after the ONT upgrade. Example: 1.0.0.164 |
| Task Status | Specifies the ONT firmware download status. The supported values are. <ul style="list-style-type: none"> • DOWNLOAD-ON-ONT-IN-PROGRESS • DOWNLOAD-ON-ONT-PENDING • DOWNLOAD-ON-ONT-STOPPED • DOWNLOAD-ON-ONT-SUCCESS • DOWNLOAD-ON-ONT-FAILED • DOWNLOAD-ON-ONT-FAILED-RETRYING • ACTIVATE-COMMIT-SUCCESS • AUTO-ACTIVATE-COMMIT-IN-PROGRESS • ACTIVATE-COMMIT-FAILED |
| Remarks | Displays any remarks. |
| Get Progress | |
| ONT ID | Specifies the unique ID of the ONT. |
| ONT Name | Specifies the name of the ONT. |
| Status | Specifies the download status (in percentage) of the ONT firmware. |
| Reason | Displays any reason. |

ONT Bulk Firmware Upgrade

The following table describes the ONT bulk firmware upgrade task details.

Table 121. ONT Bulk Firmware Upgrade Task Details

| Field | Description |
|--------------------------|---|
| Basic Information | |
| Name | Specifies the name of the task. Example: ONT Bulk Firmware Upgrade |
| Type | Specifies the type of the task. Example: ONT_BULK_FIRMWARE_UPGRADE |

Table 121. ONT Bulk Firmware Upgrade Task Details (continued)

| Field | Description |
|---|---|
| Description | Specifies description of the task. |
| Status | Specifies the status of the task. The supported values are. <ul style="list-style-type: none"> • CREATED • RUNNING • COMPLETED |
| Creation Time | Specifies the date and time when the ONT bulk firmware task was created. |
| Device Type | Specifies the device type. |
| Download on OLT Execution Type | Specifies the option to download the ONT bulk firmware on the OLT. Example: Immediate. |
| Download on ONT Execution Type | Specifies the option to download the ONT bulk firmware on the ONT. Example: Immediate. |
| Enable Auto Commit | Specifies whether the auto commit is enabled. |
| Enable Activate Commit on ONT Reboot | Enables the auto-activation and commits the new ONT firmware after the ONT reboot. |
| Activate Commit on ONT Reboot | Enables and auto commits the ONT firmware on the ONT. |
| Activate and Commit on ONT Execution Type | Specifies the option to auto-activate and commit the new ONT firmware after the ONT reboot. Example: Immediate |
| OLT List | |
| Device Name | Specifies the name of the OLT device. |
| ONT Firmware Version | Specifies the ONT firmware version. |
| Status (Download on OLT) | Specifies the status of ONT firmware download on OLT. Example: SUCCESS |
| Remarks | Displays any remarks. |
| Creation Time | Specifies the date and time when the task was created. |
| ONT List | |
| Device Name | Specifies the name of the ONT device. |

Table 121. ONT Bulk Firmware Upgrade Task Details (continued)

| Field | Description |
|-------------------------------------|---|
| ONT Firmware Version (Upgrade From) | Specifies ONT firmware version before the ONT upgrade. Example: 1.0.0.161 |
| ONT Firmware Version (Upgrade To) | Specifies ONT firmware version after the ONT upgrade. Example: 1.0.0.164 |
| Task Status | Specifies the ONT firmware download status. The supported values are. <ul style="list-style-type: none"> • DOWNLOAD-ON-ONT-IN-PROGRESS • DOWNLOAD-ON-ONT-PENDING • DOWNLOAD-ON-ONT-STOPPED • DOWNLOAD-ON-ONT-SUCCESS • DOWNLOAD-ON-ONT-FAILED • DOWNLOAD-ON-ONT-FAILED-RETRYING • ACTIVATE-COMMIT-SUCCESS • AUTO-ACTIVATE-COMMIT-IN-PROGRESS • ACTIVATE-COMMIT-FAILED |
| Remarks | Displays any remarks. |

The following table shows the ONT bulk firmware upgrade, which contains the detailed information about the task.

Figure 44. Bulk Firmware Upgrade

| Device Name | ONT Firmware Version | Status (Download On OLT) | Remarks | Creation Time |
|-------------|----------------------|--------------------------|---------|--------------------------|
| OLT-134 | 1.1.0.002 | SUCCESS | | Aug 29, 2023, 4:10:59 PM |

OLT Firmware Upgrade

The following table describes the basic information about the OLT firmware upgrade task.

Table 122. OLT Firmware Upgrade Task

| Field | Description |
|-------------------------------|--|
| Basic Task Information | |
| Name | Specifies the name of the task. |
| Type | Specifies the upgrade type. Example: FIRMWARE-UPGRADE |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. Example: COMPLETED |
| Creation Time | Specifies the date and time when the task was created. Example: Sep 8, 2023, 9:32:55 PM |
| Device Details List | |
| Device Name | Specifies the device name. |
| Current Version | Specifies the OLT firmware version before upgrade. |
| Version to be Upgraded | Specifies the OLT firmware version after upgrade. |
| Task execution Status | Specifies the task executed status. Example: COMPLETED. |
| Status | Specifies the status of the device. Example: UPGRADE-SUCCESSFUL |
| Remarks | Display any remark. |

Inventory Collection

The following table describes the basic information about the inventory collection task.

Table 123. Inventory Collection Task

| Field | Description |
|---|---------------------------------|
| Basic Task Information-OLT or Controller | |
| Name | Specifies the name of the task. |

Table 123. Inventory Collection Task (continued)

| Field | Description |
|-------------------|--|
| | Example: ME Inventory |
| Type | Specifies the type of the task. Example: INVENTORY COLLECTION |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. The supported values are. <ul style="list-style-type: none"> • CREATED • RUNNING • COMPLETED |
| Creation Time | Specifies the date and time when the task was created. |
| Time Policy | Specifies the time policy whether the task is executed immediately or scheduled for a later date and time. |
| Type | Specifies the type of the managed element for which the inventory is created. Example: OLT |
| Admin State | Specifies the admin state of the OLT. The supported values are. <ul style="list-style-type: none"> • ACTIVE • DEACTIVE |
| Operational State | Specifies the operational state of the OLT. The supported values are. <ul style="list-style-type: none"> • UP • DOWN |
| OLT | Specifies the type of the managed element. |
| Download | |
| Name | Specifies the name of the inventory report. Example: IC_2023-08-29_13_43_46_824 |
| Status | Specifies the status of the inventory report. Example: SUCCESS |
| Description | Specifies the description of the task. Example: Inventory collection exported successfully |
| Download | Specifies the CSV file download option. Click on the download icon () to download the CSV file. |

Table 123. Inventory Collection Task (continued)

| Field | Description |
|---------------|---|
| | You can open the .csv file using an application such as Microsoft Excel. Optionally, you can save this file on your PC for later use. |
| Creation Time | Specifies the date and time when the report was created. |

The following figure shows the inventory collection report of the managed element (OLT).

Figure 45. Inventory Collection

Service Collection

The following table describes the basic information about the service collection task.

Table 124. Service Collection Task

| Field | Description |
|---|---|
| Basic Task Information-OLT or Controller | |
| Name | Specifies the name of the task. Example: Service1 |
| Type | Specifies the type of the task. Example: SERVICE_COLLECTION |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. The supported values are. <ul style="list-style-type: none">• CREATED• RUNNING• COMPLETED |
| Creation Time | Specifies the date and time when the task was created. |

Table 124. Service Collection Task (continued)

| Field | Description |
|-------------------------------|--|
| Time Policy | Specifies the time policy whether the task is executed immediately or scheduled for a later date and time. |
| ADMIN_STATE | Specifies the admin state of the OLT. The supported values are. <ul style="list-style-type: none"> • ACTIVE • DEACTIVE |
| OPERATIONAL_STATE | Specifies the operational state of the OLT. The supported values are. <ul style="list-style-type: none"> • UP • DOWN |
| OLT | Specifies the OLT ID. Example: 12d2b150-b7ba-11eb-8019-8a531cd806e3-53 |
| SITE_GROUP_ID | Specifies the site group ID. |
| SERVICE_INFO. SERVICE_NAME | Specifies the service name. |
| Download | |
| Name | Specifies the name of the service collection report. |
| Status | Specifies the status of the service collection report. |
| Description | Specifies the description of the task. |
| Download | Displays the downloaded report that you can open and save. See Figure 46: Service Collection (on page 269) . |
| Creation Time | Specifies the date and time when the report was created. |

The following figure shows the service collection report, which contains the detailed information about the subscriber service.

Figure 46. Service Collection

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
|----|----------|------------------|-----------|----------|----------------|------------|---------|-----------|------------|------------|-------|----------|----------|----------|---|
| 1 | name | admin_stolt_name | olt_port | ont_name | operator | subscriber | aes_enc | allow_tra | circuit_id | circuit_id | ovlan | ds_band | ds_cosq | ds_shap | |
| 2 | ad | DEACTIVE | | QAZWSX1 | QAZ | TRUE | | | | | | Cosq1 | shaper | | |
| 3 | Subscrib | DEACTIV | ISKOLTF | PON-2 | ONT1404 | Pooja14C | TRUE | | | | | Cosq1 | shaper1 | | |
| 4 | Subscrib | DEACTIV | ISKOLTF | PON-2 | ONT1404 | Pooja14C | TRUE | | | | | Cosq1 | shaper1 | | |
| 5 | Subscrib | DEACTIV | ISKOLTF | PON-2 | ONT1404-new | Pooja14C | TRUE | | | | | Cosq2 | shaper1 | | |
| 6 | Subscrib | DEACTIV | ISKOLTF | PON-2 | ONT1404-new | Pooja14C | TRUE | | | | | Cosq4 | shaper1 | | |
| 7 | Serv1 | ACTIVE | MS-Test | PON-1 | MS-test_UP | MS-Test | TRUE | ENABLED | | | | bandcir | Cosq1 | shaper | |
| 8 | Serv1 | ACTIVE | MS-Test | PON-1 | MS-test_UP | MS-Test | TRUE | ENABLED | | | | bandwidt | Cosq1 | shaper | |
| 9 | Subscrib | DEACTIV | LocalCont | ISKOLT | MS-Testing-ONT | TestSub | TRUE | | | | | Res_JHv | Resident | Res_JHv | |
| 10 | subscrib | DEACTIV | LocalCont | ISKOLT | MS-Testing-ONT | TestSub | TRUE | | | | | Cosq | shaper | | |
| 11 | Subscrib | ACTIVE | ISKOLT2 | PON-2 | ONTName2205 | Subscrib | TRUE | | | | | Cosq1 | shaper1 | | |
| 12 | Service | ACTIVE | ISKOLT2 | PON-10 | ONT_testing_2E | Subscrib | TRUE | | | | | bandwidt | Cosq1 | shaper1 | |
| 13 | Test_1 | ACTIVE | ISKOLT2 | PON-1 | MehulONTName23 | Subscrib | TRUE | | | | | Cosq1 | shaper1 | | |
| 14 | Test_2 | DEACTIV | ISKOLT2 | PON-1 | MehulONTName23 | Subscrib | TRUE | | | | | Cosq1 | shaper1 | | |
| 15 | Test_4 | ACTIVE | ISKOLT2 | PON-1 | MehulONTName2E | Subscrib | TRUE | | | | | Cosq1 | shaper1 | | |
| 16 | Test_3 | DEACTIV | ISKOLT2 | PON-1 | MehulONTName2E | Subscrib | TRUE | | | | | Cosq1 | shaper1 | | |
| 17 | Test_6 | ACTIVE | ISKOLT2 | PON-1 | MehulONTName2E | Subscrib | TRUE | | | | | Cosq1 | shaper1 | | |
| 18 | Service_ | DEACTIV | ISKOLT2 | PON-10 | ONT_testing_2E | Subscrib | FALSE | | | | | 2 | Cosq3 | shaperic | |
| 19 | ServiceR | ACTIVE | MS-Test | PON-1 | ONT_testing_2E | ONTIDF | TRUE | ENABLED | | | | 4 | Cosq2 | shaper | |
| 20 | Service_ | DEACTIV | ISKOLT_ | PON-12 | Card_7thMay | 7thMay | TRUE | | | | | 7thMay_1 | 7thMay | 7thMay | |
| 21 | ServiceR | ACTIVE | MS-Test | PON | ONT_testing_6E | Subscrib | TRUE | | | | | bandwidt | Resident | Res_HSL | |
| 22 | | | | | | | | | | | | | | | |
| 23 | | | | | | | | | | | | | | | |
| 24 | | | | | | | | | | | | | | | |
| 25 | | | | | | | | | | | | | | | |
| 26 | | | | | | | | | | | | | | | |
| 27 | | | | | | | | | | | | | | | |
| 28 | | | | | | | | | | | | | | | |
| 29 | | | | | | | | | | | | | | | |
| 30 | | | | | | | | | | | | | | | |
| 31 | | | | | | | | | | | | | | | |

Fault Collection

You can view and download the faults list for the particular managed element.

The following table describes the information about the report generation task.

Table 125. Fault Collection Task

| Field | Description |
|-------------------------------|---|
| Basic Task Information | |
| Name | Specifies the name of the task. |
| Type | Specifies the type of the task. Example: FAULT-COLLECTION |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. Example: COMPLETED |
| Time Policy | Specifies whether the report is scheduled for immediate execution or for a later date and time. Example: IMMEDIATE |
| Download | |
| Name | Specifies the name of the fault collection. Example: FC_2023-08-29_14_00_53_831 |
| Status | Specifies the status of the inventory report. |

Table 125. Fault Collection Task (continued)

| Field | Description |
|---------------|--|
| | Example: SUCCESS |
| Description | Specifies the description of the task. Example: Fault collection exported successfully |
| Download | Specifies the CSV file download option. Click on the download icon () to download the CSV file. You can open the .csv file using an application such as Microsoft Excel. Optionally, you can save this file on your PC for later use. |
| Creation Time | Specifies the date and time when the report was created. |

The following figure shows the fault collection report, which contains the detailed information about the fault.

Figure 47. Fault Collection

| A | B | C | D | E | F | G | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
|----------|-------------------------------|----------------|-------------------------|--------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---|--------|---------|---------|------------|-----------|------------|------------------------|---|---|---|---|
| severity | fault_code | entity_name | entity_display | entity | entity | error_c | first_oc | creation | last_oc | last_oc | device | device | control | control | fault_data | service_a | native_pri | proposed_repair_action | | | | |
| MAJOR | PON-LOS-DGI | SFPON-10 | /rack=1/shelf=1/me_port | TC_OLT_09_05 | Sep 06, 20 1.69E+12 | ["num_uni_pcSA_NON_SEUnknown ON if the discovered ONT is valid, then add the ONT. | | | | | | | | | | | |
| MINOR | UNKNOWN-ME-DISCOVERED UNKNOWN | ONU1244187745 | CNT | TC_OLT_09_05 | Sep 08, 20 1.69E+12 | ["num_uni_pcSA_NON_SEUnknown ON if the discovered ONT is valid, then add the ONT. | | | | | | | | | | | |
| MINOR | UNKNOWN-ME-DISCOVERED UNKNOWN | ONU0252710023 | ONT | TC_OLT_09_05 | Sep 08, 20 1.69E+12 | ["num_uni_pcSA_NON_SEUnknown ON if the discovered ONT is valid, then add the ONT. | | | | | | | | | | | |
| MINOR | UNKNOWN-ME-DISCOVERED UNKNOWN | ONU14176928781 | CNT | TC_OLT_09_05 | Sep 08, 20 1.69E+12 | ["num_uni_pcSA_NON_SEUnknown ON if the discovered ONT is valid, then add the ONT. | | | | | | | | | | | |
| MINOR | UNKNOWN-ME-DISCOVERED UNKNOWN | ONU1815650827 | ONT | TC_OLT_09_05 | Sep 08, 20 1.69E+12 | ["num_uni_pcSA_NON_SEUnknown ON if the discovered ONT is valid, then add the ONT. | | | | | | | | | | | |
| MINOR | UNKNOWN-ME-DISCOVERED UNKNOWN | ONU18156322204 | CNT | TC_OLT_09_05 | Sep 08, 20 1.69E+12 | ["num_uni_pcSA_NON_SEUnknown ON if the discovered ONT is valid, then add the ONT. | | | | | | | | | | | |
| Critical | SFP-MISSING | SFPON-10 | /rack=1/shelf=1/me_port | AB01 | Sep 08, 20 1.69E+12 | ["CONTROLLEISA_SERVICE SFP module (Check if the SFP module is present in the PON interface. | | | | | | | | | | | |
| Critical | SFP-MISSING | SFPON-9 | /rack=1/shelf=1/me_port | AB01 | Sep 08, 20 1.69E+12 | ["CONTROLLEISA_SERVICE SFP module (Check if the SFP module is present in the PON interface. | | | | | | | | | | | |
| Critical | OLT-ALTERNATE-POWER-SUP | TC_OLT_09_05 | OLT | | INVENTO | Sep 11, 20 1.69E+12 | ["CONTROLLEISA_NON_SEThe alternati | | | | | | | | | | | |
| Critical | OLT-ALTERNATE-POWER-SUP | AB01 | OLT | | INVENTO | Sep 11, 20 1.69E+12 | ["CONTROLLEISA_NON_SEThe alternati | | | | | | | | | | | |

Event Collection

You can view and download the events list for the particular managed element.

The following table describes the basic information about the report generation task.

Table 126. Event Collection Task

| Field | Description |
|-------------------------------|--|
| Basic Task Information | |
| Name | Specifies the name of the task. Example: Event_Report |
| Type | Specifies the type of the task. Example: Reports |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. |

Table 126. Event Collection Task (continued)

| Field | Description |
|---------------|--|
| | Example: COMPLETED |
| Time Policy | Specifies whether the report is scheduled for immediate execution or for a later date and time. Example: IMMEDIATE |
| Creation Time | Specifies the date and time when the report was created. |
| Download | |
| Name | Specifies the name of the task. Example: Event_Report |
| Status | Specifies the event collection export status. Example: SUCCESS |
| Description | Specifies the description of event collection export status. Example: Event collection exported successfully |
| Download | Specifies the CSV file download option. Click on the download icon () to download the CSV file. You can open the .csv file using an application such as Microsoft Excel. Optionally, you can save this file on your PC for later use. |
| Creation Time | Specifies the date and time when the report was generated. |

The following figure shows the event collection report, which contains the detailed information about the events.

Figure 48. Event Collection

Audit Log Collection

The following table describes the basic information and device details about the audit log collection.

Table 127. Audit Log Collection

| Field | Description |
|-------------------------------|--|
| Basic Task Information | |
| Name | Specifies the name of the task. Example: AuditLogs. |
| Type | Specifies the type of the task. Example: AUDIT-LOG-COLLECTION |
| Description | Specifies the description of the task. Example: COMPLETED |
| Status | Specifies the status of the task. Example: COMPLETED |
| Creation Time | Specifies the date and time when the task was created. Example: Apr 3, 2024, 5:43:38 AM |
| Time Policy | Specifies whether the report is scheduled for immediate execution or for a later date and time. Example: IMMEDIATE |
| Download | |
| Name | Specifies the name of the device. |
| Status | Specifies the status of the inventory report. Example: SUCCESS |
| Description | Specifies the description of the task. |
| Download | Specifies the CSV file download option. Click on the download icon () to download the CSV file. You can open the .csv file using an application such as Microsoft Excel. Optionally, you can save this file on your PC for later use. |
| Creation Time | Specifies the date and time when the report was created. Example: Apr 3, 2024, 5:45:00 AM |

OLT Configuration Update

The following table describes the basic information and device details about the OLT configuration update task.

Table 128. OLT Configuration Update Task

| Field | Description |
|-------------------------------|--|
| Basic Task Information | |
| Name | Specifies the name of the task. Example: Config Update |
| Type | Specifies the type of the task. Example: UPDATE-CONFIGURATION |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. Example: COMPLETED |
| Creation Time | Specifies the date and time when the task was created. Example: Aug 19, 2021, 9:32:55 PM |
| Device Type | Specifies the device type. Example: OLT |
| Execution Time | Specifies the date and time when the update was executed. Example: Aug 19, 2021, 9:33:24 PM |
| Time Policy | Specifies whether the configuration update is scheduled for immediate execution or at a later date and time. Example: IMMEDIATE |
| Configurations | You can view the updated configuration of the OLT. |
| Device Details List | |
| Device Name | Specifies the name of the device. |
| Status | Specifies the status of the device. Example: UPDATE-CONFIGURATION-SUCCESSFUL |
| Remarks | Specifies any remarks. |

ONT Configuration Update

The following table describes the basic information and device details about the ONT configuration update task.

Table 129. ONT Configuration Update Task

| Field | Description |
|-------------------------------|--|
| Basic Task Information | |
| Name | Specifies the name of the task. Example: Config Update |
| Type | Specifies the type of the task. Example: UPDATE-CONFIGURATION |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. Example: COMPLETED |
| Time Policy | Specifies whether the configuration update is scheduled for immediate execution or at a later date and time. Example: IMMEDIATE |
| Creation Time | Specifies the date and time when the task was created. Example: Aug 19, 2023, 9:32:55 PM |
| Device Type | Specifies the device type. Example: ONT |
| Execution Time | Specifies the date and time when the update was executed. Example: Aug 19, 2023, 9:33:24 PM |
| Configurations | You can view the updated configuration of the OLT. |
| Device Details List | |
| Device Name | Specifies the name of the device. |
| Status | Specifies the status of the device. Example: UPDATE-CONFIGURATION-SUCCESSFUL |
| Remarks | Specifies any remarks. |

The following figure shows the bulk port modification, which contains the detailed information about the task.

Figure 49. ONT Configuration Update

The screenshot shows the Radisys Monitoring Tasks interface. At the top, there is a header with the Radisys logo and the text 'Monitoring Tasks'. Below the header, the title 'Figure 49. ONT Configuration Update' is displayed. The main content area is a 'Task Details' card. The card has two sections: 'Basic Task Information' and 'Device Details List'. The 'Basic Task Information' section contains fields for Name (demo-1), Type (UPDATE-CONFIGURATION), Description, and Status (COMPLETED). It also includes Time Policy (IMMEDIATE), Creation Time (Oct 6, 2023, 12:42:42 PM), Device Type (ONT), Execution Time (Oct 6, 2023, 12:43:04 PM), and Configurations. The 'Device Details List' section shows a table with three entries, each with a Device Name (ARDNB5C56073, ARDN9E74454D, ARDN9E741838) and a Status (UPDATE-CONFIGURATION-SUCCESSFUL). A search bar and various navigation buttons are also present at the bottom of the card.

Bulk Port Modification

The following table describes the bulk port modification task details.

Table 130. Bulk Port Modification Details

| Field | Description |
|-------------------------------|---|
| Basic Task Information | |
| Name | Specifies the name of the bulk port modification. |
| Type | Specifies the modification type. |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. Example: COMPLETED |
| Task Type | Specifies the task type. The supported values are. <ul style="list-style-type: none"> • Activate • Deactivate • Configuration update |
| Time Policy | Specifies whether the bulk port modification is scheduled for immediate execution or at a later date and time. Example: IMMEDIATE |
| Creation Time | Specifies the date and time when the task was created. Example: Sep 8, 2023, 9:32:55 PM |
| Device Type | Specifies the device type. Example: PON |

Table 130. Bulk Port Modification Details (continued)

| Field | Description |
|----------------------------|---|
| Execution Time | Specifies the date and time when the task was executed. Example: Sep 8, 2023, 9:43:24 PM |
| Device Details List | |
| Device Name | Specifies the device name. Example: SFPON-30 |
| Task execution Status | Specifies the task executed status. Example: COMPLETED. |
| Status | Specifies the status of the device. Example: ACTIVATE-SUCCESSFUL |
| Remarks | Display any remark. |

The following figure shows the bulk port modification, which contains the detailed information about the task.

Figure 50. Bulk Port Modification

The screenshot displays the 'ONT Firmware Task Details' interface. It includes three main sections: 'Basic Information', 'ONT List', and 'OLT List'.

Basic Information:

| | | | |
|---------------|---|--------------------------------------|-----------|
| Task ID | a391c265-3542-11ef-b113-0205ec03104a-75 | Download on OLT Execution Type | Immediate |
| Name | ont-newskip | Download on ONT Execution Type | Immediate |
| Type | ONT FIRMWARE UPGRADE | Enable Auto Commit | Yes |
| Description | | Enable Activate Commit on ONT Reboot | No |
| Status | RUNNING | Activate and Commit on ONT | No |
| Creation Time | Aug 8, 2024, 4:56:57 AM | | |
| Device Type | ONT | | |

ONT List:

| Device Name | ONT Firmware Version | Task Status | Remarks |
|-------------|----------------------|-------------------------|---------|
| ont-74 | 1.0.0.168 | DOWNLOAD-ON-OLT-SUCCESS | |

OLT List:

| Device Name | ONT Firmware Version (Upgrade From) | ONT Firmware Version (Upgrade To) | Task Status | Remarks |
|-------------|-------------------------------------|-----------------------------------|-----------------------------|---------|
| ont-pon-5 | 1.0.0.171 | 1.0.0.168 | DOWNLOAD-ON-ONT-IN-PROGRESS | |

Reboot

The following table describes the OLT reboot task details.

Table 131. Reboot Task Details

| Field | Description |
|-------------------------------|-------------|
| Basic Task Information | |

Table 131. Reboot Task Details (continued)

| Field | Description |
|-------------|--|
| Name | Specifies the name of the reboot. |
| Type | Specifies the reboot type. |
| Status | Specifies the status of the task. Example: COMPLETED |
| Description | Specifies the description of the task. |
| Time Policy | Specifies whether the reboot is scheduled for immediate execution or at a later date and time. Example: IMMEDIATE |
| Created At | Specifies the date and time when the task was created. Example: Aug 19, 2021, 9:32:55 PM |
| Executed At | Specifies the date and time when the update was executed. Example: Aug 19, 2021, 9:33:24 PM |

PON Port Migration

The following table describes the PON port migration task details.

Table 132. PON Port Migration Task Details

| Field | Description |
|-------------------------------|--|
| Basic Task Information | |
| Name | Specifies the name of the PON port migration. |
| Type | Specifies the movement type. |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. Example: COMPLETED |
| Time Policy | Specifies whether the PON port migration is scheduled for immediate execution or at a later date and time. Example: IMMEDIATE |
| Creation Time | Specifies the date and time when the task was created. Example: Aug 19, 2021, 9:32:55 PM |
| Source OLT | Specifies the source OLT. |

Table 132. PON Port Migration Task Details (continued)

| Field | Description |
|----------------------------|--|
| Source Port | Specifies the source port of the OLT. |
| Destination OLT | Specifies the destination OLT.  Note: PON port migration on different OLT is not supported. |
| Destination Port | Specifies the destination PON port of the OLT. These ports are in deactivated and free state. |
| Movement Type | Specifies the movement type. Example: Move on same ME |
| Execution Time | Specifies the date and time when the update was executed. Example: Aug 19, 2021, 9:33:24 PM |
| Device Details List | |
| Service Name | Specifies the service name. Example: ser-rsys |
| Subscriber Name | Specifies the subscriber name. Example: sub-rsys |
| Device Name | Specifies the device name. Example: RDSYD9F27888 |
| Movement Status | Specifies the movement status. Example: SUCCESS |
| Device Status | Specifies the device status. Example: SERVICE-MOVEMENT-SUCCESSFUL |
| Step Details | Specifies the status of steps involved in the PON port migration. 1. ONT-ACTIVATION 2. ONT-UPDATE-WITH-NEW-PORT 3. ONT-DEACTIVATION 4. SERVICE-UPDATE-WITH-NEW-PORT |
| Remarks | Displays any remark. |

The following figure shows the PON port migration, which contains the detailed information about the task.

Figure 51. PON Port Migration

Task Details

Basic Task Information

| | | | |
|---------------|---------------------------|------------------|---------------------------|
| Name | PPM | Source OLT | OLT-1 |
| Type | PON Port Migration | Source Port | SFPON-10 |
| Description | | Destination OLT | |
| Status | CREATED | Destination Port | SFPON-1 |
| Time Policy | TIMING | Movement Type | MOVE ON SAME ME |
| Creation Time | Mar 18, 2024, 12:48:28 PM | Execution Time | Mar 19, 2024, 12:00:00 AM |

Device Details List

| Service Name | Subscriber Name | Device Name | Movement Status | Device Status | Steps Details | Remarks |
|----------------|-------------------|-------------|-----------------|---------------|---------------|---------|
| service-config | subscriber-config | ont-1 | SCHEDULED | | N/A | |

Showing 1 to 1 of 1 entries

Banner Update

The following table describes the banner update task details.

Table 133. Banner Update Task Details

| Field | Description |
|-------------------------------|--|
| Basic Task Information | |
| Name | Specifies the name of the task. |
| Type | Specifies the type of the task. Example: BANNER_UPDATE |
| Description | Specifies the description of the task. |
| Status | Specifies the status of the task. |
| Creation Time | Specifies the date and time when the task was created. Example: Dec 29, 2022, 10:46:24 PM |
| OLT List | |
| Device Name | Specifies the device name. Example: olt-34 |
| Status | Specifies the status of the banner update. Example: SUCCESS |
| Remarks | Displays any remark. |

Table 133. Banner Update Task Details (continued)

| Field | Description |
|---------------|---|
| Creation Time | Specifies the date and time when the task was created. Example: Aug 14, 2023, 9:32:55 PM |

The following figure shows the banner update, which contains the detailed information about the task.

Figure 52. Banner Update

The screenshot shows a web-based monitoring interface for a 'Banner Update' task. The top section, 'Basic Information', displays the following details:

| | |
|---------------|---------------------------|
| Name | Banner-update |
| Type | BANNER UPDATE |
| Description | |
| Status | COMPLETED |
| Creation Time | Aug 14, 2023, 11:41:44 AM |

The bottom section, 'OLT List', shows a table with one entry:

| Device Name | Status | Remarks | Creation Time |
|-------------|---------|---------|---------------------------|
| olt-34 | SUCCESS | | Aug 14, 2023, 11:42:08 AM |

At the bottom of the table, it says 'Showing 1 to 1 of 1 entries'.

Monitoring Utilities

You can perform the following tasks from the utilities page.

- [Ping \(on page 281\)](#)
- [TraceRoute \(on page 281\)](#)

Ping

You can ping controller to check whether it is reachable from RMS. If the ping is successful, it indicates the controller is reachable from RMS.

Perform the following steps to ping from the RMS.

1. Select **Monitor > Utilities**.

The Utilities page appears.

2. Click the **Ping** tab.
3. Complete the configuration according to the guidelines provided in the following table.

Table 134. Ping

| Field | Description |
|---------------------------|--|
| IP Address | Specifies the controller IP address in IPv4 or IPv6 format. |
| Overall Timeout (Seconds) | Specifies the duration after which ping execution command stops. The supported value ranges from 4 to 25. The default value is 4. |

4. Click **Execute**.

A Result page appears indicating the ping details.

TraceRoute

Traceroute is a tool to trace the path of an IP packet as it traverses routers between a source and a destination.

Perform the following steps to traceroute from the RMS.

1. Select **Monitor > Utilities**.

The Utilities page appears.

2. Click the **TraceRoute** tab.

3. Complete the configuration according to the guidelines provided in the following table.

Table 135. TraceRoute

| Field | Description |
|-----------------------------------|---|
| IP Address | Specifies the controller IP address in IPv4 or IPv6 format. |
| Maximum Hops | <p>Specifies the maximum number of hops after which the traceroute command stops. The supported value ranges from 3 to 30. The default value is 10.</p> <p>The overall timeout of a traceroute command can be defined as Maximum Hops * Timeout per try per hop * Number of tries per hop.</p> <p>For example, If the maximum hop is 5, the timeout per try per hop is 10 seconds, and a number of tries per hop is 3. The overall timeout can be calculated as $5*10*3$.</p> |
| Timeout per try per hop (seconds) | <p>Specifies the timeout per try for each hop. The overall timeout for each hop can be defined as Timeout per try per hop * Number of tries per hop.</p> <p>The supported value ranges from 1 to 10. The default value is 3.</p> |
| Number of tries per hop | <p>Specifies the number of tries attempted for each hop in case of failure. The supported value ranges from 1 to 3. The default value is 3.</p> |
| Enable domain name resolution | <p>Select this checkbox to view DNS name of the hop IP. By default, this field is not selected.</p> <p> Note: The command execution time can be reduced if you disable this field.</p> |
| Protocol | <p>Specifies the supported protocol for tracing the path to the destination IP. The supported values are.</p> <ul style="list-style-type: none"> ◦ UDP ◦ ICMP <p>The default value is UDP.</p> |

4. Click **Execute**.

A Result page appears indicating the traceroute details.

Topology

To access this page, click **Topology** from the top right corner of the page.

Topology management enables you to view the physical and logical topology of the OLT.

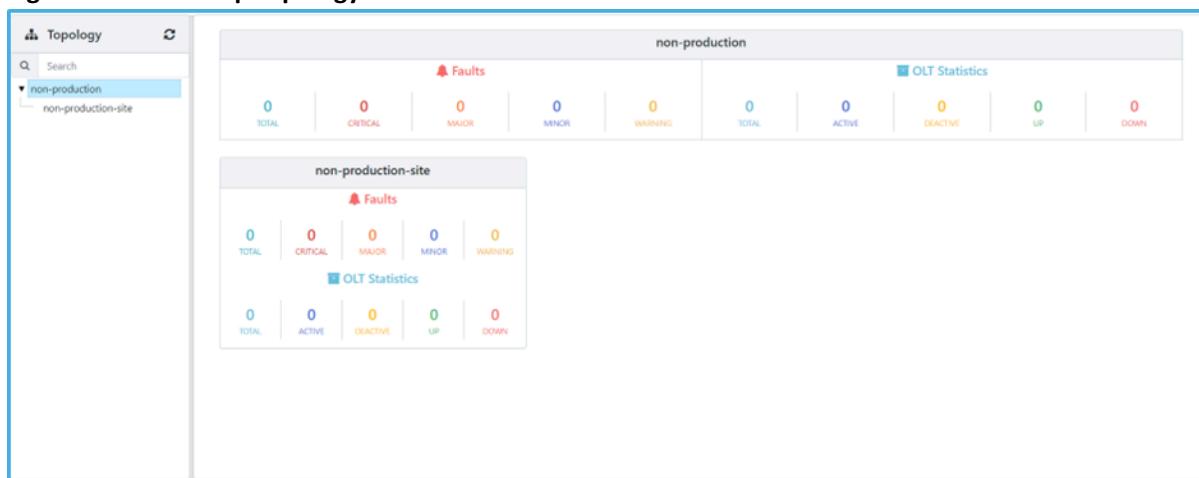
After the successful creation of the site group, sites, and managed elements (OLT and ONT), the physical and logical topology of the OLT are created on this page.

You can view the fault summary details and topology statistics of the site group and the sites belonging to the site group. This information helps you monitor the entire network in real-time.

The left pane of the page shows the hierarchy of site group type, sites, and devices underneath. You can expand and collapse the hierachal tree by clicking the arrow button to view the site group, the number of sites associated with it, and the number of devices associated with it.

The following figure shows the site group hierarchy, where the **site grp-1** is the site group, and the **PTP** is the site, and the **olt-2** is the OLT name and the list of PON ports connected to the OLT.

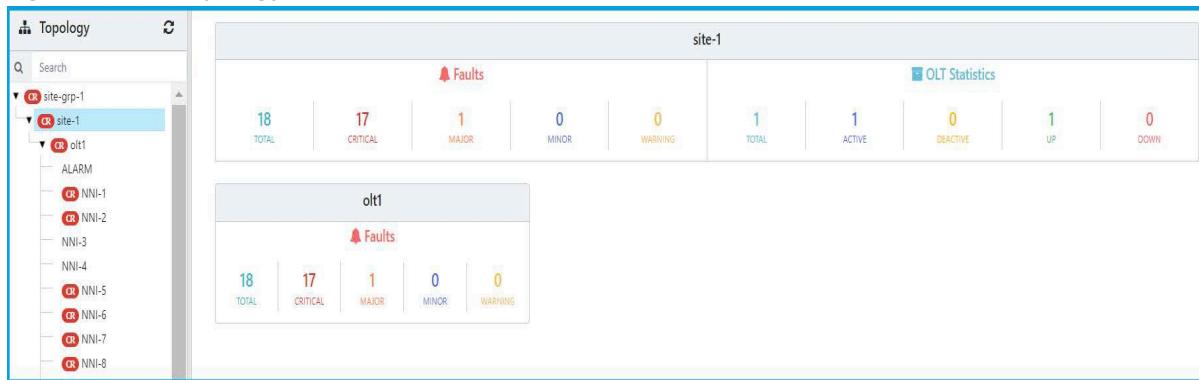
Figure 53. Site Group Topology



- Click on the site group name (for example, site grp-1) to view the following information for the site group, site, and OLT.
 - Fault summary of all sites in the site group.
 - Total number of faults including all severity level (CRITICAL, MAJOR, MINOR, and WARNING)
 - Total number of faults by severity level (CRITICAL, MAJOR, MINOR, and WARNING)
 - OLT statistics of all the OLTs in the site group.
 - Total number of OLTs from the site group
 - Total number of OLTs in active state
 - Total number of OLTs in deactive state
 - Total number of OLTs that are up
 - Total number of OLTs that are down

- Fault summary of the particular site in the site group.
 - Total number of faults including all severity level (CRITICAL, MAJOR, MINOR, and WARNING)
 - Total number of faults by severity level (CRITICAL, MAJOR, MINOR, and WARNING)
- OLT statistics of the particular OLT in the site.
 - Total number of OLTs from the particular site
 - Total number of OLTs in active state
 - Total number of OLTs in deactive
 - Total number of OLTs that are up
 - Total number of OLTs that are down

Figure 54. Site Topology



- Click on the site name (for example, site-1) to view the following information of the site.
 - Fault summary of the site.
 - Total number of faults including all severity level (CRITICAL, MAJOR, MINOR, and WARNING)
 - Total number of faults by severity level (CRITICAL, MAJOR, MINOR, and WARNING)
 - OLT statistics of the site.
 - Total number of OLTs from the particular site
 - Total number of OLTs in active state
 - Total number of OLTs in deactive state
 - Total number of OLTs that are up
 - Total number of OLTs that are down
- Click on the OLT name (for example, olt1) to view the following information.
 - Physical and logical topology of the OLT and ONT
 - Monitor OLT information
- Click on the port name (for example, olt1) to view the following information.
 - Physical and logical topology of the port
 - Monitor port information



Note: For the topology view to render successfully, ensure that the site group hierarchy is created, sites are created under the site groups, and the OLT is associated with the site group. For more information, refer to the following sections.

- [Creating Site Group Type Configuration \(on page 292\)](#)
- [Creating Site Group Configuration \(on page 290\)](#)
- [Creating Site Configuration \(on page 289\)](#)
- [Creating OLT Configuration \(on page 318\)](#)

Physical Topology of the OLT

This section explains the physical topology of the OLT.

This topology shows the OLT ports connected to the splitter and splitter out ports are connected to the ONT. The OLT devices, splitters, ONTs, and the PON and NNI ports connected to the OLT are displayed in a certain color.

You can create and view the physical topology of the OLT using the **Physical Topology** option from the OLT actions. A user needs to specify the splitter in port connected with the OLT PON port. Similarly, a physical link can be created from the splitter ports with the ONTs.

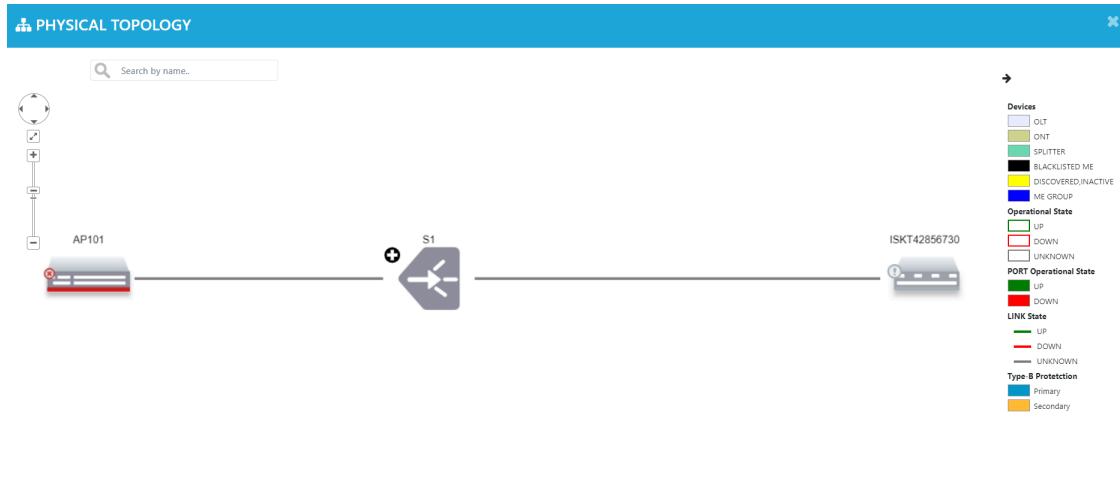


Note: RMS supports creation of physical link only in the forward direction. For example, you can only create a physical link from the OLT PON port to splitter port and not opposite.

You can perform the following tasks from the topology page.

- Click the zoom slider to zoom in and zoom out to the topology.
- Reposition the topology view (left, right, up, or down) by clicking the respective arrow button.
- You can search for various elements of your network infrastructure.

The following figure shows the physical topology of the OLT.

Figure 55. Physical Topology—OLT

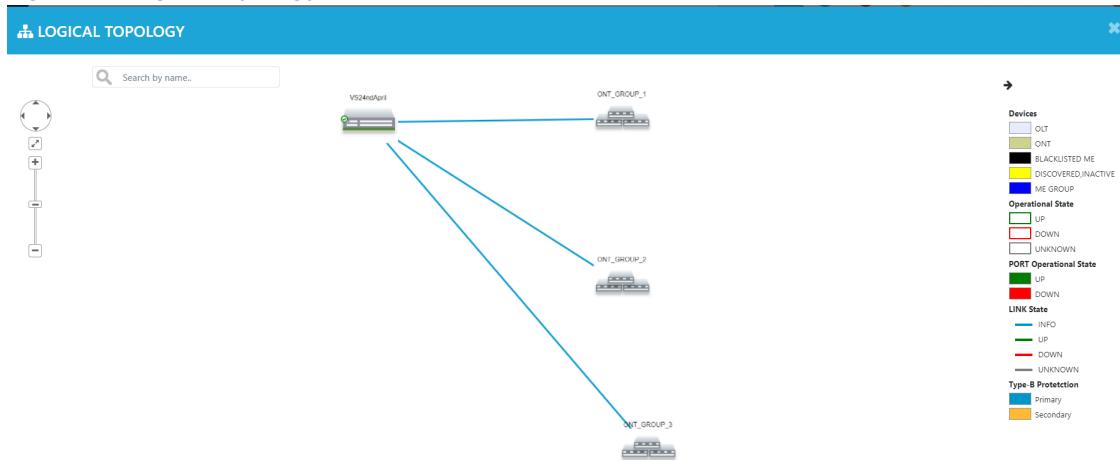
Logical Topology of the OLT

This section explains the logical topology of the OLT.

You can perform the following tasks from the topology page.

- Click the zoom slider to zoom in and zoom out to the topology.
- Reposition the topology view (left, right, up, or down) by clicking the respective arrow button.
- You can search for various elements of your network infrastructure.

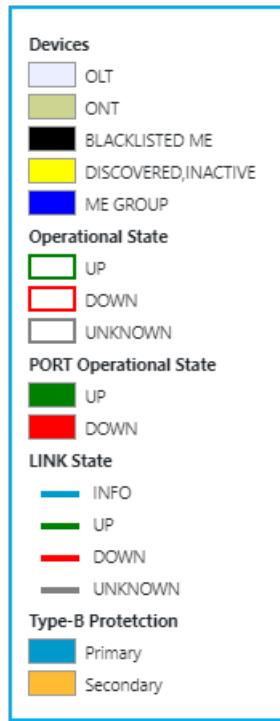
This topology shows the logical connection between the OLT and ONTs.

Figure 56. Logical Topology—OLT

Legends in the OLT Topology

The OLT topology provides a legend, a visual reference that helps you understand the resources operational state.

Figure 57. OLT and ONT Topology—Legends



The following table describes the OLT and ONT topology legends.

Table 136. OLT and ONT Topology Legends

| Item | Description |
|------------------------|---|
| Devices | Displays the following devices. <ul style="list-style-type: none">OLTONTBLACKLISTED MEDISCOVERED, INACTIVE. Indicates the state of the blacklisted ME.ME GROUP |
| Operational State | Specifies the operational state of the OLT. <ul style="list-style-type: none">UP. Green color indicates that the OLT is up.DOWN. Red color indicates that the OLT is down.UNKNOWN. Grey color indicates that the OLT state is unknown. |
| PORT Operational State | Specifies the operational state of the port. |

Table 136. OLT and ONT Topology Legends (continued)

| Item | Description |
|-------------------|---|
| | <ul style="list-style-type: none">• UP. Green color indicates that the port is up.• DOWN. Red color indicates that the port is down. |
| LINK State | Specifies the physical or logical link state of the OLT. <ul style="list-style-type: none">• INFO. Blue color indicates that the link is used for information purpose.• UP. Green color indicates that the link is up.• DOWN. Red color indicates that the link is down.• UNKNOWN. Grey color indicates that the link status is unknown. |
| Type-B Protection | Specifies the type-b protection state. <ul style="list-style-type: none">• Primary. Blue color indicates the primary port protection state.• Secondary. Yellow color indicates the secondary port protection state. |

Configuration

You can configure and manage controller, site group, site, managed elements (OLT, ONT, BNG, Splitter, CPE, card, rack, shelf, SFP, and cable), subscriber, service, and Managed Element (ME) group.

Site

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Site** from the left-hand side of the menu.

Sites are the branch offices or remote locations where the OLTs are located, and the customers access the network services provided by CBAC. You can create one or more sites with the same name and assign site(s) to the site group.



Note: You can create one or more sites with the same name for different OLT site location in different or same cities.

Creating Site Configuration

Perform the following steps to create a site group configuration.

1. Select **Configuration > Site**.
The Site List page appears.
2. Click **Create** to create a site.
The Site Configuration page appears.
3. Complete the configuration according to the guidelines provided in the following table.

Table 137. Site Configuration

| Field | Description |
|------------|---|
| Name | <p>Enter a name for the site. You can use any number of alphanumeric characters.</p> <p> Note: You can create multiple sites with the same name.</p> <p>The following special characters are supported.</p> <ul style="list-style-type: none">• Underscore (_)• Hyphen (-)• Space |
| Short Name | Enter a short name for the site. |

| Field | Description |
|-------------|--|
| Address | Enter the address of the site. |
| Display Id | Enter the display ID of the site. |
| Parent Site | Enter the site group. |
| Latitude | Enter the latitude of the site. The value ranges from -90 to +90. |
| Longitude | Enter the longitude of the site. The value ranges from -180 to +180. |

4. Click **Create**.

A new site is created on the Site List page.

To edit, clone, and delete the Site configuration, see [Common Operations \(on page 27\)](#).

Site Group

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Site Group** from the left-hand side of the menu.

Site groups enable you to group sites logically, thereby easing site management. If there are multiple sites, you can create site groups to ensure consistent settings. For example, you could create a site group for each region (for example, East, West, North, and South) or each purpose. You can add one or more site groups with the same name to the site group type.



Note:

- You can create one or more site groups with the same name for different cities.
- Before you create a site group, you must create a site group type. For creating site group type, refer to the [Creating Site Group Type Configuration \(on page 292\)](#).

Creating Site Group Configuration

Perform the following steps to create a site group configuration.

1. Select **Configuration > Site Group**.
The Site Group List page appears.
2. Click **Create** to create a site group.
The Site Group Configuration page appears.
3. Complete the configuration according to the guidelines provided in the following table.

Table 138. Site Group Configuration

| Field | Description |
|------------|---|
| Name | <p>Enter a name for the site group. You can use any number of alphanumeric characters.</p> <p> Note: You can create multiple site groups with the same name.</p> <p>The following special characters are supported.</p> <ul style="list-style-type: none">Underscore (_)Hyphen (-)Space |
| Short Name | Enter the short name for the site group. |
| Display Id | Enter the display ID for the site group. |
| Site Type | Select the site type from the list. If the site group does not exist, click the plus icon (+) to create the site type. See Creating Site Group Type Configuration (on page 292) . |

4. Click **Create**.

A new site group is created on the Site Group List page.

To edit, clone, and delete the Site Group configuration, see [Common Operations \(on page 27\)](#).

Viewing and Creating Site Sub Groups

You can also create one or more sub site groups under the parent site group.

Perform the following steps to create a site sub group.

1. Select **Configuration > Site Group**.

The Site Group List page appears.

2. Click the view/create site sub groups icon under the **Action** column.

The Site Group page appears and displays the parent site group name.

3. Click the plus icon (+) to add a sub group.

The Site Group Configuration page appears.

4. Complete the configuration according to the guidelines provided in [Table 138: Site Group Configuration \(on page 291\)](#).

A sub site group is created under the parent site group.

Site Group Type

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Site Group Type** from the left-hand side of the menu.

A user can add one or more site groups of a particular region to the site group type.

Field Descriptions

The following table describes the fields on the Site Group Type List page.

Table 139. Site Group Type List

| Field | Description |
|-----------------|---|
| Site Group Type | <p>Specifies the name of the site group type. The possible values of the site group types are.</p> <ul style="list-style-type: none">• Country• Region• State• City <p>You can create a site group as India under the site group type Country.</p> |
| Action | <p>Specifies the action that you can perform on the site group type. The supported actions are.</p> <ul style="list-style-type: none">• Edit• Clone• Delete |
| Creation Time | Specifies the date and time when the site group type was created. |

Creating Site Group Type Configuration

Perform the following steps to create a site group type configuration.

1. Select **Configuration > Site Group Type > Create**.
The Site Type Group Configuration page appears.
2. Complete the application configuration according to the guidelines provided in the following table.

Table 140. Site Group Type Configuration

| Field | Description |
|-------|--|
| Name | Enter a unique name for the site group type. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space |

3. Click **Create**.

A new site group is created on the Site Group Type page.



Note: Editing site group type is not allowed after mapping to a site group.

To edit, clone, and delete the Site Group Type configuration, see [Common Operations \(on page 27\)](#).

ME Group

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > ME Group** from the left-hand side of the menu.

The ME group is the parent element group to which you can add one or more managed elements and perform a particular task on all the managed elements of this group simultaneously.

Creating ME Group Configuration

Perform the following steps to create ME group configuration.

1. Select **Configuration > ME Group**.

The ME Group page appears.

2. Click **Create**.

The ME Group Configuration page appears.

3. Complete the configuration according to the guidelines provided in the following table.

Table 141. ME Group Configuration

| Field | Description |
|-------|---|
| Name | Enter a unique name for the ME group. You can use any number of alphanumeric characters. Only the following special characters are supported. |

| Field | Description |
|-------|---|
| | <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space |

4. Click **Create**.

A newly created ME group appears on the **ME Group List** page.

To edit, clone, and delete the ME Group configuration, see [Common Operations \(on page 27\)](#).

ME Group Member

To access this page, click on the **ME Member** icon from the Action column.

The ME group members are parent element group member on which a particular tasks to be performed within the parent ME Group simultaneously.

Creating ME Group Member

After successful creation of the ME group, you can create one or more managed elements (OLT or ONT) to the group.

1. Select **Configuration > ME Group**.

The ME Group page appears.

2. Click on the **ME Member** icon from the Action column.

The ME Group Member page appears.

3. Click **Add Member**.

4. Complete the configuration according to the guidelines provided in the following table.

Table 142. ME Group Member Configuration

| Field | Description |
|-------|---|
| Type | Select the ME type for which you want to add members. The supported values are. <ul style="list-style-type: none">◦ OLT◦ ONT |
| Me | Select one or more managed elements from the list. |

5. Click **Create**.

A newly created ME group member appears on the **ME Group Member List** page.

Controller

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Controller** from the left-hand side of the menu.

The controller represents the southbound entity on which RMS communicates to provide all the functionalities. Each CBAC instance is configured as a controller with the adaptor type as SDPON. You must configure the IP address for Kafka and the REST server.

You can also configure the security settings for CBAC user accounts. The controller acts as the REST server for the CRUD (Create, Read, Update, and Delete) operations initiated by RMS acting as the client. CBAC immediately responds to all REST requests with a job ID, which is used to track the request. CBAC reports RMS and KPIs to RMS for its consumption, which is realized through notifications on the Kafka message bus.

Configure infrastructure monitoring, which enables monitoring of the CBAC microservices (through the Grafana dashboard) and alerting (through the Prometheus alert manager) on the alert channels such as E-mail, Microsoft Teams, and Telegram based on the alert rules.

Operators can monitor the status and resource utilization metrics of the CBAC microservices deployment.

- The dashboard enables monitoring of the following metrics for each microservice.
 - Status
 - Node
 - Age
 - Number of restarts
 - CPU utilization
 - Memory utilization
- Alerting is supported through the following alert channels.
 - E-mail notifications
 - Microsoft Teams
 - Telegram

An operator can configure the alert rules, alert channels, and account subscriptions for receiving the alert notifications. Based on the alerts generated, the operator can take appropriate actions.



Note: If the user wants to create multiple controllers, they need not create multiple management domains. RMS does not verify and validate the management domain anywhere. Hence, creating a single management domain is sufficient for creating multiple controllers.

Tasks

You can perform the following tasks on this page.

- Create a controller configuration. See [Creating Controller Configuration \(on page 297\)](#).
- Activate the controller. See [Activating the Controller \(on page 305\)](#).
- Deactivate the controller. See [Deactivating the Controller \(on page 306\)](#).
- Backup and restore of a controller. See [Controller Backup and Restore \(on page 307\)](#).
- Replace the password for the CBAC user accounts. See [Replacing the Password \(on page 306\)](#).
- Monitor the controller details. See [Monitoring Controller \(on page 184\)](#).

Field Descriptions

The following table describes the fields on the controller list page.

Table 143. Controller List

| Field | Description |
|--------------------------|--|
| Name | Specifies the name of the controller. |
| Admin State | Specifies the admin state of the controller. The supported states are. <ul style="list-style-type: none">• Active• Deactive |
| Mode | Specifies the type of controller. The supported values are. <ul style="list-style-type: none">• DISTRIBUTED• CENTRALIZED |
| Adaptor | Specifies the name of the adaptor. |
| Management Domain | Specifies the name of the management domain. |
| Kafka Host | Specifies the host address of Kafka. |
| Kafka Port | Specifies the external Kafka port number. |
| Kafka User Name | Specifies the username for the CBAC server. Example: SDPON |
| Kafka Alarm Topic | Specifies the name of the CBAC alarm topic. |
| Kafka Notification Topic | Specifies the name of the CBAC notification topic. |
| Kafka KPI topic | Specifies the name of the CBAC KPI topic. |
| REST Base URL | Specifies the IP address for the CBAC REST server. Example: <a href="https://<IP>:31082/sdpn/v1">https://<IP>:31082/sdpn/v1 |
| REST Super User Name | Specifies the valid REST server super username. Example: SDPON |
| Backup Status | Specifies the controller backup status. The supported values are. |

Table 143. Controller List (continued)

| Field | Description |
|------------------|---|
| | <ul style="list-style-type: none"> • BACKUP-INITIATED • BACKUP-FAILED • BACKUP-SUCCESSFUL |
| Restore Status | <p>Specifies the controller restore status. The supported values are.</p> <ul style="list-style-type: none"> • RESTORE-INITIATED • RESTORE-FAILED • RESTORE-SUCCESSFUL |
| Upgrade Status | <p>Specifies the software upgrade status of the controller. The supported values are.</p> <ul style="list-style-type: none"> • UPGRADE-INITIATED • UPGRADE-FAILED • UPGRADE-SUCCESSFUL <p>If the upgrade task is stuck and terminated automatically, the Upgrade Status is shown as DOWNLOAD-FAILED or UPGRADE-FAILED.</p> |
| Version | Specifies the version of the controller. |
| Creation Time | Specifies the date and time when the controller was created. |
| Action | <p>Specifies the action that you can perform on the site. The supported actions are.</p> <ul style="list-style-type: none"> • Edit • Clone • Delete |
| Infra Monitoring | Specifies the monitoring endpoint IP and port details. |

Creating Controller Configuration

Perform the following steps to create a controller configuration.



Note:

- You must create a management domain before you configure the controller. See [Creating Management Domain \(on page 765\)](#).
- If the user is creating a controller configuration, then the **Management Domain** field is mandatory. If the controller configuration is created through the auto-discovery process, then the **Management Domain** field is not required.

1. Select **Configuration > Controller**.
The Controller List page appears.
2. Click **Create**.
The Controller Configuration page appears.
3. Complete the configuration according to the guidelines provided in the following table.

Table 144. Controller Configuration

| Field | Description |
|--------------------|--|
| Controller | |
| Name | Enter a unique name for the controller. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space |
| Adaptor | Select the adaptor from the list. <ul style="list-style-type: none">◦ SDPON |
| Mode | Select the CBAC controller mode. <ul style="list-style-type: none">◦ CENTRALIZED. This mode enables RMS to connect to all the OLTs that are configured in the system.◦ DISTRIBUTED. This mode enables RMS to connect to only one OLT. |
| Management Domain | Select the management domain from the list. If the management domain does not exist, click the plus icon (+) to create the management domain. See Creating Management Domain (on page 765) . |
| Version | Enter the version for the controller. |
| Auto Activate | Enable this option to activate the controller automatically. |
| Kafka | |
| Host | Enter the Kafka host address of the CBAC controller. Example: 172.27.1.1 |
| Port | Enter the external Kafka port number. Example: 30000 |
| Alarm Topic | Displays the CBAC alarm topic to listen and receive faults. The default topic name is EMSFAULT. |
| Notification Topic | Displays the CBAC notification topic to listen and receive notifications. The default topic name is EMSNOTIFICATION. |

| Field | Description |
|------------------------------------|--|
| KPI Topic | Displays the CBAC KPI topic to listen and receive the KPIs. The default topic name is EMSKPINOTIFICATION. |
| Current KPI Topic | Displays the CBAC KPI topic to listen and receive the live KPIs. The default topic name is EMSLIVEKPI. |
| CLI Topic | Displays the CBAC CLI topic to listen and receive the CLI. The default topic name is EMSCLISYNCNOTIFICATION. |
| SSH Port | Enter the SSH port number. The port number is similar to the CBAC CLI cut through node. Enter the port number as 22 if the OLT IP is IPv4. Enter the port number as 31022 if the OLT IP is IPv6. |
| REST | |
| REST Base URL | Enter a valid IP address for the CBAC REST server. The REST server fetch login details (username and password) from RMS. Example: <a href="https://<IP>:31082/sdpon/v1">https://<IP>:31082/sdpon/v1 |
| Settings | |
| Security Settings | |
| Block Invalid User Count | Enter the number of days to block the invalid user accounts. The default value is 3 days. The minimum value is 3 days. The maximum value is 5 days. |
| Account Lockout Duration (minutes) | Enter the account lockout duration. The default value is 10 minutes. The minimum value is 10 minutes. The maximum value is 30 minutes. |
| Idle Session Time (minutes) | Enter the value for idle session time. The default value is 15 minutes. The minimum value is 15 minutes. The maximum value is 20 minutes. |
| Password Expiry Days | Enter the number of days after which the password expires and must be changed. The default value is 180 days. The minimum value is 180 days. The maximum value is 365 days. |
| Password Expiry Notice Period | Enter the duration to send the password expiry notification emails to the users. |

| Field | Description |
|-----------------------------|---|
| |  Note: Admin users do not get password expiry notification. The default value is 14 days. The minimum value is 7 days. The maximum value is 14 days. |
| Password Minimum Length | Enter the minimum length for the password. The default length is 8 characters. The minimum length is 8 characters. The maximum length is 32 characters. |
| Password History Count | Enter the password history count to restrict the password reuse. The password history is enforced to ensure that users are forced to select unique and new passwords upon password expiry. The default value is 7. The minimum value is 7. The maximum value is 32. |
| Event Log Retention Period | Enter the number of days to retain CBAC security event logs. The default value is 30 days. The minimum value is 7 days. The maximum value is 30 days. |
| Account Expiry (Days) | Enter the account expiry duration (in days) for user accounts. The default value is 180 days. The minimum value is 90 days. The maximum value is 365 days. |
| Inactive Account (Days) | Enter the duration (in days) to deactivate the user accounts if the user has not logged into the RMS application. The default value is 60 days. After 60 days, the user account becomes a dormant state, and the user cannot login to the RMS application. The minimum value is 60 days. The maximum value is 90 days. |
| Maximum Concurrent Sessions | Specifies the maximum number of sessions allowed per user at a given time. The default value is 25. The value ranges from 1 to 512. |
| |  Note: The controller must be deactivated and activated if the maximum concurrent session changes. The maximum concurrent session minus the current sessions is the number of sessions allowed. |

| Field | Description |
|---------------------------------------|---|
| | Example: If the maximum concurrent session is changed to 10, and the admin opens two sessions to deactivate the controller, then the maximum concurrent session allowed is eight because even after deactivating the controller, CBAC counts the previous two sessions. |
| Concurrent Access from Multiple IPs | <p>Provides support for multiple concurrent sessions for a user from different IPs. The supported values are:</p> <ul style="list-style-type: none"> ◦ True ◦ False <p>The default value is True.</p> |
| Settings | |
| SDPON Settings | |
| Log server | <p>Specifies the IP address/FQDN of the log server for all CBAC components including the OLT. Initially, the log server IP address is configured while deploying the CBAC setup. From the CBAC CLI, the IP address can be modified. However, the following values are not supported:</p> <ul style="list-style-type: none"> ◦ Loopback IP (127.0.0.1) ◦ 0.0.0.0 ◦ localhost |
| Log level | <p>Specifies the log level of the system log error message. The values are:</p> <ul style="list-style-type: none"> ◦ INFO. Provides high level understanding of the system, which is useful to understand what is happening on the system. ◦ DEBUG. Detailed debug information for the programmers to debug the system issues. ◦ WARNING. Warning, if the correct behavior cannot be ensured. This type of behavior is not generally expected, but you cannot determine at that level if it is an error or warning. ◦ ERROR. Error with impact on correct functionality. For example, range errors, key errors, wrong parameters, and so on. <p>The default value is ERROR.</p> |
| Alarm Retention Policy (In Days) | <p>Enter the number of days to retain alarms by CBAC. The alarms are purged by CBAC after the specified number of days.</p> <p>The default value is 7 days.</p> |
| Audit Logs Retention Policy (In Days) | <p>Enter the number of days to retain audit logs by CBAC. The audits logs are purged by CBAC after the specified number of days.</p> <p>The default value is 2 days.</p> |

| Field | Description |
|--------------------------------------|---|
| KPI Retention Policy (In Days) | Enter the number of days to retain the KPIs by CBAC. The KPIs are purged by CBAC after the specified number of days. The default value is 2 days. |
| KPI Reporting Intervals (In Minutes) | Specifies the reporting interval of KPIs from CBAC to RMS. You can configure multiple intervals. A maximum of four KPI intervals are supported. The supported values are. <ul style="list-style-type: none"> ◦ 15 Minutes ◦ 60 Minutes (One hour) ◦ 1440 Minutes (One day) The minimum interval is 15 minutes, and the maximum interval is 1440 minutes. |
| SFTP Username | Enter a valid username for the SFTP server. |
| SFTP Password | Enter a valid password for the SFTP server. |
| Artifact Repo IP | Specifies the IPv4/IPv6 address of the repository server. Artifact repository server is used for storing and downloading the ONL/ONT firmware image to the ME. |
| Artifact SFTP Username | Enter a valid username for the artifact SFTP server. |
| Artifact SFTP Password | Enter a valid password for the artifact SFTP server. |
| Inter SDPON Endpoint (IP) | Enter the inter CBAC IP address. Each CBAC instance has an IP address and port number. When the OLT and CBAC-D are co-located, the IP address is used for internal communication between one CBAC to another. |
| Inter SDPON Endpoint (Port) | Enter the port number of the CBAC controller, which is used for internal communication. This is applicable only for type-B dual homing. |
| IGMP | |
| Max Response | Enter the maximum response time (in seconds), which is used to calculate the max response code inserted into the periodic IGMP queries. The value ranges from 5 to 12 seconds. The minimum value is 5 seconds, and the maximum value is 12 seconds. The default value is 10 seconds. |
| Unsolicited timeout | Enter the time interval (in seconds) between the IGMP proxy application membership report messages to receive multicast service for a group or channel. The minimum value must be > = "Max Response" value. |

| Field | Description |
|---------------------|--|
| | The maximum value is 255 seconds. The default value is 12 seconds. |
| Keep Alive Interval | Enter the time interval (in seconds) between the IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent by the IGMP proxy application. The minimum value must be > = “Max Response” value. The maximum value is 255 seconds. The default value is 120 seconds. |
| Keep Alive Count | Enter the number of IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent before the IGMP application assumes that there are no local members. The value ranges from 1 to 255. The default value is 3. |
| Last Query Interval | Enter the time interval (in seconds) between the IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent by the IGMP proxy before it assumes that there are no local members for a group. The minimum value must be > = “Max Response” value. The maximum value is 255 seconds. The default value is 12 seconds. |
| Last Query Count | Enter the number of IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent before the IGMP application assumes that there are no local members. The value ranges from 1 to 255. The default value is 2. |
| COS | Enter the priority bit value in the IGMP packet. The value ranges from 0 to 7. The default value is 7. |
| Version | Enter the IGMP report version (IGMPv2/IGMPv3) to be sent to the multicast server or Broadband Network Gateway (BNG). The default value is v3. |
| Source IP | Enter the IGMP source IP address. Example: 192.168.56.1 The default source IP address is 1.2.3.4 if the source IP address is not mentioned. |
| MLD Version Server | Specifies the MLD version supported by the network. The supported values are. <ul style="list-style-type: none">◦ v1◦ v2 The default value is v2. |

| Field | Description |
|--------------------------|--|
| MLD Source IP | Specifies the MLD source IP. It only accepts IPv6 link-local address. Example: FE80::0102:0304. |
| Fast Leave | Enable this option if the IGMP application needs to send IGMP Group-Specific Queries^b to the individual member in the group when the leave message is received. This option is enabled by default. |
| Periodic Query | Enable this option if the IGMP application needs to perform periodic queries. <ul style="list-style-type: none"> ◦ Enable. Enables the IGMP application to perform periodic queries. ◦ Disable. May cause the ONU to delete the IGMP routing table. This option is enabled by default. |
| RA Uplink | Enable this option if the IGMP application needs to add a route alert (IgmpReport, Igmpjoin, and Igmpleave) packet into the uplink packets. This option is enabled by default. |
| RA Downlink | Enable this option if the IGMP application needs to add a route alert (IgmpQuery) packet into the downlink packets. This option is enabled by default. |
| Infra Monitoring | |
| Monitoring Endpoint IP | Enter the monitoring REST server IP address, which is running on the RMS server or an external server. Example: <code>http://<host-ip>:<monitoring-rest-servernodeport></code> Where, Host IP is the system IP where monitoring PODs (Grafana, Prometheus, and monitoring REST server) are running. These PODs can either run with RMS PODs or as a separate entity. |
| Monitoring Endpoint Port | Specifies the port number of the monitored entity. Example: 30014 |
| Grafana IP | Enter the IP address of Grafana. Example: 10.157.251.207 |
| Grafana Port | Enter the port number of Grafana. Example: 30013 |
| Users | |
| Username | Specifies the username of the user who has initiated the task. |
| Type | Specifies the type of the user. |
| Account State | Specifies the state of the user account. |

| Field | Description |
|-----------------------|---|
| Creation time | Specifies the date and time when the user was created. |
| Authentication | |
| TACACS Profile | Select the TACACS profile from the list of global TACACS profile. |

IGMP General Membership Queries^a. The IGMP query is sent to all system groups (224.0.0.1). IGMP general queries are destined to the address 224.0.0.1 (all systems on a subnet).

IGMP Group Specific Queries^b. The IGMP query is sent to individual members subscribed to a specific multicast group. IGMP group-specific queries are destined to the group IP address for which the device is querying.

4. Click **Create**.

A new controller is created on the Controller List page.



Note:

- Only a TACACS user with an **admin** role can activate/deactivate a controller/CBAC. A TACACS user has the following permissions to activate/deactivate a controller/CBAC.
 - Role.** Create, Modify, and Get
 - User.** Create, Modify, Get, and Activate
 - Controller.** Create, Modify, Get, and Activate
- You cannot modify or delete a controller without deactivating it.

To edit, clone, and delete the Controller configuration, see [Common Operations \(on page 27\)](#).

Activating the Controller

You can activate the controller after successful creation of the controller.



Note:

- The OLT and Controller IP must be same.
- The IP addresses must not be duplicated across the multiple nodes.

Perform the following steps to activate the controller.

1. Select **Configuration > Controller**.

The Controller List page appears.

2. Click on the three dots (⋮) corresponding to the controller on which you want to activate and click the **Activate** option.

A confirmation message appears indicating the status of the activate operation and the admin state of the controller changes to ACTIVATION IN PROGRESS and then changes to ACTIVE.

**Note:**

- RMS starts listening the faults, events, and KPI notifications on the Kafka message bus only when the controller is active.
- If duplicate IP addresses are detected, deactivate the Controller, resolve the duplicate IP, and reactivate the Controller.

Deactivating the Controller

Perform the following steps to deactivate the controller.

1. Select **Configuration > Controller**.

The Controller List page appears.

2. Click on the three dots (⋮) corresponding to the controller on which you want to deactivate and click the **Deactivate** option.

A confirmation message appears indicating the status of the deactivate operation and the admin state of the controller changes to DEACTIVATION IN PROGRESS and then changes to DEACTIVE.

Replacing the Password

You can replace the password for the CBAC user account (admin, viewer, operator, and custom/third party user) with the RMS password for the same user account. This feature enables the user to have a common password to access CBAC and RMS.

Perform the following steps to replace the password.

1. Select **Configuration > Controller**.

The Controller List page appears.

2. Select **Configuration > Controller**.

The Controller List page appears.

3. Click on the three dots (⋮) corresponding to the controller on which you want to replace the password and click the **Replace** option.

A confirmation message appears indicating the status of the replace operation.

**Note:**

- You can replace the password of the controller only when the controller is in ACTIVATE state. After replacing the password, you must deactivate and activate the controller to configure the IGMP, CBAC settings, and CBAC security settings.
- The password replace is required when the password is updated from RMS to CBAC and the CBAC is re-deployed due to some reasons. If RMS has an updated password and CBAC has a default password, to synchronize the RMS and CBAC password, the user needs to perform replace operation.

Controller Backup and Restore

This section covers the backup and restore procedures of the controller.



Note:

- Northbound operations cannot be performed when the backup or restore operation is in progress.
- The backup and restore of CBAC-D is supported across releases from x to $x+1$, where $x+1$ is the current CBAC-D version. The previous backed-up CBAC configuration (x) can be restored on the current CBAC release ($x+1$). After restoration, you must run a reconciliation between RMS and CBAC. The assumption is that RMS is already on the current release ($x+1$).

Backup Controller Configuration

RMS provides a way to backup and restore the entire controller configuration data. RMS enables this feature without affecting the services provided to any of the subscribers. The configuration data of the controller includes the following.

- System configurations of all OLTs that are managed by the CBAC instance.
- PON port configurations (per OLT) that are managed by the CBAC instance.
- Inventory configurations of Field Replaceable Units (FRUs) that are managed by the OLTs.
- All provisioned ONT configurations are managed by the CBAC instance.
- All subscriber and service configurations are managed by CBAC.
- All profiles (including Alarm and KPIs) and CBAC specific configurations.

RMS sends a request to CBAC to back up the entire controller configuration.

- If the request is accepted, CBAC sends the “202 Accepted” response to RMS and backs up the configuration data.
- If the request is invalid, CBAC responds with the “400 Bad Request” error message to RMS.

RMS raises an alarm upon failure to take a backup of the running configuration or contexts of the entire CBAC database. RMS also supports scheduled backup for the entire controller configuration. RMS raises an event when backup is taken and stored successfully.

When you backup and restore a configuration file, an audit log entry is automatically generated. From the audit log entry, you can identify the user who initiated the backup operation, the IP address from which this task was initiated, and so on.

RMS also supports scheduled backup configuration for the controller. If you want to schedule the controller backup to occur only once, daily, weekly, or monthly, you must create a task. See [Creating Task for Controller or OLT Backup \(on page 661\)](#).

Perform the following steps to back up the controller configuration data.

1. Select **Configuration > Controller**.
The Controller List page appears.
2. Click on the three dots (⋮) corresponding to the controller on which you want to take a backup of the configuration and click the **Backup** option.
The Backup Path page appears.
3. Select the **File Store** from the list on which the backed-up controller configuration needs to be stored or click the plus icon (+) icon to create a file store configuration. See [Creating File Store Configuration \(on page 618\)](#).



Note: The OLT and the SFTP server must have the same IP protocol for OLT and CBAC related operations such as backup and restore.

4. Click **Submit**.

A confirmation message appears indicating the status of the backup operation.

The controller configuration data is backed-up in the SFTP server.



Note: The sub sequence controller backup schedule is not allowed within 15 minutes. The immediate backup does not execute within 15 minutes if any backup is already scheduled during that time.

A maximum of two scheduled controller backups are allowed.

Restore Controller Configuration

CBAC ensures that all services provided during the backup of the CBAC database are restored with the same state without RMS intervention.

You can restore the following controller configuration data.

- System configurations of all OLTs that are managed by the CBAC instance.
- PON port configurations (per OLT) that are managed by the CBAC instance.
- Inventory configurations of Field Replaceable Units (FRUs) that are managed by the OLTs.
- All provisioned ONT configurations are managed by the CBAC instance.
- All subscriber and service configurations are managed by CBAC.
- All profiles (including Alarm and KPIs) and CBAC specific configurations.

Perform the following steps to restore the controller configuration data.

1. Select **Configuration > Controller**.
The Controller List page appears.
2. Click on the three dots (⋮) corresponding to the controller on which you want to restore the backed-up configuration and click the **Restore** option.
3. Select the **File Store** from the list from which the backed-up controller needs to be restored.



Note: The OLT and the SFTP server must have the same IP protocol for OLT and CBAC related operations such as backup and restore. SFTP server must be reachable from the OLT.

4. Enter the **File Name** of the controller that must be restored.
5. Click **Submit**.

A confirmation message appears indicating the status of the restore operation. The controller data is restored from the SFTP server.

6. Note the timestamp when the event (SDPON-RESTORE-CONFIG-SUCCESSFUL) was generated.
7. Execute the following steps to clear the alarms raised by the old OLT.
 - a. In RMS, navigate to **Monitor > Faults**.
 - b. See step [6 \(on page 309\)](#) to determine the timestamp for generation of successful restore event and manually clear any active OLT alarms (including the Controller's alarm) raised for the restored Controller with a proper message (such as *Controller Restore*) for all the alarms reported before the Controller Restore timestamp.

RMS also supports scheduled restore configuration for the controller. If you want to schedule the controller restore for a later date and time, you must create a task. See [Creating Task for Controller or OLT Restore \(on page 667\)](#).

Download Controller Software

This feature enables on-demand download and upgrade of the CBAC software through the RMS GUI. The CBAC software package is downloaded from the repository server. Upgrade of the CBAC software is allowed once the CBAC software download is successful. Upon successful download of the CBAC package, a "CBAC Software Download Success" notification is triggered in RMS. If the CBAC package download fails, the "CBAC Software Download Failed" alarm is triggered in RMS.

Perform the following steps to download the controller software.

1. Select **Configuration > Controller**.
The Controller List page appears.
2. Click on the three dots (⋮) corresponding to the controller on which you want to download the software and click the **Download Software** option.
The Software Download page appears.
3. Enter the software version and click **Submit**.

A confirmation message appears indicating the status of the software download.



Note: Navigate to the **Monitor > Events** page and view the latest event for **SDPON-NEW-SOFTWARE-VERSION-AVAILABLE** to check the latest software version.

Upgrade Controller Software



Note: Before upgrading the controller software, you must download the controller software. For software download, refer to [Download Controller Software \(on page 309\)](#).

Perform the following steps to upgrade the controller software.

1. Select **Configuration > Controller**.
The Controller List page appears.
2. Click on the three dots (⋮) corresponding to the controller on which you want to upgrade the software and click the **Software Upgrade** option.
The Software Upgrade page appears.

Figure 58. Controller Upgrade

| Controller List 0 | | | | | |
|-----------------------------|---------------------------|-------------|-------------|-------------------------|--|
| Show 10 entries | | | | | |
| Name | Management Domain | Mode | Admin State | Creation Time | Action |
| VIMCTRL | DEFAULT MANAGEMENT DOMAIN | DISTRIBUTED | ACTIVE | Dec 6, 2022, 4:16:59 PM | ⋮ Restore Backup Monitor Download Software Software Upgrade Repair |
| Showing 1 to 1 of 1 entries | | | | | |

3. Select the SDPON version from the list.

Figure 59. Controller Version

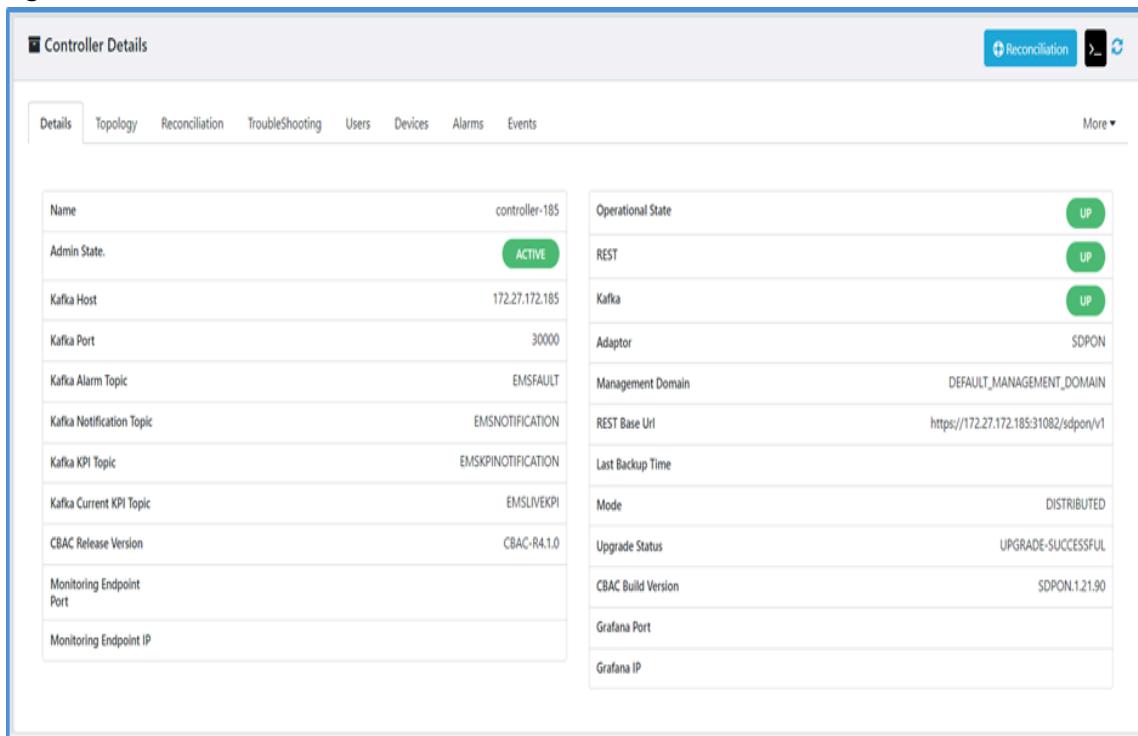
Software Upgrade

Version *
SDPON.1.17.111

Close Submit

4. Click **Submit**.
The **SDPON-SOFTWARE-UPGRADE-SUCCESSFUL** event is reported in the RMS to confirm the controller upgrade is successful.
5. Navigate to **Configuration > Controller > Monitor > Details** and verify the following fields.

- CBAC Release Version
- Upgrade Status
- CBAC Build Version

Figure 60. Controller Details

The screenshot shows a 'Controller Details' page with two tables of data. The left table contains general configuration details, and the right table contains operational status information. Both tables have a header row and several data rows.

| Controller Details | | | | | | | | |
|--------------------------|--------------------|----------------|-----------------|-------|---------|--------|--------|--------|
| Details | Topology | Reconciliation | Troubleshooting | Users | Devices | Alarms | Events | More ▾ |
| Name | controller-185 | | | | | | | |
| Admin State | ACTIVE | | | | | | | |
| Kafka Host | 172.27.172.185 | | | | | | | |
| Kafka Port | 30000 | | | | | | | |
| Kafka Alarm Topic | EMSFault | | | | | | | |
| Kafka Notification Topic | EMSNotification | | | | | | | |
| Kafka KPI Topic | EMSKPINotification | | | | | | | |
| Kafka Current KPI Topic | EMSLIVEKPI | | | | | | | |
| CBAC Release Version | CBAC-R4.1.0 | | | | | | | |
| Monitoring Endpoint Port | EMS | | | | | | | |
| Monitoring Endpoint IP | | | | | | | | |

| Operational State | UP |
|--------------------|---------------------------------------|
| REST | UP |
| Kafka | UP |
| Adaptor | SDPON |
| Management Domain | DEFAULT MANAGEMENT DOMAIN |
| REST Base Url | https://172.27.172.185:31082/sdpdn/v1 |
| Last Backup Time | |
| Mode | DISTRIBUTED |
| Upgrade Status | UPGRADE-SUCCESSFUL |
| CBAC Build Version | SDPON.1.21.90 |
| Grafana Port | |
| Grafana IP | |

Controller Monitored Entity

Monitoring and alerting ecosystem enables the monitoring of CBAC microservices through Grafana dashboard and alerting through Prometheus alert manager on the alert channels such as Email and Telegram.

The monitoring and alerting ecosystem can be separately deployed or co-located on the RMS VM or server.

The additional microservices in CBAC such as node exporter, metrics server, and kube-state metrics are deployment configurable and these microservices can be enabled or disabled for the CBAC deployment.

An operator can perform the following operations using the controller monitored entity.

- Monitor the current status and resource utilization metrics of the CBAC K8s microservices deployment.
- Configure the alert rules, alert channels, and account subscriptions for receiving the alert notifications.

Creating Controller Entity

After successful creation of the CBAC controller and the controller is activated, you can configure the controller monitored entity.

Perform the following steps to create a controller monitored entity.

1. Select **Configuration > Controller**.

The Controller List page appears.

2. Click **Create**.

The Controller Configuration page appears.

3. Click on the icon under the **Infra Monitoring** column.



Note: The icon is enabled only when you configure the infrastructure monitoring related field while creating a controller.

The Controller Monitored Entity page appears.

4. Complete the configuration according to the guidelines provided in the following table.

Table 145. Controller Entity Configuration

| Field | Description |
|-----------------------------|--|
| Name | Enter a unique name for the controller entity. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space |
| Metrics | |
| Type | Select the metrics types. The supported values are. <ul style="list-style-type: none">◦ Node◦ Microservice |
| Endpoint | Specifies the IP address of the monitored entity, which is used for scraping the health status and metrics (CPU and memory) for microservices and nodes. Example: https://10.6.0.55:31800/sdpon/v1/microservices/metrics |
| Alert Channel Config | |
| SMTP Server | Enter the IP address of the SMTP server. |
| Email Address List | Enter the email address list to send the alert notifications. You can add more than one email address separated by comma. |
| Telegram Group Name | Enter the telegram group name. |
| Telegram Group Token | Enter the telegram group token. |

5. Click **Create**.

A new controller entity is created on the Controller Monitored Entity page.

Inventory

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Inventory** from the left-hand side of the menu.

Create and manage inventory information for the following managed elements.

- OLT
- ONT
- CPE
- Splitter
- BNG
- Card
- Rack
- SFP
- Cable

Tasks

You can perform the following tasks from this page.

- Create OLT configuration. See [Creating OLT Configuration \(on page 318\)](#).
- Create ONT configuration. See [Creating ONT Configuration \(on page 427\)](#).
- Create CPE configuration. See [Creating CPE Configuration \(on page 438\)](#).
- Create splitter configuration. See [Creating Splitter Configuration \(on page 441\)](#).
- Create BNG configuration. See [Creating BNG Configuration \(on page 442\)](#).
- Create card configuration. See [Creating Card Configuration \(on page 444\)](#).
- Create rack configuration. See [Creating Rack Configuration \(on page 446\)](#).
- Create cable configuration. See [Creating Cable Configuration \(on page 451\)](#).
- Export the details of OLT, ONT, SFP, CPE, splitter, BNG, card, rack, and cable. See [Exporting Managed Elements \(on page 66\)](#).
- Import the details of OLT, ONT, SFP, CPE, splitter, BNG, card, rack, and cable. See [Importing Managed Elements \(on page 453\)](#).
- A pattern search using partial or complete keywords is supported for the following fields on the OLT inventory page.
 - Name (NEID)

OLT

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Inventory > OLT** from the left-hand side of the menu.

OLT is a physical device connected to the network through the management interface that is physically connected to the BNG. OLT implements basic hardware functions such as PON MAC to connect to Customer Premise Equipment (CPEs) and Ethernet MAC to connect to the upstream network of BNG.

Each OLT implements the interface toward CBAC and registers with the CBAC running at the associated aggregation network, located at the central office (CO), for terminating the PON protocol.

OLT supports only secure logins using SSH and disables other forms of login that are not secure. In addition, OLT implements a username and password method to authenticate logins. The OLT also supports RADIUS-based authentication for centrally configuring the operations logins.

OLT supports multiple privilege levels for users logging into the network, the same privileges are available for local users, and the RADIUS authenticated users. Based on the user's privilege level, certain operations are not allowed for users with less privileges.

Tasks

You can perform the following tasks from this page.

- Create OLT configuration. See [Creating OLT Configuration \(on page 318\)](#).
- Configuring Network Services. See [Configuring Network Services \(on page 326\)](#).
- Activate and deactivate the OLT. See [Activating and Deactivating the OLT \(on page 324\)](#).
- Associate the Storm Profile to the OLT. See [Associate the Storm Profiles to the OLT \(on page 325\)](#).
- Dissociate the Storm Profile from the OLT. See [Dissociate the Storm Profiles from the OLT \(on page 326\)](#).
- Reboot and reset the OLT. See [Reboot the OLT \(on page 388\)](#).
- View the physical and logical topology of the OLT. See [Topology \(on page 283\)](#).
- View the ZTP variable list of the OLT.
- View PON and NNI port configuration. See [Viewing PON and NNI Ports \(on page 372\)](#).
- Upgrade OLT software. See [Upgrade the OLT Software \(ONL or OLT BINS\) \(on page 388\)](#).
- Enable and Disable anti theft configuration on OLT. See [Enabling and Disabling OLT Anti Theft Configuration \(on page 422\)](#).
- Download ATP report for an OLT. See [Downloading ATP Report \(on page 423\)](#).
- Monitor the OLT details such as OLT health status and basic information. See [Monitoring OLT \(on page 67\)](#).
- Activate the application software running on the OLT.
- Commit the activated software on the OLT.
- Rollback software on the OLT.
- View the physical link of the OLT.

- Filter the OLT list based on the following fields. Filter enables you to quickly find and display the entries that are relevant to your specific needs.
 - Name
 - Admin State
 - Operational State
 - Make
 - Model
 - Display ID
 - Resource State
 - Software Version
- Click on the  icon to clear the applied filters.

Field Descriptions

The following table describes the fields on the OLT Inventory page.

Table 146. OLT Inventory List

| Field | Description |
|-------------------|---|
| Name | Specifies the name of the OLT. |
| Admin State | Specifies the admin state of the OLT. <ul style="list-style-type: none">• Green. Indicates that the OLT is ACTIVE.• Red. Indicates that the OLT is INACTIVE. |
| Operational State | Specifies the operational state of the OLT. <ul style="list-style-type: none">• Green. Indicates that the OLT is UP.• Red. Indicates that the OLT is DOWN. |
| Make | Specifies the vendor name who manufactured the OLT. Example: Edgecore |
| Model | Specifies the model name of the OLT. |
| Display ID | Specifies the display ID of the OLT. |
| MAC Address | Specifies the MAC address of the OLT. Example: 28:b9:d9:e2:6f:5e |
| Serial No | Specifies the serial number of the OLT. |
| Management IP | Specifies the management IP address of the OLT. Example: 10.232.232.232 |

Table 146. OLT Inventory List (continued)

| Field | Description |
|-------------------------------|--|
| Site | Specifies the site on which the OLT is installed. |
| Software Upgrade Status | Specifies the software upgrade status of the OLT. Example: NOT DOWNLOADED If the upgrade task is struck and terminated automatically, the Software Upgrade Status is shown as DOWNLOAD-FAILED/ACTIVATE-FAILED/COMMIT-FAILED. |
| Device Profile | Specifies the name of the OLT device profile. |
| Management Domain | Specifies the name of the management domain. |
| Controller | Specifies the name of the controller. |
| Shelf | Specifies the shelf name on which the OLT is installed. |
| Slot No | Specifies the slot number of the shelf on which the OLT is installed. |
| Alarm Profile | Specifies the alarm profile configured for the OLT. |
| Log Profile | Specifies the log profile configured for the OLT. |
| Authentication Type | Specifies the authentication type of the OLT. The supported values are. <ul style="list-style-type: none"> LOCAL RADIUS |
| Resource State | Specifies the resource state of the OLT. The supported values are. <ul style="list-style-type: none"> PLANNED INSTALLED RETIRED |
| Hardware Version | Specifies the hardware version of the OLT. |
| Supervision State | Specifies the supervision state of the OLT. The supported values are. <ul style="list-style-type: none"> NONE SUPERVISED |
| Software Version | Specifies the software version running on the OLT. |
| Software Release ETSI Version | Specifies the ETSI software version of the OLT. |
| Backup Status | Specifies the backup operation state of the OLT. The supported values are. |

Table 146. OLT Inventory List (continued)

| Field | Description |
|-------------------------------|---|
| | <ul style="list-style-type: none"> • BACKUP-INITIATED • BACKUP-FAILED • BACKUP-SUCCESSFUL |
| Restore Status | <p>Specifies the restore operation state of the OLT. The supported values are.</p> <ul style="list-style-type: none"> • RESTORE-INITIATED • RESTORE-FAILED • RESTORE-SUCCESSFUL |
| Up Since Time | <p>Specifies the date and time from when the OLT is UP.</p> <p> Note: If the OLT is added to the network for the first time, it shows the time since it was activated. If the OLT is rebooted, it reflects the time since the reboot.</p> |
| Me Group | Specifies the managed element group to which this OLT belongs to. |
| ZTP Status | <p>Specifies the ZTP status of the OLT.</p> <p>EXAMPLE: INITIATED</p> |
| ONT Firmware Upgrade Status | <p>Specifies the ONT firmware upgrade status.</p> <p>Example: DOWNLOADED</p> |
| ONT Firmware Version | Specifies the current version of the ONT firmware. |
| ONT Firmware Download Version | Specifies the version of the ONT firmware that was downloaded. |
| Creation Time | Specifies the date and time when the OLT was configured. |
| Network Services | <p>Specifies the list of network services that you can configure for the OLT. The supported network services are.</p> <ul style="list-style-type: none"> • LAG • ELine • ELAN |
| Local Profile | <p>Specifies the list of local profile. The supported values are.</p> <ul style="list-style-type: none"> • Log Profile • TACACS Profile • IGMP Profile • VNet Profile |

Table 146. OLT Inventory List (continued)

| Field | Description |
|--------|--|
| | <ul style="list-style-type: none">• Bandwidth Profile• Shaper Profile• COSQ Profile• MEP Profile• ERPS Profile |
| Action | Specifies the action that you can perform on the OLT. The supported actions are. <ul style="list-style-type: none">• Edit• Delete• Clone• View the list of port associated with the OLT |

Creating OLT Configuration

Each OLT has a MAC address and serial number as its unique identifiers at the time of factory manufacturing. In OSS/BSS, at the time of commissioning, associate each OLT with a human-readable name for the easy association of the OLT with its location. This information is made available to both RMS and CBAC through RMS. CBAC uses this information to identify and discover an OLT when it is powered on. CBAC supports the add, update, and delete operations of management ACL for the trusted management subnet. The same operations can be performed on alarm profiles, RADIUS profiles, and log profiles associated with OLTs.

After deploying an OLT in the field, extensive network service configurations and integration into the RMS system are required. The successful execution of ATP test cases ensures the OLTs operational status is UP and the OLT is Ready For Service (RFS). These OLTs are Handover Takeover (HOTO) OLTs.

Any OLTs awaiting RFS declaration and handover must be assigned to a non-HOTO OLT. Once the OLT is moved into a HOTO site group, it cannot be transferred back to a non-HOTO site group.



Note: Before you create an OLT, you must create the following.

- Management domain
- Make
- Model
- Device profile
- Controller

Perform the following steps to create the OLT.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab.
3. Click **Create**.
The OLT Configuration page appears.
4. Complete the configuration according to the guidelines provided in the following table.

Table 147. OLT Configuration

| Field | Description |
|----------------------|--|
| Basic Details | |
| Management Domain | Select the management domain from the list. If the management domain does not exist, click the plus icon (+) to create a management domain. See Creating Management Domain (on page 765) . |
| Name | Enter a unique name for the OLT. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Make | Select the make from the list. If the make does not exist, click the plus icon (+) to create a make configuration for the OLT. See Creating Make Configuration (on page 606) . |
| Model | Select the device model from the list. If the device model does not exist, click the plus icon (+) to create a model for the OLT. See Creating Model Configuration (on page 610) . |
| Device Profile | Select the device profile from the list. If the device profile does not exist, click the plus icon (+) to create a device profile for the OLT. See Creating OLT Device Profile (on page 509) . |
| Display Id | Enter the display ID for the OLT. |
| Serial No | Enter the serial number for the OLT. Example: ZEDD00633G |
| Controller | Enter the controller name. If the controller does not exist, click the plus icon (+) to create a controller. See Creating Controller Configuration (on page 297) . |
| MAC Address | Enter the MAC address for the OLT. Example: 00:d0:50:09:c6:44 |
| Management IP | Enter a valid IPv4 address for the OLT. |

| Field | Description |
|-----------------------------|--|
| | Example: 172.27.173.225 |
| HOTO Status | <p>Specifies the Handover Takeover status. The supported values are.</p> <ul style="list-style-type: none"> ◦ HOTO ◦ Non HOTO <p>The default value is Non HOTO.</p> |
| Site | Select the site from the list. If the site does not exist, click the plus icon (+) to create a site. See Creating Site Configuration (on page 289) . |
| Max Temperature | Enter the maximum temperature for the OLT. Example: 90° Celsius |
| Management VLAN ID | Enter the management VLAN ID. |
| Enable PM Collection Policy | Enable this option to retrieve the historical performance monitoring (PM) counters collection from CBAC through Kafka. |
| PM Collection Policy | Select the PM collection policy from the list. This field is displayed only when you enabled the PM Collection Policy option. |
| External Alarm VLAN ID | <p>Specifies the VLAN ID to be used for external alarm device management. The external VLAN ID must not be same as the management VLAN ID.</p> <p>The value ranges from 2 to 4094.</p> <p>Example: 2000</p> |
| Auto Activate | Enable this option to activate the OLT automatically after the successful creation of the OLT. |
| Force Delete | <p>Deletes the OLT configuration forcefully. The supported values are.</p> <ul style="list-style-type: none"> ◦ TRUE ◦ FALSE <p>The default value is FALSE.</p> |
| Service MAC Limit | <p>Specifies the number of MACs to be learned at service per OLT. This field can be modified only when OLT is in a DEACTIVE state. The supported value ranges from 0 to 65535.</p> <p>The MAC value 65535 indicates there is no MAC limit.</p> <p>The user is allowed to configure the value from 1 to 65535.</p> <p>The value zero (0) indicates the existing MAC limit configuration is removed.</p> |
| Enterprise Number | Specifies the vendor's registered enterprise number as registered with Internet Assigned Numbers Authority (IANA). The supported value ranges from 0 to 65535. The default value is 4337. |

| Field | Description |
|-------------------------|---|
| Advanced Details | |
| Shelf Info | |
| SHELF | Select the rack shelf present on the same site on which the OLT is present. For creating rack and shelf, see Creating Rack Configuration (on page 446) and Creating Shelf Configuration (on page 448) . |
| Alias | Enter the alias name for the OLT. |
| Profiles | |
| Alarm Profile | Select the alarm profile from the list. If the alarm profile does not exist, click the plus icon (+) to create an alarm profile for the OLT. See Alarm Profile (on page 473) . |
| Log Profile | Select the log profile from the list. If the log profile does not exist, click the plus icon (+) to create a log profile for the OLT. See Creating Log Profile (on page 503) . |
| NTP Profile | Select the NTP profile from the list. If the NTP profile does not exist, click the plus icon (+) to create a NTP profile for the OLT. See Creating NTP Profile (on page 553) . |
| TACACS Profile | Select the TACACS profile from the list. If the TACACS profile does not exist, click the plus icon (+) to create a TACACS profile for the OLT. See Creating TACACS Profile (on page 559) . |
| Alarm Soak Profile | Select the alarm soak profile from the list. If the alarm soak profile does not exist, click the plus icon (+) to create an alarm soak profile for the OLT. See Creating Alarm Soak Profile (on page 561) . |
| ZTP | |
| ZTP Template | Select the ZTP template from the list. |
| Bandwidth | |
| Bandwidth Validation | <p>Enable this option to allow automatic calculation of the bandwidth overhead. The supported values are:</p> <ul style="list-style-type: none"> • ENABLED. If you associate the bandwidth profile to a service and activate it, the error message is displayed if sufficient bandwidth is unavailable at the PON port of the OLT. The bandwidth overhead calculation can vary depending on parameters such as TCONT type, FEC, CIR, and AIR value. |

| Field | Description |
|--|--|
| | <ul style="list-style-type: none"> • DISABLED. It skips the bandwidth overhead calculation and creates the service without checking the available bandwidth at the PON port of the OLT. The service can fail if sufficient bandwidth is not available. <p>The default value is ENABLED.</p> <p> Note:</p> <ul style="list-style-type: none"> ◦ To disable the bandwidth validation after creating the OLT, all the services of that OLT must be in disabled state. See Disabling Bandwidth Validation (on page 323). ◦ The user can disable the bandwidth validation during the creation of the OLT. |
| Authentication | |
| Authentication Type | Select the authentication type from the list. <ul style="list-style-type: none"> ◦ LOCAL ◦ RADIUS |
| When the authentication type is selected as LOCAL, the following fields are displayed. | |
| User Name | Enter a valid username for the user. |
| Password | Enter a valid password for the user. |
| When the authentication type is selected as RADIUS, the following field is displayed. | |
| Authentication Profile | Select the authentication profile from the list. If the authentication profile does not exist, see Creating Authentication Profile (on page 537) . |
| State | |
| Resource State | Select the resource state from the list. The supported states are. <ul style="list-style-type: none"> ◦ PLANNED ◦ INSTALLED ◦ RETIRED |
| Supervision State | Select the supervision state from the list. The supported states are. <ul style="list-style-type: none"> ◦ NONE ◦ SUPERVISED |
| Version | |

| Field | Description |
|-------------------------------|---|
| Hardware Version | Enter the hardware version for the OLT. Example: x86_64-accton_asxvolt16-r0 |
| Firmware Version | Enter the firmware version of the OLT. Example: BAL.3.5.3 |
| Software Version | Enter the software version running on the OLT. Example: AN6520PO_1.0.0.0.012 |
| Software Release ETSI Version | Enter the software release ETSI version for the OLT. |
| Additional Info | Specifies the additional information about the OLT. Whenever there is a service request from the OSS/BSS systems, the additional information in the OLT helps to find any match and replace the name value pair, which comes from the OSS/BSS system with this value. |
| Key | Enter the variable name for the key. Example: networkVlanName:SRV_VLAN_RES |
| Value | Enter the key value. Example: 34 |

5. Click **Create**.

A new OLT is created on the Inventory List page.



Note: After the successful creation of the OLT, the device view diagram is created in the *Monitor* page. You can monitor the OLT device information and how the OLT is placed in the rack shelf, the splitter connected to the OLT, and the SFP associated with the OLT. For more information, see [Monitoring OLT \(on page 67\)](#).

Disabling Bandwidth Validation

Perform the following steps to disable the bandwidth validation if the bandwidth validation is already enabled during OLT configuration. If the OLT configuration is not created you can disable the bandwidth validation during OLT configuration. See [Creating OLT Configuration \(on page 318\)](#).

1. Navigate to **Monitor > Inventory > Inventory > OLT**.
2. Select the applicable OLT.
The OLT Details page appears.
3. Select **Services** tab.



Note: Make a note of all the services attached to the OLT.

4. Deactivate all the service attached to the OLT. See [Activating and Deactivating the Service for the Subscriber \(on page 467\)](#).
5. Navigate to **Configuration > Inventory > OLT**.
6. Click on Edit icon under **Action** Column.
The OLT Configuration page appears.
7. Select **Advanced Details** tab.
8. Navigate to **Bandwidth Validation** field and select **DISABLED** from the list.
9. Click **Save** to save the OLT configuration.
10. Activate all the service attached to the OLT. See [Activating and Deactivating the Service for the Subscriber \(on page 467\)](#).

Activating and Deactivating the OLT

You must activate the OLT before you connect the OLT to subscribers and provide services to the subscribers.



Note:

- The OLT and Controller IP must be same.
- The IP addresses must not be duplicated across the multiple nodes.

Once the OLT, PON, and NNI cards are created, you can activate the OLT.

Perform the following steps to activate the OLT.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the OLT tab.
3. Click on the three dots (⋮) corresponding to the OLT that you want to activate and click the **Activate** option.

A confirmation message appears indicating that the OLT is activated successfully. The operational state of the OLT is changed to UP and the admin state OLT is changed to ACTIVE.

You can deactivate the OLT if the OLT is prepared for decommissioning.



Note: If duplicate IP addresses are detected, deactivate the OLT, resolve the duplicate IP, and reactivate the OLT.

Perform the following steps to deactivate the OLT.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the OLT tab.
3. Click on the three dots (⋮) corresponding to the OLT that you want to deactivate and click the **Deactivate** option.

A warning pop-up message appears stating, Deactivating <olt-name> results in reboot of the OLT to complete the deactivation process, affecting active subscriber's services. Wait for the controller state to become up before further operations can be performed. Are you sure to proceed with the deactivation of <olt-name>?

4. Click **Yes, Deactivate** to deactivate the OLT.

A confirmation message appears indicating that the OLT is deactivated successfully.



Note: The "Deactivate OLT" procedure involves the deactivation of the PON ports, clean up of the subscriber services, ONTs, and network services. The "OLT-DOWN" event is sent from CBAC to RMS upon completion of the deactivation procedure. The successive operations such as activate OLT and delete OLT from RMS can be performed only after the "OLT-DOWN" event is received.

Associate the Storm Profiles to the OLT

When you associate the storm profile to the OLT, the storm profile rules are applied to the set of ports on the OLT.



Note: Before you associate the storm profile to the OLT, you must create the following profile configuration.

- [Creating Policer Profile \(on page 587\)](#)
- [Creating Storm Control Profile \(on page 588\)](#)

Perform the following steps to associate the storm control profile to the OLT.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the OLT tab.
3. Click on the three dots (⋮) corresponding to the OLT that you want to associate the storm control profile and click the **Storm Profiles** option.
The Storm Profile [Inventory - <OLT-Name>] page appears.
4. Click the **Add** option.
The Select Storm Profile page appears.
5. Select the respective storm profile that you want to associate to the OLT.
6. Select the **Port Type** from the list. The supported values are.

- PON
 - NNI
 - LAG
7. Select the port from the Port List.
 8. Click the **Add** option.
The storm profile is added on the Storm Profiles page.
 9. Click the **Associate** option from the Associate/Dissociate column.
 10. The Storm profile is added to the OLT and a confirmation message appears, indicating the status of the associate operation.

Dissociate the Storm Profiles from the OLT

You can remove the storm profile from the OLT.

Perform the following steps to dissociate the storm control profile from the OLT.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the OLT tab.
3. Click on the three dots (⋮) corresponding to the OLT that you want to disassociate the storm control profile and click the **Storm Profiles** option.
The Storm Profile [Inventory - <OLT-Name>] page appears.
4. Click the **Dissociate** option from the Associate/Dissociate column.
The storm profile is removed from the OLT and a confirmation message appears, indicating the status of the disassociate operation.

Configuring Network Services

You can configure the following network services for the OLT.

- Link Aggregation Group (LAG)
- Ethernet Line (ELine)
- Ethernet LAN (ELAN)

LAG

LAG combines many physical ports to create a single high-bandwidth data path. LAG implements traffic load sharing among the member ports in the group and enhances the connection reliability.

RMS or CBAC supports aggregating one or more physical interfaces on an OLT to create a LAG.

LAG is used in the network to increase the bandwidth and provide traffic resiliency if there are any port failures.

Link aggregation addresses the following problems with Ethernet connections.

- Bandwidth limitations
- Lack of resilience

Tasks

You can perform the following tasks on this page.

- Create, enable, and disable LAG. See [Creating LAG Configuration \(on page 328\)](#).
- Delete and clone LAG.
- Initiate and cancel MAC dump on LAG port. See [Initiate and Cancel MAC Dump on LAG \(on page 329\)](#).
- MAC lookup on LAG. See [MAC Lookup for LAG \(on page 331\)](#).

Field Descriptions

The following table describes the fields on the Link Aggregation List page.

Table 148. LAG Fields

| Field | Description |
|-------------------|---|
| Name | Specifies the name of the LAG. |
| MTU Size | Specifies the Maximum Transmission Unit (MTU) size. |
| Alarm Profile | Specifies the name of the LAG alarm profile. |
| Admin State | Specifies the admin state of the LAG. The supported states are. <ul style="list-style-type: none">• ACTIVE. When the LAG configuration is enabled.• INACTIVE. When the LAG configuration is disabled.• UNKNOWN. When the LAG configuration is created. |
| Operational State | Specifies the operational state of the LAG. The supported states are. <ul style="list-style-type: none">• Green. Indicates that the operational state of the LAG is up.• Red. Indicates that the operational state of the LAG is down. |
| Controller State | Specifies state of the controller. The supported states are. <ul style="list-style-type: none">• ADD_IN_PROGRESS• ADDED• ENABLE_IN_PROGRESS• ENABLED• DISABLE_IN_PROGRESS• DISABLED• DELETE_IN_PROGRESS• ADD_FAILED |

Table 148. LAG Fields (continued)

| Field | Description |
|----------------------|---|
| | <ul style="list-style-type: none"> • DELETE_FAILED • ENABLE_FAILED • DISABLE_FAILED • ASSOCIATION_FAILED • DISSOCIATION_FAILED |
| LACP | Specifies the Link Aggregation Control Protocol (LACP) mode. |
| LACP Timeout | Specifies the Link Aggregation Control Protocol Data Unit (LACPDU) transmission interval. |
| LACP System Priority | Specifies the LACP system priority. |
| Creation At | Specifies the date and time when the LAG was created. |
| Ports | Specifies the type of port. |
| Action | Specifies the action that can be performed on LAG. The supported actions are. <ul style="list-style-type: none"> • Clone • Delete |

Creating LAG Configuration



Note: Before you create LAG, you must create the LAG alarm profile. For more information, see [Alarm Profile \(on page 473\)](#).

Perform the following steps to create LAG.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab and then click **LAG** from the **Network Services** column.
The Link Aggregation List page appears.
3. Complete the configuration according to the guidelines provided in the following table.

Table 149. LAG Configuration

| Field | Description |
|-------|--|
| Name | Enter a unique name for the LAG. You can use any number of alphanumeric characters. Only the following special characters are supported. |

| Field | Description |
|----------------------|---|
| | <ul style="list-style-type: none"> Underscore (_) Hyphen (-) |
| Alarm Profile | Select the LAG alarm profile from the list. |
| MTU Size | <p>Enter the MTU size. The OLT cannot transmit the packets on the NNI/LAG interface more than the configured MTU size. The value ranges from 68 bytes to 9600 bytes (9KB). The default value is 9600 bytes.</p> <p> Note: The MTU size is applied to all the NNI members ports of the selected LAG.</p> |
| LACP | <p>Specifies the Link Aggregation Control Protocol (LACP) mode. It indicates whether LACP is enabled and in active mode. The supported values are.</p> <ul style="list-style-type: none"> Disabled Active Passive <p>The default value is Disabled.</p> |
| LACP Timeout | <p>Specifies the Link Aggregation Control Protocol Data Unit (LACPDU) transmission interval. The supported values are.</p> <ul style="list-style-type: none"> Slow Fast <p>The default value is Fast.</p> |
| LACP System Priority | <p>Specifies the LACP system priority. The supported value ranges from 0 to 65,535. The default value is 128.</p> |

4. Click **Create**.

A LAG configuration is created for the OLT.

The admin state of the LAG is UNKNOWN when it was created. You must enable the LAG for the LAG to become ACTIVE.

Initiate and Cancel MAC Dump on LAG

Perform the following steps to initiate the MAC dump on LAG.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the OLT tab
The OLT List tab appears.
3. Click on **LAG** corresponding to a particular OLT from the **Network Services** column.
The Link Aggregation List page appears.
4. Click on the three dots (⋮) corresponding to the LAG and click **Initiate MAC Dump** option.
5. Complete the configuration according to the guidelines provided in the following table.

Table 150. Initiate MAC Dump Configuration

| Field | Description |
|-------------|---|
| OVlan | Specifies the outer VLAN. This field is applicable for the MAC dump request on PON port, NNI port, and services. The supported value ranges from 2 to 4094. |
| IVlan | Specifies the inner VLAN. This field is applicable only for the NNI port. |
| MAC Address | Specifies the MAC address. |



Note: The **OVlan**, **IVlan**, and **MAC Address** fields are optional.

6. Click **Submit**.

A confirmation message appears indicating that the MAC dump is initiated successfully.

7. Click on the three dots (⋮) corresponding to LAG and click **Monitor** option to view the MAC dump on LAG. For more information, see [LAG Details \(on page 135\)](#).

Perform the following steps to cancel the MAC dump on LAG.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the OLT tab

The OLT List tab appears.

3. Click on **LAG** corresponding to a particular OLT from the **Network Services** column.

The Link Aggregation List page appears.

4. Click on the three dots (⋮) corresponding to the LAG and click **Cancel MAC Dump** option.

A confirmation message appears indicating that the MAC dump is canceled successfully.

MAC Lookup for LAG

Perform the following steps to perform MAC lookup on LAG.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab.
The OLT List tab appears.
3. Click on **LAG** corresponding to a particular OLT from the **Network Services** column.
The Link Aggregation List page appears.
4. Click on the three dots (⋮) corresponding to the LAG and click **MAC Lookup** option.
5. Complete the configuration according to the guidelines provided in the following table.

Table 151. MAC Lookup Configuration

| Field | Description |
|-------------|---|
| OVlan | Specifies the outer VLAN. This field is applicable for the MAC dump request on PON port, NNI port, and services. The supported value ranges from 2 to 4094. |
| IVlan | Specifies the inner VLAN. This field is applicable only for the NNI port. |
| MAC Address | Specifies the MAC address. |



Note: The **OVlan** and **MAC Address** fields are mandatory whereas the **IVlan** field is optional to perform MAC lookup.

A confirmation message appears indicating that the MAC for a particular resource ID is learned successfully.



Note: When the incorrect values are entered for the **OVlan** and **MAC Address** fields, an error message appears indicating that the MAC lookup is failed for a particular resource id.

ELine

ELine is a point-to-point connection between two nodes. You can configure an ELine per OLT with VLAN ID and the NNI or LAG port.

OLT supports the Ethernet functionality over NNI ports to support the VLAN-tagged traffic (single or double VLAN tag). NNI ports must be configured with ELine service to enable the traffic flow between the PON and NNI network with a proper VLAN tag. You can configure an ELine with a single NNI or LAG port as part of ELine, along with a VLAN ID.

ELine is configured only when the traffic needs to be switched from the Ethernet network to the PON network on the same OLT device. Data traffic resiliency in the upstream network is not possible if ELine is created.

Tasks

You can perform the following tasks on this page.

- Create an ELine configuration. See [Creating ELine Configuration \(on page 332\)](#).
- Enable and disable ELine configuration. See [Enabling and Disabling ELine Configuration \(on page 333\)](#).
- Delete ELine.

Field Descriptions

The following table describes the fields on the ELine List page.

Table 152. ELine Fields

| Field | Description |
|-------------|--|
| Name | Specifies the name of the ELine. |
| VLAN | Specifies the VLAN ID. |
| Port | Specifies the type of port. |
| Admin State | Specifies the admin state of the ELine. The supported states are. <ul style="list-style-type: none">• ENABLED• DISABLED |
| Creation At | Specifies the date and time when ELine was created. |
| Action | Specifies the action that can be performed on ELine. The supported action is Delete. |

Creating ELine Configuration

When the OLT, PON, and NNI cards are created and the OLT is activated, you can create an ELine configuration and activate it.

Perform the following steps to create an ELine configuration.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab and then click **ELine** from the **Network Services** column.
The ELine List page appears.
3. Complete the configuration according to the guidelines provided in the following table.

Table 153. ELine Configuration

| Field | Description |
|---------|---|
| Name | Enter a unique name for the ELine. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| VLAN ID | Enter the VLAN ID. The value ranges from 2 to 4094. |
| Port | Select the port from the list. |

4. Click **Create**.

A new ELine configuration is created.

Enabling and Disabling ELine Configuration

Perform the following steps to enable the ELine.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the OLT tab and then click **ELine** from the **Network Services** column.

The ELine List page appears.

3. Click on the three dots (⋮) corresponding to ELine on which you want to enable and click the **Enable** option.

A confirmation message appears indicating that the ELine is enabled successfully.

Perform the following steps to disable the ELine.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the OLT tab and then click **ELine** from the **Network Services** column.

The ELine List page appears.

3. Click on the three dots (⋮) corresponding to ELine on which you want to disable and click the **Disable** option.

A warning pop-up message appears stating, *Disabling ELine could result in an impact on subscriber service. Are you sure to perform this action?*

4. Click **Confirm** to disable the ELine.

A confirmation message appears indicating that the ELine is disabled successfully.

ELAN

ELAN is a full mesh network and multipoint-to-multipoint connection between two nodes.

ELANs are generally used when data traffic resiliency is required in the upstream network towards BNG.

ELAN internally uses the VLAN based MAC forwarding functionality to enable traffic switching between the NNI ports. ELAN can be configured with multiple NNI or LAG ports along with a VLAN ID. An ELine or ELAN must be created for all the S-VLANs that are used to provide service to the subscriber.

Tasks

You can perform the following tasks on this page.

- Create an ELAN configuration. See [Creating ELAN Configuration \(on page 335\)](#).
- Enable and disable ELAN configuration. See [Enabling and Disabling ELAN Configuration \(on page 335\)](#).
- You update the ELAN configuration to add or remove the NNI port from ELAN on the fly.
- Delete ELAN.

Field Descriptions

The following table describes the fields on the ELAN List page.

Table 154. ELAN Fields

| Field | Description |
|-----------------------|--|
| Name | Specifies the name of the ELAN. |
| Vlan | Specifies the VLAN ID. |
| Port | Specifies the type of port. |
| Router Port | Specifies the OLT ports connected to the router. |
| Sub Port | Specifies the OLT ports connected to the subtending OLT. |
| Admin State | Specifies the admin state of the LAG. The supported states are. <ul style="list-style-type: none">• ENABLED• DISABLED |
| Configuration Status | Specifies the configuration status of the ELAN. |
| Config Failure Reason | Specifies the reason for the configuration failure. |

Table 154. ELAN Fields (continued)

| Field | Description |
|-------------|---|
| Creation At | Specifies the date and time when ELAN was created. |
| Action | Specifies the action that can be performed on ELAN. The supported action is Delete. |

Creating ELAN Configuration

Perform the following steps to create the ELAN.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab and then click **ELAN** from the **Network Services** column.
The ELAN List page appears.
3. Complete the configuration according to the guidelines provided in the following table.

Table 155. ELAN Configuration

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the ELAN. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| VLAN ID | Enter the VLAN ID. The value ranges from 2 to 4094. |
| Port List | Select the port (NNI or LAG) from the list. |
| Router Ports List | Select the OLT ports that are connected to the router. |
| Sub Ports List | Select the OLT ports that are connected to the subtending OLT. <p> Note: The sub ports must be the subset of ports. The sub port and the router port are mutually exclusive (For example, a router port cannot be sub-port and vice versa).</p> |

4. Click **Create**.
A new ELAN configuration is created.

Enabling and Disabling ELAN Configuration

Perform the following steps to enable the ELAN.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the OLT tab and then click **ELAN** from the **Network Services** column.

The ELAN List page appears.

3. Click on the three dots (⋮) corresponding to ELAN on which you want to enable and click the **Enable** option.

A confirmation message appears indicating that the ELAN is enabled successfully.

Perform the following steps to disable the ELAN.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the OLT tab and then click **ELAN** from the **Network Services** column.

The ELAN List page appears.

3. Click on the three dots (⋮) corresponding to ELAN on which you want to disable and click the **Disable** option.

A confirmation message appears indicating that the ELAN is disabled successfully.



Note:

- The following fields cannot be modified.
 - ID
 - Manageable Device
 - Management Domain
 - Make
 - Model
 - Device Profile
- You cannot delete the OLT when it is in activate state. Before deleting the OLT, ensure that you deactivate the OLT.
- RMS deletes all the events, alarms (current and historical), and historical KPIs from its database post successful deletion of the OLT device.

To edit, clone, and delete the OLT configuration, see [Common Operations \(on page 27\)](#).

Force Deletion of OLT

A forced delete operation deletes the OLT along with its associated resources, such as subscribers, services, local profiles, ONU devices, and configurations related to type-B, Eline, Elan, and so on.

Perform the following steps to force delete.



Note: The OLT must be in deactivate state for deleting the OLT.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab, select **Edit** icon set the Force Delete flag as true and **Save**.
3. Click on the OLT tab and then click the Delete icon from the **Action** column.
A warning pop-up message appears stating, Deleting an OLT is a critical operation that impacts active subscribers. Once deleted, this operation cannot be undone. Are you sure to proceed with the deletion of <olt-name>?.
4. Click **Yes, Delete**.
A confirmation message appears, indicating the acceptance of the delete operation.

Once the force delete operation is complete the OLT and all its associated resources are deleted from the RMS.

All clean-up operations are performed internally using the force delete operation. When the OLT is configured with dual home type-B or subtended OLT, consider the following recommendation.

- If the OLT is configured with dual home type- B and both primary and secondary OLTs are planned for decommissioning, the secondary OLT must be deleted first.
- If the OLT is configured with subtended OLT and both parent and subtended OLTs are planned for decommissioning, the subtended OLT must be deleted first.

For more information about configuring the type-B and subtended OLT, refer to *CBAC Feature Description Guide*.

Editing the OLT Name

In some scenarios, the OLT needs to be moved from one location to another, and all the subscribers connected to the OLT need to be retained in the same OLT. Since the OLT is moved to the new location, the OLT name needs to be updated according to the new location.

Perform the following steps to update the OLT name.

1. Deactivate the OLT and ensure that the OLT reboots. See [Activating and Deactivating the OLT \(on page 324\)](#).
2. Power off the OLT.
3. Update the new OLT NEID/OLT Name.
4. Turn on the OLT. Ensure the controller state is UP.

5. Select **Monitor > Inventory > OLT Details**.
The OLT Details page appears.
6. Activate the OLT.
7. Optional step: update the controller name only if the controller name is maintained the same as OLT name and controller type is distributed.
Select **Configuration > Controller**.
The Controller List page appears.
 - a. Deactivate the controller
 - b. Update the controller name
 - c. Activate the controller

All references related to OLT name must be updated with the new OLT Name in RMS and CBAC.

Configuring Local Profile

You can configure the following local profiles for the OLT.

- Local Log Profile. See [Local Log Profile \(on page 340\)](#).
- Local TACACS Profile. See [Local TACACS Profile \(on page 342\)](#).
- Local IGMP Profile. See [Local IGMP Profile \(on page 343\)](#).
- Local VNet Profile. See [Local VNet Profile \(on page 347\)](#).
- Local Bandwidth Profile. See [Local Bandwidth Profile \(on page 350\)](#).
- Local Shaper Profile. See [Local Shaper Profile \(on page 353\)](#).
- Local COSQ Profile. See [Local COSQ Profile \(on page 355\)](#).
- Local MEP Profile. See [Local MEP Profile \(on page 360\)](#).
- Local ERPS Profile. See [Local ERPS Profile \(on page 364\)](#).

Local Alarm Profile

RMS supports the following alarm profiles.

- Local Alarm Profile
- Global Alarm Profile

The local alarm profile is synchronized to a specific OLT, and the global alarm profile is synchronized with all the OLTs. If you want to apply the configuration on a single OLT, create a local alarm profile. If you want to apply the configuration on all the OLTs, create a global alarm profile. For more information about the global alarm profile, see [Creating Alarm Profile \(on page 339\)](#).



Note: The global profile and local profile cannot have the same name.

Field Descriptions

The following table describes the fields on the local alarm profile list page.

Table 156. Local Alarm Profile

| Field | Description |
|---------------|--|
| Name | Specifies the name of the alarm profile. |
| Type | Specifies the type of resource (OLT, OLT PORT, ONT, LAG, ACE, SFP, and ANI-G). |
| Creation Time | Specifies the date and time when the alarm profile was created. |
| Action | Specifies the action that you can perform on the alarm profile. The supported actions are. <ul style="list-style-type: none"> • Edit • Delete • Clone |

Creating Alarm Profile

Perform the following steps to create a local alarm profile.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab and then click the  icon from the **Local Profiles** column.
The Local Profile page appears.
3. Click on the **Alarm Profile** tab from the top left corner of the page.
The Alarm Profile List page appears.
4. Click **Create**.
The Alarm Profile Configuration page appears.
5. Complete the configuration according to the guidelines provided in the following table.

Table 157. Local Alarm Profile Configuration

| Field | Description |
|---------------|--|
| Name | Specifies the name of the alarm profile. |
| Type | Specifies the type of resource (OLT, OLT PORT, ONT, LAG, ACE, SFP, and ANI-G). |
| Creation Time | Specifies the date and time when the alarm profile was created. |
| Action | Specifies the action that you can perform on the alarm profile. The supported actions are. |

| Field | Description |
|-------|---|
| | <ul style="list-style-type: none">◦ Edit◦ Delete◦ Clone |

6. Click **Create**.

A local alarm profile configuration is created for the OLT.

To edit, clone, and delete the local alarm profile configuration, see [Common Operations \(on page 27\)](#).

Local Log Profile

RMS supports the following log profiles.

- Local Log Profile
- Global Log Profile

The local log profile is synchronized to a specific OLT, and the global log profile is synchronized with all the OLTs. If you want to apply the configuration on a single OLT, create a local log profile. If you want to apply the configuration on all the OLTs, create a global log profile. For more information about the global log profile, see [Creating Log Profile \(on page 503\)](#).



Note: The global profile and local profile cannot have the same name.

Field Descriptions

The following table describes the fields on the local log profile list page.

Table 158. Local Log Profile

| Field | Description |
|---------------|--|
| Name | Specifies the name of the local log profile. |
| Log Server | Specifies the IP address of the log server or FQDN of the log server. |
| Log Level | Specifies the log level of the device. |
| Creation Time | Specifies the date and time when the local log profile was created. |
| Action | Specifies the action that you can perform on the local log profile. The supported actions are. <ul style="list-style-type: none">• Edit• Clone• Delete |

Creating Local Log Profile

Perform the following steps to create a local log profile.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab and then click the  icon from the **Local Profiles** column.
The Local Profile page appears.
3. Click on the **Log Profile** tab from the top left corner of the page.
The Log Profile List page appears.
4. Click **Create**.
The Log Profile Configuration page appears.
5. Complete the configuration according to the guidelines provided in the following table.

Table 159. Local Log Profile Configuration

| Field | Description |
|------------|---|
| Name | Enter a unique name for the local log profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">Underscore (_)Hyphen (-) |
| Log Server | Specifies the IP address of the log server or FQDN of the log server. |
| Log Level | Specifies the log level of the device. The supported values are. <ul style="list-style-type: none">INFO. Logs are generated for informational messages.DEBUG. Logs are useful for debugging the system.WARNING. Logs are generated for warning conditions.ERROR. Logs are generated for any error conditions. This is the default log level. |

6. Click **Create**.
A local log profile configuration is created for the OLT.



Note:



Note: You cannot modify the ID field.

To edit, clone, and delete the local log profile configuration, see [Common Operations \(on page 27\)](#).

Local TACACS Profile

RMS supports the following TACACS profiles.

- Local TACACS Profile
- Global TACACS Profile

The local TACACS profile is synchronized to a specific OLT, and the global TACACS profile is synchronized with all the OLTs. If you want to apply the configuration on a single OLT, create a local TACACS profile. If you want to apply the configuration on all the OLTs, create a global TACACS profile. For more information about the global TACACS profile, see [Creating TACACS Profile \(on page 559\)](#).



Note: The global profile and local profile cannot have the same name.

Field Descriptions

The following table describes the fields on the local TACACS profile list page.

Table 160. Local TACACS Profile

| Field | Description |
|---------------|---|
| Name | Specifies the name of the local TACACS profile. |
| Host | Specifies the IP address or Fully Qualified Domain Name (FQDN) of the local TACACS server. |
| Port | Specifies the port number of the local TACACS server, which is exposed to access the server-client communication. |
| Secret Key | Specifies the secret key, which is used to encrypt the payload. |
| Creation Time | Specifies the date and time when the local TACACS profile was created. |
| Action | Specifies the action that you can perform on the local TACACS profile. The supported actions are. <ul style="list-style-type: none">• Edit• Clone• Delete |

Creating Local TACACS Profile

Perform the following steps to create a local TACACS profile.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab and then click the



icon from the **Local Profiles** column.

The Local Profile page appears.

3. Click on the **TACACS Profile** tab from the top left corner of the page.

The TACACS Profile page appears.

4. Click **Create**.

The TACACS Profile Configuration page appears.

5. Complete the configuration according to the guidelines provided in the following table.

Table 161. Local TACACS Profile Configuration

| Field | Description |
|----------------|---|
| Name | Enter a unique name for the local TACACS profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Servers | |
| Host | Specifies the IP address or Fully Qualified Domain Name (FQDN) of the local TACACS server. |
| Port | Specifies the port number of the local TACACS server, which is exposed to access the server-client communication. The default value is 49. The supported value ranges from 0 to 65,535. |
| Secret Key | Specifies the secret key, which is used to encrypt the payload. The minimum length of this field must be 32 characters. |

6. Click **Create**.

A local TACACS profile configuration is created for the OLT.



Note: You cannot modify the **ID** and **name** fields.

To edit, clone, and delete the local TACACS profile configuration, see [Common Operations \(on page 27\)](#).

Local IGMP Profile

RMS supports the following IGMP profiles.

- Local IGMP Profile
- Global IGMP Profile

The local IGMP profile is synchronized to a specific OLT, and the global IGMP profile is synchronized with all the OLTs. If you want to apply the configuration on a single OLT, create a local IGMP profile. If you want

to apply the configuration on all the OLTs, create a global IGMP profile. For more information about the global IGMP profile, see [Creating IGMP Profile \(on page 584\)](#).



Note: The global profile and local profile cannot have the same name.

Field Descriptions

The following table describes the fields on the local IGMP profile list page.

Table 162. Local IGMP Profile

| Field | Description |
|---------------------|--|
| Name | Specifies the name of the local IGMP profile. |
| Unsolicited Timeout | Specifies the time interval (in seconds) between the IGMP proxy application membership report messages to receive multicast service for a group or channel. |
| Max Response | Specifies the maximum response time (in seconds), which is used to calculate the max response code inserted into the periodic IGMP queries. |
| Keep Alive Interval | Specifies the time interval (in seconds) between the IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent by the IGMP proxy application. |
| Keep Alive Count | Specifies the number of IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent before the IGMP application assumes that there are no local members. |
| Last Query Interval | Specifies the time interval (in seconds) between the IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent by the IGMP proxy before it assumes that there are no local members for a group. |
| Last Query Count | Specifies the number of IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent before the IGMP application assumes that there are no local members. |
| Fast Leave | Specifies whether the IGMP application needs to send IGMP Group-Specific Queries^b to the individual member in the group when the leave message is received. |
| Periodic Query | Specifies if the IGMP application needs to perform periodic queries. |
| IGMP Cos | Specifies the priority bit value in the IGMP packet. |
| RA Uplink | Specifies if the IGMP application needs to add a route alert (IgmpReport, Igmpjoin, and Igmpleave) packet into the uplink packets. |

Table 162. Local IGMP Profile (continued)

| Field | Description |
|------------------------|---|
| RA Downlink | Specifies if the IGMP application needs to add a route alert (IgmpQuery) packet into the downlink packets. |
| IGMP Version to Server | Specifies the IGMP report version number to be sent to the multicast server or Broadband Network Gateway (BNG). |
| Creation Time | Specifies the date and time when the IGMP profile was created. |
| Action | Specifies the action that you can perform on the IGMP profile. The supported actions are. <ul style="list-style-type: none"> • Edit • Clone • Delete |

Creating Local IGMP Profile

Perform the following steps to create a local IGMP profile.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the OLT tab and then click the  icon from the **Local Profiles** column.

The Local Profile page appears.

3. Click on the **IGMP Profile** tab from the top left corner of the page.

The IGMP Profile List page appears.

4. Click **Create**.

The IGMP Profile Configuration page appears.

5. Complete the configuration according to the guidelines provided in the following table.

Table 163. Local IGMP Profile Configuration

| Field | Description |
|--------------|--|
| Name | Enter a unique name for the local IGMP profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Max Response | Specifies the maximum response time (in seconds), which is used to calculate the max response code inserted into the periodic IGMP queries. The accepted range is 5-12 seconds. |

| Field | Description |
|------------------------|---|
| Unsolicited Timeout | Specifies the time interval (in seconds) between the IGMP proxy application membership report messages to receive multicast service for a group or channel. |
| Keep Alive Interval | Enter the time interval (in seconds) between the IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent by the IGMP proxy application. The default value is 120 seconds. |
| Keep Alive Count | Enter the number of IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent before the IGMP application assumes that there are no local members. The default value is 3. |
| Last Query Interval | Enter the time interval (in seconds) between the IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent by the IGMP proxy before it assumes that there are no local members for a group. |
| Last Query Count | Enter the number of IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent before the IGMP application assumes that there are no local members. The default value is 2. |
| IGMP Cos | Enter the priority bit value in the IGMP packet. The value ranges from 0 to 7. The default value is 7. |
| IGMP Version to Server | Enter the IGMP report version number to be sent to the multicast server or Broadband Network Gateway (BNG). Example: v3. |
| MLD Version Server | Specifies the MLD version. The supported values are. <ul style="list-style-type: none"> ◦ v1 ◦ v2 The default value is v2. |
| Fast Leave | Enable this option if the IGMP application needs to send IGMP Group-Specific Queries^b to the individual member in the group when the leave message is received. |
| Periodic Query | Enable this option if the IGMP application needs to perform periodic queries. <ul style="list-style-type: none"> ◦ Enable. Enables the IGMP application to perform periodic queries. ◦ Disable. May cause the ONU to delete the IGMP routing table. |

| Field | Description |
|-------------|---|
| RA Uplink | Enable this option if the IGMP application needs to add a route alert (IgmpReport, Igmpjoin, and Igmpleave) packet into the uplink packets. |
| RA Downlink | Enable this option if the IGMP application needs to add a route alert (IgmpQuery) packet into the downlink packets. |

IGMP General Membership Queries^a. The IGMP query sent to all system groups (224.0.0.1). IGMP general queries are destined to the address 224.0.0.1 (all systems on a subnet).

IGMP Group Specific Queries^b. The IGMP query sent to individual members subscribed to a specific multicast group. IGMP group-specific queries are destined to the group IP address for which the device is querying.

6. Click **Create**.

A local IGMP profile configuration is created for the OLT.

To edit, clone, and delete the local IGMP profile configuration, see [Common Operations \(on page 27\)](#).

Local VNet Profile

RMS supports the following VNet profiles.

- Local VNet Profile
- Global VNet Profile

The local VNet profile is synchronized to a specific OLT, and the global VNet profile is synchronized with all the OLTs. If you want to apply the configuration on a single OLT, create a local VNet profile. If you want to apply the configuration on all the OLTs, create a global VNet profile. For more information about the global VNet profile, see [Creating VNet Profile \(on page 577\)](#).



Note: The global profile and local profile cannot have the same name.

Field Descriptions

The following table describes the fields on the local VNet profile list page.

Table 164. Local VNet Profile

| Field | Description |
|---------------|--|
| Name | Specifies the unique name of the local VNet profile. |
| SVLAN | Specifies the subscriber's S-Tag value. |
| CVLAN | Specifies the subscriber's C-Tag value. |
| Encapsulation | Specifies the type of access protocol used to establish the access link. |

Table 164. Local VNet Profile (continued)

| Field | Description |
|------------------------------|---|
| ONT Ethertype Classification | Specifies whether the ONT Ethertype is enabled. |
| Allow Transparent VLAN | Specifies the configuration to allow the transparent VLAN from RG. |
| MAC Learning Type | Specifies the MAC learning type. |
| Uni Vlan | Specifies the VLAN for UNI port. |
| Vlan Control | Specifies the VLAN tagging to be supported at the ONU and OLT. |
| Creation Time | Specifies the date and time when the VNet profile was created. |
| Action | Specifies the action that you can perform on the VNet profile. The supported actions are. <ul style="list-style-type: none"> • Edit • Clone • Delete |

Creating Local VNet Profile

Perform the following steps to create a local VNet profile.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab and then click the  icon from the **Local Profiles** column.
The Local Profile page appears.
3. Click on the **VNet Profile** tab from the top left corner of the page.
The VNet Profile page appears.
4. Click **Create**.
The VNet Profile Configuration page appears.
5. Complete the configuration according to the guidelines provided in the following table.

Table 165. Local VNet Profile Configuration

| Field | Description |
|-------|--|
| Name | Enter a unique name for the local VNet profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |

| Field | Description |
|------------------------------|---|
| SVLAN | Enter the subscriber's S-Tag value. The supported value ranges from 2 to 4094. |
| CVLAN | Enter the subscriber's C-Tag value. The supported value ranges from 2 to 4094. |
| Encapsulation | Select the type of access protocol used to establish the access link. The supported values are. <ul style="list-style-type: none"> ◦ IPoE ◦ PPPoE ◦ PPPoE-IA |
| ONT Ethertype Classification | Enable this option if the upstream traffic needs to be classified based on the Ether type. The supported values are. <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED |
| MAC Learning Type | Select the type of method to be used to learn the device MAC address. For more information on MAC Learning Type, see Table 268: MAC Learning Type (on page 580) . |
| Uni VLAN | Specifies the UNI VLAN ID. The supported value ranges from 0 to 4094. <p> Note:</p> <ul style="list-style-type: none"> ◦ The value uni vlan=0 indicates the priority tagged packet classification, which is a valid value. ◦ When uni vlan is configured, ONU is programmed to accept the tagged traffic on the UNI port with VLAN as UNI VLAN. ◦ When uni vlan is not configured, it is considered as an untagged packet configuration for the subscriber. |
| Vlan Control | Specifies the VLAN tagging to be supported at the ONU and OLT. The supported values are. <ul style="list-style-type: none"> ◦ ONU_CVLAN_OLT_SVLAN ◦ OLT_CVLAN_OLT_SVLAN ◦ ONU_CVLAN ◦ OLT_SVLAN ◦ ONU_CVLAN_ONU_SVLAN ◦ NONE |

| Field | Description |
|------------------------|--|
| Allow Transparent VLAN | Specifies the configuration to allow the transparent VLAN from RG. Indicates that the upstream traffic needs to be classified based on the Ether type. The supported values are. <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED When set to "ENABLED", the traffic from RG is passed transparently. |
| CoSQ Profile | Select the CoSQ profile from the list. |
| SVLAN TPID | Specifies the TPID that must be used with S-Tag. The supported values are. <ul style="list-style-type: none"> ◦ 0x88A8 ◦ 0x8100 The default value is 0x8100. |
| PON Hair Pinning | Specifies whether the PON hair pinning is enabled for the VLAN model. The supported values are. <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED The default value is DISABLED. |
| Remote Id Profile | Specifies the Remote ID profile name to be used to generate the RemoteID string in DHCP relay and PPPoE Intermediate Agent. |

6. Click **Create**.

A local VNet profile configuration is created for the OLT.



Note: You cannot modify the **ID** and **name** fields.

To edit, clone, and delete the local VNet profile configuration, see [Common Operations \(on page 27\)](#).

Local Bandwidth Profile

RMS supports the following bandwidth profiles.

- Local Bandwidth Profile
- Global Bandwidth Profile

The local bandwidth profile is synchronized to a specific OLT, and the global bandwidth profile is synchronized with all the OLTs. If you want to apply the configuration on a single OLT, create a local bandwidth profile. If you want to apply the configuration on all the OLTs, create a global bandwidth profile. For more information about the global bandwidth profile, see [Creating Bandwidth Profile \(on page 564\)](#).



Note: The global profile and local profile cannot have the same name.

Field Descriptions

The following table describes the fields on the local bandwidth profile list page.

Table 166. Local Bandwidth Profile

| Field | Description |
|-----------------------------------|--|
| Name | Specifies the name of the local bandwidth profile. |
| Committed Information Rate (Kbps) | Specifies the Committed Information Rate (CIR) in kilo bits per second. The configurable value ranges from 0, 255Kbps >= 10 Gbps. |
| Assured Information Rate (Kbps) | Specifies the Assured Information Rate (AIR) in kilo bits per second. The configurable value ranges from 0, 255Kbps >= 10 Gbps. |
| Excess Information Rate (Kbps) | Specifies the Excess Information Rate (EIR) in kilo bits per second. The configurable value ranges from 0, 255Kbps >= 10 Gbps. |
| Delay Tolerance | Specifies the frequency at which the containers (T-CONT) are allocated to ensure that the required user quality of experience (QoE) for the user is achieved. |
| Creation Time | Specifies the date and time when the bandwidth profile was created. |
| Action | Specifies the action that you can perform on the bandwidth profile. The supported actions are. <ul style="list-style-type: none">• Edit• Clone• Delete |



Note:

- By default, the values of CIR, AIR, and EIR are in Kbps.
- If the value of CIR, AIR, and EIR are in Gbps, the value ranges from 0 to 10 Gbps.
- The value of CIR<=AIR <=EIR.

Creating Local Bandwidth Profile

Perform the following steps to create a local bandwidth profile.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the OLT tab and then click the  icon from the **Local Profiles** column. The Local Profile page appears.
3. Click on the **Bandwidth Profile** tab from the top left corner of the page. The Bandwidth Profile page appears.
4. Click **Create**. The Bandwidth Profile Configuration page appears.
5. Complete the configuration according to the guidelines provided in the following table.

Table 167. Local Bandwidth Profile Configuration

| Field | Description |
|-----------------------------------|--|
| Name | <p>Enter a unique name for the local bandwidth profile. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Committed Information Rate (Kbps) | <p>Enter the Committed Information Rate (CIR) in kilo bits per second. The guaranteed traffic rate is committed to the subscriber with specific SLA parameters.</p> <p>0, 256Kbps<=CIR (1.25 Gbps for GPON) 0, 256Kbps<=CIR (10 Gbps for XGS-PON)</p> <p>Example: 256</p> |
| Assured Information Rate (Kbps) | <p>Enter the Assured Information Rate (AIR) in kilo bits per second.</p> <p>0, 256Kbps<=CIR (1.25 Gbps for GPON) 0, 256Kbps<=CIR (10 Gbps for XGS-PON)</p> <p>Example: 256</p> |
| Excess Information Rate (Kbps) | <p>Enter the Excess Information Rate (EIR) in kilo bits per second. The maximum traffic rate that the subscriber can receive above the CIR traffic is subject to bandwidth availability.</p> <p>0, 256Kbps<=CIR (1.25 Gbps for GPON) 0, 256Kbps<=CIR (10 Gbps for XGS-PON)</p> <p>Example: 256</p> <p> Note: The EIR value must be greater than the AIR value.</p> |
| Delay Tolerance | <p>Specifies the frequency at which the transmission containers (T-CONT) are allocated to ensure that the required user quality of experience (QoE) for the user is achieved. An operator can ensure that the user experience is not compromised by controlling the maximum latency between two consecutive grants at the OLT.</p> <p>The supported value ranges from 0 to 128. The unit is in the number of bandwidth frames.</p> |

| Field | Description |
|-------|---|
| | The default value is zero if not configured. The value zero means that no specific latency is required for service. |

6. Click **Create**.

A local bandwidth profile configuration is created for the OLT.

To edit, clone, and delete the local bandwidth profile configuration, see [Common Operations \(on page 27\)](#).

Local Shaper Profile

RMS supports the following shaper profiles.

- Local Shaper Profile
- Global Shaper Profile

The local shaper profile is synchronized to a specific OLT, and the global shaper profile is synchronized with all the OLTs. If you want to apply the configuration on a single OLT, create a local shaper profile. If you want to apply the configuration on all the OLTs, create a global shaper profile. For more information about the global shaper profile, see [Creating Shaper Profile \(on page 567\)](#).



Note: The global profile and local profile cannot have the same name.

Field Descriptions

The following table describes the fields on the local shaper profile list page.

Table 168. Local Shaper Profile

| Field | Description |
|-----------------------------------|---|
| Name | Specifies the name of a local shaper profile. |
| Committed Information Rate (Kbps) | Specifies the Committed Information Rate (CIR) in kilo bits per second. The configurable value ranges from 0 Kbps >= 10 Gbps. |
| Excess Information Rate (Kbps) | Specifies the Excess Information Rate (EIR) in kilo bits per second. The configurable value ranges from 0 Kbps >= 10 Gbps. |
| Committed Burst Size (KB) | Specifies the committed burst size. |
| Creation Time | Specifies the date and time when the shaper profile was created. |
| Action | Specifies the action that you can perform on the shaper profile. The supported actions are. |

Table 168. Local Shaper Profile (continued)

| Field | Description |
|-------|---|
| | <ul style="list-style-type: none"> • Edit • Clone • Delete |

**Note:**

- By default, the values of CIR and EIR are in Kbps.
- If the value of CIR and EIR are in Gbps, the value ranges from 0 to 10 Gbps.
- The value of CIR <=EIR.

Creating Local Shaper Profile

Perform the following steps to create a local shaper profile.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the OLT tab and then click the  icon from the **Local Profiles** column.

The Local Profile page appears.

3. Click on the **Shaper Profile** tab from the top left corner of the page.

The Shaper Profile page appears.

4. Click **Create**.

The Shaper Profile Configuration page appears.

5. Complete the configuration according to the guidelines provided in the following table.

Table 169. Local Shaper Profile Configuration

| Field | Description |
|-----------------------------------|---|
| Name | <p>Enter a unique name for the local shaper profile. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Committed Information Rate (Kbps) | <p>The Committed Information Rate (CIR) is the minimum guaranteed rate for traffic that the ONT provides for the particular Ethernet service. CIR defines the average rate in bytes of packets up to which the network delivers and meets the performance objectives defined by the Class of Service (CoS) service attribute.</p> <p>The CIR value must be ≥ 0.</p> |

| Field | Description |
|--------------------------------|---|
| | The unit is in kilobits per second. |
| Excess Information Rate (Kbps) | Enter the Excess Information Rate (EIR). EIR is the maximum allowed traffic during non-busy times without any guarantee. The unit is in kilo bits per second.  Note: The EIR value must be ≥ 0 or $EIR \geq CIR$. |
| Committed Burst Size | Enter the committed burst size in kilobytes. CBS limits the maximum number of bytes available for a burst of packets sent at the UNI speed to remain CIR-conformant. The CBS value must be ≥ 0 (0 to 10000000). The unit is in kilobytes. |

6. Click **Create**.

A local shaper profile configuration is created for the OLT.



Note: You cannot modify the **ID** and **name** fields.

To edit, clone, and delete the local shaper profile configuration, see [Common Operations \(on page 27\)](#).

Local COSQ Profile

RMS supports the following COSQ profiles.

- Local COSQ Profile
- Global COSQ Profile

The local COSQ profile is synchronized to a specific OLT, and the global COSQ profile is synchronized with all the OLTs. If you want to apply the configuration on a single OLT, create a local COSQ profile. If you want to apply the configuration on all the OLTs, create a global COSQ profile. For more information about the global COSQ profile, see [Creating COSQ Profile \(on page 570\)](#).



Note: The global profile and local profile cannot have the same name.

Field Descriptions

The following table describes the fields on the local COSQ profile list page.

Table 170. Local COSQ Profile

| Field | Description |
|---------------------------|---|
| Name | Specifies the name of the local COSQ profile. |
| Default DSCP Pbit Marking | Specifies the default DSCP pbit that needs to be marked. |
| Creation Time | Specifies the date and time when the packet queue configuration was created. |
| Action | Specifies the action that you can perform on the COSQ profile. The supported actions are. <ul style="list-style-type: none"> • Edit • Clone • Delete |

Creating Local COSQ Profile

Perform the following steps to create a local COSQ profile.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab and then click the  icon from the **Local Profiles** column.
The Local Profile page appears.
3. Click on the **COSQ Profile** tab from the top left corner of the page.
The COSQ Profile page appears.
4. Click **Create**.
The COSQ Profile Configuration page appears.
5. Complete the configuration according to the guidelines provided in the following table.

Table 171. Local COSQ Profile Configuration

| Field | Description |
|-------|--|
| Name | Enter a unique name for the local COSQ profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| DSCP | Enter the default DSCP pbit value that needs to be marked. This applies to DSCP values that are not mentioned in the "dscp" field. The value ranges from 0 to 7. |

| Field | Description |
|-------------------------------|---|
| | <p>The value 0 is the lowest precedence and the value 7 is the highest precedence.</p> <p> Note: This field is disabled if you select Ether Type.</p> |
| Ether Type | <p>Enter the default ether type pbit value that needs to be marked. This applies to Ethertype values that are not mentioned in the "Ether Type" field.</p> <p>The value ranges from 0 to 7.</p> <p> Note: This field is disabled if you select DSCP.</p> |
| Configure Packet Queue | |
| Scheduler Config Policy | <p>Select the scheduler configuration policy from the list. The supported values are.</p> <ul style="list-style-type: none"> ◦ Weighted Round Robin. In WRR mode, the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight, the more frames are sent). The queues are serviced until their quota is used and then another queue is serviced. ◦ Strict Priority. Egress traffic from the highest priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue is transmitted, which provides the highest level of priority of traffic to the highest numbered queue. The priority sets the order in which queues are serviced, starting with queue 8 (the highest priority queue) and going to the next lower queue when each queue is completed. |
| Discard Config Policy | <p>Select the packet discard policy followed in the access network. The supported values are.</p> <ul style="list-style-type: none"> ◦ Tail Drop. In tail drop, when the queue is filled to its maximum capacity, the newly arriving packets are dropped until the queue has enough room to accept the incoming traffic. ◦ Random Early Detection (RED). The RED preemptively drop packets before the buffer becomes completely full. It uses predictive models to decide which packets to drop. ◦ Weighted Random Early Detection (WRED). The weighted RED supports different probabilities for different priorities (IP precedence and DSCP) and/or queues. |

| Field | Description |
|------------------------------------|--|
| Discard Config Maximum Queue Size | <p>Enter the maximum size of the packet queue. The unit is in packet count. This field is used when the discard policy is selected as Tail Drop. The value depends on the available memory as to how many packets the queue can take. The default value is auto. Otherwise, it takes the size of the queue.</p> |
| Discard Config Minimum Threshold | <p>Enter the minimum threshold value for the packet queue. This field is configured only when the discard policy is selected as RED or WRED. The unit is in packet count.</p> |
| Discard Config Maximum Threshold | <p>Enter the maximum threshold value for the packet queue. This field is configured only when the discard policy is selected as RED or WRED. The unit is in packet count.</p> |
| Discard Config Maximum Probability | <p>Enter the maximum probability value for the packet queue. This field configured only when the discard policy is selected as RED or WRED. The unit is in percentage. The value ranges from 0 to 100.</p> |
| Traffic Class Config | <p>Click on the Traffic Class Config option to add the traffic class configuration.</p> |
| Allowed Pbits | <p>Specifies the list of allowed p-bits. The values of all pbits mentioned in the "default_dscp_pbit_marking" and "pbit" fields must be specified in this field. Any other value other than the pbit would be for non-dscp-to-pbit packets.</p> <p>Example: 1 2 3</p> <p>The pbits configured in allowed the pbits are allowed in the data path. In addition to this, the allowed pbits can be used to configure pbit remarking.</p> <p>Example: 0-7:2</p> <ul style="list-style-type: none"> ◦ If the pbit remarking is configured in the upstream CoSQ profile, the traffic that comes from RG with any pbit (0-7) is remarked to pbit 2. ◦ If the pbit remarking is configured in the downstream CoSQ profile, the traffic comes from BNG with any pbit (0-7) is remarked to pbit 2. <p>Example: 1:2</p> |

| Field | Description |
|------------------------|---|
| | <ul style="list-style-type: none"> ◦ If the pbit remarking is configured in the upstream CoSQ profile, the traffic that comes from RG with pbit 1 is remarked to pbit 2. ◦ If the pbit remarking is configured in the downstream CoSQ profile, it becomes invalid. <p> Note: Only any pbit to the single pbit is allowed in the downstream CoSQ profile.</p> <p>You can delete the traffic class configuration using the Delete icon.</p> |
| DSCP Pbit Marking | <p>Click on the DSCP Pbit Marking to add the DSCP to p-bit mapping configuration. You can add one or more DSCP pbit marking configuration. When you click on this field, the “DSCP” and “PBIT” fields are displayed.</p> <p>You can delete the DSCP pbit marking configuration using the Delete icon.</p> <p> Note:</p> <ul style="list-style-type: none"> ◦ A user can configure one or more DSCP mappings for each PBIT for each queue. ◦ This field is disabled if you select Ethertype Pbit Marking. |
| DSCP | <p>Specifies the DSCP values associated with packet queues. The associated value can be a range or an individual DSCP value. The maximum value allowed is 63.</p> <p>Example: ["0-5", "8-12", and "16"]</p> <p>The supported value ranges from 0 to 63.</p> <p> Note: You must use the hyphen (-) to specify the range.</p> |
| PBIT | <p>Specifies the priority bit associated with packet queues. The value ranges from 0 to 7. The value 0 indicates the lowest PBIT and the value 7 indicates the highest PBIT.</p> <p>Example: 0</p> |
| Ethertype Pbit Marking | <p>Click on the Ethertype Pbit Marking to add the Ethertype to p-bit mapping configuration. You can add one or more Ethertype pbit marking configuration. When you click on this field, the “Ethertype” and “PBIT” fields are displayed.</p> <p>You can delete the Ethertype pbit marking configuration using the Delete icon.</p> |

| Field | Description |
|-----------|---|
| |  Note: <ul style="list-style-type: none"> ◦ A user can configure one or more Ethertype mappings for each PBIT for each queue. ◦ This field is disabled if you select DSCP Pbit Marking. |
| Ethertype | <p>Specifies the Ethertype values associated with packet queues. The supported values are.</p> <ul style="list-style-type: none"> ◦ ARP. Enables CBAC to use the same pbit for IPoE and IPv6 internally. ◦ IPoE. Enables CBAC to use the same pbit for ARP and IPv6 internally. ◦ IPv6. Enables CBAC to use the same pbit for ARP and IPoE internally. ◦ PPPoE. Other strings are not allowed to be configured. |
| PBIT | <p>Specifies the priority bit associated with packet queues. The value ranges from 0 to 7. The value 0 indicates the lowest PBIT and the value 7 indicates the highest PBIT.</p> <p>Example: 0</p> |

6. Click **Create**.

A local COSQ profile configuration is created for the OLT.

To edit, clone, and delete the local COSQ profile configuration, see [Common Operations \(on page 27\)](#).

Local MEP Profile

RMS supports the following MEP profiles.

- Local MEP Profile
- Global MEP Profile

The local MEP profile is synchronized to a specific OLT, and the global MEP profile is synchronized with all the OLTs. If you want to apply the configuration on a single OLT, create a local MEP profile. If you want to apply the configuration on all the OLTs, create a global MEP profile. For more information about the global MEP profile, see [Creating MEP Profile \(on page 550\)](#).



Note: The global profile and local profile cannot have the same name.

Field Descriptions

The following table describes the fields on the local MEP profile list page.

Table 172. Local MEP Profile

| Field | Description |
|-------------------|---|
| Name | Specifies the name of the local MEP profile. |
| Association Type | Specifies the maintenance association name type |
| Association Name | Specifies the maintenance association name. |
| CCM Interval Unit | Specifies the unit for the Continuity Check Messages (CCMs) interval. |
| CCM Interval | Specifies the interval at which CCMs are sent. |
| Remote MEP Id | Specifies the remote MEP ID. |
| Local MEP Id | Specifies the local MEP ID. |
| Control VLAN | Specifies the control VLAN ID of the MEP. |
| MD Level | Specifies the level of the maintenance domain. |
| Creation Time | Specifies the date and time when the packet queue configuration was created. |
| Action | Specifies the action that you can perform on the COSQ profile. The supported actions are. <ul style="list-style-type: none">• Edit• Clone• Delete |

Creating Local MEP Profile

Perform the following steps to create a local MEP profile.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the OLT tab and then click the  icon from the **Local Profiles** column.

The Local Profile page appears.

3. Click on the **MEP Profile** tab from the top left corner of the page.

The MEP Profile page appears.

4. Click **Create**.

The MEP Profile Configuration page appears.

5. Complete the configuration according to the guidelines provided in the following table.

Table 173. Local MEP Profile Configuration

| Field | Description |
|-----------------------|---|
| Name | Enter a unique name for the local MEP profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Association Name Type | Specifies the maintenance association name type. The supported types are. <ul style="list-style-type: none"> ◦ Character-string ◦ Unsigned-integer |
| Association Name | Specifies the maintenance association name. <ul style="list-style-type: none"> ◦ If the association name type is selected as 'character-string', then the association name type must be alphabets or alphanumeric string. The name length must be 1 to 45 characters. ◦ If the association name type is selected as 'unsigned-integer', then the association name type must be Uint16. The value ranges from 0 to 65,535. |
| CCM Interval Unit | Specifies the unit for CCMs interval. The supported values are. <ul style="list-style-type: none"> ◦ Milliseconds ◦ Seconds ◦ Minutes The default value is seconds. |
| CCM Interval | Specifies the interval at which CCMs are sent. The supported values are. <ul style="list-style-type: none"> ◦ 3.3, 10, and 100 (If the ccm interval unit is in milliseconds) ◦ 1 and 10 (If the ccm interval unit is in seconds) ◦ 1 and 10 (If the ccm interval unit is in minutes) The default value is 1. |
| Remote MEP ID | Specifies the remote MEP ID. The value ranges from 1 to 8191. |
| Local MEP ID | Specifies the local MEP ID. The value ranges from 1 to 8191. |
| Control VLAN | Specifies the control VLAN ID of the MEP. The value ranges from 2 to 4094. |
| MD Level | Specifies the maintenance domain level. The value ranges from 0 to 7. The default value is 7. |

6. Click **Create**.

A local MEP profile configuration is created for the OLT.

To edit, clone, and delete the local MEP profile configuration, see [Common Operations \(on page 27\)](#).

Local NTP Profile

RMS supports the following NTP profiles.

- Local NTP Profile
- Global NTP Profile

The local NTP profile is synchronized to a specific OLT, and the global NTP profile is synchronized with all the OLTs. If you want to apply the configuration on a single OLT, create a local NTP profile. If you want to apply the configuration on all the OLTs, create a global NTP profile. For more information about the global NTP profile, see [Creating Local NTP Profile \(on page 363\)](#).



Note: The global profile and local profile cannot have the same name.

Field Descriptions

The following table describes the fields on the local NTP profile list page.

Table 174. Local NTP Profile

| Field | Description |
|---------------|--|
| Name | Enter a unique name for the NTP profile. |
| Server | |
| Host | Specifies the IP address (IPv4 or IPv6) of the NTP server or FQDN of the NTP server. |
| Preferred | Specifies if the NTP server host is the preferred server in the NTP server pool. |

Creating Local NTP Profile

Perform the following steps to create a local NTP profile.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the OLT tab and then click the



icon from the **Local Profiles** column.

The Local Profile page appears.

3. Click on the **NTP Profile** tab from the top left corner of the page.

The NTP Profile page appears.

4. Click **Create**.

The NTP Profile Configuration page appears.

5. Complete the configuration according to the guidelines provided in the following table.

Table 175. Local NTP Profile Configuration

| Field | Description |
|---------------|--|
| Name | Enter a unique name for the NTP profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">Underscore (_)Hyphen (-) |
| Server | |
| Host | Specifies the IP address (IPv4 or IPv6) of the NTP server or FQDN of the NTP server. |
| Preferred | Specifies if the NTP server host is the preferred server in the NTP server pool. This host must be chosen for synchronization among a set of correctly operating hosts. |

6. Click **Create**.

A local NTP profile configuration is created for the OLT.

To edit, clone, and delete the local NTP profile configuration, see [Common Operations \(on page 27\)](#).

Local ERPS Profile

RMS supports the following ERPS profiles.

- Local ERPS Profile
- Global ERPS Profile

The local ERPS profile is synchronized to a specific OLT, and the global ERPS profile is synchronized with all the OLTs. If you want to apply the configuration on a single OLT, create a local ERPS profile. If you want to apply the configuration on all the OLTs, create a global ERPS profile. For more information about the global ERPS profile, see [Creating ERPS Profile \(on page 546\)](#).



Note: The global profile and local profile cannot have the same name.

Field Descriptions

The following table describes the fields on the local ERPS profile list page.

Table 176. Local ERPS Profile

| Field | Description |
|-------|---|
| Name | Specifies the name of the local ERPS profile. |

Table 176. Local ERPS Profile (continued)

| Field | Description |
|----------------|---|
| Control VLAN | Specifies the ERPS profile control VLAN. |
| Mode | Specifies the ERPS profile data VLAN list. |
| East Port Role | Specifies the ERPS east port role. |
| West Port Role | Specifies the ERPS west port role. |
| Creation Time | Specifies the date and time when the ERPS profile was created. |
| Action | Specifies the action that you can perform on the ERPS profile. The supported actions are. <ul style="list-style-type: none"> • Edit • Clone • Delete |

Creating Local ERPS Profile

Perform the following steps to create a local ERPS profile.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab and then click the  icon from the **Local Profiles** column.
The Local Profile page appears.
3. Click on the **ERPS Profile** tab from the top left corner of the page.
The ERPS Profile page appears.
4. Click **Create**.
The ERPS Profile Configuration page appears.
5. Complete the configuration according to the guidelines provided in the following table.

Table 177. Local ERPS Profile Configuration

| Field | Description |
|----------------|--|
| Name | Enter a unique name for the local ERPS profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Control VLAN | Enter the ERPS profile control VLAN. The value ranges from 2 to 4094. |
| Data VLAN List | Enter the ERPS profile data VLAN list. The value ranges from 2 to 4094. |

| Field | Description |
|-----------------------------|---|
| Mode | <p>Specifies the mode of the ERPS ring protection. The supported values are.</p> <ul style="list-style-type: none">◦ REVERTIVE◦ NON-REVERTIVE |
| East Port Role | <p>Enter the ERPS east port role. The supported values are.</p> <ul style="list-style-type: none">◦ Ring Protection Link (RPL)◦ NORMAL◦ NEIGHBOUR◦ NEXT-NEIGHBOUR |
| West Port Role | <p>Enter the ERPS west port role. The supported values are.</p> <ul style="list-style-type: none">◦ RPL◦ NORMAL◦ NEIGHBOUR◦ NEXT-NEIGHBOUR |
| Guard Timer (ms) | <p>Enter the ERPS guard timer value in milliseconds. All the Ethernet ring nodes uses this time while changing the state. This timer blocks the latent outdated messages from causing unnecessary state changes. The value ranges from 10 ms to 2000 ms. The default value is 500 ms.</p> |
| Wait-to-Restore Timer (min) | <p>Enter the ERPS restore timer value in minutes.</p> <ul style="list-style-type: none">◦ After a signal failure, this timer verifies that the signal failure is not intermittent.◦ After a forced switch or manual switch, this timer verifies that no background condition exists. <p>The value ranges from 1 to 12 minutes. The default value is 5 minutes.</p> |
| Hold off Times (ms) | <p>Enter the ERPS hold off timer value. This timer is used by the underlying Ethernet layer to filter out intermittent link faults. The value ranges from 0 to 10000 ms. The default value is 0 ms.</p> |
| Wait-to-Block Timer (ms) | <p>Enter the ERPS wait to block timer value. The default is value 5500 ms. The value ranges from 0 to 86400000 ms.</p> |
| R-APS Intervals (ms) | <p>Enter the ERPS R-APS interval value. The default value is 5000 ms. The value ranges from 10 to 3600000 ms.</p> |

6. Click **Create**.

A local ERPS profile configuration is created for the OLT.

To edit, clone, and delete the local ERPS profile configuration, see [Common Operations \(on page 27\)](#).

Local IP Host Profile

RMS supports the following IP Host profiles.

- Local IP Host Profile
- Global IP Host Profile

The local IP Host profile is synchronized to a specific OLT, and the global IP Host profile is synchronized with all the OLTs. If you want to apply the configuration on a single OLT, create a local IP Host profile. If you want to apply the configuration on all the OLTs, create a global IP Host profile. For more information about the global IP Host profile, see [Creating IP Host Profile \(on page 549\)](#).



Note: The global profile and local profile cannot have the same name.

Field Descriptions

The following table describes the fields on the local IP Host profile list page.

Table 178. IP Host Profile List

| Field | Description |
|---------------------|---|
| Name | Specifies the name of the local IP host profile. |
| Type | Specifies the type of the local IP host profile. |
| Enable DHCP | Specifies whether to enable DHCP. |
| Network Mask | Specifies the network mask of static IP address of the IP host interface. |
| Gateway | Specifies the gateway static IP address of the IP host interface. |
| Primary DNS | Specifies the primary DNS static IP address of the IP host interface. |
| Secondary DNS | Specifies the secondary DNS static IP address of the IP host interface. |
| ONT Identifier | Specifies the ONT identifier. |
| Relay Agent Options | Specifies one or more DHCP relay agent options. |
| IPv6 Options | Specifies whether to enable DHCPv6 and router solicitation. |
| Default Router | Specifies the default router IPv6 address of the IPv6 host interface. |
| On Link Prefix | Specifies the IPv6 prefix. |

Table 178. IP Host Profile List (continued)

| Field | Description |
|---------------|--|
| Creation Time | Specifies the date and time when the IP host profile was created. |
| Action | Specifies the action that you can perform on the IP host profile. The supported actions are. <ul style="list-style-type: none"> • Edit • Clone • Delete |

Creating Local IP Host Profile

Perform the following steps to create a local IP Host profile.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the OLT tab and then click the  icon from the **Local Profiles** column.

The Local Profile page appears.

3. Click on the **IP Host profile** tab from the top left corner of the page.

The IP Host Profile page appears.

4. Click **Create**.

The IP Host Profile Configuration page appears.

5. Complete the configuration according to the guidelines provided in the following table.

Table 179. Local IP Host Profile Configuration

| Field | Description |
|-------------|---|
| Name | Enter a unique name for the local IP host profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Type | Specifies the type of the local IP host profile. Example: IPv4 or IPv6. |
| Enable DHCP | Specifies whether to enable DHCP. <ul style="list-style-type: none"> ◦ If this option is enabled, the IP interface of the ONT is learned dynamically. ◦ If this option is disabled, the following options must be configured. |

| Field | Description |
|---------------------|---|
| | <ul style="list-style-type: none"> ▪ Network Mask ▪ Gateway |
| Network Mask | <p>Enter the network mask static IP address of the IP host interface. This is mandatory if the Enable DHCP field is disabled.</p> <p>Example: 255.255.255.0</p> |
| Gateway | <p>Enter the gateway static IP address of the IP host interface. This is mandatory if the Enable DHCP field is disabled.</p> <p>Example: 172.27.172.254</p> |
| Primary DNS | <p>Enter the primary DNS static IP address of the IP host interface. This is applicable on the ONT, if the DHCP is disabled.</p> <p>Example: 172.27.173.101</p> |
| Secondary DNS | <p>Enter the secondary DNS static IP address of the IP host interface. This is applicable on the ONT, if the DHCP is disabled.</p> <p>Example: 172.27.173.102</p> |
| ONU Identifier | <p>Enter the ONU identifier, which is used (instead of MAC address) to retrieve the DHCP parameters.</p> <p>The maximum length is 25 characters.</p> <p>Example: voice-service</p> |
| Relay Agent Options | Enter one or more DHCP relay agent options. |
| IPv6 Options | <p>Specifies whether to enable DHCPv6 and router solicitation. The supported values are.</p> <ul style="list-style-type: none"> ◦ DHCPv6 ◦ Router-Solicitation ◦ DHCPv6andRouterSolicitation ◦ Disable <p>When it is configured as Disable, the IPv6 address from Add IPv6-Host interface API and all the following parameters must be configured.</p> <ul style="list-style-type: none"> ◦ default_router ◦ primary_dns ◦ secondary_dns ◦ on_link_prefix |
| Default Router | Specifies the default router IPv6 address of the IPv6 host interface. This is mandatory if the IPv6 Options parameter is disabled. |

| Field | Description |
|----------------|---|
| On Link Prefix | Specifies the IPv6 prefix. The prefix must be in <i>prefixstring:/prefixlength</i> format, where, the prefix string is 16 bytes and prefix length is 1 byte. This is mandatory if the IPv6 Options parameter is disabled. |

6. Click **Create**.

A new IP host profile is created on the IP Host Profile List page.

To edit, clone, and delete the local IP Host profile configuration, see [Common Operations \(on page 27\)](#).

Local Alarm Soak Profile

RMS supports the following alarm soak profiles.

- Local alarm soak Profile
- Global alarm soak Profile

The local alarm soak profile is synchronized to a specific OLT, and the global alarm soak profile is synchronized with all the OLTs. If you want to apply the configuration on a single OLT, create a local alarm soak profile. If you want to apply the configuration on all the OLTs, create a global alarm soak profile. For more information about the global alarm soak profile, see [Creating Alarm Soak Profile \(on page 371\)](#).



Note: The global profile and local profile cannot have the same name.

Field Descriptions

The following table describes the fields on the local alarm soak profile list page.

Table 180. Local Alarm Soak Profile

| Field | Description |
|----------------------------------|--|
| Name | Enter a unique name for the alarm soak profile. |
| Global Default Soak Period Raise | Specifies the soak duration before raising the alarm. |
| Global Default Soak Period Clear | Specifies the soak duration before clearing the reported alarm. |
| Alarms | Specifies the list of supported alarms. |
| Resource Type | Specifies resource type if the same alarm name is used for multiple resource types. This field is applicable if the same alarm name is used for multiple resource types. |

Table 180. Local Alarm Soak Profile (continued)

| Field | Description |
|-------------------------|--|
| Soak Raise Period (Sec) | Enter the value to update the field for that specific alarm other than Global Default Soak Period Raise . |
| Soak Clear Period (Sec) | Enter the value to update the field for that specific alarm other than Global Default Soak Period Clear . |

Creating Alarm Soak Profile

Perform the following steps to create a local alarm soak profile.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab and then click the  icon from the **Local Profiles** column.
The Local Profile page appears.
3. Click on the **Alarm Soak Profile** tab from the top left corner of the page.
The Alarm Soak Profile page appears.
4. Click **Create**.
The Alarm Soak Profile Configuration page appears.
5. Complete the configuration according to the guidelines provided in the following table.

Table 181. Local Alarm Soak Profile Configuration

| Field | Description |
|----------------------------------|--|
| Name | Enter a unique name for the alarm soak profile. The following special characters are supported. <ul style="list-style-type: none"> Underscore (_) Hyphen (-) |
| Global Default Soak Period Raise | Specifies the soak duration before raising the alarm. The default value is 2.5. The supported value ranges from 0 to 3600. |
| Global Default Soak Period Clear | Specifies the soak duration before clearing the reported alarm. The default value is 10. The supported value ranges from 0 to 3600. |
| Alarms | Specifies the list of supported alarms. |
| Resource Type | Specifies resource type if the same alarm name is used for multiple resource types. This field is applicable if the same alarm name is used for multiple resource types. |

| Field | Description |
|-------------------------|---|
| | <p>The same soak period configuration is applied for all resource types if this field is not provided.</p> <p>For example:</p> <p>Name: LOSS-OF-SIGNAL resource_type: ME-PORT/ONT</p> |
| Soak Raise Period (Sec) | Enter the value to update the field for that specific alarm other than Global Default Soak Period Raise . |
| Soak Clear Period (Sec) | Enter the value to update the field for that specific alarm other than Global Default Soak Period Clear . |

6. Click **Create**.

A local alarm soak profile configuration is created for the OLT.

To edit, clone, and delete the local alarm soak profile configuration, see [Common Operations \(on page 27\)](#).

Viewing PON and NNI Ports

You can view the PON and NNI ports configured for the OLT. The PON and NNI ports are retrieved from the CARD device profile once the OLT activation is successful.

OLT monitors both PON and NNI ports and reports the status of the ports to RMS. RMS reports the port status using RMS and events. You can also activate and deactivate the ports.

Perform the following steps to view the list of PON and NNI ports configured for the OLT.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the **OLT** tab.

3. Click on the ports () icon corresponding to the OLT on which you want to view the port details.

The *Ports List [Inventory - OLT Name]* page appears with the list of port details.

Tasks

You can perform the following tasks from this page.

- Activate the port. See [Activating the PON and NNI Port \(on page 380\)](#).
- Deactivate the port. See [Deactivating the PON and NNI Port \(on page 381\)](#).
- Initiate and cancel the MAC dump on PON and NNI port. See [Initiate and Cancel MAC Dump on PON and NNI Port \(on page 381\)](#).
- Perform MAC lookup for NNI port. See [MAC Lookup for NNI Port \(on page 383\)](#).

- View the operational state of the port by clicking the Logical Topology option.
- Edit PON and NNI port configuration. See [Editing PON Port Configuration \(on page 375\)](#).
- Export PON and NNI port details. See [Exporting PON and NNI Port Information \(on page 385\)](#).
- View the physical link list of the port. See [Viewing Physical Link List of the OLT or ONT \(on page 386\)](#).
- Add member port to LAG. See [Adding Member Port to LAG \(on page 383\)](#).
- Remove member port from LAG. See [Removing Member Port from LAG \(on page 384\)](#).

Field Descriptions

The following table describes the fields on the Ports List [Inventory List - *OLT Name*] page.

Table 182. OLT Ports List

| Field | Description |
|-------------------|---|
| Name | Specifies name of the port. The port can be either NNI or PON port. Example: NNI-1 |
| Admin State | Specifies the admin state of the port. The supported values are. <ul style="list-style-type: none">• ACTIVE• DEACTIVE |
| Operational State | Specifies the operational state of the PON or NNI port. The supported values are. <ul style="list-style-type: none">• UP• DOWN• UNKNOWN |
| Media | Specifies the media type of the port. The supported values are. <ul style="list-style-type: none">• PON• ETHERNET• LTE• VOICE PORT |
| Display ID | Specifies the display ID of the port. Example: card1/port=1 |
| Port No | Specifies the port number associated with the OLT. Example: 4 |
| Port Direction | Specifies the port direction type. The supported values are. |

Table 182. OLT Ports List (continued)

| Field | Description |
|---|---|
| | <ul style="list-style-type: none"> • UNI • NNI • ANY |
| Capacity | Specifies the capacity of the port. Example: 1 |
| Unit | Specifies the unit of capacity of the port. The supported values are. <ul style="list-style-type: none"> • Megabit • Gigabit |
| Description | Specifies the description of the port. |
| PON Encryption Enabled | Specifies PON encryption. The OLT supports the PON downstream unicast encryption. |
| PON Encryption Key Interval | This field is displayed only when the “PON Encryption Enabled” field is selected. Specifies the PON encryption key exchange interval in milliseconds. The default value is 3600000 milliseconds (1 hour). If this field is configured as ‘0’, one-time key exchange is considered. However, for the security, always periodic key exchange is recommended. |
| ONT Capacity | Specifies the number of ONTs can be configured on the PON port based on the PON technology. The supported value ranges from 1 to 2000. You cannot decrease the value for ONT capacity after configuration. |
| Inventory System ID | Enter the inventory system ID. Example: 1/1/1/4 |
| Auto-negotiation | Specifies whether the auto-negotiation is enabled. |
| Periodic Rogue ONT Detection Control | Select whether the periodic rogue ONT detection needs to be enabled. The supported values are. <ul style="list-style-type: none"> • ENABLED • DISABLED The default value is ENABLED. |
| Periodic Rogue ONT Detection Measurement Type | Select the RSSI measurement window type. The supported values are. <ul style="list-style-type: none"> • SILENT-WINDOW. Detects and identifies an ONU that is responding to allocations belonging to another ONT but detects most other types of rogue ONT behavior. • CUTOFF-WINDOW. Detects an ONT that stops the laser transmit later than it should, potentially interfering with the next allocation. |

Table 182. OLT Ports List (continued)

| Field | Description |
|---|---|
| | The default value is SILENT-WINDOW. |
| Alloc Type to Scan | Select the alloc ID type to scan. The supported values are. <ul style="list-style-type: none"> UNUSED. AllocIDs that are currently not in use (not yet assigned to any ONTs). PREVIOUSLY-USED. AllocIDs that are used once and cleared. ALL. Scan both unused and previously used AllocIDs. The default value is PREVIOUSLY-USED. |
| Periodic Rogue ONU Detection Interval (in milliseconds) | Enter the periodic rogue ONU detection procedure initiation interval in milliseconds. The value ranges from 1000 to 10000000. The default value is 1000. |
| MTU Size | Specifies the maximum transmission unit (MTU) size in bytes on the OLT port. |
| Creation Time | Specifies the date and time when the PON or NNI port was created. |
| Action | Specifies an action that can be performed on the port. The supported action is Edit. |

Editing PON Port Configuration

After the successful creation of the PON port, a port ID is automatically generated.

Perform the following steps to modify the parameters configured for the port.

1. Select **Configuration > Inventory**.
2. Navigate to the OLT tab.
3. Click on the ports (grid) icon.
The *Ports List [Inventory - OLT Name]* page appears with the list of port details.
4. Click the edit icon corresponding to the PON port from the **Action** column.

The Port Configuration page appears, displaying the existing configuration information.



Note:

- You cannot edit the following fields on PON port configuration page.
 - ID
 - Name
 - Port
 - Display ID



- Port Media
- Port Direction
- Discovered Port Mode
- DBA Mode
- Capacity
- The **Admin State** of the PON port must be **DEACTIVE** to update the following fields.
 - Configured Port Mode
 - GPON Downstream FEC
 - XGSPON Downstream FEC
 - Enable PON Encryption
 - PON Encryption Key Interval

You can modify the following fields of the PON configuration according to the guidelines provided in the following table.

Table 183. PON Port Configuration

| Field | Description |
|--|--|
| Description | Enter a meaningful description about the PON or NNI port configuration. |
| Enable PON Encryption | Specifies PON encryption. The OLT supports the PON downstream unicast encryption. |
| PON Encryption Key Interval (milliseconds) | This field is displayed only when the “PON Encryption Enabled” field is selected. Enter the PON encryption key exchange interval in milliseconds. The default value is 3600000 milliseconds (1 hour). If this field is configured as ‘0’, a one-time key exchange is considered. However, for security, a periodic key exchange is always recommended. |
| Configured Port Mode | Configured Port Mode Select the configured port mode from the list. The supported values are. <ul style="list-style-type: none">◦ Auto◦ GPON◦ XGSPON◦ CPON The default value is Auto. |



Note:

| Field | Description |
|-----------------------|--|
| |  <ul style="list-style-type: none"> ◦ You can configure and change PON port modes based on your requirements without rebooting or restarting the OLT. ◦ If the port mode is Auto or CPON, the default value for GPON and XGSPON Downstream FEC is DISABLED and ENABLED respectively. ◦ If the port mode is GPON, the default value for GPON Downstream FEC is DISABLED. XGSPON Downstream FEC option is grayed out and cannot be selected. ◦ If the port mode is XGSPON, the default value for XGSPON Downstream FEC is ENABLED. GPON Downstream FEC option is grayed out and cannot be selected. |
| Discovered Port Mode | <p>This field is not configurable. The default value is GPON.</p> <p> Note:</p> <ul style="list-style-type: none"> ◦ If the configured port mode is auto, the discovered port mode is selected as GPON. ◦ If the configured port mode is non-auto, the discovered port mode is the same as the configured port mode. |
| GPON Downstream FEC | <p>Specifies whether the Forward Error Correction (FEC) is enabled in the downstream traffic for GPON port. This field is applicable for GPON and CPON port mode. The supported values are:</p> <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED <p>The default value for GPON Downstream FEC is DISABLED.</p> |
| XGSPON Downstream FEC | <p>Specifies whether the Forward Error Correction (FEC) is enabled in the downstream traffic for XGSPON port. This field is applicable for XGSPON and CPON port mode. The supported values are:</p> <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED <p>The default value for XGSPON Downstream FEC is ENABLED.</p> |
| Capacity Type | <p>Select the capacity type from the list. The supported values are.</p> <ul style="list-style-type: none"> ◦ Megabit ◦ Gigabit |

| Field | Description |
|--------------------------------------|--|
| Inventory System ID | Enter the inventory system ID. Example: 1/1/1/4 |
| Maximum Logical Distance | Specifies the maximal logical distance in kilometers between the ONU and the OLT on the PON port. The supported value ranges from 0 to 60. The default value is 20. |
| Maximum Differential Reach | Specifies the maximum distance in kilometers between the closest ONU to the farthest ONU from the OLT. The value ranges from 0 to 40. The default value is 20. |
| ONT Capacity | Specifies the number of ONTs can be configured on the PON port based on the PON technology. The supported value ranges from 1 to 384. You cannot decrease the value for ONT capacity after configuration. |
| GPON Multicast Shaper Profile | Select the multicast shaper profile. This field is applicable only for the PON port. This field is applicable for GPON and CPON port mode. |
| XGSPON Multicast Shaper Profile | Select the multicast shaper profile. This field is applicable only for the PON port. This field is applicable for Auto, XGSPON, and CPON port mode. |
| Multicast Queue Priority | Specifies the priority to be applied on the downstream multicast queue. The default value is 3. This field is applicable only for the PON port. |
| Active IGMP Channels | Specifies the active IGMP channels for the PON port. The supported value ranges from 0 to 11,648. The default value is 1024. |
| GPON Alarm Profile | Select the OLT port alarm profile from the list. This field is applicable for GPON and CPON port mode. |
| XGSPON Alarm Profile | Select the OLT port alarm profile from the list. This field is applicable for Auto, XGSPON, and CPON port mode. |
| SFP Alarm Profile | Select the SFP alarm profile from the list. |
| Periodic Rogue ONT Detection Control | Select whether the periodic rogue ONT detection needs to be enabled. The supported values are. <ul style="list-style-type: none">◦ ENABLED◦ DISABLED |

| Field | Description |
|---|---|
| | The default value is ENABLED. |
| Periodic Rogue ONT Detection Measurement Type | Select the RSSI measurement window type. The supported values are. <ul style="list-style-type: none"> ◦ SILENT-WINDOW. Detects and identifies an ONU that is responding to allocations belonging to another ONT but detects most other types of rogue ONT behavior. ◦ CUTOFF-WINDOW. Detects an ONT that stops the laser transmission later than it should, potentially interfering with the next allocation. The default value is SILENT-WINDOW. |
| Alloc Type to Scan | Select the alloc ID type to scan. The supported values are. <ul style="list-style-type: none"> ◦ UNUSED. AllocIDs that are currently not in use (not yet assigned to any ONTs). ◦ PREVIOUSLY-USED. AllocIDs that are used once and cleared. ◦ ALL. Scan both unused and previously used AllocIDs. The default value is PREVIOUSLY-USED. |
| Periodic Rogue ONT Detection Interval (in milliseconds) | Enter the periodic rogue ONU detection procedure initiation interval in milliseconds. The value ranges from 1000 to 10000000 milliseconds. The default value is 1000 milliseconds. |

Editing NNI Port Configuration

After a successful creation of the NNI port, a port ID is automatically generated.

Perform the following steps to modify the parameters configured for the port.

1. Select **Configuration > Inventory**.
2. Navigate to the OLT tab.
3. Click on the ports (grid) icon.
The *Ports List [Inventory - OLT Name]* page appears with the list of port details.
4. Click the edit icon corresponding to the NNI port from the **Action** column.

The Port Configuration page appears, displaying the existing configuration information.



Note: You cannot edit the following fields on NNI port configuration page.

- ID
- Name
- Port



- Display ID
- Port Media

You can modify the following fields of the NNI configuration according to the guidelines provided in the following table.

Table 184. NNI Port Configuration

| Field | Description |
|---------------------|---|
| Description | Enter a meaningful description about the PON or NNI port configuration. |
| Port Direction | Select the port direction from the list. The supported values are. <ul style="list-style-type: none">◦ UNI◦ NNI◦ ANY |
| Capacity | Enter the capacity of the port. Example: 1 |
| Capacity Type | Select the capacity type from the list. The supported values are. <ul style="list-style-type: none">◦ Megabit◦ Gigabit |
| Inventory System ID | Enter the inventory system ID. Example: 1/1/1/NNI-3 |
| Alarm Profile | Select the OLT port alarm profile from the list. |
| SFP Alarm Profile | Select the SFP alarm profile from the list. |
| MTU Size | Specifies the maximum transmission unit (MTU) size in bytes on the NNI port. The field is applicable for the NNI port. The supported value ranges from 68 to 9600 bytes. The default value is 9600 bytes. |

Activating the PON and NNI Port

Similar to OLT activation and deactivation, you can activate and deactivate the PON ports of the OLT. This enables a controlled environment for the operator where an unused port does not cause any undesired activity in the network.

Once the PON or NNI port is successfully added to the OLT, you can activate the port. When a port is active, it sends optical energy on the link and consumes power. CBAC does not accept connections from a PON port that is not operational. A PON port is operational only when the PON port is activated by RMS.

CBAC activates NNI ports by default and sends the notification to RMS with the admin and operational states. Upon receiving the event, RMS updates the admin and operational state of the NNI port.

Perform the following steps to activate the PON/NNI port.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the OLT tab.

The OLT List page appears.

3. Click on the ports (grid) icon.

The *Ports List [Inventory - OLT Name]* page appears with the list of PON/NNI port details.

4. Click on the three dots (dots) corresponding to the port on which you want to activate and click the **Activate** option.

A confirmation message appears indicating that the port is activated successfully.

Deactivating the PON and NNI Port

When the ports are not in use, you can deactivate the ports to save power.

Perform the following steps to deactivate the PON/NNI port.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the OLT tab.

The OLT List page appears.

3. Click on the ports (grid) icon.

The *Ports List [Inventory - OLT Name]* page appears with the list of PON/NNI port details.

4. Click on the three dots (dots) corresponding to the port on which you want to deactivate and click the **Deactivate** option.

A warning pop-up message appears stating, Deactivating port could result in an impact on subscriber service. Are you sure to perform this action?

5. Click **Confirm** to deactivate the port.

A confirmation message appears indicating that the port is deactivated successfully.

Initiate and Cancel MAC Dump on PON and NNI Port

RMS allows you to initiate and cancel the MAC dump on PON and NNI port.

You can query multiple MAC addresses learned by the OLT on each PON and NNI port.



Note: To query the MAC dump on each PON and NNI port, the operational state must be UP and admin state must be enabled for each port.

Perform the following steps to initiate the MAC dump on PON or NNI port.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the OLT tab.

The OLT List tab appears.

3. Click on the ports (grid icon) corresponding to the OLT on which you want to view the port details.

The Ports List [*Inventory - OLT Name*] page appears with the list of PON and NNI port details.

4. Click on the three dots (dots icon) corresponding to the PON or NNI port and click **Initiate MAC Dump** option.
5. Complete the configuration according to the guidelines provided in the following table.

Table 185. Initiate MAC Dump on PON or NNI Port

| Field | Description |
|-------------|---|
| OVlan | Specifies the outer VLAN. This field is applicable for the MAC dump request on PON port, NNI port, and services. The supported value ranges from 2 to 4094. |
| IVlan | Specifies the inner VLAN. This field is applicable only for the NNI port. |
| MAC Address | Enter the MAC address. |



Note: The **OVlan**, **IVlan**, and **MAC Address** fields are optional.

6. Click **Submit**.

A confirmation message appears indicating that the MAC dump is initiated successfully.

Click on the three dots (dots icon) corresponding to the service and click **Monitor** option. For more information, see [PON Port \(on page 82\)](#) and [NNI Port Details \(on page 99\)](#).

Perform the following steps to cancel the MAC dump on PON or NNI port.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the OLT tab.

The OLT List tab appears.

3. Click on the ports (grid icon) corresponding to the OLT on which you want to view the port details.

The Ports List [*Inventory - OLT Name*] page appears with the list of PON and NNI port details.

4. Click on the three dots (⋮) corresponding to the port on which the MAC dump is initiated and click **Cancel MAC Dump** option.
5. Click **Submit**.

A confirmation message appears indicating that the MAC dump is canceled successfully.

MAC Lookup for NNI Port

Perform the following steps to perform MAC lookup for the NNI port.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the OLT tab.
The OLT List page appears.
3. Click on the ports icon (grid icon) corresponding to the OLT on which you want to view the port details.
The Ports List [*Inventory - OLT Name*] page appears with the list of PON and NNI port details.
4. Click on the three dots (⋮) corresponding to the NNI port and click **MAC Lookup** option.
5. Complete the configuration according to the guidelines provided in the following table.

Table 186. MAC Lookup Configuration

| Field | Description |
|-------------|---|
| OVlan | Specifies the outer VLAN. This field is applicable for the MAC dump request on PON port, NNI port, and services. The supported value ranges from 2 to 4094. |
| IVlan | Specifies the inner VLAN. This field is applicable only for the NNI port. |
| MAC Address | Specifies the MAC address. |

A confirmation message appears indicating that the MAC for a particular resource ID is learned successfully.



Note:

- The **OVlan** and **MAC Address** fields are mandatory whereas the **IVlan** field is optional to perform MAC lookup.
- When the incorrect values are entered for the **OVlan** and **MAC Address** fields, an error message appears indicating that the MAC lookup is failed for a particular service.

Adding Member Port to LAG

You can add the member port (NNI) to LAG (when LAG is enabled or disabled state).

Perform the following steps to add member port to LAG.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the OLT tab.
The OLT List page appears.
3. Click on the ports () icon.
The Ports List [*Inventory - OLT Name*] page appears with the list of NNI ports.
4. Click on the three dots () corresponding to the NNI port on which you want to add the member port.
5. Click **Attach LAG**.
The LAG Availability List appears. For more information, see [Creating LAG Configuration \(on page 328\)](#).
6. Click the **Associate** option from the Associate/Disassociate column.
The Add LAG Member Port Payload page appears.
7. Complete the configuration according to the guideline provided in the following table.

Table 187. LAG Member Port Payload Configuration

| Field | Description |
|---------------|---|
| LACP Key | Specifies the LACP key for the port. The supported value ranges from 0 to 65,535. The default value is 0. |
| LACP Priority | Specifies the LACP priority. The supported value ranges from 0 to 65,535. The default value is 255. |

8. Click **Create**.
A confirmation message appears and indicates the status of the operation.
The port controller state is changed to ASSOCIATION_IN_PROGRESS and then changes to ASSOCIATED.

Removing Member Port from LAG

You can remove the member port (NNI) from LAG (when LAG is enabled or disabled state).

Perform the following steps to remove member port from LAG.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the OLT tab.
The OLT List page appears.
3. Click on the ports () icon.

The Ports List *[Inventory - OLT Name]* page appears with the list of port details.

4. Click on the three dots () corresponding to the NNI port from which you want to remove the member port and click the **Remove LAG** option.

You are taken to the LAG Availability List page.

5. Click the **Disassociate** option from the Associate/Disassociate column.

A confirmation message appears, indicating the status of the delete operation.

The port controller state is changed to DISSOCIATION_IN_PROGRESS and then changes to DISASSOCIATED.

Exporting PON and NNI Port Information

You can export the PON and NNI port configured for the OLT as a CSV file from RMS to your local computer. The CSV file can be opened or edited using an application such as Microsoft Excel. You can view and analyze the exported port information, as needed.

Perform the following steps to export the subscriber information.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the **OLT** or **CARD** tab.

3. Click on the ports () icon corresponding to the OLT/CARD on which you want to view the PON/NNI port details.

The *Ports List [Inventory - OLT Name]* page appears with the list of port details.

4. Click **Export**.

The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file using an application such as Microsoft Excel. Optionally, you can save this file on your PC for later use.

The downloaded file contains the following information about the PON or NNI port details.

- Name
- Admin State
- Operational State
- Media
- Display ID
- Port No
- Port Direction
- Capacity
- Unit
- Description
- PON Encryption Enabled
- PON Encryption Key Interval
- ONT Capacity

- Inventory System ID
- Auto-negotiation
- Periodic Rogue ONT Detection Control
- Periodic Rogue ONT Detection Measurement Type
- Alloc type to Scan
- Periodic Rogue ONT Detection Interval (in milliseconds)
- Creation Time
- Action

Viewing Physical Link List of the OLT or ONT

You can view the OLT device on which the PON or NNI port is connected.

Perform the following steps to view the physical list of the port.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the **OLT or ONT** tab.
3. Click on the three dots (⋮) corresponding to the port on which you want to view the physical link list and click the **Physical Link** option.

The Physical Link List [Inventory - *OLT Name/ONT Name*] page appears with the list of port details.

The following table describes the fields on the Physical link List [Inventory - *OLT Name/ONT Name*] page.

Table 188. Port Physical Link List

| Field | Description |
|--------------|--|
| A-End | |
| Device Name | Specifies the a-end device (OLT or ONT) name. |
| Type | Specifies the a-end device (OLT or ONT) type. |
| Port Name | Specifies the a-end device (OLT or ONT) port name. |
| Z-End | |
| Device Name | Specifies the z-end device (OLT or ONT) name. |
| Type | Specifies the z-end device (OLT or ONT) type. |
| Port Name | Specifies the z-end device (OLT or ONT) port name. |

| Field | Description |
|---------------|---|
| Action | Specifies the action. |
| Creation Time | Specifies the date and time when the physical link was created. |

Creating Physical Link Configuration

You can create the physical link configuration of the OLT or ONT.

Perform the following steps to create physical link configuration.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the **OLT** or **ONT** tab.
3. Click on the three dots (⋮) corresponding to the OLT or ONT on which you want to create the physical link and click the **Physical Link** option.
The *Physical Link List [Inventory - OLT Name/ONT Name]* page appears with the list of physical link details.
4. Click **Create**.
The Physical Link Configuration page appears.
5. Complete the configuration according to the guideline provided in the following table and click **Create**.

Table 189. Physical Link Configuration

| Field | Description |
|--------------|--|
| A-End | |
| Device | Specifies the a-end device (OLT or ONT) name. |
| Device Type | Specifies the a-end device (OLT or ONT) type. |
| Port | Specifies the a-end device (OLT or ONT) port name. |
| Cable | Specifies the cable name. |
| Z-End | |
| Device Type | Specifies the z-end device (OLT or ONT) type. |
| Device | Specifies the z-end device (OLT or ONT) name. |
| Port | Specifies the z-end device (OLT or ONT) port name. |

Reboot the OLT

OLT reboot recovers the system. Faults such as excessive memory usage due to memory leaks may require a system reboot. In addition, a periodic reboot helps save the hardware life. RMS supports an immediate reboot of the OLT remotely.

Perform the following steps to reboot the OLT.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the OLT tab.
3. Click on the three dots (⋮) corresponding to the OLT that you want to reboot and click the **Reboot** option.
The following warning message appears.

Rebooting OLT could result in an impact on subscriber service. Are you sure to perform this action?

4. Click **Confirm** to reboot the OLT.
5. Enter the reason in the **Reason** field for rebooting the OLT. The maximum length is 256 characters.
RMS sends a reboot request to CBAC. CBAC reboots the OLT if the request is valid.

Upgrade the OLT Software (ONL or OLT BINS)

Prerequisites

- The user must upgrade the controller software first and then proceed with OLT software upgrade. For more information, see [Upgrade Controller Software \(on page 310\)](#).
- If the upgrade is only for the OLT applications, ensure that the OLT is upgraded to the latest version before upgrading the OLT BINS image.

You can upgrade the OLT software from the current version to the latest version.

You can either perform the complete ONL upgrade or only the OLT applications upgrade.

Use the ONL image for the complete ONL upgrade and the OLT BINS image for the OLT applications upgrade.



Note: Before you download the OLT software (ONL or OLT BINS), you must specify the OLT software version. For more information, see [Creating Model Version Configuration \(on page 612\)](#).

The OLT software upgrade (ONL or OLT BINS) process involves the following steps.

- Download the OLT software
- Activate the OLT software
- Commit the OLT software
- Rollback the OLT software to previous version if there is any malfunction during the upgrade process



Note: Rollback must be done before committing the OLT software.

Perform the following steps to upgrade the OLT software (ONL or OLT BINS) immediately.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the **OLT** tab.

3. Click on the three dots (⋮) corresponding to the OLT for which you want to upgrade the software.

4. Click the **Download Software** option.

The Download Software appears.

Figure 61. Download OLT Software

| Name | Admin State | Operational State | Make | Model | Display Id | Serial No. | Management IP | Local Profiles |
|--------|-------------|-------------------|---------|-----------|------------|--------------|----------------|----------------|
| olt-64 | ACTIVE | UP | Radisys | RLT-3200G | olt-64 | 742306205380 | 172.17.173.155 | 1 |
| olt-74 | ACTIVE | UP | Radisys | RLT-3200G | olt-74 | 722033538838 | 172.17.173.155 | 1 |

5. Select the OLT software version that must be downloaded from the list.

Figure 62. Software Version

6. Click **Download**.

A confirmation message appears that the OLT software download is success.

Figure 63. Success Message

| Name | Admin State | Operational State | Make | Model | Display Id | Serial No. | Management IP | Software Upgrade Status | ZTP Status | Creation Time | Network Services | Local Profiles | Action |
|-------|-------------|-------------------|---------|-----------|------------|-------------|----------------|-------------------------|------------|------------------------|------------------|----------------|--------|
| VMOLT | ACTIVE | UP | Radisys | RLT-1600C | VMOLT | 72210211150 | 172.27.173.155 | DOWNLOAD-SUCCESSFUL | UNKNOWN | Dec 6 2022, 4:24:14 PM | LAG | Line | ELAN |

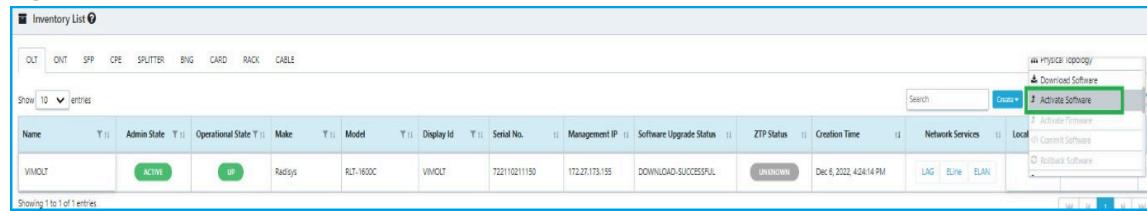
**Note:**

- If the ONL download fails for some issues, the subsequent ONL download request resumes the ONL download from where it stopped.
- By default, the options **Activate Software**, **Commit Software**, and **Rollback Software** are disabled, and these options are enabled only when the OLT download operation is success.

7. Click the **Activate Software** option to activate the OLT software.

The Activate Software page appears.

Figure 64. Activate Software



8. Click **Confirm** to activate the software.



Note: Wait for 20 minutes to upgrade the ONL.

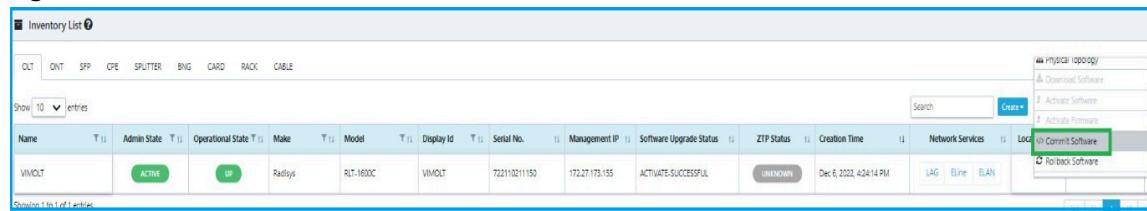
The **Software Upgrade Status** for the OLT must be **ACTIVATE-SUCCESSFUL**, indicating that the OLT activation is successful.

Figure 65. Software Activation Confirm



9. Click the **Commit Software** option to commit the OLT software.

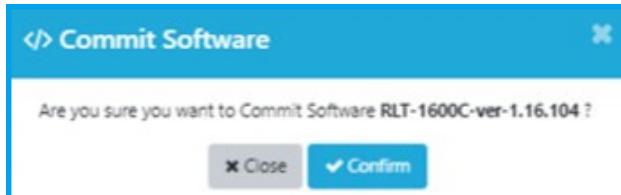
Figure 66. Commit Software



10. Click **Confirm** to commit the software.

The **Software Upgrade Status** for the OLT must be **COMMIT-SUCCESSFUL**, indicating that the OLT commit is successful.

Figure 67. Software Commit Confirm



The **ME-SOFTWARE-COMMIT-SUCCESSFUL** event is reported in the RMS to confirm the OLT software commit is successful.

If you want to schedule the OLT software update for a later date and time, you must create a task. For more information, see [Creating Task for Single or Bulk OLT Software Upgrade \(ONL or OLT BINS\) \(on page 647\)](#).

Upgrade the OLT Firmware

You can upgrade the OLT firmware from the current version to the latest version. The OLT firmware components are.

- BIOS
- Complex Programmable Logic Device (CPLD)
- Field Programmable Gate Array (FPGA)



Note: Before you download the OLT firmware, you must specify the OLT firmware version. For more information, see [Creating Model Version Configuration \(on page 612\)](#).

The OLT firmware upgrade process involves the following steps.

- Download the OLT software
- Activate the OLT Firmware

Perform the following steps to upgrade the OLT firmware immediately.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the **OLT** tab.
3. Click on the three dots (⋮) corresponding to the OLT for which you want to upgrade the software.
4. Click the **Download Software** option.
The Download Software page appears.
5. Select the OLT software version that must be downloaded from the list.
6. Click **Download**.

A confirmation message appears that the OLT download is success.

**Note:**

- If the OLT software package contains ONL or OLT BINS image, the **Activate Software** option is enabled.
- If the OLT software package contains firmware image (BIOS, CPLD, and FPGA), the **Activate Firmware** option is enabled.

7. Click **Activate Firmware** to activate the OLT firmware.

A confirmation message appears that the OLT is upgraded with the new firmware.

If you want to schedule the OLT firmware upgrade for a later date and time, you must create a task from the **Maintenance > Task** menu. For more information, see [Creating Task for OLT Firmware Upgrade \(on page 687\)](#).

Associate the ACL Profile to the OLT

When you associate the ACL profile with the OLT, the ACL rules are applied to the ports on the OLT. OLT must configure an ACL to ensure that only valid IP packets can enter and exit from the OLT.

Perform the following steps to associate the ACL profile to the OLT.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the **OLT** tab.

3. Click on the three dots (⋮) corresponding to the OLT that you want to associate the ACL profile and click the **ACL Profile** option.

The ACL Profile [Inventory - <OLT-Name>] page appears with both data path and management ACL profiles. For more information, see [Creating ACL Profile \(on page 538\)](#).

4. Click **Add**.

The Select ACL Profile page appears.

5. Select the respective ACL profile (data path ACL profile or management ACL profile) that you want to associate to the OLT.

6. Select the port from the Port List.



Note: The user can select the PON port, NNI port, or both PON and NNI port.

7. Click **Add**.

The ACL profile is added on the page ACL Profiles page.

8. Click the **Associate** option from the **Associate/Dissociate** column.

The ACL profile is added to the OLT and a confirmation message appears, indicating the status of the associate operation.



Note: ACL rules are not applicable on node ports.

Dissociate the ACL Profile from the OLT

You can remove the ACL profile from the OLT.

Perform the following steps to remove the ACL profile from the OLT.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the **OLT** tab.
3. Click on the three dots (⋮) corresponding to the OLT that you want to associate the ACL profile and click the **ACL Profile** option.
The ACL Profile [Inventory - <OLT-Name>] page appears with both data path and management ACL profiles.
4. Select the ACL profile (data path ACL profile management ACL profile) that you want to remove from the OLT and click the **Dissociate** option from the **Associate/Disassociate** column.
The ACL profile is removed from the OLT and a confirmation message appears, indicating the status of the disassociate operation.

OLT Replacement

Prerequisites

Execute the following command in the new OLT console to view the product name, serial number, and MAC address of the OLT.

```
sudo onlpd -s
```

Figure 68. New OLT Product Name Serial Number and MAC Address

```
root@143-OLT> sudo onlpd -s
System Information:
  Product Name: RLT-1600G
  Part Number: RSJVASB1063455
  Serial Number: 722020923444
  MAC: 28:b9:d9:e2:ef:96
  MAC Range: 64
  Manufacturer: JABIL
  Manufacture Date: 08/14/2020-16:33:42
  Vendor: Radisys
  Platform Name: 3708-32-256
  Device Version: 1
  Label Revision: 14
  Country Code: CN
  Diag Version: 1.26
  Service Tag: 000000000000
  ONIE Version: 0324
  UUID: 0000000000000000
  CLEI: 0000000000
  CPN: RSJVPBA1063503A
  CSN: 722021624417
  Component Version: 22
  Manufacturer ID: JABIL
  CC: CN
  Vendor ID: Radisys
  Manufacturer Date: 08/14/2020-16:33:42
```

The OLT replacement scenario is used only when the OLT goes into an irrecoverable state of function.

The following scenario indicates that the OLT is in an irrecoverable state and needs replacement.

- The OLT reboots frequently and is unable to recover and the OLT-REBOOT event is generated in RMS.
- The controller Kafka operational state becomes DOWN, and the OLT operational state is DOWN due to damage. A ME-DOWN alarm is generated in RMS.
- The ME-DOWN alarm can be raised due to network issues or damaged OLT. In a few scenarios, the OLT is recovered by doing some workarounds. If the OLT is not recoverable, then replace the OLT.



Note: The **Make** and **Model** of the new OLT must be the same as the old OLT. For example, the RLT-1600G cannot be replaced with the RLT-3200G.

Perform the following steps to replace the OLT.

1. The user must have a backup of the old OLT. For more information, see [Creating Task for Controller or OLT Backup \(on page 661\)](#) or [Backup OLT Configuration \(on page 400\)](#). It is recommended to schedule a daily backup of every OLT-CBAC and keep the last few backup copies.
2. Get the snapshot or output for the following old OLT files. These snapshots must be updated on the new OLT.
 - *cat /etc/network/interface*
 - *cat /broadcom/olt_config*
3. Execute the following command to get the time zone details from the old OLT. The same time zone must be updated on the new OLT after replacement.

```
sudo timedatectl show --property=Timezone --value
```

Figure 69. OLT Time Zone

```
22.05.2023@11:46:50 : /home/oltausr
oltausr@143-OLT:~$ sudo timedatectl show --property=Timezone --value
Etc/UTC
22.05.2023@11:46:52 : /home/oltausr
```

4. Physically replace the old OLT with the new OLT.
5. Shift SFPs and fibers from the old OLT to the new OLT.



Note: You must use the same NNI and PON ports as per the old OLT.

6. Install the ONL on the new OLT of the same version present on the old OLT. Check RMS for version information. For more information on how to install the ONL on the OLT, refer to the *CBAC-D Installation Guide*.
7. Execute the following command to check the CPLD, BIOS, and FPGA version in the new OLT.

```
sudo sdpon-firmware-install --version
```



Note: Ensure that the firmware version of the old OLT matches correctly with the new OLT. If there is a mismatch, install the appropriate firmware version. For more information on firmware upgrades, refer to the *CBAC-D Installation Guide*.

Figure 70. OLT Firmware Version

```
22.05.2023@11:39:19 : /home/oltausr
oltausr@143-OLT:~$ sudo sdpon-firmware-install --version

Platform      : x86-64-radisys-phoenix-r0
Build Date   : 25/04/23

Component    Current Version    Upgrade Bundle Version
-----
BIOS          1.0.07            1.0.07
MB FPGA       20110520          20110520
CPLD          63                63
```

8. Update the */etc/network/interface* file with the old OLT IPs.



Note: The old OLT IP addresses are 172.27.181.210 (out of band IP) and 2250::210 (inband IP).

Figure 71. Network Interface File

```
auto lo
iface lo inet loopback
auto ma1
iface ma1 inet static
    address 172.27.181.210
    netmask 255.255.252.0
    up ip route add 172.0.0.0/8 via 172.27.183.254 || true
auto eno1
iface eno1 inet6 static
    address 2250::210
    netmask 64
    gateway 2250::254
    accept-ra: no
```

9. Update the */broadcom/olt_config* file same as the old OLT file.

Figure 72. OLT Configuration File

```
{
    "_comments": "This is a comment. For making changes in this file, user is advised to go through CBACd_Installation_Guide o
f Release documentation",
    "vlan": 1001,
    "nni": [
        3
    ],
    "pon_device_mode0": "gpon",
    "iwf_mode0": "per_flow",
    "pon_device_mode1": "gpon",
    "iwf_mode1": "per_flow",
    "inband_storm_control_rate": 100000,
    "version": "v.0.0.01",
    "alarmthreshold_max_events": 10,
    "alarmthreshold_window_time": 5
}
```

10. If the old OLT has a LACP-based setup and the OLT is accessible, then take the backup of */mnt/onl/sdpon/oltfiles/olt_hidden_config* file and copy the same on the new OLT at the same place.
11. If you cannot take the backup of the old OLT *olt_hidden_config.json*, copy the *olt_hidden_config.json* template to the new OLT home directory.



Note: Skip this step if NNI or static LAG is used.

Figure 73. OLT Hidden Config

```
{  
    "dhcp_interface" : 4,  
    "east_port" : {  
        "lacp_mode" : true,  
        "lacp_priority" : 128,  
        "lacp_status" : true,  
        "lacp_timeout" : true,  
        "member_ports" : [ 4, 2 ],  
        "member_ports_lacp_key" : [ 1, 1 ],  
        "member_ports_lacp_priority" : [ 255, 255 ],  
        "port_id" : 129,  
        "port_type" : "lag"  
    }  
}
```

12. Perform one of the following step to update the *olt_hidden_config.json* template, so that it is same as */mnt/onl/sdpon/oltfiles/olt_hidden_config* file in the old OLT. This can be done either in manual or automated way.

Manual File Creation

- Edit the *olt_hidden_config.json* template and copy it to the */mnt/onl/sdpon/oltfiles/* location on the new OLT.

OR**Automated File Creation**

- Copy the *inband_lacp_config.sh* file to the new OLT home directory and execute the following command (provide the appropriate inputs as prompted).

```
sudo ./inband_lacp_config.sh
```

**Note:**

- It automatically generates the *olt_hidden_config.json* template and copy it to the */mnt/onl/sdpon/oltfiles/* location.
- The field engineer must have the *inband_lacp_config.sh* and *olt_hidden_config.Json* template file.

13. Reboot the OLT.



Note: Once the OLT is up, ping the repository server from OLT console to check the repository reachability.

14. Execute the following command to configure the time zone of the new OLT as per the old OLT configuration. The command syntax is.

```
sudo timedatectl set-timezone <output from Step 3 (on page 394)>
```

Example:

```
sudo timedatectl set-timezone Etc/UTC
```

Figure 74. Old OLT Time Zone

```
22.05.2023@11:46:50 : /home/oltausr
oltausr@143-OLT> sudo timedatectl show --property=Timezone --value
Etc/UTC
22.05.2023@11:46:52 : /home/oltausr
oltausr@143-OLT>
```

15. Execute the following command to set the time and date according to the current time zone.

The command syntax is.

```
sudo timedatectl set-time "<yyyy-mm-dd hh:mm:ss>"
```

Example:

```
sudo timedatectl set-time "2023-07-11 07:12:00"
```

1. Deploy CBAC on the new OLT of the same version which was present on the old OLT. Check RMS for the version information. For more information on how to deploy the CBAC, refer to the *CBAC-D Installation Guide*.
2. Navigate to the **Monitor > Inventory > Controller** in the RMS GUI.

 **Note:** For the applicable controller, the admin state must be ACTIVE. The operational state of the Rest, and Kafka must be UP.
3. Perform the following steps from RMS to replace the faulty OLT.
 - a. Navigate to **Configuration > Controller**.
 - b. Select the controller associated with the OLT, click on the three dots (⋮) icon and click the **Replace** option to synchronize the updated admin user password. For more information, see [Replacing the Password \(on page 306\)](#).
 - c. Click on the three dots (⋮) icon and click the **Restore** option. For more information, see [Restore OLT Configuration \(on page 401\)](#).
 - d. Select the **File Store** from the list from which the backed-up OLT needs to be restored.
 - e. Enter the **File Name** of the OLT that must be restored.
 - f. Click **Submit** and wait for successful restoration (10 minutes) of OLT.
 - g. After successful restoration, CBAC reports the OLT-DOWN event and raises an OLT- CONFIG-MISMATCH alarm, indicating a mismatch in the OLT serial number and MAC address. Note the **Last Occurrence Time** of the alarm.

- **Scenario 1 (General).** If the admin state of the OLT is ACTIVE in both CBAC and RMS, navigate to **Configuration > Inventory > OLT** and deactivate the OLT, replace the serial number and MAC address of the old OLT with the new OLT.
 - **Scenario 2 (Exceptional).** If the OLT admin state of the RMS is ACTIVE and CBAC is DEACTIVE, you must deactivate the OLT and update the serial number and MAC address of the new OLT.
 - **Scenario 3 (Exceptional).** If the OLT admin state at RMS is DEACTIVE and CBAC is ACTIVE, you must activate and deactivate the OLT from RMS and then update the serial number and MAC address of the new OLT.
- h. The OLT reboots as part of the OLT deactivation process. Wait until the OLT is back on-line before initiating the OLT activation.

**Note:**

- Upon OLT activation, If the OLT moves to the ACTIVE/DOWN state, reboot the OLT to bring the OLT to the ACTIVE/UP state.
- If the operational state of the OLT is ACTIVE/UP after updating the MAC address and serial number, it indicates that the OLT replacement is successful.

4. In RMS, navigate to **Monitor > Inventory > Inventory > OLT > Alarms > Alarm Purge and Fetch** to clear the alarms raised by the old OLT and fetch the active alarms from CBAC.

| Severity | First Occurrence Time | Last Occurrence Time | Device Reported Time | Controller Reported Time | Fault | Site | Error Code |
|----------|--------------------------|--------------------------|--------------------------|--------------------------|-----------------------------------|------|---------------------|
| CRITICAL | Aug 20, 2024, 6:31:45 AM | Aug 20, 2024, 6:31:45 AM | Aug 20, 2024, 6:26:29 AM | Aug 20, 2024, 6:26:29 AM | OLT-ALTERNATE-POWER-SUPPLY-FAILED | N/A | INVENTORY_NOT_FOUND |



Note: You can perform **Purge and Fetch** operations for all active alarms including OLT, Ports, ONT, Controller, Service, Subscriber, LAG, and so on. This operation deletes all active alarms from RMS, fetches the active alarms from CBAC, and rebuilds them in RMS. However, the cleared alarm entries remain in the system and can be ignored.

OLT Backup and Restore

This section covers the backup and restore procedures for the physical OLT.

Backup OLT Configuration

RMS provides a way to backup and restore the OLT configuration data. RMS enables this feature without affecting the services provided to any of the subscribers.

The OLT backup configuration data includes the following.

- OLT system configurations configured on the OLT (System log server, RADIUS server, and so on).
- PON port configurations on the specified OLT.
- ONT, subscriber, and services configurations served by the OLT.
- Inventory configurations of Field Replaceable Units (FRUs) that are managed by the OLT.
- ONT, subscriber, and services configurations attached to the OLT.
- All profiles configured from RMS for MEs, subscribers, services, ports, and network services.

RMS sends a request to CBAC to back up the entire OLT configuration.

- If the request is accepted, CBAC sends the “202 Accepted” response to RMS and the configuration data is backed-up.
- If the request is invalid, CBAC responds with the “400 Bad Request” error message to RMS.

RMS raises an alarm upon inability to take a backup of the running configuration/contexts of entire OLT.

An audit log entry is automatically generated when you backup and restore a configuration file. You can identify the user who initiated the backup operation from the audit log entry, the system's IP address from which the task was initiated, and so on.

RMS also supports scheduled backup configuration for the OLT. You must create a task if you want to schedule the OLT backup on a one-time, daily, weekly, or monthly. For more information, see [Creating Task for Controller or OLT Backup \(on page 661\)](#).

Perform the following steps to back up OLT configuration data.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the OLT tab.

The OLT List page appears.

3. Click on the three dots (⋮) corresponding to the OLT on which you want to take a backup of the configuration and click the **Backup** option.

The Backup Path page appears.

4. Select the **File Store** from the list on which the backed-up configuration needs to be stored or click the plus icon (+) icon to create a file store configuration. See [Creating File Store Configuration \(on page 618\)](#).



Note: The OLT and the SFTP server must have the same IP protocol for OLT and CBAC related operations such as backup and restore.

5. Click **Submit**.

A confirmation message appears, indicating the status of the backup operation.

The OLT configuration data is backed-up in the SFTP server location.



Note: The sub sequence OLT backup schedule is not allowed within 15 minutes. The immediate backup does not execute within 15 minutes if any backup is already scheduled during that time.

A maximum of two scheduled OLT backups are allowed.

Restore OLT Configuration

RMS supports the restoration of the last backed-up configuration of the OLT. RMS uses the unique ID generated by CBAC to restore the OLT configuration. This unique identifier is used to restore the last successfully backed-up configuration for the corresponding OLT.



Note: The restoration of the OLT configuration affects the services associated with the OLT. However, the services configured on the other OLTs do not get affected.

You can restore the following configuration data of the OLT with the same state when it was backed-up.

- OLT system configurations (System log server, RADIUS server, and so on).
- PON port configurations on the specified OLT.
- ONT, subscriber, and services configurations served by the OLT.
- Inventory configurations of Field Replaceable Units (FRUs) that are managed by the OLT.
- ONT, subscriber, and services configurations attached to the OLT.
- All profiles configured from RMS for MEs, subscribers, services, ports, and network services.

RMS sends a request to CBAC to restore the entire OLT configuration.

- If the request is accepted, CBAC sends the “202 Accepted” response to RMS and the configuration data is restored.
- If the request is invalid, CBAC responds with the “400 Bad Request” error message to RMS.

Perform the following steps to restore the OLT configuration data.

1. Select **Configuration > Inventory**.
2. Click on the OLT tab.

The OLT List page appears.

3. Click on the three dots (⋮) corresponding to the OLT on which you want to restore the backed-up configuration and click the **Restore** option.
4. Select the **File Store** from the list from which the backed-up OLT needs to be restored.



Note: The OLT and the SFTP server must have the same IP protocol for OLT and CBAC related operations such as backup and restore. SFTP server must be reachable from the OLT.

5. Enter the **File Name** of the OLT that must be restored.
6. Click **Submit**.

A confirmation message appears, indicating the status of the restore operation.

The OLT configuration data is restored from the SFTP server.

RMS also supports scheduled restore configuration for the OLT. If you want to schedule the OLT restore for a later date and time, you must create a task. See [Creating Task for Controller or OLT Restore \(on page 667\)](#).

Updating the OLT IP Address with Active Installation

OLT IP address change is required when the operator changes the IP address of the subnet within the same location with active subscribers. This use case is different from the OLT change of location.

The following procedure must be performed in the maintenance window, as the OLT reboot impacts the service.



Note: The static IP change is supported on **eno1** (inband) and **ma1** (out-of-band) interfaces. DHCP IP change is supported only on **eno1** (inband) interface. Only one type of IP, either ipv4- to-ipv4 or ipv6-to-ipv6 change is supported.

The following are the valid IP address change procedure.

1. Static-to-Static.

Initial CBAC deployment uses the static IP address assigned to the **eno1** (inband) or **ma1** (out-of-band) interface. The IP address can be changed manually by using the CBAC script that is present in SDPON package or by changing the IP address of the management interface (**ma1/eno1**) through the */etc/network/interfaces* file.

2. DHCP-to-DHCP.

CBAC was initially deployed using the field procedure. For more information on the CBAC deployment, refer to the *CBAC-D Installation Guide*.



Note: For more information on the IP change and service recovery, refer to the *RMS User Guide*.

IP Change and Service Recovery

The section explains how to change the IP address of the OLT. The following steps are applicable to both IPv4 and IPv6.

1. Once the RMS and CBAC are up and running in the IPv4 environment, verify the existence of services and subscribers in the **Inventory List** of RMS.
2. Verify the subscriber service status.
3. Deactivate the OLT. For more details, see [Activating and Deactivating the OLT \(on page 324\)](#).
4. Skip the following steps for the DHCP IP address change procedure.

Follow **Procedure 1** to update the network interfaces file automatically through CBAC script (or) follow **Procedure 2** to update the network interfaces file manually and then trigger the CBAC script to reconfigure CBAC without affecting the network configuration.



Note: It is recommended to use the CBAC script to reconfigure the CBAC onto the new IP address. Copy the latest CBAC script from SDPON package to `/mnt/onl/sdpon` before triggering reconfigure.

Procedure 1

This procedure updates the network interfaces on OLT as per the given inputs.

- In case of CBAC reconfiguration from **ma1** to **eno1** interface, **ma1** IP is reverted to factory default IP (192.168.1.1) to allow further SSH locally.
 - In case of CBAC reconfiguration from **eno1** to **ma1** interface, **eno1** IP is removed from the interfaces file.
- a. The `cbac` script file is present in the untarred SDPON package `<latest SDPON version>/cbac`. Copy the latest `cbac` script file from SDPON package to OLT under `/mnt/onl/sdpon/`.
 - b. Execute the following command to navigate to the `cbac` script directory.

```
oltausr@localhost:~$ cd /mnt/onl/sdpon/
```

- c. Execute the following command and provide the inputs as prompted.

```
oltausr@localhost:/mnt/onl/sdpon$ bash cbac reconfigure
```



Note: During CBAC reconfiguration, if **eno1** is provided as the management interface, the script further prompts for the VLAN ID and NNI port details.

Figure 75. CBAC Reconfiguration

```
oltausr@localhost:/mnt/onl/sdpon/SDPON.1.19.94$ bash cbac reconfigure
#####
May 03 2024 19:52:01: CBAC Reconfigure
#####
Current management interface is ma1
Available Interface options are ma1 (out of band), eno1 (inband)
Enter the Management Interface name (Default: eno1) :
Enter OLT Management IP (IPV4 or IPV6) : 10.4.4.49
Enter netmask for eno1 interface : 255.255.254.0
Enter Gateway IP for eno1 interface : 10.4.4.254
Enter valid Repository IP (IPv4) : 10.4.4.48
Enter vlan ID ( Default: 1001 ) :
Enter nni ports : 1,3
May 03 2024 19:52:29 : Updated management interface to eno1 and address to 10.4.4.49
To reconfigure cbac with updated IP : 10.4.4.49,
  1. Reboot the OLT
    sudo reboot
  OR
  2. Restart necessary services
    sudo systemctl restart networking.service
    Note: If any SSH session is lost, re-connect via eno1 with 10.4.4.49
    sudo systemctl restart sdpondeployment.service
```

- d. Once the CBAC reconfigure script has run successfully, either reboot the OLT or restart the necessary system services to finish the reconfiguration.

```
oltausr@localhost:/mnt/onl/sdpon/SDPON.1.19.58$ sudo reboot
```

or

```
oltausr@localhost:~$ sudo systemctl restart networking.service
oltausr@localhost:~$ sudo systemctl restart sdpondeployment.service
```



Note: If SSH session is lost after networking service restart, re-connect the session through the updated IP address.

- e. Check for the progress of SDPON deployment on new IP in the */var/log/sdpondeployment_service.log* file.
- f. Execute the following command to check the status of SDPON deployment service. The status of the service must be **active (exited)** after deployment.

```
oltausr@localhost:~$ sudo systemctl status sdpondeployment.service
```

Figure 76. SDPON Deployment Service Status

```
oltausr@localhost:~$ sudo systemctl status sdpondeployment.service
● sdpondeployment.service - SDPON deployment service on upgrade of pOLT software(major).
   Loaded: loaded (/lib/systemd/system/sdpondeployment.service; enabled; vendor preset: enabled)
   Active: active (exited) since Sun 2024-03-03 16:21:04 IST; 39min ago
     Process: 2642495 ExecStart=/bin/bash /usr/bin/sdpondeployment (code=exited, status=0/SUCCESS)
   Main PID: 2642495 (code=exited, status=0/SUCCESS)

Mar 03 16:21:03 localhost bash[2655839]: deploy_services : Stop the acl_rules service ..... 2.30s
Mar 03 16:21:03 localhost bash[2655839]: deploy_services : Fluentbit service deployment ..... 2.26s
Mar 03 16:21:03 localhost bash[2655839]: Gathering Facts ..... 2.23s
Mar 03 16:21:03 localhost bash[2655839]: deploy_services : Etcd service deployment ..... 2.05s
Mar 03 16:21:04 localhost sudo[2655838]: pam_unix(sudo:session): session closed for user root
Mar 03 16:21:04 localhost sudo[2686022]:      root : PWD=/mnt/onl/sdpon/deployment_ansible ; USER=root ; COMMAND=/bin/sed
Mar 03 16:21:04 localhost sudo[2686022]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=0)
Mar 03 16:21:04 localhost sudo[2686022]: pam_unix(sudo:session): session closed for user root
Mar 03 16:21:04 localhost sudo[2642881]: pam_unix(sudo:session): session closed for user root
Mar 03 16:21:04 localhost systemd[1]: Finished SDPON deployment service on upgrade of pOLT software(major)..
```

- g. Execute the following command to check if all the pods are up and running.

```
oltausr@localhost:~$ sudo kubectl get pods
```

Figure 77. CBAC Pods Status

```
oltausr@localhost:~$ sudo kubectl get pods
NAME          READY   STATUS    RESTARTS   AGE
etcd-etcd-0   1/1     Running   0          29m
etcd-etcd-defrag-28492201-b2wgq 0/1     Completed  0          13m
external-kafka-0 1/1     Running   1          29m
external-kafka-zookeeper-0 1/1     Running   0          29m
fluent-bit-wlhd8 1/1     Running   0          29m
influxdb-6cd6869469-m7dqg 1/1     Running   0          29m
internal-kafka-0 1/1     Running   0          29m
internal-kafka-zookeeper-0 1/1     Running   0          29m
intersdpontegateway-5856558b56-x4c86 1/1     Running   0          29m
log-manager-58d8f9d57-kzxhp 1/1     Running   0          29m
lwc-64bcc4ffb9-zndhr 1/1     Running   0          29m
msm-f976fc8f-6rnpd 1/1     Running   2          29m
openolt-b5f9f899c-5pkn7 1/1     Running   0          29m
openonu-59fd684bb7-k5kn1 1/1     Running   0          29m
redis-master-0 1/1     Running   0          29m
rwc-core-d8bd699f4-kmgmg 1/1     Running   0          29m
sdponaccessgateway-5ddf84f768-2vc7m 1/1     Running   0          29m
sdpondevicemanager-689d75f7d5-k9kzs 1/1     Running   0          29m
sdponemscli-6cccbc8f4-ws1zc 1/1     Running   0          29m
sdponemsgateway-5d79649b6-8fzmd 1/1     Running   3          29m
sdponmonmgr-576b4458bf-ghwmp 1/1     Running   0          29m
sdponncm-7cb88677c8-rcdfz 1/1     Running   0          29m
sdponnda-7d66c6994c-d45gs 1/1     Running   0          29m
sdponsecurity-7578f648b9-2kl2r 1/1     Running   3          29m
sdponsubscribermanager-5bd67648bc-s6b9s 1/1     Running   0          29m
sdponlemetry-79579f9f94-xcwz8 1/1     Running   0          29m
voltctl-7cdd49ff85-6n9ml 1/1     Running   0          29m
```

- h. Execute the following command to check the Kubernetes IP address.

```
oltausr@localhost:~$ sudo kubectl get nodes -o wide
```

Figure 78. Kubernetes Nodes List after IP Change

```
oltausr@localhost:~$ sudo kubectl get nodes -o wide
NAME     STATUS   ROLES          AGE   VERSION   INTERNAL-IP   EXTERNAL-IP
OS-IMAGE   STATUS   ROLES          AGE   VERSION   INTERNAL-IP   EXTERNAL-IP
localhost   Ready   control-plane,master 39m   v1.21.5   10.3.3.59   <none>
          Debian GNU/Linux 11 (bullseye) 5.10.201-OpenNetworkLinux docker://20.10.8
```

If OLT IP change also includes the repo server IP change, the latest repo server IP must be pushed from RMS as explained in [Changing IP Address \(on page 409\)](#). If the setup is not added to RMS, the latest repo server IP must be pushed from SDPON CLI using `sdpon_update_settings` option. For more information, refer to [CBAC CLI Reference](#).

Procedure 2

In this procedure, the CBAC reconfigure has no control of network configuration. This allows the advanced users to perform the configuration of `/etc/network/interfaces` manually and then trigger the CBAC reconfigure script.

- Execute the following command to open the network interfaces file and edit as per the requirement.

```
oltausr@localhost:~$ sudo vi /etc/network/interfaces
```

Figure 79. Update Interface File

```
auto eno1
iface eno1 inet static
address 10.3.3.49
netmask 255.255.255.0
up ip route add 3.3.3.0/24 via 10.3.3.254 || true
```

- The `cbac` script file is present in the untarred SDPON package `<latest SDPON version>/cbac`. Copy the latest `cbac` script file from SDPON package to OLT under `/mnt/onl/sdpon/`.
- Execute the following command to navigate to the `cbac` script directory.

```
oltausr@localhost:~$ cd /mnt/onl/sdpon/
```

- Execute the following command to reconfigure CBAC without affecting the network configuration.

```
oltausr@localhost:/mnt/onl/sdpon$ bash cbac reconfigure --skip-network-setup
```

Figure 80. CBAC Reconfiguration without Network Configuration

```
oltausr@localhost:/mnt/onl/sdpon$ bash cbac reconfigure --skip-network-setup
[sudo] password for oltausr:
#####
May 03 2024 20:20:27: CBAC Reconfigure
#####
Current management interface is eno1
Available Interface options are ma1 (out of band), eno1 (inband)
Enter the Management Interface name (Default: eno1) : ma1
Enter valid Repository IP (IPv4) : 172.27.172.42
May 03 2024 20:20:33 : Updated management interface to ma1 and address to 172.27.174.38
To reconfigure cbac with updated IP : 172.27.174.38,
  1. Reboot the OLT
     sudo reboot
  OR
  2. Restart SDPON deployment service
     sudo systemctl restart sdpondeployment.service
```

- Once the CBAC reconfigure script has run successfully, either reboot the OLT or restart the necessary system services to finish the reconfiguration. CBAC deployment is up in few minutes.

```
oltausr@localhost:/mnt/onl/sdpon/SDPON.1.19.58$ sudo reboot
```

or

```
oltausr@localhost:~$ sudo systemctl restart sdpondeployment.service
```

- f. Check for the progress of SDPON deployment on new IP in the */var/log/sdpondeployment_service.log* file.
- g. Execute the following command to check the status of SDPON deployment service. The status of the service must be **active (exited)** after deployment.

```
oltausr@localhost:~$ sudo systemctl status sdpondeployment.service
```

Figure 81. SDPON Deployment Service Status

```
oltausr@localhost:~$ sudo systemctl status sdpondeployment.service
● sdpondeployment.service - SDPON deployment service on upgrade of pOLT software(major).
  Loaded: loaded (/lib/systemd/system/sdpondeployment.service; enabled; vendor preset: enabled)
  Active: active (exited) since Sun 2024-03-03 16:21:04 IST; 39min ago
    Process: 2642495 ExecStart=/bin/bash /usr/bin/sdpondeployment (code=exited, status=0/SUCCESS)
   Main PID: 2642495 (code=exited, status=0/SUCCESS)

Mar 03 16:21:03 localhost bash[2655839]: deploy_services : Stop the acl_rules service ..... 2.30s
Mar 03 16:21:03 localhost bash[2655839]: deploy_services : Fluentbit service deployment ..... 2.26s
Mar 03 16:21:03 localhost bash[2655839]: Gathering Facts ..... 2.23s
Mar 03 16:21:03 localhost bash[2655839]: deploy_services : Etcd service deployment ..... 2.05s
Mar 03 16:21:04 localhost sudo[2655838]: pam_unix(sudo:session): session closed for user root
Mar 03 16:21:04 localhost sudo[2686022]:      root : PWD=/mnt/onl/sdpon/deployment_ansible ; USER=root ; COMMAND=/bin/sed
Mar 03 16:21:04 localhost sudo[2686022]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=0)
Mar 03 16:21:04 localhost sudo[2686022]: pam_unix(sudo:session): session closed for user root
Mar 03 16:21:04 localhost sudo[2642881]: pam_unix(sudo:session): session closed for user root
Mar 03 16:21:04 localhost systemd[1]: Finished SDPON deployment service on upgrade of pOLT software(major)..
```

- h. Execute the following command to check if all the pods are up and running.

```
oltausr@localhost:~$ sudo kubectl get pods
```

Figure 82. CBAC Pods Status

| NAME | READY | STATUS | RESTARTS | AGE |
|---|-------|-----------|----------|-----|
| etcd-etcd-0 | 1/1 | Running | 0 | 29m |
| etcd-etcd-defrag-28492201-b2wgq | 0/1 | Completed | 0 | 13m |
| external-kafka-0 | 1/1 | Running | 1 | 29m |
| external-kafka-zookeeper-0 | 1/1 | Running | 0 | 29m |
| fluent-bit-wlhd8 | 1/1 | Running | 0 | 29m |
| influxdb-6cd6869469-m7dqg | 1/1 | Running | 0 | 29m |
| internal-kafka-0 | 1/1 | Running | 0 | 29m |
| internal-kafka-zookeeper-0 | 1/1 | Running | 0 | 29m |
| intersdpngateway-5856558b56-x4c86 | 1/1 | Running | 0 | 29m |
| log-manager-58d8f9d57-kzxhp | 1/1 | Running | 0 | 29m |
| lwc-64bcc4fffb9-zndhr | 1/1 | Running | 0 | 29m |
| msm-f976fc8f-6rnpd | 1/1 | Running | 2 | 29m |
| openolt-b5f9f899c-5pkn7 | 1/1 | Running | 0 | 29m |
| openonu-59fd684bb7-k5kn1 | 1/1 | Running | 0 | 29m |
| redis-master-0 | 1/1 | Running | 0 | 29m |
| rwcore-d8bd699f4-kmgmg | 1/1 | Running | 0 | 29m |
| sdponaccessgateway-5ddfb84f768-2vc7m | 1/1 | Running | 0 | 29m |
| sdpondevicemanager-689d75f7d5-k9kzs | 1/1 | Running | 0 | 29m |
| sdponemscli-6cccbc8df4-wslzc | 1/1 | Running | 0 | 29m |
| sdponemsgateway-5d79649b6-8fzmd | 1/1 | Running | 3 | 29m |
| sdponmonmgr-576b4458bf-ghwmp | 1/1 | Running | 0 | 29m |
| sdponncm-7cb88677c8-rcdfz | 1/1 | Running | 0 | 29m |
| sdponnda-7d66c6994c-d45gs | 1/1 | Running | 0 | 29m |
| sdponsecurity-7578f648b9-2kl2r | 1/1 | Running | 3 | 29m |
| sdponsubscribermanager-5bd67648bc-s6b9s | 1/1 | Running | 0 | 29m |
| sdpontelemetry-79579f9f94-xcwz8 | 1/1 | Running | 0 | 29m |
| voltctl-7cdd49ff85-6n9ml | 1/1 | Running | 0 | 29m |

- Execute the following command to check the Kubernetes IP address.

```
oltausr@localhost:~$ sudo kubectl get nodes -o wide
```

Figure 83. Kubernetes Nodes List after IP Change

| NAME | STATUS | ROLES | OS-IMAGE | INTERNAL-IP | EXTERNAL-IP | KERNEL-VERSION | CONTAINER-RUNTIME |
|-----------|--------|----------------------|--------------------------------|-------------|-------------|---------------------------|-------------------|
| localhost | Ready | control-plane,master | Debian GNU/Linux 11 (bullseye) | 39m | v1.21.5 | 10.3.3.59 | <none> |
| | | | | | | 5.10.201-OpenNetworkLinux | docker://20.10.8 |

- DHCP procedure for the IP address change.


Note:

- You must perform the DHCP initial deployment. For more information on the DHCP procedure, refer to the *CBAC-D Installation Guide*.
- OLT device registration must be successful.

The following figure illustrates the successful registration of the device before the IP address change.

Figure 84. Device Registration Before IP Address Change

```
Linux localhost 4.19.81-OpenNetworkLinux #1 SMP Mon Jan 23 09:45:05 UTC 2023 x86_64
Last login: Fri Feb  3 10:47:00 2023 from 172.24.56.225
oltausr@localhost:~$ cat /mnt/onl/sdpon/oltregister.txt
OLT Auto discovery - Registered OLT
oltausr@localhost:~$
```

The following figure illustrates the network interfaces file for the DHCP assignment on the **eno1** interface of the existing configuration.

Figure 85. Network Interface File

```
oltausr@localhost:~$ cat /etc/network/interfaces

iface lo inet loopback
auto ma1
iface ma1 inet static
    address 172.27.180.132
    netmask 255.255.252.0
    up ip route add 172.0.0.0/8 via 172.27.183.254 || true

allow-hotplug eno1
iface eno1 inet dhcp
```

- Reboot the OLT to get a new DHCP IP address on the inband interface.
- Verify the status of the CBAC deployment in the */var/log/sdpon_deploy.log* file.
- After the successful CBAC deployment, execute the following command to verify the CBAC deployment status.

```
sudo kubectl get nodes -o wide
```

If OLT IP change also includes the repo server IP change, the latest repo server IP must be pushed from RMS as explained in [Changing IP Address \(on page 409\)](#). If the setup is not added to RMS, the latest repo server IP must be pushed from SDPON CLI using *sdpon_update_settings* option. For more information, refer to *CBAC CLI Reference*.

Changing IP Address

Perform the following steps to change the IP address of the OLT.



Note: You cannot modify a controller without deactivating it.

1. Select **Configuration > Controller**.
2. Click the edit icon from the **Action** column.

The Controller Configuration page appears.

3. Click the Kafka tab and enter the new IP of the controller in the **Host** field.
4. Click the Rest tab and modify the URL with the latest IP in the **REST Base URL** field.
5. If there is a change in Repository Server IP, navigate to **Settings > SDPON settings** and modify the **new Repo IP** in **Artifact Repo IP** field.
6. Click **Save** to save your changes.
7. Click on the three dots (⋮) corresponding to the controller and click the **Activate** option.
8. Execute the following steps to ensure that the controller is active and up.

- a. Click on the three dots (⋮) corresponding to the controller and click the **Monitor** option.
The Controller Details Page is displayed.
 - b. Ensure the following status of the controller.
 - Admin state must be Active.
 - Operational state, Rest, and Kafka must be Up.
9. Select **Configuration > Inventory > OLT**.
10. Click the edit icon from the **Action** column.
- The OLT Configuration page appears.
11. Enter the latest IP in the **Management IP** field and click **Save**.
 12. Click on the three dots (⋮) corresponding to the OLT and click the **Activate** option.
 13. Execute the following steps to ensure the OLT is Up with the latest IP and all services are resumed.
 - a. Click on the three dots (⋮) corresponding to the OLT and click the **Monitor** option.
The OLT Details Page appears.
 - b. Ensure the following status of the OLT.
 - Admin state must be Active.
 - Controller and Operational state must be Up.

Resolving IP Conflict

Sometimes software needs to be restored due to logical corruption or other reasons. If the OLT IP is changed after the last successful backup, the reconciliation process shows an IP conflict in the **Conflict** tab of the **Reconciliation** page.

Perform the following steps to resolving the IP conflict.

1. Select **Monitor > Inventory > Controller**.
The Controller List page appears.
2. Click on the controller name from the **Name** column.
The Controller details page appears.
3. Click the **Reconciliation** tab and then click the **Conflict** tab.
4. Select the applicable resource name checkbox and click on the eye icon from the **Compare** column.
RMS vs Controller Compare page is displayed, indicating the conflict.
5. Deactivate and activate the OLT from RMS to resolve the IP conflict. For more information, see [Activating and Deactivating the OLT \(on page 324\)](#).
6. Select **Configuration > Subscriber > Service** and verify that the OLT is up and services are resumed.

Perform the following steps to update Kafka and rest with the new OLT IP.

If the OLT IP is changed after the RMS backup, restoring the RMS to a previous backup can show IP conflicts on the reconciliation page. Follow the below procedure to resolve the IP conflict in RMS.



Note: You cannot modify a controller without deactivating it.

1. Select **Configuration > Controller**.
2. Click the edit icon from the **Action** column.

The Controller Configuration page appears.

3. Click the Kafka tab and enter the new IP of the controller in the **Host** field.
4. Click the Rest tab and modify the URL with the latest IP in the **REST Base URL** field.
5. Click **Save** to save your changes.
6. Click on the three dots (⋮) corresponding to the controller and click the **Activate** option.
7. Execute the following steps to ensure that the controller is active and up.
 - a. Click on the three dots (⋮) corresponding to the controller and click the **Monitor** option.

The Controller Details Page is displayed.

- b. Ensure the following status of the controller.
 - Admin state must be active.
 - Operational state, Rest, and Kafka must be up.
8. Resolve all the orphans, conflicts, and pending state of resources during the reconciliation process.
9. Deactivate and activate the OLT from RMS to resolve the IP conflict. For more details, see [Activating and Deactivating the OLT \(on page 324\)](#).

10. Select **Configuration > Inventory > OLT**.
11. Click the edit icon from the **Action** column.

The OLT Configuration page appears.

12. Enter the latest IP in the **Management IP** field and click **Save**.
13. Click on the three dots (⋮) corresponding to the OLT and click the **Activate** option.
14. Select **Configuration > Subscriber > Service** and verify that the OLT is up and services are resumed.

Rings

A ring is formed to define the physical ring topology to which the OLT belongs.

A ring is formed on the OLT by associating two NNI ports of the OLT. A ring ID is provided to identify the physical ring topology.

The same ring ID is configured on all the nodes in the physical RING.

You can configure the ring ID in the range of 1 to 239 for each ERPS instance. The ring ID is used in the R-APS message transmission function to determine the value of the last octet value of the MAC destination address field of the R-APS protocol data units (PDUs), which is generated by the ERPS protocol on a particular RING Node.

The validity check function also uses the ring ID to discard any R-APS PDUs received by the ERPS protocol on a particular ring node with a non-matching ring ID.

When you configure the ring ID, the following rules must apply.

- All ring nodes in a ring must be identified by a unique (ring ID and Control [R-APS] VID) pair.
- For a ring, all ERPS instances must be assigned a different value of the control VLAN ID on the same underlying physical ring.
- Across the rings, the ERPS instances can be assigned the same control VLAN ID.

Field Descriptions

The following table describes the fields on the Ring List page.

Table 190. Ring List

| Field | Description |
|------------------------------|--|
| Name | Specifies the unique name of the ring. |
| Ring ID | Specifies the ring ID. |
| Ring Type | Specifies the ring type. |
| East port | Specifies the ERPS instance east port. |
| West port | Specifies the ERPS instance west port. |
| Configuration Status | Specifies the configuration status of the ring. |
| Configuration Failure Reason | Specifies the reason for the configuration failure. |
| Creation Time | Specifies the date and time when the ring was created. |
| Action | Specifies the action that you can perform on the ring. |

Creating Ring Configuration

Perform the following steps to create a ring configuration.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab.
3. Click on the three dots (⋮) corresponding to the OLT on which you want to add a ring and select the **Rings** option.

The Ring List page appears.

4. Complete the configuration according to the guidelines provided in the following table.

Table 191. Ring Configuration

| Field | Description |
|-----------|---|
| Name | Enter a unique name for the ring. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space |
| Ring ID | Enter the ring ID used for creating the ring. The value ranges from 1 to 255. |
| Ring Type | Specifies the ring topology type. <ul style="list-style-type: none">◦ MAJOR. In this type of rings, nodes are connected in full circular topology.◦ SUB-RING. This type does not support R-APS virtual channel. The default value is SUB-RING. |
| East port | Enter the port on OLT, which is connected towards the east side of the physical ring. This can be either NNI port or LAG port. Example: NNI-1 |
| West port | Specifies the port on OLT, which is connected towards the west side of the physical ring. This can be either NNI port or LAG port. Example: NNI-2 |

ERPS Instance

Ethernet Ring Protection Switching (ERPS) is a protection switching mechanism for Ethernet networks and it uses the G.8032 defined Ring Automatic Protection Switching (R-APS) protocol to provide protection for Ethernet traffic in a ring topology.

ERPS uses a specific link to protect the entire Ethernet ring and the link is called Ring Protection Link (RPL).

Field Descriptions

The following table describes the fields on the ERPS Instance List page.

Table 192. ERPS Instance

| Field | Description |
|-----------------------------|---|
| Name | Specifies the ERPS instance name. |
| ERPS Profile | Specifies the ERPS profile ID. |
| State | Specifies the ERPS instance state. The supported states are. <ul style="list-style-type: none"> • Initializing • Idle • Pending • Protection • Force-switch • Manual-switch |
| Port | Specifies the port details. |
| Port Role | Specifies the port role. The supported roles are. <ul style="list-style-type: none"> • RPL • NORMAL • NEIGHBOR • NEXT NEIGHBOR |
| Port State | Specifies the port state. The supported statuses are. <ul style="list-style-type: none"> • forwarding • blocked • failed • local-ms • local-fs |
| Configuration Status | Specifies the port configuration status. |
| Config Failure Reason | Specifies the reason for the configuration failure. |
| East Port Mep Instance | Specifies the MEP instance that must be used on the east port to detect the port status. The ERPS Instance creation fails if the MEP instance mentioned is not created. |
| West Port Mep Instance | Specifies the MEP instance that must be used on the west port to detect the port status. The ERPS Instance creation fails if the MEP instance mentioned is not created. |
| East Port Mep Instance List | Specifies the MEP instance list that must be used on the east port to detect the port link status. |

Table 192. ERPS Instance (continued)

| Field | Description |
|-----------------------------|--|
| | The ERPS instance creation fails if the MEP instance list mentioned is not created with the port. If the east port is a LAG port, the MEP instances are created with the LAG member ports. |
| West Port Mep Instance List | Specifies the MEP instance list that must be used on the west port to detect the port link status. The ERPS instance creation fails if the MEP instance list mentioned is not created with the port. If the east port is a LAG port, the MEP instances are created with the LAG member ports. |
| Creation Time | Specifies the date and time when the ERPS instance was created. |
| Action | Specifies the action that you can perform on the ERPS instance. <ul style="list-style-type: none"> Delete Clone |

Creating ERPS Instance



Note: Before you create an ERPS instance, you must create a Ring configuration. See [Creating Ring Configuration \(on page 412\)](#).

Perform the following steps to create a ERPS instance configuration.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab.
3. Click on the three dots (⋮) corresponding to the OLT and select the **Rings** option.
The Ring List page appears.
4. Select ERPS Instance from the **Action** column.
The ERPS Instance List page appears.
5. Complete the configuration according to the guidelines provided in the following table.

Table 193. ERPS Instance Configuration

| Field | Description |
|-------|---|
| Name | Enter a unique name for the ERPS instance. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> Underscore (_) Hyphen (-) |

| Field | Description |
|-----------------------------|--|
| ERPS Profile | Enter the ERPS profile ID. |
| East Port Mep Instance | Select the MEP instance that must be used on the east port to detect the port status. The ERPS Instance creation fails if the MEP instance mentioned is not created. |
| West Port Mep Instance | Select the MEP instance that must be used on the west port to detect the port status. The ERPS Instance creation fails if the MEP instance mentioned is not created. |
| East Port Mep Instance List | Select the MEP instance list that must be used on the east port to detect the port link status. The ERPS instance creation fails if the MEP instance list mentioned are not created with the port. If the east port is a LAG port, the MEP instances are created with the LAG member ports. |
| West Port Mep Instance List | Select the MEP instance list that must be used on the west port to detect the port link status. The ERPS instance creation fails if the MEP instance list mentioned are not created with the port. If the east port is a LAG port, the MEP instances are created with the LAG member ports. |

6. Click **Create**.

A new ERPS instance is created on the ERPS Instance List page.

MEP Instance

You can create Managed End Point (MEP) instance using the MEP profile. One or more MEP instances can be added for the same physical link.

Field Descriptions

The following table describes the fields on the MEP Instance List page.

Table 194. MEP Instance List

| Field | Description |
|----------------------|--|
| Name | Specifies the unique name of the MEP instance. |
| MEP Profile Name | Specifies the name of the MEP profile. |
| Port | Specifies the name of the port. |
| Configuration Status | Specifies the port configuration status. |

Table 194. MEP Instance List (continued)

| Field | Description |
|-----------------------|--|
| Config Failure Reason | Specifies the reason for the configuration failure. |
| Loc State | Specifies the loss of connectivity with the remote MEP. The supported values are. <ul style="list-style-type: none"> True False |
| Creation Time | Specifies the date and time when the MEP instance was created. |
| Action | Specifies the action that you can perform on the ERPS instance. <ul style="list-style-type: none"> View the MEP instance configuration Delete Clone |

Creating MEP Instance



Note: Before you create an MEP instance, you must create a MEP profile. See [Creating MEP Profile \(on page 550\)](#).

Perform the following steps to create an MEP instance,

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the OLT tab.
3. Click on the three dots (⋮) corresponding to the OLT on which you want to add an MEP instance.
The MEP Instance List page appears.
4. Complete the configuration according to the guidelines provided in the following table.

Table 195. MEP Instance Configuration

| Field | Description |
|-------------|--|
| Name | Enter a unique name for the MEP instance. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> Underscore (_) Hyphen (-) |
| Port | Select the port from the list. |
| MEP Profile | Select the MEP profile from the list. |

5. Click **Create**.

A new MEP instance is created on the MEP Instance List page.

ONT Firmware Download on OLT

The Internet Service Provider (ISP) or an operator deploys the OLT and ONT to use GPON or XGSPON technology in their network to provide different types of services to the subscribers. Once these devices are deployed, the ISP provider or operator may have to upgrade the firmware on these devices to improve subscriber services. The firmware can have new features and enhancements to the existing features.

The ONTs are the devices that provide network services to the end users, but they are not accessible directly using an IP address, that is, the ONTs may not have a management IP address. As these ONTs are located on the remote premises such as a subscriber home or apartment, the OMCI standard specifies a procedure to upload software to the ONTs.

There are multiple components of CBAC involved in downloading software to the ONTs. The components are RMS/EMS-CLI, EMS-GW, Device Manager, Subscriber Manager, AccessGw, RWCore, OpenONU Adaptor, OpenOLT Adaptor, and OpenOltAgent.

You can upgrade the firmware for a single ONT or a bulk of ONTs that belongs to the OLT. However, for a bulk upgrade, the time taken to finish the upgrade may vary based on the number of ONTs.

You must follow the steps to download the ONT firmware.

1. Download the ONT firmware on the OLT.
2. Download the ONT firmware on the ONT.
3. Activate and commit the ONT firmware.

The above operations must be performed in a sequential manner and the next option is enabled only if the previous operation was successful.

Perform the following steps to download the ONT firmware on the OLT.



Note:

- Before performing the ONT firmware upgrade, you must create the version for the ONT for which you want to upgrade the software. For more information, see [Creating Model Version Configuration \(on page 612\)](#).
- Before performing the ONT firmware upgrade, you must create a make and model configuration for the respective ONTs. For more information, see [Creating Make Configuration \(on page 606\)](#) and [Creating Model Configuration \(on page 610\)](#).
- Ensure the ONT firmware image on the repository server must have read and write permission to everyone (0666).

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the **OLT** tab.
3. Click on the three dots (⋮) corresponding to the OLT on which you want to download the ONT firmware and select the **ONT Firmware Download on OLT** option.

The Download ONT Firmware page appears.

4. Complete the configuration according to the guidelines provided in the following table.

Table 196. ONT Firmware Download

| Field | Description |
|---------|---|
| Make | Specifies the make of the ONT. If the make configuration does not exist, see Creating Make Configuration (on page 606) . |
| Model | Specifies the model of the ONT. If the model configuration does not exist, see Creating Model Configuration (on page 610) . |
| Version | Specifies the ONT software version that you want to download on the OLT. |

5. Click **Download**.

A success message appears and indicates that the ONT firmware download on OLT is successful. The ONT firmware is downloaded into the OLT file system.

6. Now the **ONT Firmware Download on ONT** option is enabled. Click this option.

The ONT Firmware Download ONT <Version Number> page appears.

7. Select one or more ONTs from the list.
8. Enable the **Auto Activate** option if you want to automatically activate the ONT software once the download operation is successful.
9. Click **Download**.

A success message appears and indicates that the ONT firmware download on the ONT is successful.



Note: If you have not selected the **Auto Activate** option, you can activate and commit the ONT software explicitly using the **Activate Commit ONT Firmware** option.

10. Select the **Activate Commit ONT Firmware** option.

The ONT Firmware Activate ONT <Version Number> page appears.

11. Select the ONTs to activate and click **Activate**.

A success message appears and indicates that the ONT firmware activate and commit operations is successful.

You can also schedule the ONT firmware upgrade for a later date and time. For more information, see [Creating Task for ONT Firmware Upgrade \(on page 674\)](#).

ONT Firmware Partition Cleanup

Perform the following steps to cleanup the ONT images downloaded on the OLT file system.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the OLT tab.
3. Click on the three dots (⋮) corresponding to the OLT and select the **ONT Firmware partition cleanup** option.
A confirmation message appears to indicate that the partition is cleaned-up successfully.

Multicast Configuration

A user can add multicast configuration for each OLT added to the network. The multicast configuration specifies a tuple of (MVLAN Profile + IGMP Profile + IGMP source IP) bound for the given OLT. Multiple multicast configurations can be added to an OLT, each corresponding to a unique MVLAN profile.

Field Descriptions

The following table describes the fields on the Multicast Configuration List page.

Table 197. Multicast Configuration List

| Field | Description |
|----------------|---|
| Multicast Name | Specifies the unique name of the multicast configuration name. |
| Mvlan Profile | Specifies the name of the MVLAN profile. |
| IGMP Profile | Specifies the name of the IGMP profile. |
| IGMP Source IP | Specifies the IGMP source IP address. |
| Creation Time | Specifies the date and time when the multicast configuration was created. |
| Action | Specifies the action that you can perform on the multicast configuration. <ul style="list-style-type: none">• Edit• Delete• Clone |

Creating Multicast Configuration



Note: Before you create an MEP instance, you must create an MVLAN profile. See [Creating MVLAN Profile \(on page 568\)](#).

Perform the following steps to create a multicast configuration.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the **OLT** tab.
3. Click on the three dots (⋮) corresponding to the OLT on which you want to edit the multicast configuration.
4. Click the **Multicast Config** option.
The Multicast Configuration List page appears.
5. Complete the configuration according to the guidelines provided in the following table.

Table 198. Multicast Configuration

| Field | Description |
|----------------|--|
| Name | Enter a unique name for the multicast configuration. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">Underscore (_)Hyphen (-)Space |
| Mvlan Profile | Select the MVLAN profile. |
| IGMP Profile | Select the IGMP profile. |
| IGMP Source IP | Specifies the source IP that the IGMP proxy should be using towards the network. Example: 192.168.56.1 |
| MLD Source IP | Specifies the MLD source IP. It only accepts IPv6 link-local address. Example: FE80::0102:0304 |

6. Click **Create**.

A new multicast configuration is created on the Multicast Configuration List page.

To edit, clone, and delete the multicast configuration, see [Common Operations \(on page 27\)](#).

Enabling and Disabling OLT Anti Theft Configuration

Due to the increase in hardware (OLT) theft, OLT is designed with an anti-theft mechanism such that the OLT is unusable outside the operator's network when it is stolen.



Note: Before enabling anti-theft support on OLT, ensure that the name resolution for FQDN is completed either by using the DNS name server or configuring it in the `/etc/hosts` files.

Perform the following steps to enable the OLT anti theft configuration.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the **OLT** tab.
3. Click on the three dots (⋮) corresponding to the OLT on which you want to enable the anti-theft configuration and click the **Enable Anti Theft** option.

The Grace Period page appears.

4. Configure the grace period as shown in the following table.

Table 199. Grace Period Configuration

| Field | Description |
|-----------------------------------|--|
| Grace Period (Days/Hours/Minutes) | <p>Specifies the duration for OLT to be moved to locked state from pre-locked state.</p> <ul style="list-style-type: none">◦ If the selected unit is Days, the value ranges from 1 to 7.◦ If the selected unit is Hours, the value ranges from 1 to 23.◦ If the selected unit is Minutes, the value ranges from 1 to 59. <p> Note: You can configure a maximum of seven days.</p> |

5. Click **Submit**.

A confirmation message appears indicating that the anti theft configuration on the OLT is enabled successfully.

6. Click on the three dots (⋮) corresponding to the OLT and click **Monitor** option to monitor the OLT anti theft status and lock state of the OLT. For more information, see [Monitoring OLT \(on page 67\)](#).

Perform the following steps to disable the OLT anti theft configuration.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the **OLT** tab.
3. Click on the three dots (⋮) corresponding to the OLT on which you want to disable the anti theft configuration and click the **Disable Anti Theft** option.

A confirmation message appears indicating that the anti theft configuration on the OLT is disabled successfully.

4. Click on the three dots (⋮) corresponding to the OLT and click **Monitor** option. For more information, see [Monitoring OLT \(on page 67\)](#).

Downloading ATP Report

The Acceptance Test Procedure (ATP) report specifies network and service related test cases for an OLT.



Note: A user with admin privilege can download the report.

Perform the following steps to download the ATP report for the OLT.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the **OLT** tab.
3. Click on the three dots (⋮) corresponding to the OLT for which you want to download the ATP report and click the **ATP Report** option.

The Configuration Summary Report page appears.

4. Click **Print Report**.

The file is downloaded in PDF format and appears at the bottom of the page.

ONT

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Inventory > ONT** from the left-hand side of the menu.

An optical network terminal (ONT) is the device that terminates PON to the subscriber's residence or an enterprise office. ONT is applied to the end user and is present in the CPE. A subscriber is configured to a specific PON port of a particular OLT. Hence, a subscriber can gain access only when the CPE is connected to the configured PON port of the OLT. The OLT and ONUs communicate through the optical distribution network (ODN).

The CBAC network admits a PON connection only from the known ONT serial numbers. When CBAC discovers an ONT, it validates the serial number of the ONT and allows it if the serial number is detected on the configured OLT and PON port. If the ONT is unknown or is detected on a PON port that is not configured, CBAC raises authentication failure traps or sends an alarm to RMS.

Tasks

You can perform the following tasks from this page.

- Create ONT configuration. See [Creating ONT Configuration \(on page 427\)](#).
- Activate the ONT. See [Activating the ONT \(on page 431\)](#).
- Deactivate the ONT. See [Deactivating the ONT \(on page 431\)](#).
- Reboot the ONT. See [Rebooting the ONT \(on page 432\)](#).
- ONT Firmware Activate Standby Partition. See [Activating Standby Partition \(on page 436\)](#).
- HTTP Configuration. See [HTTP Configuration \(on page 432\)](#).
- View the physical and logical topology of the ONT. See [Topology \(on page 283\)](#).
- View UNI port details of the ONT. See [UNI Port Configuration \(on page 434\)](#).
- Monitor the OLT details such as OLT health status and basic information. See [Monitoring ONT \(on page 156\)](#).
- View the physical link of the ONT.
- Filter the ONT list based on the following field. Filter enables you to quickly find and display the entries that are relevant to your specific needs.
 - Name
 - Admin State
 - Operational State
 - Display ID
 - Click on the icon  to clear the applied filters.

Field Descriptions

The following table describes the fields on the ONT page.

Table 200. ONT Inventory

| Field | Description |
|-------------------|---|
| Name | Specifies the name of the ONT. |
| Admin State | Specifies the admin state of the ONT. <ul style="list-style-type: none">• Green. Indicates that the ONT is ACTIVE.• Red. Indicates that the ONT is DEACTIVE. |
| Operational State | Specifies the operational state of the ONT. |

Table 200. ONT Inventory (continued)

| Field | Description |
|---------------------|--|
| | <ul style="list-style-type: none">• Green. Indicates that the ONT is UP.• Red. Indicates that the ONT is DOWN. |
| Make | Specifies the vendor name of the ONT. |
| Model | Specifies the model name of the ONT. |
| Display ID | Specifies the display ID of the ONT. Example: rack=1/shelf=1/slot=ETH1/port=1/remote_unit=onu1 |
| Serial No | Specifies the serial number of the ONT. Example: ISKT429D8B45 |
| Serial No Status | Specifies whether the serial number is enabled. The supported values are. <ul style="list-style-type: none">• ENABLED• DISABLED |
| Device Profile | Specifies the name of the ONT device profile. |
| Management Domain | Specifies the name of the management domain. |
| Controller | Specifies the name of the controller. |
| Alarm Profile | Specifies the ONT alarm profile. |
| Log Profile | Specifies the log profile configured for the ONT. |
| ZTP Template | Specifies the ZTP template of the ONT. |
| Server | Specifies the server name. |
| Authentication Type | Specifies the authentication type of the ONT. The supported values are. <ul style="list-style-type: none">• LOCAL• RADIUS |
| OLT | Specifies the name of the OLT to which the ONT is connected. |
| Port | Specifies the port name associated with the ONT. |
| Registration ID | Specifies the registration ID of the ONT. |
| Vendor ID | Specifies the vendor ID of the ONT. |
| Equipment ID | Specifies the equipment ID. |

Table 200. ONT Inventory (continued)

| Field | Description |
|-------------------------------|---|
| Time of Day | Specifies whether the time of day (TOD) distribution is supported. If the value is set to True, CBAC or the OLT enables the transfer of TOD information to the ONT over the OMCI channel. |
| Up Since Time | Specifies the date and time from when the ONT is UP. |
| ONT Firmware Upgrade Status | Specifies the ONT firmware upgrade status on the OLT. The supported values are. <ul style="list-style-type: none"> • DOWNLOAD-SUCCESSFUL • ACTIVATE-COMMIT-INITIATED • ACTIVATE-COMMIT-SUCCESSFUL • DOWNLOAD-FAILED |
| ONT Firmware Version | Specifies the current version of the ONT firmware. |
| ONT Firmware Download Version | Specifies the firmware version of the ONT that was downloaded. |
| Hardware Version | Specifies the hardware version of the ONT. |
| Active Firmware Version | Specifies the firmware version of the active ONT. |
| Standby Firmware Version | Specifies the firmware version of the standby ONT. |
| Software Version | Specifies the software version of the ONT. |
| Connectivity Mode | Specifies the connectivity mode that is used for the services on the ONU. |
| Me Group | Specifies the ME group to which the ONT belongs. |
| ONT Number | Specifies the ONT number. |
| ONU Physical Distance | Specifies the physical distance of an ONU in Km from the OLT on the PON port. |
| Upstream FEC | Specifies whether Forward Error Correction (FEC) is enabled in upstream traffic. The supported values are. <ul style="list-style-type: none"> • ENABLED • DISABLED The default values are specific to the PON technology. The default value for GPON is ENABLED. The default value for XGSPON is ENABLED. |
| Rx Optical Power (in dBm) | Specifies the current measurement of optical received power level. |
| Creation Time | Specifies the date and time when the ONT was created. |

Table 200. ONT Inventory (continued)

| Field | Description |
|--------|--|
| Action | Specifies the action that you can perform on the ONT. The supported actions are. <ul style="list-style-type: none">• Edit• Delete• Clone |

Creating ONT Configuration



Note: Before you create an ONT, you must create the following.

- Management domain
- Make
- Model
- Device profile
- Controller

Perform the following steps to create the ONT.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the **ONT** tab.
3. Click **Create**.
The ONT Configuration page appears.
4. Complete the configuration according to the guidelines provided in the following table.

Table 201. ONT Configuration

| Field | Description |
|----------------------|--|
| Basic Details | |
| Name | Enter a unique name for the ONT. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Make | Select the make from the list. If the make does not exist, click the plus icon (+) to create a make configuration for the ONT. See Creating Make Configuration (on page 606) . |

| Field | Description |
|-------------------------|---|
| Model | Select the device model from the list. If the device model does not exist, click the plus icon (+) to create a model for the ONT. See Creating Model Configuration (on page 610) . |
| Device Profile | Select the device profile from the list. If the device profile does not exist, click the plus icon (+) to create a device profile for the ONT. See Creating OLT Device Profile (on page 509) . |
| OLT | Enter the OLT to which you want to connect the ONT. |
| Port | Enter the OLT PON port. |
| Active Firmware Version | Specifies the firmware version of the active ONT. |
| Serial No | Enter the serial number for the ONT. The maximum length is 12 characters, where the first four characters must be ASCII text (plain text) and the remaining eight characters must be hexadecimal. Example: TWSH80808091 |
| Registration Id | Enter the registration ID for the ONT. <ul style="list-style-type: none"> ◦ The registration ID can be either alphanumeric or hexadecimal value. ◦ If the registration ID is alphanumeric, the maximum allowed characters are 36. ◦ If the registration ID is hexadecimal, the maximum allowed characters are 74 including the prefixed (0x) hex representation character and must be an even set of characters. ◦ There is no minimum character length. Example (Alpha numeric): 123456789123456789ABCDEFGHabcdefghi Example (Hexadecimal): 0x 30316566676869707172 |
| ONT Number | Enter the ONT number. The number must be in integer. |
| Enable Time of Day | Specifies whether the Time of Day (ToD) distribution is supported. If the value is set to Yes , CBAC or the OLT enables the transfer of ToD information to the ONT over the OMCI channel. |
| Upstream FEC | Specifies whether Forward Error Correction (FEC) is enabled in the upstream traffic. The supported values are. <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED The default values are specific to the PON technology. The default value for GPON is ENABLED. The default value for XGSPON is ENABLED. |

| Field | Description |
|-------------------|--|
| Connectivity Mode | <p>Selects the connectivity mode that must be used for the services on the ONU. The supported values are.</p> <ul style="list-style-type: none"> ◦ N:1 bridging ◦ 1:M mapping ◦ 1:P filtering ◦ N:M bridge-mapping ◦ 1:MP map-filtering ◦ N:P bridge-filtering ◦ N:MP bridge-map-filtering <p>The default value must be same as the <i>current_connectivity_mode</i> reported by the ONU.</p> <p>The default value for residential service is 1:MP map-filtering.</p> |
| Force Delete | <p>Deletes the ONT configuration forcefully. The supported values are.</p> <ul style="list-style-type: none"> ◦ TRUE ◦ FALSE <p>The default value is FALSE.</p> |
| MAC Limit | <p>Specifies the MAC learning depth attribute of the ME MAC bridge service profile on the ONU.</p> <p>This attribute specifies the maximum number of UNI MAC addresses to be learned by the bridge. The default value is 0 and it specifies that there is no administratively imposed limit.</p> <p>The supported value ranges from 0 to 255.</p> <p>This value can be modified when the ONT is in the deactivated state.</p> |
| MAC Ageing Time | <p>Specifies the MAC ageing time in seconds.</p> <p>This attribute specifies the maximum time an ONT can hold a MAC entry in the MAC table when there is no data received from the device.</p> <p>The supported value ranges from 0 to 1000000.</p> <p>The accepted values are 10 to 1000000 and 0.</p> <p>The default value is 0 and indicates behavior is specific to the ONT implementation.</p> <p>This value can be modified when the ONT is in the deactivated state.</p> |
| Auto Upgrade | <p>Specifies whether the ONU must be upgraded with the firmware version, that is mentioned in the ONT Firmware Version Table when the CBAC detects that the firmware version is not matching with the version mentioned in the table.</p> <p>The ONT is upgraded when the ONT is activated after the PON fluctuation or ONT reboot process.</p> <p>The default value is false.</p> |

| Field | Description |
|--------------------------|--|
| Planned Firmware Version | Specifies the expected firmware version of the ONT when the ONT is discovered. |
| DBA Type | Selects the DBA type to be used for ONTs that are created for the ONUs for services. The supported values are. <ul style="list-style-type: none"> ◦ NSR ◦ SR The default value is NSR. If ONU does not support the value SR, CBAC defaults to the value NSR internally. The user can see the supported DBA Type modes in ONU Monitoring capability. |
| Auto Activate | Enable this option to activate the ONT automatically after the successful creation of the ONT. |
| Advanced Details | |
| Profiles | |
| Alarm Profile | Select the alarm profile from the list. If the alarm profile does not exist, click the plus icon (+) to create an alarm profile for the ONT. See Alarm Profile (on page 473) . |
| ANI-G Alarm Profile | Select the ONT ANI-G alarm profile from the list. |
| State | |
| Resource State | Select the resource state from the list. The supported states. <ul style="list-style-type: none"> ◦ PLANNED ◦ INSTALLED ◦ RETIRED |
| Lock State | Select the lock state from the list. The supported states. <ul style="list-style-type: none"> ◦ NONE ◦ LOCKED ◦ TESTING ◦ UNLOCKED |
| Alias | Enter the alias name for the ONT. |

**Note:**

- Before you edit the ONT, you must deactivate the ONT.
- You cannot modify the following fields.



- ONT ID
 - Manageable Device
 - Display ID
 - Connectivity Mode
 - Vendor ID
 - Equipment ID
 - Active Firmware Version
 - Connectivity Mode
 - MAC Ageing Time
- You cannot delete the ONT when it is in activate state or any service is associated with the ONT. Before deleting the ONT, ensure that you deactivate the associated service with the ONT and then deactivate the ONT.
 - RMS deletes all the events, alarms (current and historical), and historical KPIs from its database after the ONT deletion.

To edit, clone, and delete the ONT configuration, see [Common Operations \(on page 27\)](#).

Activating the ONT

You can activate the ONT after successful creation of the ONT.

Perform the following steps to activate the ONT.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the ONT tab.
3. Click on the three dots (⋮) corresponding to the ONT that you want to activate and click the **Activate** option.
A confirmation message appears indicating the status of the operation and the admin state of the ONT changes to ACTIVE.

Deactivating the ONT

Perform the following steps to deactivate the ONT.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the ONT tab.
3. Click on the three dots (⋮) corresponding to the ONT on which you want to deactivate and click the **Deactivate** option.
A warning pop-up message appears stating, Deactivating <ont-name> disrupts associated subscriber's services. Are you sure to proceed with the deactivation of <ont-name>?

4. Click **Yes, Deactivate** to deactivate the ONT.

A confirmation message appears, indicating the status of the deactivate operation. After ONT deactivation, the admin state of the ONT changes to DEACTIVE.

Rebooting the ONT

ONT reboot recovers the system. RMS supports an immediate reboot of the ONT remotely.

Perform the following steps to reboot the ONT.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the ONT tab.

3. Click on the three dots (⋮) corresponding to the ONT that you want to reboot and click the **Reboot** option.

The following warning message appears.

Rebooting ONT could result in an impact on subscriber service. Are you sure to perform this action?

4. Click **Confirm** to reboot the ONT.

RMS sends a reboot request to CBAC. CBAC reboots the ONT if the request is valid.

HTTP Configuration

Port 80 (HTTP configuration) on ONT is enabled or disabled for ONT's Web GUI access from OMCI. It works in the fire-and-forget model (GET on this feature may not be the actual value). You must enable the Port 80 (HTTP configuration) on the ONT to access the ONT Web GUI using the WAN interface, and the values must be set as **Enable**.

The ONT HTTP access is required to log into the ONT web GUI to perform the following operations for the ONT.

- Configure a Wifi username and password
- Use port diagnostics
- Initiate a ping
- Modify wireless parameter
- Upgrade ONT
- View port statistics

If the ONT does not support this feature, it is reported as NOT SUPPORTED and the following error message is displayed.

Service on WAN interface of the ONT should be operationally UP before performing this operation.

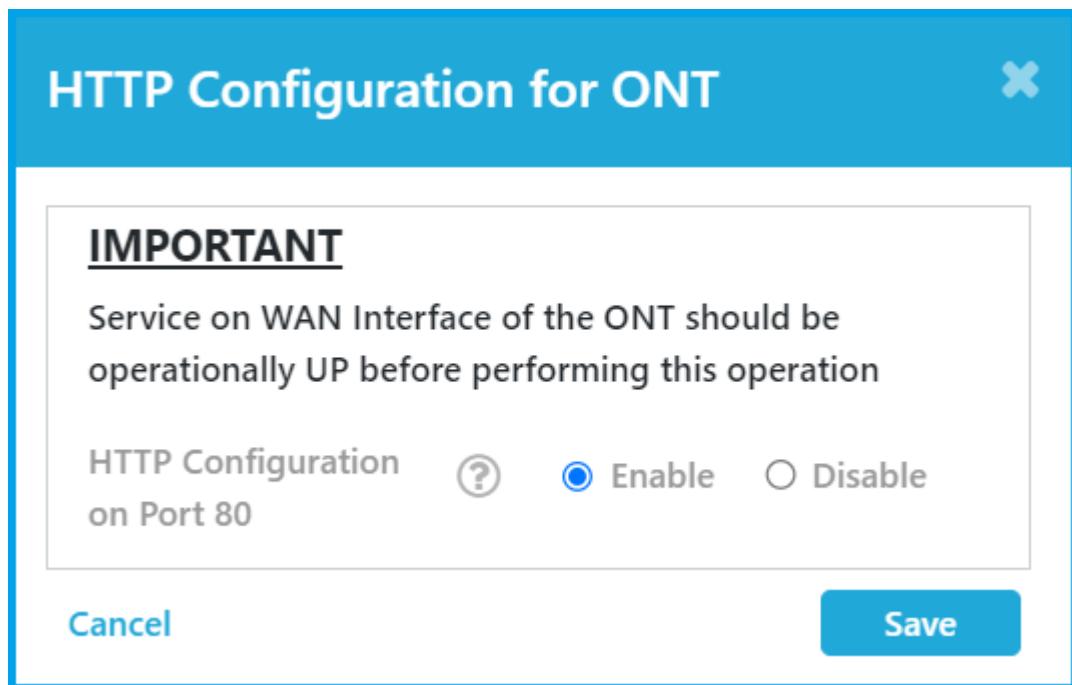
ONT removes the user from the live Web GUI if the session is inactive for 15 minutes. If IP-HOST is used for the PPPoE WAN service creation, you must activate the port after attaching the PPPoE profile. After the port activation, the PPPoE service on the WAN must be activated.



Note: The HTTP configuration on an ONT is allowed only when the ONT operational state is UP.

Perform the following steps to configure the HTTP on an ONT.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the ONT tab.
3. Click on the three dots (⋮) corresponding to the ONT and select the **HTTP Configuration** option.
The following image appears.



4. Complete the HTTP configuration according to the guidelines provided in the following table.

Table 202. HTTP Configuration

| Field | Description |
|-------------------------------|--|
| HTTP Configuration on Port 80 | Enable this field to configure the HTTP for ONT and access the Web GUI. Note: Ensure that the service on WAN interface is created and operationally UP. The HTTP configuration can then be applied on the ONT. |

5. Click **Save** to save the configuration.

UNI Port Configuration

To access this page, click on the **Ports List** from the **Action** column in the ONT.

RMS adds UNI ports to CBAC as managed entities. The UNI port is added to the sub-service configuration. The UNI port number and UNI port ID coexist in the service configuration. If the UNI port number and UNI port ID are configured, then the UNI port ID precedes the service configuration.

Perform the following steps to view the list of UNI ports configured for the ONT.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the **ONT** tab.
3. Click on the ports (grid icon) corresponding to the ONT on which you want to view the port details.

The *Ports List [Inventory - ONT Name]* page appears with the list of UNI port details.

Viewing UNI Port Configuration

You can view the existing UNI port details configured for the ONT. However, you cannot edit the UNI port configuration.

Field Descriptions

The following table describes the fields on the UNI port page.

Table 203. UNI Port List [Inventory - <ONT Name>]

| Field | Description |
|----------------|--|
| Name | Specifies name of the UNI port. Example: uni1 |
| Display ID | Specifies the display ID of the port. Example: onu-2/port=1 |
| Port Number | Specifies the port number associated with the ONT. Example: 1 |
| Port Direction | Specifies the port direction type. Example: UNI |
| UNI Port Type | Specifies the UNI port type. The supported UNI port types are. <ul style="list-style-type: none">• PPTP-POTS• PPTP-ETHERNET |

Table 203. UNI Port List [Inventory - [<ONT Name>] (continued)

| Field | Description |
|---------------------|---|
| | <ul style="list-style-type: none"> • IP-HOST • VEIP • IPv6-HOST <p>Example: PPTP-ETHERNET</p> |
| Description | Specifies the description of the UNI port. |
| Capacity | Specifies the capacity of the port. Example: 1 |
| Unit | Specifies the capacity unit of the port. Example: Gigabit, Megabit |
| Admin State | Specifies the admin state of the UNI port. The supported values are. <ul style="list-style-type: none"> • ACTIVE • DEACTIVE |
| Operational State | Specifies the operational state of the UNI port. <ul style="list-style-type: none"> • UP • DOWN • UNKNOWN |
| Action | Specifies the action that you can perform on the UNI port. The supported actions are. <ul style="list-style-type: none"> • Edit. You can edit the UNI port configuration only if the port state is “DEACTIVE”. • View. View the UNI port configuration. |
| Creation Time | Specifies the date and time when the UNI port was created. |
| Choose Profile Type | Select the profile type as PPPoE. |
| PPPoE Profile | Select the applicable PPPoE profile. |
| Service Name | Enter the service name. |
| User Name | Enter the username. |
| Password | Enter the password. |

Activating Standby Partition



Note: The standby partition on an ONT is not allowed when the auto-upgrade flag is enabled as true.

Perform the following steps to activate the standby partition on the ONT.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the ONT tab.
3. Click on the three dots (⋮) corresponding to the ONT and select the **ONT Firmware activate standby partition** option.
A confirmation message appears indicate that the standby partition is activate successfully.

Activating the UNI Port

Similar to PON port activation and deactivation, you can activate and deactivate the UNI ports of the ONT. This enables a controlled environment for the operator where an unused port does not cause any undesired activity in the network.

Once the UNI port is successfully added to the ONT, you can activate the port. When a port is active, it sends optical energy to the link and consumes power. CBAC does not accept connections from a UNI port that is not operational. A UNI port is operational only when RMS activates the UNI port.

Perform the following steps to activate the UNI port.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the ONT tab.
The ONT List page appears.
3. Click on the ports (grid) icon.
The *Ports List [Inventory - ONT Name]* page appears with the list of UNI port details.
4. Click on the three dots (⋮) corresponding to the port on which you want to activate and click the **Activate** option.
A confirmation message appears indicating that the UNI port is activated successfully.

Deactivating the UNI Port

When the ports are not in use, you can deactivate the ports to save power.

Perform the following steps to deactivate the UNI port.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Navigate to the ONT tab.

The ONT List page appears.

3. Click on the ports () icon.

The *Ports List [Inventory - ONT Name]* page appears with the list of UNI port details.

4. Click on the three dots () corresponding to the port on which you want to deactivate and click the **Deactivate** option.

A confirmation message appears indicating that the UNI port is deactivated successfully.

Initiate and Cancel MAC Dump on UNI Port

RMS allows you to initiate and cancel the MAC dump on UNI port.

You can query multiple MAC addresses of end devices connected to the ONT bridge port by initiating the MAC dump request on the UNI port based on the MAC limit configured.



Note: To query the MAC dump for each UNI port, the ONU operational state must be UP and UNI admin state must be enabled.

Perform the following steps to initiate the MAC dump on the UNI port.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the **ONT** tab.

3. Click on the ports () icon corresponding to the ONT on which you want to view the port details.

The *Ports List [Inventory - ONT Name]* page appears with the list of UNI port details.

4. Click on the three dots () corresponding to the port and click the **Initiate MAC Dump** option.

The Initiate MAC Dump page appears.

5. Complete the configuration according to the guidelines provided in the following table.

Table 204. Initiate MAC Dump on UNI port

| Field | Description |
|-------------|---|
| Vlan | Specifies the outer VLAN. This field is applicable for the MAC dump request on PON port, NNI port, and services. The supported value ranges from 2 to 4094. |
| MAC Address | Enter the MAC address. |



Note: The **Vlan** and **MAC Address** fields are optional.

6. Click **Submit**.

A confirmation message appears indicating that the MAC dump is initiated successfully.

Click on the three dots (⋮) corresponding to the UNI port and click Monitor option. For more information, see [UNI Port Details \(on page 166\)](#).

Perform the following steps to cancel the MAC dump on the UNI port.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the **ONT** tab.
3. Click on the ports (grid) icon corresponding to the ONT on which you want to view the port details.

The *Ports List [Inventory - ONT Name]* page appears with the list of UNI port details.

4. Click on the three dots (⋮) corresponding to the port and click **Cancel MAC Dump** option.
5. Click **Submit**.

A confirmation message appears indicating that the MAC dump is canceled successfully.

CPE

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Inventory > CPE** from the left-hand side of the menu.

OLTs inter-operate with diverse Customer Premises Equipment's (CPEs). All the subscribers are connected to the OLTs using CPEs that include RG and ONT components. In a network, a subscriber is assigned a CPE device that includes RG and the ONT component. Thus, the network is aware of the identity PON element located at each end point and its ODN and OLT identities.

Creating CPE Configuration



Note: Before you create the CPE, you must create the following.

- Management domain
- Make
- Model
- Device profile
- Controller

Perform the following steps to create the CPE.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the CPE tab.
3. Click **Create**.

The CPE Configuration page appears.

4. Complete the configuration according to the guidelines provided in the following table.

Table 205. CPE Configuration

| Field | Description |
|----------------------|--|
| Basic Details | |
| Management Domain | Select the management domain from the list. If the management domain does not exist, click the plus icon (+) to create a management domain. See Creating Management Domain (on page 765) . |
| Name | Enter a unique name for the CPE. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-) |
| Make | Select the make from the list. If the make does not exist, click the plus icon (+) to create a make configuration for the CPE. See Creating Make Configuration (on page 606) . |
| Model | Select the device model from the list. If the device model does not exist, click the plus icon (+) to create a model for the CPE. See Creating Model Configuration (on page 610) . |
| Device Profile | Select the device profile from the list. If the device profile does not exist, click the plus icon (+) to create a device profile for the CPE. See Creating OLT Device Profile (on page 509) . |
| Display Id | Enter the display ID for the CPE. |
| Serial No | Enter the serial number for the CPE. |
| MAC Address | Enter a valid IPv4 address for the CPE. |
| Management IP | Enter the management address for the CPE. |
| Site | Select the site from the list. If the site does not exist, click the plus icon (+) to create a site. See Creating Site Configuration (on page 289) . |
| Controller | Select the controller from the list. If the site does not exist, click the plus icon (+) to create a controller. See Creating Controller Configuration (on page 297) . |

Table 205. CPE Configuration (continued)

| Field | Description |
|--|--|
| Tenant | Specifies a tenant for tenant users. Tenant users configure the access for RMS specific to a tenant. |
| Profiles | |
| Alarm Profile | Select the alarm profile from the list. If the alarm profile does not exist, click the plus icon (+) to create an alarm profile for the CPE. See Alarm Profile (on page 473) . |
| Log Profile | Select the log profile from the list. If the log profile does not exist, click the plus icon (+) to create a log profile for the CPE. See Creating Log Profile (on page 503) . |
| Alias | Enter the alias name for the CPE. |
| ZTP | |
| ZTP Template | Select the ZTP template from the list. If the template does not exist, click the plus icon (+) to create a ZTP template for the CPE. |
| ZTP Server | Select the ZTP server from the list. If the template does not exist, click the plus icon (+) to create a ZTP server for the CPE. |
| Authentication | |
| When the authentication type is selected as LOCAL, the following fields are displayed. | |
| User Name | Enter a valid username for the user. |
| Password | Enter a valid password for the user. |
| When the authentication type is selected as RADIUS, the following field is displayed. | |
| Authentication Profile | Select the authentication profile from the list. |



Note: You cannot modify the **CPE ID**, **Manageable Device**, **Management Domain**, and **Controller** fields.

To edit, clone, and delete the CPE configuration, see [Common Operations \(on page 27\)](#).

Splitter

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Inventory > Splitter** from the left-hand side of the menu.

In the PON network, optical splitters play an important role in the PON by allowing a single PON interface to be shared among many subscribers. Optical splitters are installed in each optical network between the PON OLT and the ONTs that the OLT serves. As a passive device, the splitter acts as a distribution point, with a single feed of downstream data broadcast to all connected ONT endpoints.

The OLT is connected to the optical splitter through a single optical fiber, and the optical splitter is then connected to ONTs. On the other side of the OLT splitter, the number of (1: N) fibers are connected to subscribers.

Creating Splitter Configuration



Note: Before you create a splitter, you must configure the following.

- Management domain
- Make
- Model
- Device profile

Perform the following steps to create a splitter.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the **SPLITTER** tab.
3. Click **Create**.

The SPLITTER Configuration page appears.

4. Complete the configuration according to the guidelines provided in the following table.

Table 206. Splitter Configuration

| Field | Description |
|-------------------|---|
| Management Domain | Select the management domain from the list. If the management domain does not exist, click the plus icon (+) to create a management domain. See Creating Management Domain (on page 765) . |
| Name | Enter a unique name for the splitter. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |

| Field | Description |
|----------------|---|
| Make | Select the make from the list. If the make does not exist, click the plus icon (+) to create a make configuration for the splitter. See Creating Make Configuration (on page 606) . |
| Model | Select the device model from the list. If the device model does not exist, click the plus icon (+) to create a model for the splitter. See Creating Model Configuration (on page 610) . |
| Device Profile | Select the device profile from the list. If the device profile does not exist, click the plus icon (+) to create a device profile for the splitter. See Creating OLT Device Profile (on page 509) . |
| Display Id | Enter the display ID for the splitter. |
| Serial No | Enter the serial number for the splitter. |
| Alias | Enter the alias name for the splitter. |



Note: You cannot modify the **Splitter ID**, **Manageable Device**, and **Management Domain** fields.

To edit, clone, and delete the splitter configuration, see [Common Operations \(on page 27\)](#).

BNG

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Inventory > BNG** from the left-hand side of the menu.

Broadband Network Gateway (BNG) is the access point through which the subscribers connect to the broadband network. BNG aggregates traffic from various subscriber sessions and routes to the service providers' network.

Creating BNG Configuration



Note: Before you create a BNG, you must create the following.

- Make
- Model
- Device profile

Perform the following steps to create a BNG.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the **BNG** tab.

3. Click **Create**.

The BNG Configuration page appears.

4. Complete the configuration according to the guidelines provided in the following table.

Table 207. BNG Configuration

| Field | Description |
|------------------------|--|
| Basic Details | |
| Name | Enter a unique name for the BNG. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Make | Select the make from the list. If the make does not exist, click the plus icon (+) to create a make configuration for the BNG. See Creating Make Configuration (on page 606) . |
| Model | Select the device model from the list. If the device model does not exist, click the plus icon (+) to create a model for the BNG. See Creating Model Configuration (on page 610) . |
| Device Profile | Select the device profile from the list. If the device profile does not exist, click the plus icon (+) to create a device profile for the BNG. See Creating OLT Device Profile (on page 509) . |
| Display Id | Enter the display ID for the BNG. |
| Part Number | Enter the part number for the BNG. |
| Serial No | Enter the serial number for the BNG. |
| Site | Select the site from the list. If the site does not exist, click the plus icon (+) to create a site. See Creating Site Configuration (on page 289) . |
| Hardware Type | Select the hardware type from the list. <ul style="list-style-type: none">◦ ON BOARD◦ PLUGGABLE |
| Hardware Version | Enter the hardware version for the card. |
| Advance Details | |
| Resource State | Select the resource state from the list. The supported states. <ul style="list-style-type: none">◦ PLANNED◦ INSTALLED◦ RETIRED |

| Field | Description |
|--------------|---|
| Lock State | Select the lock state from the list. The supported states. <ul style="list-style-type: none">◦ NONE◦ LOCKED◦ UNLOCKED |
| Planned Type | Enter the planned type. |
| CLEI Code | Enter the Common Language Equipment Identifier (CLEI) code. |
| Alias | Enter the alias name for the BNG. |

CARD

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Inventory > CARD** from the left-hand side of the menu.

A Single card can be configured with NNI, PON, and Alarm ports for the OLT. you must create make, model, and device profile before creating a card.

Creating Card Configuration



Note: Before you create a card, you must create the following.

- Make
- Model
- Device profile

Perform the following steps to create a card.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the **CARD** tab.
3. Click **Create**.
The CARD Configuration page appears.
4. Complete the configuration according to the guidelines provided in the following table.

Table 208. Card Configuration

| Field | Description |
|----------------------|-------------|
| Basic Details | |

| Field | Description |
|-------------------------|---|
| Name | <p>Enter a unique name for the card. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Make | Select the make from the list. If the make does not exist, click the plus icon (+) to create a make configuration for the card. See Creating Make Configuration (on page 606) . |
| Model | Select the device model from the list. If the device model does not exist, click the plus icon (+) to create a model for the card. See Creating Model Configuration (on page 610) . |
| Device Profile | Select the device profile from the list. If the device profile does not exist, click the plus icon (+) to create a device profile for the card. See Creating OLT Device Profile (on page 509) . |
| Display ID | <p>Specifies the display ID of the card.</p> <p> Note: This field is applicable only for editing.</p> |
| Part Number | Enter the part number for the card. |
| Serial No | Enter the serial number for the card. |
| Site | Select the site from the list. If the site does not exist, click the plus icon (+) to create a site. See Creating Site Configuration (on page 289) . |
| Hardware Type | <p>Select the hardware type from the list.</p> <ul style="list-style-type: none"> ◦ ON BOARD ◦ PLUGGABLE |
| Hardware Version | Enter the hardware version for the card. |
| Technology Capabilities | <p>Specifies the technology supported by card profile. For example, GPON or XGSPON.</p> <p>The default value is GPON.</p> |
| Advance Details | |
| Association | |
| OLT | Enter the name of the OLT. |
| Slot | Enter the slot number of the OLT. |

| Field | Description |
|----------------|--|
| | For example: MP185-Rack1-Shelf1-LT-1 |
| State | |
| Resource State | Select the resource state from the list. The supported states. <ul style="list-style-type: none">◦ PLANNED◦ INSTALLED◦ RETIRED |
| Lock State | Select the lock state from the list. The supported states. <ul style="list-style-type: none">◦ NONE◦ LOCKED◦ UNLOCKED |
| Card Type | Select the card type from the list. <ul style="list-style-type: none">◦ NONE◦ ACU-CARD◦ NT-CARD◦ LT-CARD◦ LT-NT-CARD |
| CLEI Code | Enter the Common Language Equipment Identifier (CLEI) code. |
| Alias | Enter the alias name for the card. |

Rack

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Inventory > Rack** from the left-hand side of the menu.

A rack serves as a container for OLTs and the OLTs are mounted in the rack. Ensure that the rack is spaced widely enough to accommodate the OLTs. The rack must be strong enough to support the weight of the OLTs. You can create one or more shelves within the rack.

Creating Rack Configuration



Note: Before you create rack, you must create the following.

- Make. See [Creating Make Configuration \(on page 606\)](#).
- Model. See [Creating Model Configuration \(on page 610\)](#).
- Device profile. See [Creating OLT Device Profile \(on page 509\)](#).

Perform the following steps to create a rack.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the **RACK** tab.
3. Click **Create**.
The RACK Configuration page appears.
4. Complete the configuration according to the guidelines provided in the following table.

Table 209. Rack Configuration

| Field | Description |
|----------------|---|
| Name | Enter a unique name for the rack. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Make | Select the make from the list. If the make does not exist, click the plus icon (+) to create a make configuration for the rack. See Creating Make Configuration (on page 606) . |
| Model | Select the device model from the list. If the device model does not exist, click the plus icon (+) to create a model for the rack. See Creating Model Configuration (on page 610) . |
| Device Profile | Select the device profile from the list. If the device profile does not exist, click the plus icon (+) to create a device profile for the rack. See Creating OLT Device Profile (on page 509) . |
| Display Id | Enter the display ID for the rack. |
| Serial No | Enter the serial number for the rack. |
| Site | Enter the site name. If the site does not exist, click the plus icon (+) to create a site. See Creating Site Configuration (on page 289) . |
| Resource State | Select the resource state from the list. The supported states are. <ul style="list-style-type: none">◦ PLANNED◦ INSTALLED◦ RETIRED |
| Holder State | Select the holder state from the list. The supported states are. <ul style="list-style-type: none">◦ EMPTY◦ INSTALLED AND EXPECTED◦ EXPECTED AND NOT INSTALLED◦ INSTALLED AND NOT EXPECTED◦ MISMATCH INSTALLED AND EXPECTED |

| Field | Description |
|--------------|--|
| | <ul style="list-style-type: none"> ◦ UNAVAILABLE ◦ UNKNOWN |
| Planned Type | Enter the planned type. |
| Alias | Enter the alias name for the rack. |
| RACK Number | Enter the rack number. |



Note: You cannot modify the **ID** and **Manageable Device** fields.

To edit, clone, and delete the Rack configuration, see [Common Operations \(on page 27\)](#).

Shelf

Creating Shelf Configuration

Perform the following steps to create a shelf.

1. Select **Configuration > Inventory**.
The Inventory List page appears.
2. Click on the **RACK** tab.
3. Click on the shelf icon under the **Action** column.
The Shelf List page appears.
4. Click **Create**.
The Shelf Configuration page appears.
5. Complete the shelf configuration according to the guidelines provided in the following table.

Table 210. Shelf Configuration

| Field | Description |
|--------------|---|
| Name | Enter a unique name for the shelf. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| ME Type | Displays the ME type as SHELF. This field cannot be modified. |
| Display ID | Enter the display ID for the shelf. |
| Shelf Number | Enter the shelf number. |

| Field | Description |
|----------------|---|
| Resource State | Select the resource state from the list. The supported states are. <ul style="list-style-type: none">◦ PLANNED◦ INSTALLED◦ RETIRED |
| Holder State | Select the holder state from the list. The supported states are. <ul style="list-style-type: none">◦ EMPTY◦ INSTALLED AND EXPECTED◦ EXPECTED AND NOT INSTALLED◦ INSTALLED AND NOT EXPECTED◦ MISMATCH INSTALLED AND EXPECTED◦ UNAVAILABLE◦ UNKNOWN |
| Planned Type | Enter the planned type. |
| Lock State | Select the lock state. The supported types are. <ul style="list-style-type: none">◦ NONE◦ LOCKED◦ UNLOCKED |
| Size (U) | Enter the size for the shelf rack unit. |
| Start (U) | Enter the starting point for the shelf rack unit. |

Editing and Deleting Shelf Configuration

You can edit and delete the shelf configuration.

Perform the following steps to modify the parameters configured for the shelf.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the Rack tab and then click the Shelf icon from the **Action** column.

The Shelf List [Inventory - <Rack Name>] page appears.

3. Click on the Edit icon under the **Action** column.

The Shelf Configuration page appears.

4. Modify the shelf fields as needed.



Note: You cannot modify the **ID** and **ME Type**.

5. Click **Save** to save the changes.

A confirmation message appears, indicating the status of the edit operation.

Perform the following steps to delete the shelf.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the Rack tab and then click the Shelf icon from the **Action** column.

The Shelf List [Inventory - <Rack Name>] page appears.

3. Click on the Delete icon under the **Action** column.

An alert message appears, asking you to confirm the delete operation.

4. Click **Confirm** to delete the shelf.

A confirmation message appears, indicating the status of the delete operation.

SFP

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Inventory > SFP** from the left-hand side of the menu.

The SFP (small form-factor pluggable) is a compact, hot-pluggable optical transceiver module used for data communication. The SFP inventory details are retrieved from the PORT-SFPINVENTORY event and displayed on this page.

Viewing Field Descriptions

The following table describes the fields on the SFP Inventory page.

Table 211. SFP Configuration

| Field | Description |
|------------|--|
| Name | Specifies the name of the SFP. Example: SFP_UTXA7000093 |
| Make | Specifies the make for the SFP. Example: FINISAR CORP |
| Model | Specifies the model for the SFP. |
| Display Id | Specifies the display ID for the SFP. |

Table 211. SFP Configuration (continued)

| Field | Description |
|-----------------------------|--|
| | Example: SFP_H2783Z00047 |
| Serial No | Specifies the serial number for the SFP. Example: UTXA7000093 |
| Device Profile | Specifies the SFP device profile. Example: SFP_FINISAR CORP |
| OLT | Enter the OLT name to which the SFP is connected. Example: olt61 |
| Port | Specifies the port name (NNI or PON) on which the SFP is associated. Example: PON-1 |
| Manufacturing Date | Specifies the manufacturing date of the SFP. |
| SFP Missing | Specifies if the OLT detects that an SFP module is missing on the port during the port activation or when the SFP module is removed. Example: False |
| Part Number | Specifies the part number of the SFP. Example: FTLX8571D3BCL |
| Nominal Bitrate (gbps) | Enter the nominal Bitrate of the SFP. Example: 10.3 |
| Signal Range (km) | Specifies the signal range for the SFP. Example: 20 |
| Transmitter Wavelength (nm) | Specifies the transmitter wavelength of the SFP. Example: 850 |
| Creation Time | Specifies the date and time when the SFP was created. |

Cable

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Inventory > Cable** from the left-hand side of the menu.

A cable is used to connect two or more electronic or optical devices to each other. You must create make and model before creating a cable.

Creating Cable Configuration



Note: Before you create a cable configuration, you must create the following.



- Make
- Model

Perform the following steps to create a cable.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Click on the **CABLE** tab.

3. Click **Create**.

The CABLE Configuration page appears.

4. Complete the configuration according to the guidelines provided in the following table.

Table 212. Cable Configuration

| Field | Description |
|------------|--|
| Name | Enter a unique name for the cable. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Me Type | The ME type is cable. |
| Make | Select the make from the list. If the make does not exist, click the plus icon (+) to create a make configuration for the cable. See Creating Make Configuration (on page 606) . |
| Model | Select the device model from the list. If the device model does not exist, click the plus icon (+) to create a model for the cable. See Creating Model Configuration (on page 610) . |
| Display Id | Enter the display ID for the cable. |
| Serial No | Enter the serial number for the cable. |



Note: You cannot modify the **ID**, **Manageable Device**, and **Me Type** fields.

To edit, clone, and delete the Cable configuration, see [Common Operations \(on page 27\)](#).

Exporting Managed Elements

You can export managed elements (OLT, ONT, SFP, CPE, splitter, BNG, card, rack, and cable) as a CSV file from RMS to your local computer. The CSV file can be opened or edited using an application such as Microsoft Excel. You can view and analyze the exported managed element information, as needed.

Perform the following steps to export managed elements.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the respective managed element tab.
3. Select the numbers from the **show entries** list.



Note: The supported values are 10, 25, 50, and 100. It defines the number of managed elements you can export. For example, suppose there are 14 managed elements on the page, and you have selected the value 10 from the **show entries** list. In that case, it exports only 10 managed elements and skips the remaining 4 managed elements. To export all 14 managed elements, you must select the next maximum value (25) from the **show entries** list.

4. Click **Export** to export the details.



Note: You can export a maximum of 100 managed elements through the inventory page. If there are more than 100 managed elements, see [Creating Task for Inventory Collection \(on page 689\)](#) to export all the listed managed elements.

The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file using an application such as Microsoft Excel. Optionally, you can save this file on your computer for later use.

Importing Managed Elements

You can import the managed elements (OLT, ONT, CPE, splitter, BNG, rack, and cable) configuration from your local computer to RMS by uploading a Microsoft Excel file. This method enables you to modify only the required parameters without going through the managed element creation workflow.



Note: You can download a sample Microsoft Excel file from the **Download Template** link and configure the parameters of the managed element that you want to configure.

A user can create multiple managed elements using the import functionality. RMS validates the uploaded file, and the validation errors are shown to the user. A user can fix all the errors, upload the file again, and start creating the file. A user can also use this functionality to modify the managed elements.

Perform the following steps to import a managed element configuration to RMS.

1. Select **Configuration > Inventory**.

The Inventory List page appears.

2. Navigate to the respective managed element tab.
3. Click **Import**.

The Import page appears.

4. Download a sample Microsoft Excel file from the **Download Template** link.
5. Enter the parameters that you want to configure for the managed element.
6. Save the file in your local system.
7. Click on the **Upload Resource File** text box.

The File Window opens.

Navigate to the directory containing the managed element configuration data file.

8. Select the file and click **Open**.
9. Click the upload icon to upload the file to RMS.

A success message appears and indicates that the file is uploaded successfully. Once the import is successful, the managed element details are shown in the managed element dashboard page.

Subscriber

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Subscriber** from the left-hand side of the menu.

A subscriber is a logical entity and assigned with a unique name and identity on the interface towards RMS. RMS associates the physical network termination devices with the subscriber.

A subscriber is configured to a specific PON port of a specific OLT. Hence, a subscriber can gain access only when the CPE is connected to the configured PON port of the OLT.

When a subscriber is on-boarded by the Operations Support Systems (OSS), Business Support Systems (BSS), RMS accesses the information of the PON port of the OLT, ONT identities, and the services of the subscriber.

Tasks

You can perform the following tasks from this page.

- Create a subscriber. See [Creating Subscriber \(on page 455\)](#).
- Export subscriber information. See [Exporting Subscriber Information \(on page 456\)](#).
- View, create, and remove services of the subscriber. See [Service \(on page 456\)](#).
- Activate the service for the subscriber. See [Activating and Deactivating the Service for the Subscriber \(on page 467\)](#).
- Initiate and cancel MAC dump for Service. See [Initiate and Cancel MAC Dump for Service \(on page 468\)](#).
- MAC lookup for service. See [MAC Lookup for Services \(on page 470\)](#).

Creating Subscriber

Perform the following steps to create a subscriber configuration.

1. Select **Configuration > Subscriber**.

The Subscriber List page appears.

2. Click **Create** to create a new subscriber configuration.

The Subscriber Configuration page appears.

3. Complete the configuration according to the guidelines provided in the following table.

Table 213. Subscriber Configuration

| Field | Description |
|--------------|---|
| Name | Enter a unique name for the subscriber. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Display ID | Enter a display ID for the subscriber. |
| ONU | Enter the ONU to which the subscriber is connected to. |
| Address | Enter the address of the subscriber. |
| Latitude | Enter the latitude of the subscriber location. |
| Longitude | Enter the longitude of the subscriber location. |
| Force Delete | Specifies if the force delete field is enabled or disabled. By default, FALSE is selected. The supported values are. <ul style="list-style-type: none">◦ TRUE◦ FALSE |

4. Click **Create**.

A new subscriber is created on the Subscriber List page.



Note: You can edit the subscriber ONU ID along with the other information. A unique ID is assigned to each subscriber. You cannot modify it.

To edit, clone, and delete the subscriber configuration, see [Common Operations \(on page 27\)](#).

Exporting Subscriber Information

You can export the subscriber information as a CSV file from RMS to your local computer. The CSV file can be opened or edited using an application such as Microsoft Excel. You can view and analyze the exported subscriber information as needed.

Perform the following steps to export subscriber information.

1. Select **Configuration > Subscriber**.

The Subscriber List page appears.

2. Click **Export**.

The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file using an application such as Microsoft Excel. Optionally, you can save this file on your PC for later use.

The downloaded file contains the following information about the subscriber.

- Name
- Display ID
- Address
- ONU
- Latitude
- Longitude
- Creation Time

Service

To access this page, click **Configuration** from the top right corner of the page and select **Configuration > Subscriber > Service** from the left-hand side of the menu.

A service is a collection of traffic that shares the same characteristics and requires a certain treatment of packets on the forwarding path for both upstream and downstream traffic. A subscriber is configured with a set of services based on the subscription. Each service configuration indicates the data rates, the DSCP marking in the packets, the priority of the packets, and the scheduler applicable to the traffic. The priority of the packets is indicated using 802.1p or 802.1ad marking value, which is applied on the packets when the packets pass through the ONT and OLT in upstream and downstream, respectively.

RMS supports the provisioning of multiple parent services per subscriber. Each parent service can be optionally configured with an aggregate downstream bandwidth limit, which is applicable for all its sub-services.

RMS supports the following type of services to subscribers. You can configure more than one service for the subscriber.

- **Unicast Services.** A unicast address is used to send a packet to a single destination. The following type of unicast services are supported.
 - High Speed Internet Access (HSIA)
 - VoIP Calling
 - Video Calling
 - Video on Demand or Streaming Video



Note: A maximum of eight sub-services can be added to the parent service.

Each of the above services is delivered to the end user considering several parameters such as QoS, flexible bandwidth allocation, redundancy, and priority. The services require appropriate packet prioritization across the network to deliver a good quality of experience to the subscribers. The applications generate the packets at both ends of the network, access, and core, mark the packets with DSCP marking associated with the service. The packets are buffered and transmitted based on the priority associated with the service, which translates to the DSCP marking to an 802.1p marking. Essentially, the DSCP marking in the packet is used to identify the packets priority and the packet is treated appropriately.

- **Multicast Services.** A multicast address is used to send a datagram to a set of hosts that can be on different subnetworks and that are configured as members of a multicast group. The following type of multicast services are supported.
 - Internet Protocol Television (IPTV)
 - IGMP Snooping
 - Any-source multicast
 - Source-specific multicast
 - IGMP JOIN/LEAVE handling
 - Multicast group handling at OLT

Task

You can perform the following tasks from this page.

- Viewing the existing service. See [Viewing the Service \(on page 457\)](#).
- Creating a subscriber service. See [Creating Service \(on page 459\)](#).
- Remove the existing service configured for the subscriber. See [Removing the Service \(on page 458\)](#).
- Export the service configuration. See [Exporting Subscriber Information \(on page 456\)](#).

Viewing the Service

You can view the list of subscribers and the services configured for each subscriber.

Perform the following steps to view the list of subscriber services.

1. Select **Configuration > Subscriber**.

The Subscriber List page appears.

2. Click on the **View/Create/Remove Services** icon under the **Services** column.

The Service List [Subscriber - *Subscriber Name*] page appears.

Field Descriptions

The following table describes the fields on the service list [Subscriber - <Subscriber Name>] page.

Table 214. Service List - [Subscriber Name] Fields

| Field | Description |
|-------------------|---|
| Name | Specifies the name of the subscriber. |
| Admin State | Specifies the admin state of the subscriber. The supported states are. <ul style="list-style-type: none">• ACTIVE• DEACTIVE |
| Operational State | Specifies the operation state of the subscriber. The supported states are. <ul style="list-style-type: none">• UP• DOWN |
| Action | Specifies the action that you can perform on the subscriber service list. The supported actions are. <ul style="list-style-type: none">• Edit• Delete• Clone• View the list of configuration variables |
| Creation Time | Specifies the date and time when the subscriber service was created. |

Removing the Service

You can delete the existing service that was configured for the subscriber. When the service is deleted, all the sub-services associated with the service are deactivated and then the parent service is deleted.

Before you delete a service, you must perform the following.

- Deactivate the service
- Delete the service



Note:

- You cannot delete the service if the service is in ACTIVATE state.
- You cannot deactivate the individual sub-service.

Perform the following steps to delete the service configured for the subscriber.

1. Select **Configuration > Subscriber**.
The Subscriber List page appears.
2. Click on the **View/Create/Remove Services** icon under the **Services** column.
The Service List [Subscriber - *Subscriber Name*] page appears.
3. Click on the Deleted icon corresponding to the subscriber service.
A success message appears and indicates the status of the operation.

Creating Service

Perform the following steps to create a service configuration.

1. Select **Configuration > Subscriber**.
The Subscriber List page appears.
2. Click on the **View/Create/Remove Services** icon under the **Services** column.
The Service List [Subscriber - *Subscriber Name*] page appears.
3. Click **Create** to create a new service configuration.
The Service Configuration page appears.
4. Complete the configuration according to the guidelines provided in the following table.

Table 215. Service Configuration

| Field | Description |
|--------------------------------------|---|
| Name | Enter a unique name for the parent service. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| MAC Limit | Specifies the number of MACs to be learned at service by OLT. This field can be modified only when OLT is in a DEACTIVE state. The supported value ranges from 0 to 65535. The MAC value 65535 indicates there is no MAC limit. The user is allowed to configure the value from 1 to 65535. |
| Aggregate Upstream Bandwidth Profile | Specifies the bandwidth profile ID for the aggregate upstream bandwidth control. This field is required only when multiple GEM to 1 T-CONT is in upstream direction. All sub-services are configured on different GEM, and they share the same T-CONT. The aggregate upstream bandwidth profile maps to the T-CONT configurations for the upstream QoS. |

| Field | Description |
|-------------------------------------|---|
| Aggregate Downstream Shaper Profile | Specifies the shaper profile ID for the aggregate downstream bandwidth control. |
| Service Queue Stats | Specifies the location where the GEM KPI must be enabled. The supported values are. <ul style="list-style-type: none"> ◦ ENABLE_ON_OLT ◦ ENABLE_ON_ONT ◦ ENABLE_OLT_ONT ◦ DISABLE The default value is DISABLE. |
| Control Packet Statistics | |
| PPPoE | Select the checkbox to enable the PPPoE historical KPIs for the service. |
| DHCPv4 | Select the checkbox to enable the DHCPv4 historical KPIs for the service. |
| DHCPv6 | Select the checkbox to enable the DHCPv6 historical KPIs for the service. |
| Force Delete | Specifies whether the force delete is enabled. The supported values are. <ul style="list-style-type: none"> ◦ TRUE ◦ FALSE The default value is FALSE. |
| Service | |
| Service Name | Enter a unique name for the sub-service. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| UNI_Port_ID | Enter the UNI port number for which the service needs to be associated. The same UNI port can have two service configurations. |
| UNI Port | Specifies the physical UNI port number of the ONT device to which the service needs to be associated. The same UNI port can have two service configurations. |
| UNI Port Type | Specifies the UNI port type. This field is mandatory if the <i>UNI Port</i> field is configured. The supported values are. <ul style="list-style-type: none"> ◦ VEIP ◦ PPTP-ETHERNET ◦ IP-HOST |

| Field | Description |
|---------------------|---|
| | <ul style="list-style-type: none"> ◦ PPTP-POTS ◦ IPv6-HOST |
| CPE MAC | <p>Specifies the MAC address of the CPE connected to the particular UNI port for the enterprise (Bridged Mode) solution. The MAC address is same for the residential solution (Gateway Mode).</p> |
| AES Encryption | <p>Select whether the AES encryption is supported for the service.</p> <ul style="list-style-type: none"> ◦ True. Supports AES encryption. ◦ False. Does not support AES encryption. <p>Example: True</p> |
| Remote ID Type | <p>Specifies the type of remote ID. The supported values are.</p> <ul style="list-style-type: none"> ◦ MAC_Address ◦ Custom <p>This field is applicable only when the MAC Learning Type is set to DHCP, PPPoE, or PPPoE-IA. Otherwise, this field is ignored.</p> <p>For more information, see Table 216: Circuit ID and Remote ID Configuration (on page 467).</p> |
| Data Rate Attribute | <p>Specifies the data rate attribute. The supported values are.</p> <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED <p>This field is enabled only when the 'encapsulation' field is set to PPPoE-IA in the V-Net profile or in the <i>vnet_config</i> file. If this field is ENABLED, the intermediate agent adds the minimum bandwidth upstream, minimum bandwidth downstream, maximum bandwidth upstream, and maximum bandwidth downstream in the upstream PPPoE control packets.</p> <p>The default value is DISABLED.</p> |
| CPE IP Type | <p>Specifies the Customer Premises Equipment (CPE) IP type. The supported values are.</p> <ul style="list-style-type: none"> ◦ IPv4 ◦ IPv6 ◦ NONE <p>The default value is NONE.</p> |
| CPE IP Address | <p>Specifies the IP address of the CPE/CE router device connected to the particular UNI port for the enterprise (Bridged Mode) solution. The length is 4 bytes. The length is 4 bytes. A standard valid IP range is supported.</p> <p>This field can take IPv4 or IPv6 addresses based on the value provided in the CPE IP Type field.</p> <p>The CPE IP Address is mandatory when the CPE IP Type is IPv4 or IPv6.</p> <p>When the CPE IP Type is NONE, CPE IP Address is not required.</p> |

| Field | Description |
|--------------------|--|
| | Example: 1.1.1.1 or 2001:db8:3333:4444:5555:6666:7777:8888 |
| CPE IP Subnet Mask | <p>Specifies the subnet mask for the CPE IP Address. The CPE IP Subnet Mask is mandatory when the CPE IP Type is IPv4 or IPv6. When the CPE IP Type is NONE, CPE IP Subnet Mask is not required.</p> <p>Example: The value is 255.255.255.255 if CPE IP Type is IPv4. The value is ffff.ffff.ffff.ffff.ffff.ffff.ffff.ffff if CPE IP Type is IPv6.</p> |
| Latency Sensitive | <p>Specifies whether the service is latency sensitive or not. The supported values are:</p> <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED <p>Setting this field to enabled (true) may improve the latency of this service, but in the cost of slightly compromising bandwidth or throughput of other best effort services in congestion.</p> <p>The default value is DISABLED.</p> <p>The Latency Sensitive field can also be updated on the fly when service is in the activated state.</p> <p> Note: This field is relevant only for assured services for SR DBA Type enabled ONUs, otherwise it will be ignored by CBAC.</p> |
| Profiles | |
| MVLAN Profile | Select the MVLAN profile from the list. |
| VNet Profile | Select the VNet profile from the list. |
| VNET CONFIG | |
| SVLAN | Specifies the subscriber S-Tag value of the subscriber. The supported value ranges from 2 to 4094. |
| CVLAN | Specifies the subscriber C-Tag value of the subscriber. The supported value ranges from 2 to 4094. |
| VLAN CONTROL | <p>Specifies the VLAN tagging supported at the ONU and OLT. The supported values are:</p> <ul style="list-style-type: none"> ◦ ONU_CVLAN_OLT_SVLAN ◦ OLT_CVLAN_OLT_SVLAN ◦ ONU_CVLAN ◦ OLT_SVLAN |

| Field | Description |
|------------------------------|--|
| | <ul style="list-style-type: none">◦ ONU_CVLAN_ONU_SVLAN◦ NONE <p>The default value is ONU_CVLAN_OLT_SVLAN. For more information, see Table 270: VLAN Tagging (on page 582).</p> |
| UNI VLAN | Specifies the VLAN or UNI port. The value UNI VLAN zero indicates an un-tagged packet classification. |
| UNI VLAN Range End | Specifies the end uni vlan for L2VPN subscriber vlans range. The UNI VLAN field is mandatory when this field is configured. |
| Allow Transparent VLAN | Specifies the configuration to allow the transparent VLAN from RG. This indicates that the upstream traffic needs to be classified based on the Ether type. The supported values are. <ul style="list-style-type: none">◦ ENABLED◦ DISABLED <p>When the field is set to ENABLED, the traffic from RG is passed transparently.</p> |
| Encapsulation | Specifies the type of access protocol used to establish the access link. The supported values are. <ul style="list-style-type: none">◦ IPoE◦ PPPoE◦ PPPoE-IA <p> Note: When this field value is selected as PPPoE-IA, the Remote-ID Type field value in the service configuration can be selected as Custom or left blank.</p> |
| ONT Ethertype Classification | Specifies if the upstream traffic needs to be classified based on the Ether type. The supported values is DISABLED. |
| Remote ID Profile | Specifies the Remote ID profile name to be used to generate the RemotID string in DHCP relay and PPPoE Intermediate Agent. |
| MAC Learning Type | Specifies the type of method used to learn device MAC address. The supported values are. <ul style="list-style-type: none">◦ NONE. CBAC does not learn MAC addresses; the MAC anti-spoofing is disabled unless the user provides a CPEMAC. The DHCP relay agent is disabled.◦ DHCP. MAC addresses are learned dynamically along with IP addresses obtained through DHCP. The MAC anti-spoofing is enabled, and the DHCP relay agent is enabled. |

| Field | Description |
|-------------------------|--|
| | <ul style="list-style-type: none"> ◦ ARP. MAC addresses are learned dynamically when devices communicate through ARP. The MAC anti-spoofing is enabled, and the DHCP relay agent is disabled. ◦ DHCP ALLOW RELEARN. Allows MAC relearning based on DHCP; the CPE device/MAC can be updated. The MAC anti-spoofing is enabled, and the DHCP relay agent is enabled. ◦ ARP ALLOW RELEARN. Allows MAC relearning based on ARP; the CPE device/MAC can be updated. The MAC anti-spoofing is enabled, and the DHCP relay agent is disabled. ◦ DHCP IP ANTISPOOFING NO MAC. IP addresses are learned based on DHCP; the IP-based anti-spoofing is enabled. The DHCP relay agent is enabled. ◦ DHCP IP ANTISPOOFING MAC. IP addresses and MAC addresses are learned based on DHCP; the IP and MAC-based anti-spoofing is enabled. The DHCP relay agent is enabled. ◦ DHCP NO MAC. CBAC learns the MAC addresses from DHCP, but MAC anti-spoofing is disabled. The DHCP relay agent is enabled. ◦ ARP NO MAC. CBAC learns MAC addresses from ARP, but MAC anti-spoofing is disabled. The DHCP relay agent is disabled. |
| CoSQ Profile | <p>Select the CoSQ profile ID.</p> <p>When this field is configured in the Vnet Config, the allowed pbits in the CoSQ profile are used for downstream control IPv6 solicit message and downstream ARP request message to remark the pbits.</p> |
| SVLAN TPID | <p>Specifies the Tag Protocol Identifier (TPID) that must be used with s-tag. The supported values are.</p> <ul style="list-style-type: none"> ◦ 0x88A8 ◦ 0x8100 <p>The default value is 0x8100.</p> |
| PON Hair Pinning | <p>Specifies whether the PON hair pinning is enabled for the VLAN model. The supported values are.</p> <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED <p>The default value is DISABLED.</p> |
| Circuit ID | <p>Select the circuit ID format from the list. For more information, see Table 216: Circuit ID and Remote ID Configuration (on page 467).</p> |
| Upstream Profile | |

| Field | Description |
|---|---|
| Bandwidth Profile | Select the bandwidth profile for the upstream traffic from the list. The bandwidth profile maps to T-CONT configuration for US QoS for 1-GEM per T-CONT model. |
| Shaper Profile | Select the shaper profile for the upstream traffic from the list. The field maps to GEM level traffic shaping for upstream QoS for the multiple-GEM to 1 TCONT model. |
| COSQ Profile | Select the COSQ profile for the upstream traffic from the list. |
| Downstream Profile | |
| Bandwidth Profile | Select the bandwidth profile for the downstream traffic from the list. |
| Shaper Profile | Select the shaper profile for the downstream traffic from the list. Specifies the traffic shaping parameters for downstream QoS. |
| COSQ Profile | Select the COSQ profile for the downstream traffic from the list. |
| The following additional fields are displayed if the UNI Port Type is selected as IP-HOST . | |
| Voice Service Config | |
| Pots UNI Port ID | Specifies the POTS port ID. The supported values are. <ul style="list-style-type: none"> ◦ ont-185-PPTP-POTS-1 ◦ ont-185-PPTP-POTS-2 |
| Pots UNI Port | Specifies the POTS port number. |
| Phone Number | Specifies the phone number. This field do not have restriction on the number of digits as it is a string. |
| User Name | Specifies the username for the voice service profile. |
| Password | Specifies the password for the voice service profile. |
| Display Name | Specifies the display name. |
| VOIP Config Method | Specifies the VoIP configuration method. The default value is OMCI. |
| Pots Signaling Code | Specifies the POTS signaling code when the port type is IP-HOST. The supported values and signaling methods are. <ul style="list-style-type: none"> ◦ 1-LoopStart ◦ 2-GroundStart ◦ 3-LoopReverseBattery ◦ 4-CoinFirst |

| Field | Description |
|-------------------------------|---|
| | <ul style="list-style-type: none">◦ 5-DialToneFirst◦ 6-MultiParty |
| Voice Protocol | Specifies the voice protocol. The default value is SIP. |
| Voice Service Profiles | |
| Pots Profile | Select the POTS profile from the list. If the profile does not exist, click the plus icon (+) to create a configuration for the POTS profile. See Creating POTS Profile (on page 589) . |
| IP Host Profile | Select the IP host profile from the list. If the profile does not exist, click the plus icon (+) to create a configuration for the IP host profile. See Creating IP Host Profile (on page 549) . |
| SIP Agent Profile | Select the SIP agent profile from the list. If the profile does not exist, click the plus icon (+) to create a configuration for the SIP agent profile. See Creating SIP Agent Profile (on page 590) . |
| SIP User Data Profile | Select the SIP user data profile from the list. If the profile does not exist, click the plus icon (+) to create a configuration for the SIP user data profile. See Creating SIP User Data Profile (on page 592) . |
| Network Dial Plan Profile | Select the network dial plan profile from the list. If the profile does not exist, click the plus icon (+) to create a configuration for the network dial plan profile. See Creating Network Dial Plan Profile (on page 593) . |
| VoIP Service Info Profile | Select the VoIP service information profile from the list. If the profile does not exist, click the plus icon (+) to create a configuration for the VoIP service information profile. See Creating VoIP Service Info Profile (on page 595) . |
| VoIP Media Info Profile | Select the VoIP media information profile from the list. If the profile does not exist, click the plus icon (+) to create a configuration for the VoIP media information profile. See Creating VoIP Media Info Profile (on page 596) . |
| RTP Info Profile | Select the RTP Information profile from the list. If the profile does not exist, click the plus icon (+) to create a configuration for the RTP information profile. See Creating RTP Info Profile (on page 598) . |
| VoIP App Service Profile | Select the VoIP application service profile from the list. If the profile does not exist, click the plus icon (+) to create a configuration for the VoIP application service profile. See Creating VoIP Application Service Profile (on page 600) . |

5. Click **Create**.

A new service is created on the Service List page.

The following table lists the circuit ID and the remote ID configuration.

Table 216. Circuit ID and Remote ID Configuration

| Circuit ID | Remote ID | Behavior |
|----------------|----------------|---|
| Configured | Configured | The option 82 is constructed with the configured circuit id value. If remote id type is equals to MAC ADDRESS, then the remote id for option 82 is <i><learnt_mac></i> , else the remote id is equals to the configured value. |
| Not Configured | Configured | The option 82 is constructed only with remote id (If remote id type is equals to MAC ADDRESS, then the remote id for option 82 is <i><learnt_mac></i> , else the remote id is equals to the configured value). |
| Configured | Not Configured | The option 82 is constructed with configured circuit id value. If remote id type is equals to MAC ADDRESS, then the remote id for option 82 is <i><learnt_mac></i> . |
| Not Configured | Not Configured | If remote id type is equals to MAC ADDRESS, then the remote id for option 82 is <i><learnt_mac></i> , else no option 82 header is constructed. |

Activating and Deactivating the Service for the Subscriber



Note: Before you activate the service for the subscriber, you must activate the UNI port. For more information, see [Activating the UNI Port \(on page 436\)](#).

RMS enables you to activate the service for the subscriber. The admin state of the service is in DEACTIVE, and the operation state of service is UNKNOWN when it is created, and you must activate the service for the subscriber to avail the service.

Perform the following steps to activate the service created for the subscriber.

1. Select **Configuration > Subscriber**.

The Subscriber List page appears.

2. Click on the **View/Create/Remove Services** icon under the Services column.

The Service List page appears.

3. Click on the three dots (⋮) corresponding to the service that you want to activate for the subscriber and click the **Activate** option.

A success message appears, indicating the status of the activate operation.

After the successful activation, the admin state of the service is changed to ACTIVE, and the operational state is changed to UP.

You can deactivate the service that was configured for the subscriber.

Perform the following steps to deactivate the service configured for the subscriber.

1. Select **Configuration > Subscriber**.

The Subscriber List page appears.

2. Click on the **View/Create/Remove Services** icon under the Services column.

The Service List page appears.

3. Click on the three dots (⋮) corresponding to the service that you want to deactivate for the subscriber and click the **Deactivate** option.

A warning pop-up message appears stating, Deactivating <service-name> disrupts associated subscriber's services. Are you sure to proceed with the deactivation of <service-name>?

4. Click **Yes, Deactivate** to deactivate the service.

A success message appears, indicating the status of the deactivate operation.

After the successful deactivation, the admin state of the service is changed to DEACTIVE, and the operational state is changed to DOWN.

When a service is provisioned from RMS using the service templates, the following operations are invoked in a specific sequence on CBAC.

1. Create ONT
2. Activate ONT
3. Add and activate UNI (Optional)
4. Add subscriber
5. Add service
6. Activate service

If there is a failure during this process, RMS needs to rollback the service configuration automatically.

Initiate and Cancel MAC Dump for Service

RMS allows you to initiate and cancel the MAC dump on service.

You can query multiple MAC addresses of each service by initiating the MAC dump request for the services. This enables the user to check whether the MAC address is learned for each service.



Note: Once the MAC dump query is triggered, the user cannot run another query before it is completed or canceled.

Perform the following steps to initiate MAC dump request for the services.

1. Select **Configuration > Subscriber**.

The Subscriber List page appears.

2. Click on the **View/Create/Remove Services** icon under the Services column.

The Service List page appears.

3. Click on the three dots (⋮) corresponding to the service and click the **Initiate MAC Dump** option.

The Initiate MAC Dump page appears.

4. Complete the configuration according to the guidelines provided in the following table.

Table 217. Initiate MAC Dump Configuration

| Field | Description |
|-------------|---|
| Vlan | Specifies the outer VLAN value. The supported value ranges from 2 to 4094. |
| MAC Address | Enter the MAC address. |



Note: The **Vlan** and **MAC Address** fields are optional.

5. Click **Submit** to initiate MAC dump for service.

A success message appears, indicating the status of the MAC dump operation.

Click on the three dots (⋮) corresponding to the service and click **Monitor** option. For more information, see #unique_437 (on page).

Perform the following steps to cancel MAC dump for the services.

1. Select **Configuration > Subscriber**.

The Subscriber List page appears.

2. Click on the **View/Create/Remove Services** icon under the Services column.

The Service List page appears.

3. Click on the three dots (⋮) corresponding to the service and click the **Cancel MAC Dump** option.
4. Click **Submit**.

MAC Lookup for Services

Perform the following steps to perform MAC lookup for the services.

1. Select **Configuration > Subscriber**.

The Subscriber List page appears.

2. Click on the **View/Create/Remove Services** icon under the Services column.

The Service List page appears.

3. Click on the three dots (⋮) corresponding to the service and click the **MAC Lookup** option.
4. Complete the configuration according to the guidelines provided in the following table.

Table 218. MAC Lookup Configuration

| Field | Description |
|-------------|---|
| OVlan | Specifies the outer VLAN value. The supported value ranges from 2 to 4094. |
| MAC Address | Specifies the MAC address. |



Note: The **OVlan** and **MAC Address** fields are mandatory for MAC lookup.

A confirmation message indicates that the MAC for a particular resource ID is learned successfully.



Note: When the incorrect values are entered for the **OVlan** and **MAC Address** fields, an error message indicates that the MAC lookup is failed for a particular service.

Editing and Deleting Service

RMS allows you to edit the service that was configured for the subscriber.

Perform the following steps to edit a service configuration.

1. Select **Configuration > Subscriber**.

The Subscriber List page appears.

2. Click on the **View/Create/Remove Services** icon under the Services column.

The Service List page appears.

3. Click the edit icon under the **Action** column.

The Service Configuration page appears.

4. Modify the service fields as required.



Note:

- You cannot edit the service ID.
- If you want to update the circuit ID format, follow the below steps.
 - a. Deactivate the service.
 - b. Update the circuit ID and save the service configuration.
 - c. Activate the service.

5. Click **Save** to save your changes.

A confirmation message appears, indicating the status of the edit operation.

Perform the following steps to delete the service configuration.



Note: Before you delete a service, you must perform the following.

- Deactivate the service
- Delete the managed element from the service
- Delete the service
- Delete the subscriber

1. Select **Configuration > Subscriber**.

The Subscriber List page appears.

2. Click on the **View/Create/Remove Services** icon under the Services column.

The Service List page appears.

3. Click the delete icon under the **Action** column.

A warning pop-up message appears stating, Deleting a service is a critical operation that impacts services. Once deleted, this operation cannot be undone. Are you sure to proceed with the deletion of <service-name>?.

4. Click **Yes, Delete** to delete the service.

A confirmation message appears indicating the status of the operation.

Exporting Service Information

You can export the service information of the entire network as a CSV file from RMS to your local computer. The CSV file can be opened or edited using an application such as Microsoft Excel. You can view and analyze the exported subscriber information, as needed.

Perform the following steps to export subscriber information.

1. Select **Configuration > Subscriber**.
The Subscriber List page appears.
2. Click on the **View/Create/Remove Services** icon under the Services column.
The Service List page appears.
3. Click **Export**.
The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file using an application such as Microsoft Excel. Optionally, you can save this file on your PC for later use.

The downloaded file contains the following information about the subscriber service.

- Name
- Admin State
- Operational State
- Address
- Service (sub-service information)

Profiles

You can create and manage alarm profiles (OLT, ONT, OLT Port, ACE, LAG, SFP, and ANI-G), log profile, PPPoE profile, device profile, authentication profile, and Access Control List (ACL) profile, Ethernet Ring Protection Switching (ERPS), Managed End Point (MEP) profile, Network Time Protocol (NTP), circuit ID format, and TACACS profile.

Alarm Profile

To access this page, click **Configuration** from the top right corner and select **Profile > Alarm Profile** from the left-hand side of the menu.

Alarm profile allows a user to specify the KPI threshold value for the RMS components.

RMS sends the alarm profile information to the controller. Once the threshold value is reached, RMS raises an alarm.

When the KPI value reaches the threshold value configured for MINOR, MAJOR, WARNING, or CRITICAL level, an alarm is raised with the respective severity level.

For example, when the KPI value reaches the MINOR threshold value, an alarm with severity level MINOR is raised.

Once an alarm is raised and if the threshold value goes lower than the WARNING threshold value, an alarm with severity level CLEARED is raised in the next reporting interval.

For information about alarm severity levels, see [Alarm Severity Levels \(on page 238\)](#).

RMS supports threshold crossed alarms for the following resources.

Table 219. Alarm Profile Information

| Alarm Profiles | For more information, see |
|-------------------------|---|
| OLT Alarm Profile | OLT Alarm Profile (on page 475) |
| OLT Port Alarm Profile | OLT Port Alarm Profile (on page 482) |
| ONT Alarm Profile | ONT Alarm Profile (on page 485) |
| LAG Alarm Profile | LAG Alarm Profile (on page 486) |
| ACE Alarm Profile | ACE Alarm Profile (on page 488) |
| SFP (NNI) Alarm Profile | SFP (NNI) Alarm Profile (on page 489) |
| SFP (PON) Alarm Profile | SFP (PON) Alarm Profile (on page 493) |
| ANI-G Alarm Profile | ANI-G Alarm Profile (on page 497) |

Creating Alarm Profile

Field Descriptions

The following table describes the fields on the Alarm Profile List page.

Table 220. Alarm Profile List

| Field | Description |
|---------------|--|
| Name | Specifies the name of the alarm profile. |
| Type | Specifies the type of resource (OLT, OLT PORT, ONT, LAG, ACE, SFP, and ANI-G). |
| Creation Time | Specifies the date and time when the alarm profile was created. |
| Action | Specifies the action that you can perform on the alarm profile. The supported actions are. <ul style="list-style-type: none"> • Edit • Delete • Clone |

The KPIs in an alarm profile are optional. A user can include or exclude any KPIs from the alarm profile. Threshold types are optional within each KPI, and users can include or exclude any threshold types.



Note:

- A user must select at least one KPI for a valid alarm profile.
- A few critical KPIs are not optional. For example,
 - Thermal sensor temperature in the OLT profile.
 - Thresholds (SF and SD) in the ANI-G profile.

The following table provides the time taken by CBAC to apply the changes made to the profile. It also indicates the time taken by CBAC to raise or clear any alarms associated with the profile thresholds if a new profile is associated with the resource.

The following table describes the synchronization time between CBAC and RMS.

Table 221. Synchronization Time

| Profile Name | Resource Type | Sync Time | Description |
|-------------------|---------------|------------|--|
| OLT Alarm Profile | OLT | 30 seconds | The device status KPI is reported every 30 seconds from the OLT. |

Table 221. Synchronization Time (continued)

| Profile Name | Resource Type | Sync Time | Description |
|------------------------|-------------------|------------|--|
| OLT PORT Alarm Profile | ME PORT (PON/NNI) | 15 minutes | The port utilization stats are calculated and reported every 15 minutes. |
| SFP Alarm Profile | ME PORT | 30 seconds | The SFP optical stats KPIs are reported every 30 seconds by OLT. |
| ANI-G Alarm Profile | ONT | 15 minutes | The ONT optical stats are collected every 15 minutes. |
| LAG Alarm Profile | LAG PORT | 15 minutes | The port utilization stats are calculated and reported every 15 minutes. |

**Note:**

- You cannot modify the alarm profile name.
- You cannot delete an alarm profile if it is associated with an active managed element. To delete the managed element alarm profile, you must first dissociate the alarm profile from the managed element.

To edit, clone, and delete the Alarm profile configuration, see [Common Operations \(on page 27\)](#).

OLT Alarm Profile

The OLT KPIs include CPU utilization, memory utilization, disk utilization, fan speed, and thermal sensor temperature for temperature and sensor. The OLT alarm profile sets the high and low thresholds for each of the parameter and the alarms are reported by CBAC to RMS based on the thresholds.

Creating OLT Alarm Profile

Perform the following steps to create an OLT alarm profile.

1. Select **Profile > Alarm Profile > Create**.
The Alarm Profile Configuration page appears.
2. Complete the OLT alarm profile configuration according to the guidelines provided in the following table.

Table 222. OLT Alarm Profile Configuration

| Field | Description |
|-------|--|
| Name | Enter a unique name for the alarm profile. You can use any number of alphanumeric characters. Only the following special characters are supported. |

| Field | Description |
|----------------------------------|---|
| | <ul style="list-style-type: none"> Underscore (_) Hyphen (-) |
| Type | Select the type as OLT from the list. |
| CPU Utilization Threshold (%) | <p>Enter the CPU utilization threshold value (in percentage) of the OLT for the following categories.</p> <ul style="list-style-type: none"> Warning Minor Major Critical <p> Note: The value ranges from 0 to 100. If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The configured value must be Critical > Major > Minor > Warning. The default value for the following severity levels is.</p> <ul style="list-style-type: none"> Warning (60) Minor (70) Major (80) Critical (90) |
| Memory Utilization Threshold (%) | <p>Enter the memory utilization threshold value (in percentage) of the OLT for the following categories.</p> <ul style="list-style-type: none"> Warning Minor Major Critical <p> Note: The value ranges from 0 to 100. If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The configured value must be Critical > Major > Minor > Warning. The default value for the following severity levels is.</p> <ul style="list-style-type: none"> Warning (65) Minor (70) Major (80) Critical (90) |

| Field | Description |
|--|--|
| Fan Speed (%) | <p>Enter the fan speed threshold value (in percentage) for the OLT for the following categories.</p> <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: The value ranges from 0 to 100. If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The configured value must be Critical > Major > Minor > Warning. The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (40) ◦ Minor (45) ◦ Major (55) ◦ Critical (60) |
| Disk Utilization Threshold (%) | <p>Enter the disk utilization threshold value (in percentage) of the OLT for the following categories.</p> <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: The value ranges from 0 to 100. If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The configured value must be Critical > Major > Minor > Warning. The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (65) ◦ Minor (70) ◦ Major (80) ◦ Critical (90) |
| Disk Utilization Threshold Per Partition | <p>Enter the disk utilization threshold value (in percentage) for each partition.</p> <p>The following partitions are supported.</p> |

| Field | Description |
|-------|---|
| | <ul style="list-style-type: none"> ◦ sda7 ◦ loop0 ◦ loop1 ◦ loop2 ◦ loop3 ◦ loop4 ◦ loop5 ◦ sda5 ◦ sda6 ◦ sda4 ◦ sda3 ◦ sda8 <p> Note: The value ranges from 0 to 100. If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The configured value must be Critical > Major > Minor > Warning.</p> |
| sda7 | <p>This partition is mounted on the <i>/or mnt/onl/data_active</i> path and represents a directory that contains data partition for <i>/or mnt/onl/data_active</i>.</p> <p>The default value for the sda7 partition severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (70) ◦ Minor (75) ◦ Major (80) ◦ Critical (85) |
| loop0 | <p>This partition is mounted on the <i>/var</i> path excluding <i>/var/tmp</i> and <i>/var/log</i> paths.</p> <p>The default value for the loop0 partition severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (60) ◦ Minor (70) ◦ Major (75) ◦ Critical (80) |
| loop1 | <p>This partition is mounted on the <i>/var/tmp</i> path and represents the directory used for IPC.</p> <p>The default value for the loop1 partition severity levels is.</p> |

| Field | Description |
|-------|---|
| | <ul style="list-style-type: none">◦ Warning (65)◦ Minor (70)◦ Major (75)◦ Critical (80) |
| loop2 | <p>This partition is mounted on the <code>/var/log</code> path, excluding <code>/var/log/audit</code> path, and represents a directory that contains CBAC or OLT application logs.</p> <p>The default value for the loop2 partition severity levels is.</p> <ul style="list-style-type: none">◦ Warning (75)◦ Minor (80)◦ Major (85)◦ Critical (90) |
| loop3 | <p>This partition is mounted on the <code>/var/log/audit</code> path and represents a directory that contains audit logs.</p> <p>The default value for the loop3 partition severity levels is.</p> <ul style="list-style-type: none">◦ Warning (50)◦ Minor (55)◦ Major (60)◦ Critical (65) |
| loop4 | <p>This partition is mounted on the <code>/home</code> path and represents a directory that contains OLT users.</p> <p>The default value for the loop4 partition severity levels is.</p> <ul style="list-style-type: none">◦ Warning (60)◦ Minor (70)◦ Major (75)◦ Critical (80) |
| loop5 | <p>This partition is mounted on the <code>/tmp</code> path and represents a directory that contains temporary files.</p> <p>The default value for the loop5 partition severity levels is.</p> <ul style="list-style-type: none">◦ Warning (70)◦ Minor (75)◦ Major (80)◦ Critical (85) |
| sda5 | <p>This partition is mounted on the <code>/mnt/onl/images</code> path and represents a directory that contains a maximum of three ONL images.</p> <p>The default value for the sda5 partition severity levels is.</p> |

| Field | Description |
|--------------------------------------|--|
| | <ul style="list-style-type: none"> ◦ Warning (70) ◦ Minor (75) ◦ Major (80) ◦ Critical (85) |
| sda6 | <p>This partition is mounted on the <code>/mnt/onl/sdpon</code> path and represents a directory that contains CBAC contents.</p> <p>The default value for the sda6 partition severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (80) ◦ Minor (85) ◦ Major (90) ◦ Critical (95) |
| sda4 | <p>This partition is mounted on the <code>/mnt/onl/config</code> path and represents a directory that contains OLT configurations.</p> <p>The default value for the sda4 partition severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (55) ◦ Minor (60) ◦ Major (65) ◦ Critical (70) |
| sda3 | <p>This partition is mounted on the <code>/mnt/onl/boot</code> path and represents a directory that contains boot related files.</p> <p>The default value for the sda3 partition is.</p> <ul style="list-style-type: none"> ◦ Warning (55) ◦ Minor (60) ◦ Major (65) ◦ Critical (70) |
| sda8 | <p>This partition is mounted on the <code>/mnt/onl/data_standby</code> path and represents a directory that contains data partition for <code>/</code> or <code>/mnt/onl/data_standby</code>.</p> <p>The default value for the sda8 partition is.</p> <ul style="list-style-type: none"> ◦ Warning (70) ◦ Minor (75) ◦ Major (80) ◦ Critical (85) |
| Thermal Sensor Temperature (Celsius) | Enter the name for the thermal sensor and the threshold value (in Celsius) for the following categories. |

| Field | Description |
|-------|---|
| | <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p>Click the Add Thermal Sensor option to add one or more thermal sensors for the OLT.</p> |

The recommended values for the different thermal sensors is mentioned in the following table.

| RLT-3200G | RLT-1600G/RLT-1600X | Minor | Warning | Major | Critical |
|------------------------------|------------------------------|-------|---------|-------|----------|
| CPU | CPU | 70 | 75 | 78 | 80 |
| MB_TMP435_1_LOCAL | MB_TMP435_1_LOCAL | 85 | 90 | 95 | 100 |
| MB_TMP435_1_REMOTE_A_SPEN | MB_TMP435_1_REMOTE_AS PEN | 85 | 90 | 95 | 100 |
| MB_TMP435_2_LOCAL | MB_TMP435_2_LOCAL | 60 | 62 | 64 | 70 |
| MB_TMP435_2_REMOTE_AIR_INLET | MB_TMP435_2_REMOTE_AIR_INLET | 60 | 62 | 64 | 70 |
| MB_TMP435_3_LOCAL | MB_TMP435_3_LOCAL | 65 | 68 | 70 | 75 |
| MB_TMP435_3_REMOTE_SWC | MB_TMP435_3_REMOTE_SWC | 85 | 90 | 95 | 100 |
| DB_TMP435_1_LOCAL | | 65 | 68 | 70 | 75 |
| DB_TMP435_1_REMOTE_A_SPEN | | 85 | 90 | 95 | 100 |
| DB_TMP435_2_LOCAL | | 60 | 62 | 64 | 70 |
| DB_TMP435_2_REMOTE | | 60 | 62 | 64 | 70 |

| RLT-3200C | RLT-1600C | Minor | Warning | Major | Critical |
|--------------------------|--------------------------|-------|---------|-------|----------|
| CPU | CPU | 70 | 75 | 78 | 80 |
| MB_TMP435_2_ASPEN_LOCAL | MB_TMP435_2_ASPEN_LOCAL | 85 | 90 | 95 | 100 |
| MB_TMP435_2_ASPEN_REMOTE | MB_TMP435_2_ASPEN_REMOTE | 85 | 90 | 95 | 100 |

| RLT-3200C | RLT-1600C | Minor | Warning | Major | Critical |
|------------------------------------|------------------------------------|-------|---------|-------|----------|
| MB_TMP435_1_INLET_LOCAL | MB_TMP435_1_INLET_LOCAL | 60 | 62 | 64 | 70 |
| MB_TMP435_1_INLET_REMOTE | MB_TMP435_1_INLET_REMOTE | 60 | 62 | 64 | 70 |
| MB_TMP435_3_OUTLET_LOCAL | MB_TMP435_3_OUTLET_LOCAL | 65 | 68 | 70 | 75 |
| MB_TMP435_3_REMOTE_SWC_THEME_DIODE | MB_TMP435_3_REMOTE_SWC_THEME_DIODE | 85 | 90 | 95 | 100 |
| DB_TMP435_2_ASPIRE_LOCAL | | 85 | 90 | 95 | 100 |
| DB_TMP435_2_ASPIRE_REMOTE | | 85 | 90 | 95 | 100 |
| DB_TMP435_1_INLET_LOCAL | | 60 | 62 | 64 | 70 |
| DB_TMP435_1_INLET_REMOTE | | 60 | 62 | 64 | 70 |

3. Click **Create**.

A new OLT alarm profile is created on the Alarm Profile List page.

OLT Port Alarm Profile

The OLT port KPIs include the NNI port downstream and upstream utilization, PON port downstream and upstream utilization, PON FCS error, PON drop of packet, and MCast active channels per PON exceeded. The OLT port alarm profile sets the high and low thresholds for each of the parameter and the alarms are reported by CBAC to RMS based on the thresholds.

Creating OLT PORT Alarm Profile

Perform the following steps to create an OLT port alarm profile.

1. Select **Profile > Alarm Profile > Create**.
The Alarm Profile Configuration page appears.
2. Complete the OLT port alarm profile configuration according to the guidelines provided in the following table.

Table 223. OLT Port Alarm Profile

| Field | Description |
|--------------------------------|---|
| Name | <p>Enter a unique name for the alarm profile. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Type | Select the type as OLT PORT from the list. |
| NNI Downstream Utilization (%) | <p>Enter the NNI port downstream utilization for the OLT (in percentage) for the following categories.</p> <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: The value ranges from 0 to 100. If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The configured value must be Critical > Major > Minor > Warning. The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (0) ◦ Minor (26) ◦ Major (51) ◦ Critical (76) |
| NNI Upstream Utilization (%) | <p>Enter the NNI port upstream utilization for the OLT (in percentage) for the following categories.</p> <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: The value ranges from 0 to 100. If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The configured value must be Critical > Major > Minor > Warning. The default value for the following severity levels is.</p> |

| Field | Description |
|--------------------------------|--|
| | <ul style="list-style-type: none"> ◦ Warning (0) ◦ Minor (26) ◦ Major (51) ◦ Critical (76) |
| PON Downstream Utilization (%) | <p>Enter the PON port downstream utilization for the OLT (in percentage) for the following categories.</p> <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: The value ranges from 0 to 100. If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The configured value must be Critical > Major > Minor > Warning. The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (0) ◦ Minor (26) ◦ Major (51) ◦ Critical (76) |
| PON Upstream Utilization (%) | <p>Enter the PON port upstream utilization of the OLT (in percentage) for the following categories.</p> <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: The value ranges from 0 to 100. If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The configured value must be Critical > Major > Minor > Warning. The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (0) ◦ Minor (26) |

| Field | Description |
|--|--|
| | <ul style="list-style-type: none"> ◦ Major (51) ◦ Critical (76) |
| PON FCS Error (15 Minutes Interval) | Enter the PON port FCS error of the OLT (in number) for 15 minutes interval for the severity level “Minor”. The default value is 8000. |
| PON FCS Error (1 Day Interval) | Enter the PON port FCS error of the OLT (in number) for one day interval for the severity level “Major”. The default value is 768000. |
| PON Drop of Packet (15 Minutes Interval) | Enter the PON port drop of packets of the OLT (in number) for 15 minutes interval for the severity level “Minor”. The default value is 10000. |
| PON Drop of Packet (1 Day Interval) | Enter the PON port drop of packets of the OLT (in number) for one day interval for the severity level “Major”. The default value is 960000. |
| MCast Active Channels per PON Exceeded (%) | Enter the number of multicast active channels on the PON port exceeded than the configured limit. The default value for the following severity levels is. <ul style="list-style-type: none"> ◦ Warning (50) ◦ Minor (70) ◦ Major (80) ◦ Critical (90) |

3. Click **Create**.

A new OLT port alarm profile is created on the Alarm Profile List page.

ONT Alarm Profile

The ONT KPIs include the lower traffic class drop of packets (minor, and major). The ONT alarm profile sets the high and low thresholds for each of the parameters, and the alarms are reported by CBAC to RMS based on the thresholds.

Creating ONT Alarm Profile

Perform the following steps to create an ONT alarm profile.

1. Select **Profile > Alarm Profile > Create**.

The Alarm Profile Configuration page appears.

2. Complete the ONT alarm profile configuration according to the guidelines provided in the following table.

Table 224. ONT Alarm Profile Configuration

| Field | Description |
|---|---|
| Name | Enter a unique name for the alarm profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Type | Select the type as ONT from the list. |
| Lower traffic class drop of packets (Minor) | Enter the number of packet drops for the lower traffic class flow for the severity level “Minor”. The default value is 100. |
| Lower traffic class drop of packets (Major) | Enter the number of packet drops for the lower traffic class flow for the severity level “Major”. The default value is 1600. |

3. Click **Create**.

A new ONT alarm profile is created on the Alarm Profile List page.

LAG Alarm Profile

The LAG KPIs include the LAG upstream and downstream utilization. The LAG alarm profile sets the high and low thresholds for each of the parameter and the alarms are reported by CBAC to RMS based on the thresholds.

Creating LAG Alarm Profile

Perform the following steps to create a LAG alarm profile.

1. Select **Profile > Alarm Profile > Create**.

The Alarm Profile Configuration page appears.

2. Complete the LAG alarm profile configuration according to the guidelines provided in the following table.

Table 225. LAG Alarm Profile Configuration

| Field | Description |
|-------|---|
| Name | Enter a unique name for the alarm profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |

| Field | Description |
|---|---|
| Type | Select the type as LAG from the list. |
| Link Aggregation Downstream Utilization (%) | <p>Enter the link aggregation downstream utilization value (in percentage) for the following categories.</p> <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: The value ranges from 0 to 100. If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The configured value must be Critical > Major > Minor > Warning. The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (10) ◦ Minor (70) ◦ Major (75) ◦ Critical (80) |
| Link Aggregation Upstream Utilization (%) | <p>Enter the link aggregation upstream utilization value (in percentage) for the following categories.</p> <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: The value ranges from 0 to 100. If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The configured value must be Critical > Major > Minor > Warning. The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (10) ◦ Minor (70) ◦ Major (75) ◦ Critical (80) |

3. Click **Create**.

A new LAG alarm profile is created on the Alarm Profile List page.

ACE Alarm Profile

The ACE KPIs include the Access Control Entry (ACE). The ACE alarm profile sets the high and low thresholds for each of the parameters and the alarms are reported by CBAC to RMS based on the thresholds.

Creating ACE Alarm Profile

Perform the following steps to create an ACE alarm profile.

1. Select **Profile > Alarm Profile > Create**.
The Alarm Profile Configuration page appears.
2. Complete the ACE alarm profile configuration according to the guidelines provided in the following table.

Table 226. ACE Alarm Profile Configuration

| Field | Description |
|--------------------------|---|
| Name | Enter a unique name for the alarm profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Type | Select the type as ACE from the list. |
| Access Control Entry (%) | Enter the ACE value (in percentage) for the following categories. <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical  Note: The value ranges from 0 to 100. If the value configured for the above categories exceeds, an alarm is raised with the respective severity. The configured value must be Critical > Major > Minor > Warning . The default value for the following severity levels is. <ul style="list-style-type: none">◦ Warning (10)◦ Minor (70)◦ Major (75)◦ Critical (80) |

3. Click **Create**.

A new ACE alarm profile is created on the Alarm Profile List page.

SFP (NNI) Alarm Profile

The SFP KPIs include the Tx power, Rx power, voltage, bias current, and temperature. The SFP alarm profile sets the high and low thresholds for each of the parameter and the alarms are reported by CBAC to RMS based on the thresholds.

Creating SFP (NNI) Alarm Profile

Perform the following steps to create an SFP alarm profile.

1. Select **Profile > Alarm Profile > Create**.

The Alarm Profile Configuration page appears.

2. Complete the SFP alarm profile configuration according to the guidelines provided in the following table.

Table 227. SFP (NNI) Alarm Profile Configuration

| Field | Description |
|------------------|--|
| Name | Enter a unique name for the alarm profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Type | Select the type as SFP from the list. |
| Port Type | Select the port type as NNI from the list. |
| High Temperature | Enter the high temperature value (in Celsius) of the NNI ports of the OLT for the following categories. <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical  Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity. The default value for the following severity levels is. <ul style="list-style-type: none">◦ Warning (70)◦ Minor (75) |

| Field | Description |
|--------------------------|---|
| | <ul style="list-style-type: none"> ◦ Major (78) ◦ Critical (82) |
| Low Temperature | <p>Enter the low temperature value (in Celsius) of the NNI ports of the OLT for the following categories.</p> <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (-10) ◦ Minor (-20) ◦ Major (-30) ◦ Critical (-35) |
| High Diag Supply Voltage | <p>Enter the high supply voltage (in Volts) of the SFP for the following categories.</p> <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (3.25) ◦ Minor (3.3) ◦ Major (3.35) ◦ Critical (3.4) |
| Low Diag Supply Voltage | <p>Enter the low supply voltage (in Volts) of the SFP for the following categories.</p> <ul style="list-style-type: none"> ◦ Warning ◦ Minor |

| Field | Description |
|------------------------|---|
| | <ul style="list-style-type: none">◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (3.2)◦ Minor (3.17)◦ Major (3.16)◦ Critical (3.15) |
| High Diag Bias Current | <p>Enter the high bias current (in milli amps) of the SFP for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (80)◦ Minor (85)◦ Major (90)◦ Critical (95) |
| Low Diag Bias Current | <p>Enter the low bias current (milli amps) of the SFP for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> |

| Field | Description |
|---------------|---|
| | <ul style="list-style-type: none">◦ Warning (1)◦ Minor (0.5)◦ Major (0.25)◦ Critical (0) |
| High Tx Power | <p>Enter the high transmit power of the SFP (in dbm) for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (-1.5)◦ Minor (-1)◦ Major (-0.5)◦ Critical (0) |
| Low Tx Power | <p>Enter the low transmit power of the SFP (in dbm) for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (-7.2)◦ Minor (-7.5)◦ Major (-7.8)◦ Critical (-8) |
| High Rx Power | Enter the high received power of the SFP (in dbm) for the following categories. |

| Field | Description |
|--------------|---|
| | <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (-1.5) ◦ Minor (-1) ◦ Major (-0.5) ◦ Critical (0) |
| Low Rx Power | <p>Enter the low received power of the SFP (in dbm) for the following categories.</p> <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (-12) ◦ Minor (-12.5) ◦ Major (-13) ◦ Critical (-14) |

3. Click **Create**.

A new SFP alarm profile is created on the Alarm Profile List page.

SFP (PON) Alarm Profile

SFP Alarm Profile. The SFP KPIs include the Tx power, Rx power, voltage, bias current, and temperature. The SFP alarm profile sets the high and low thresholds for each of the parameter and the alarms are reported by CBAC to RMS based on the thresholds.

Creating SFP (PON) Alarm Profile

Perform the following steps to create an SFP (PON) alarm profile.

1. Select **Profile > Alarm Profile > Create**.

The Alarm Profile Configuration page appears.

2. Complete the SFP alarm profile configuration according to the guidelines provided in the following table.

Table 228. SFP (PON) Alarm Profile Configuration

| Field | Description |
|------------------|---|
| Name | Enter a unique name for the alarm profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Type | Select the type as SFP from the list. |
| Port Type | Select the port type as PON from the list. |
| High Temperature | Enter the high temperature value (in Celsius) of the PON ports of the OLT for the following categories. <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical  Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity. The default value for the following severity levels is. <ul style="list-style-type: none">◦ Warning (70)◦ Minor (75)◦ Major (78)◦ Critical (82) |
| Low Temperature | Enter the low temperature value (in Celsius) of the PON ports of the OLT for the following categories. <ul style="list-style-type: none">◦ Warning◦ Minor |

| Field | Description |
|--------------------------|--|
| | <ul style="list-style-type: none">◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (-10)◦ Minor (-20)◦ Major (-30)◦ Critical (-35) |
| High Diag Supply Voltage | <p>Enter the high supply voltage (in Volts) of the SFP for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (3.25)◦ Minor (3.3)◦ Major (3.35)◦ Critical (3.4) |
| Low Diag Supply Voltage | <p>Enter the low supply voltage (in Volts) of the SFP for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> |

| Field | Description |
|------------------------|---|
| | <ul style="list-style-type: none">◦ Warning (3.2)◦ Minor (3.17)◦ Major (3.16)◦ Critical (3.15) |
| High Diag Bias Current | <p>Enter the high bias current (in milli amps) of the SFP for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (75)◦ Minor (85)◦ Major (90)◦ Critical (95) |
| Low Diag Bias Current | <p>Enter the low bias current (milli amps) of the SFP for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (1)◦ Minor (0.5)◦ Major (0.25)◦ Critical (0) |
| High Tx Power | Enter the high transmit power of the SFP (in dbm) for the following categories. |

| Field | Description |
|--------------|---|
| | <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (6) ◦ Minor (6.2) ◦ Major (6.3) ◦ Critical (6.5) |
| Low Tx Power | <p>Enter the low transmit power of the SFP (in dbm) for the following categories.</p> <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (4) ◦ Minor (3.8) ◦ Major (3.7) ◦ Critical (3.5) |

3. Click **Create**.

A new SFP alarm profile is created on the Alarm Profile List page.

ANI-G Alarm Profile

The ONT provides information such as temperature, voltage, and bias current parameters of the transceiver. These parameters play a critical role in maintaining the health of the ONTs connectivity to the OLT. As the ONTs are deployed at a remote customer location, it is difficult for the operator to know what the problem is and when the ONT is not reachable or misbehaves. The ANI-G alarm profile is attached to the ONT and monitors the parameters (temperature, voltage, and bias current) in a periodic manner.

Alarms are reported with varied severity levels so that the operator can take some preventive measures before the ONT misbehaves or connectivity is lost.

Creating ANI-G Alarm Profile

Perform the following steps to create an ANI-G alarm profile.

1. Select **Profile > Alarm Profile > Create**.

The Alarm Profile Configuration page appears.

2. Complete the ANI-G alarm profile configuration according to the guidelines provided in the following table.

Table 229. ANI-G Alarm Profile Configuration

| Field | Description |
|----------------------------|---|
| Name | <p>Enter a unique name for the alarm profile. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Type | Select the type as ANI-G from the list. |
| High Temperature (Celsius) | <p>Enter the high temperature value (in Celsius) of the transceiver for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (60)◦ Minor (63)◦ Major (65)◦ Critical (70) |
| Low Temperature (Celsius) | Enter the low temperature value (in Celsius) of the transceiver for the following categories. |

| Field | Description |
|--------------------------------|---|
| | <ul style="list-style-type: none">◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (42)◦ Minor (40)◦ Major (35)◦ Critical (30) |
| High Bias Current (milli amps) | <p>Enter the high bias current (in milli amps) of the transceiver for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (20)◦ Minor (25)◦ Major (30)◦ Critical (35) |
| Low Bias Current (milli amps) | <p>Enter the low bias current (in milli amps) of the transceiver for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> |

| Field | Description |
|----------------------------|---|
| | <ul style="list-style-type: none">◦ Warning (6)◦ Minor (5)◦ Major (4.5)◦ Critical (4) |
| High Voltage (milli-volts) | <p>Enter the high voltage (in milli-volts) of the transceiver for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (3.5)◦ Minor (3.6)◦ Major (3.7)◦ Critical (3.8) |
| Low Voltage (milli-volts) | <p>Enter the low voltage (in milli-volts) of the transceiver for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (3)◦ Minor (2.9)◦ Major (2.8)◦ Critical (2.7) |
| High Tx Power (dbm) | Enter the high transmit power of the transceiver (in dbm) for the following categories. |

| Field | Description |
|---------------------|---|
| | <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (4)◦ Minor (4.5)◦ Major (5)◦ Critical (5.5) |
| Low Tx Power (dbm) | <p>Enter the low transmit power of the transceiver (in dbm) for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none">◦ Warning (3.5)◦ Minor (3)◦ Major (2.5)◦ Critical (2) |
| High Rx Power (dbm) | <p>Enter the high receiving power (in dbm) of the transceiver for the following categories.</p> <ul style="list-style-type: none">◦ Warning◦ Minor◦ Major◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> |

| Field | Description |
|--------------------|--|
| | <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (-9) ◦ Minor (-8) ◦ Major (-6) ◦ Critical (-4) |
| Low Rx Power (dbm) | <p>Enter the low receiving power (in dbm) of the transceiver for the following categories.</p> <ul style="list-style-type: none"> ◦ Warning ◦ Minor ◦ Major ◦ Critical <p> Note: If the value configured for the above categories exceeds, an alarm is raised with the respective severity.</p> <p>The default value for the following severity levels is.</p> <ul style="list-style-type: none"> ◦ Warning (-24) ◦ Minor (-25) ◦ Major (-27) ◦ Critical (-28) |
| Thresholds | <p>Enter the threshold value for the number of BER errors seen in the downstream direction in the SF and SD fields.</p> <p>For SF threshold value, the ONT-SIGNAL-FAILURE alarm is reported.</p> <p>For SD threshold value, the OLT-SIGNAL-DEGRADE alarm is reported.</p> <p>The default value for the following thresholds is.</p> <ul style="list-style-type: none"> ◦ SF (6) ◦ SD (9) |

3. Click **Create**.

A new ANI-G alarm profile is created on the Alarm Profile List page.

Log Profile

To access this page, click **Configuration** from the top right corner and select **Profile > Log Profile** from the left-hand side of the menu.

Log profile is used to collect logs from different microservices and OLTs. Both microservice and OLT generate logs and stores the logs in the centralized server using the remote system log server (rsyslog). Using these logs, you can debug the system.

Creating Log Profile

Perform the following steps to create a log profile.

1. Select **Profiles > Log Profile > Create**.
The Log Profile Configuration page appears.
2. Complete the log profile configuration according to the guidelines provided in the following table.

Table 230. Log Profile Configuration

| Field | Description |
|------------|---|
| Name | Enter a unique name for the log server. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Log Server | Enter the valid IP address of the log server or FQDN of the log server. |
| Log Level | Specifies the log level of the device. The supported values are. <ul style="list-style-type: none">◦ INFO. Logs are generated for informational messages◦ DEBUG. Logs are useful for debugging the system◦ WARNING. Logs are generated for warning conditions.◦ ERROR. Logs are generated for any error conditions. This is the default log level. |

3. Click **Create**.

A new log profile is created on the Log Profile List page.



Note: You cannot delete a log profile if the log profile is associated with the active managed element. To delete a log profile, you must first dissociate the log profile from the managed element.

To edit, clone, and delete the log profile configuration, see [Common Operations \(on page 27\)](#).

PPPoE Profile

To access this page, click **Configuration** from the top right corner and select **Profile > PPPoE Profile** from the left-hand side of the menu.

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol that facilitates communication between network endpoints. PPPoE encapsulates PPP frames inside Ethernet frames, allowing multiple users to share a single physical connection to the Internet. It also adds a layer of control and authentication, ensuring that only authorized users can access the Internet through the shared connection.

Creating PPPoE Profile

Perform the following steps to create a PPPoE profile.

1. Select **Profiles > PPPoE Profile > Create**.
The PPPoE Profile Configuration page appears.
2. Complete the PPPoE profile configuration according to the guidelines provided in the following table.

Table 231. PPPoE Profile Configuration

| Field | Description |
|------------------------|--|
| Name | Enter a unique name for the PPPoE profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| NAT Option | Specifies the NAT option. The supported values are. <ul style="list-style-type: none">◦ Enabled◦ Disabled The default value is Enabled. |
| Authentication Type | Specifies the authentication type. The supported values are. <ul style="list-style-type: none">◦ Auto◦ CHAP◦ PAP The default value is Auto. |
| Connection Mode | Specifies the connection mode. The supported values are. <ul style="list-style-type: none">◦ Always◦ On-Demand◦ Manual The default value is Always. |
| Release Time (Seconds) | Specifies the release time for the PPPoE session in seconds. The value ranges from 1 to 65535. The default value is 1200. |

3. Click **Create**.

A new PPPoE profile is created on the PPPoE Profile List page.

PPPoE Over OMCI

OMCI allows the management and control of ONT devices. PPPoE manages the connection between a user's device and the service provider's network.

Creating PPPoE Over OMCI

Perform the following steps to create PPPoE profile and attach to a service.

1. Create PPPoE profile. See [Creating PPPoE Profile \(on page 504\)](#).
2. Perform the following steps to attach the PPPoE profile to the IP-Host port.
 - a. Navigate to **Configuration > Inventory > ONT**.
 - b. Click the **Ports** (grid icon) under the **Action** column.

The Port List [Inventory - <ONT Name>] page appears.

- c. Click the **Edit** icon under Action Column for the IP-Host port.

The Port Configuration page appears.

Figure 86. PPPoE Port Configuration

The Port Configuration dialog box displays the following settings:

- Display Id: /rack=1/shelf=1/slot=LT-1/port=SFPPON-6/remote_unit=1/port=1
- Port Direction: UNI
- Uni Port Type: IP-HOST
- Choose Profile Type: PPPoE
- PPPoE Profile: pppoe
- Service Name: pppoe-config
- User Name: radisys
- Password: (masked)

Buttons at the bottom: Close, Save.

- d. Complete the port configuration according to the guidelines provided in the following table.

Table 232. PPPoE Port Configuration

| Field | Description |
|---------------------|--------------------------------------|
| Choose Profile Type | Select the profile type as PPPoE. |
| PPPoE Profile | Select the applicable PPPoE profile. |
| Service Name | Enter the service name. |
| User Name | Enter the username. |
| Password | Enter the password. |

- e. Click **Save**.
- f. Select the three dots and click **activate** button.

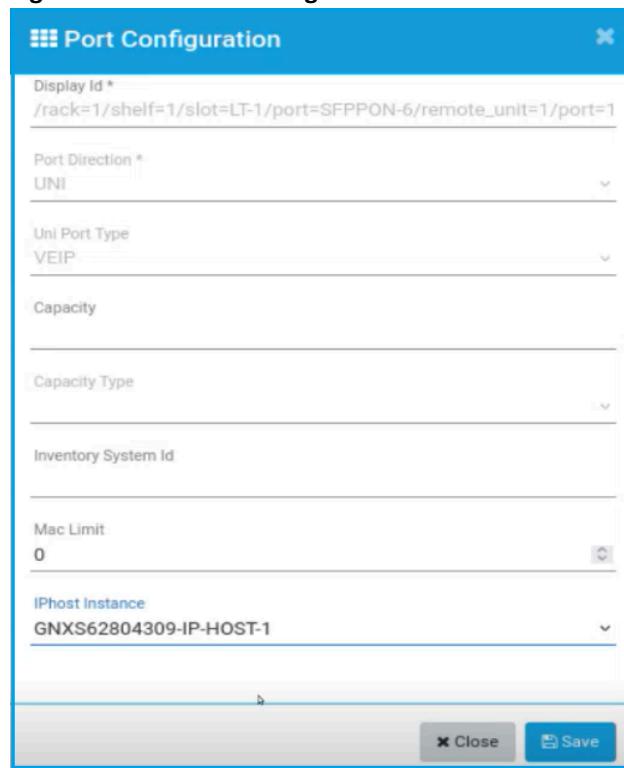
The IP-Host port is activated.

3. Perform the following steps to attach the IPhost instance to the VEIP port.
 - a. Navigate to **Configuration > Inventory > ONT**.
 - b. Click the **Ports** () icon under the **Action** column.

The Port List [**Inventory - <ONT Name>**] page appears.

- c. Click the **Edit** icon under Action Column for the VEIP.

The Port Configuration page appears.

Figure 87. VEIP Port Configuration

- d. Select the **IPHost Instance** from the list.
- e. Click **Save**.
4. Create a service. See [Creating Service \(on page 459\)](#).

The following table describes the other mandatory fields and values for the PPPoE configuration.

Table 233. PPPoE Service Configuration

| Field | Values |
|-------------------|---|
| UNI Port Id | Select the VEIP port to create the service. |
| Encapsulation | Select PPPoE-IA from the list. |
| MAC Learning Type | Select PPPoE from the list. |

5. Activate the service. See [Activating and Deactivating the Service for the Subscriber \(on page 467\)](#).

To edit, clone, and delete the PPPoE profile configuration, see [Common Operations \(on page 27\)](#).

Device Profile

To access this page, click **Configuration** from the top right corner and then select **Profile > Device Profile** from the left-hand side of the menu.

A device profile contains configuration and provision settings for a physical device, such as OLT, ONT, CPE, Splitter, Card, Rack, SFP, and Cable. You can customize the device profile to meet your specific requirements. The device profiles are specific to the type of device and solution's topology. When you create a configuration for these devices, you must assign a device profile to them (OLT, ONT, SFP, CPE, Splitter, BNG, Card, Rack, and Cable).

Creating Device Profile

You can create a device profile for the following devices.

Table 234. Device Profile List

| Device Profiles | For more information, see |
|-----------------|---|
| OLT | OLT Device Profile (on page 508) |
| ONT | ONT Device Profile (on page 515) |
| SFP | SFP Device Profile (on page 516) |
| CPE | CPE Device Profile (on page 518) |
| SPLITTER | Splitter Device Profile (on page 519) |
| BNG | BNG Device Profile (on page 521) |
| CARD | Card Device Profile (on page 522) |
| RACK | Rack Device Profile (on page 524) |
| CABLE | Cable Profile (on page 526) |

OLT Device Profile

The OLT device profile includes the following.

- Name
- ME Type
- Make
- Model
- Max Temperature
- Layout
- Creation Time
- Action

Creating OLT Device Profile

Prerequisites

Before you create a device profile for the OLT, you must create a make and model for the device. See [Creating Make Configuration \(on page 606\)](#) and [Creating Model Configuration \(on page 610\)](#).

The OLT device profile contains the OLT, rack, shelf, and slot configuration.

The following OLT devices profiles exist in RMS by default even after the RMS redeployment.



Note: The following OLTs require one rack, one self, and one slot as a default configuration.

- RLT-3200C-OLT
- RLT-1600X-OLT
- RLT-3200G-OLT
- RLT-1600G-OLT
- RLT-1600C-OLT
- Lumia-G16-DP

Perform the following steps to create an OLT device profile.

1. Select **Profiles > Device Profile**.
The Device Profile List page appears.
2. Click on the **OLT** tab and click **Create**.
The OLT Device Profile Configuration page appears.
3. Complete the OLT device profile configuration according to the guidelines provided in the following table.

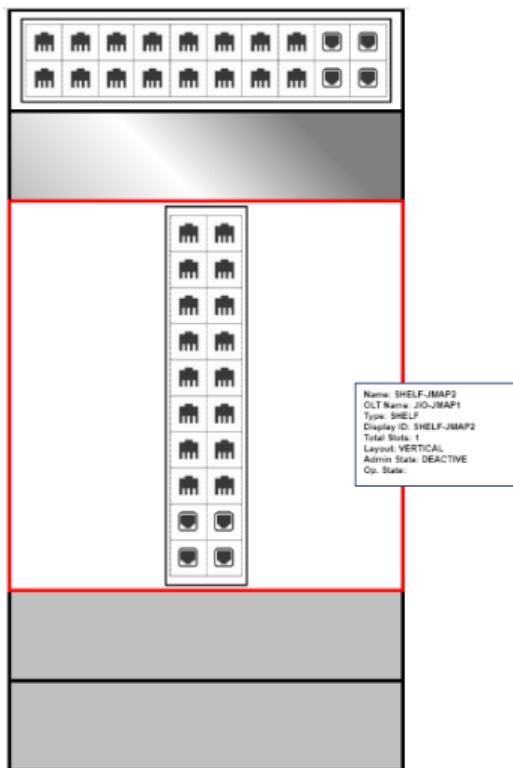
Table 235. OLT Device Profile Configuration

| Field | Description |
|---------|--|
| Name | Enter a unique name for the OLT device profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space Example: Radisys-1RU-AnyPON-DP |
| ME Type | Specifies the managed element type. This field is not editable. Example: OLT |
| Make | Select the make of the OLT from the list. Example: Radisys |

| Field | Description |
|----------------------|--|
| Model | Select the model of the OLT from the list. Example: RLT-1600C |
| Max Temperature | Enter the maximum temperature for the OLT. Example: 90° Celsius |
| Max Temperature Unit | Select the maximum temperature unit from the list. <ul style="list-style-type: none"> ◦ Celsius ◦ Fahrenheit |
| Layout | Select the layout of the OLT from the list. The supported values are. <ul style="list-style-type: none"> ◦ HORIZONTAL ◦ VERTICAL The layout specifies how the device is shown such as horizontal or vertical. If the horizontal view is chosen, all the cards in the OLT are shown as horizontal. This gives flexibility to the user to configure the device view by themselves. |

The following figure shows the OLT horizontal and vertical layout with two slots.

Figure 88. OLT Layout View



4. Click **Create**.

A new OLT device profile is created on the Device Profile List page.

As part of OLT device profile, you must create rack, shelf, and slot configuration.



Note: When you associate the device profile with any managed element, the managed element is associated with all the parameters configured in the device profile. Also, for the managed elements where the ports are configured (For example, CARD), associating a device profile creates ports automatically on the managed element.

Slot Configuration

Creating Slot Configuration

Perform the following steps to create the shelf details.

1. Select **Profiles > Device Profile**.

The Device Profile List page appears.

2. Click on the **OLT** tab.

The OLT Device Profile Configuration page appears.

3. Click on the rack icon under the **Action** column.

The RACK List [OLT - <Device Profile Name> page appears.

4. Click on the shelf icon under the **Action** column.

The SHELF List [RACK - <Rack Name> page appears.

5. Click on the slot icon under the **Action** column.

The SLOT List [SHELF - <Shelf Name> page appears.

6. Click **Create**.

The SLOT Detail Configuration page appears.

7. Complete the slot configuration according to the guidelines provided in the following table.

Table 236. Slot Detail Configuration

| Field | Description |
|----------------------|---|
| Basic Details | |
| Name | Enter a unique name for the slot. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space |
| Type | Specifies the slot type. This field cannot be modified. Example: OLT-SLOT |

| Field | Description |
|--------------|--|
| Number | Enter the slot number on which the OLT is placed. |
| Holder State | Select the holder state from the list. The supported states are. <ul style="list-style-type: none">◦ EMPTY◦ INSTALLED AND EXPECTED◦ INSTALLED AND NOT EXPECTED◦ MISMATCH INSTALLED AND EXPECTED◦ UNAVAILABLE◦ UNKNOWN |
| Layout | Specifies the layout of the slot. The supported values are. <ul style="list-style-type: none">◦ HORIZONTAL◦ VERTICAL |
| Slot Type | Specifies the slot type. The supported values are. <ul style="list-style-type: none">◦ ACU◦ NTA◦ LT1◦ LT2◦ LT3◦ LT4◦ LT5◦ LT6◦ LT7◦ LT8◦ LT9◦ LT10◦ LT11◦ LT12◦ LT13◦ LT14◦ LT15◦ LT16◦ NONE |

Rack Details Configuration

Creating Rack Details Configuration

Perform the following steps to create the rack details.

1. Select **Profiles > Device Profile**.

The Device Profile List page appears.

2. Click on the **OLT** tab.

The OLT Device Profile Configuration page appears.

3. Click on the rack icon under the **Action** column.

The RACK List <OLT - Device Profile Name> page appears.

4. Click **Create**.

The RACK Detail Configuration page appears.

5. Complete the configuration according to the guidelines provided in the following table.

Table 237. Rack Detail Configuration

| Field | Description |
|--------------|--|
| Name | Enter a unique name for the rack. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space |
| Type | Specifies the rack type. This field cannot be modified. Example: OLT-RACK |
| Number | Enter the rack number on which the OLT is placed. |
| Holder State | Select the holder state from the list. The supported states are. <ul style="list-style-type: none">◦ EMPTY◦ INSTALLED AND EXPECTED◦ INSTALLED AND NOT EXPECTED◦ MISMATCH INSTALLED AND EXPECTED◦ UNAVAILABLE◦ UNKNOWN |
| Layout | Specifies the layout of the rack. The supported values are. <ul style="list-style-type: none">◦ HORIZONTAL◦ VERTICAL |

Shelf Configuration

Creating Shelf Configuration

Perform the following steps to create the shelf details.

1. Select **Profiles > Device Profile**.

The Device Profile List page appears.

2. Click on the **OLT** tab.

The OLT Device Profile Configuration page appears.

3. Click on the rack icon under the **Action** column.

The RACK List [OLT - <Device Profile Name> page appears.

4. Click on the shelf icon under the **Action** column.

The SHELF List [RACK - <Shelf Name> page appears.

5. Click **Create**.

The SHELF Detail Configuration page appears.

6. Complete the shelf configuration according to the guidelines provided in the following table.

Table 238. Shelf Detail Configuration

| Field | Description |
|--------------|--|
| Name | Enter a unique name for the shelf. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space |
| Type | Specifies the rack type. This field cannot be modified. Example: OLT-SHELF |
| Number | Enter the shelf number on which the OLT is placed. |
| Holder State | Select the holder state from the list. The supported states are. <ul style="list-style-type: none">◦ EMPTY◦ INSTALLED AND EXPECTED◦ INSTALLED AND NOT EXPECTED◦ MISMATCH INSTALLED AND EXPECTED◦ UNAVAILABLE◦ UNKNOWN |
| Layout | Specifies the layout of the rack. The supported values are. <ul style="list-style-type: none">◦ HORIZONTAL◦ VERTICAL |

ONT Device Profile

The ONT device profile includes the following.

- Name
- ME Type
- Make
- Model
- Slot No
- Row
- Column
- Ports
- Creation Time
- Action

Creating ONT Device Profile

Prerequisites

Before you create a device profile, you must create a make and model for the device. See [Creating Make Configuration \(on page 606\)](#) and [Creating Model Configuration \(on page 610\)](#).

Perform the following steps to create an ONT device profile.

1. Select **Profiles > Device Profile**.
The Device Profile List page appears.
2. Click on the **ONT** tab and click **Create**.
The ONT Device Profile Configuration page appears.
3. Complete the ONT device profile configuration according to the guidelines provided in the following table.

Table 239. ONT Device Profile Configuration

| Field | Description |
|---------|--|
| Name | Enter a unique name for the ONT device profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space Example: Iskratel-G64-DP |
| ME Type | Specifies the managed element type. This field is not editable. Example: ONT. |

| Field | Description |
|------------------------------|--|
| Make | Select the make of the ONT from the list. |
| Model | Select the model of the ONT from the list. |
| Vendor Allocated Slot Number | Enter the slot number allocated for the ONT by the vendor. |
| Layout - Total Rows | Enter the total number of rows required for displaying the device view. |
| Layout - Total Columns | Enter the total number of columns required for displaying the device view. |

4. Click **Create**.

A new ONT device profile is created on the Device Profile List page.

SFP Device Profile

SFP Device Profile. Specifies the parameters configured for the SFP device profile. The SFP device profile includes the following.

- Name
- ME Type
- Make
- Model
- Bandwidth
- Operating Distance
- Core Size
- Wave Length
- Fibre Type
- Transmit Power Range
- Receive Power Range
- Part Number
- Nominal Bitrate
- Signal Range
- Creation Time
- Action

Cloning SFP Device Profile

The following SFP devices profiles exist in RMS by default even after the RMS redeployment.

- SFP_Hisense_SFP_Profile
- SFP_FINISAR CORP._SFP_Profile

Perform the following steps to clone and create a SFP device profile.

1. Select **Profiles > Device Profile**.
The Device Profile List page appears.
2. Click on the **SFP** tab.
3. Select the Clone icon from the **Action** column.
The SFP Device Profile Configuration page appears.
4. Modify the SFP device profile configuration according to the guidelines provided in the following table.

Table 240. SFP Device Profile Configuration

| Field | Description |
|--------------------|--|
| SFP | |
| Name | <p>Enter a unique name for the SFP device profile. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space <p>Example: SFP_FINISAR CORP._SFP_Profile</p> |
| ME Type | <p>Specifies the managed element type. This field displays the ME type as SFP and it is not editable.</p> <p>Example: SFP</p> |
| Make | <p>Select the make for the SFP from the list. If the make does not exist for the SFP, click the plus icon (+) to create a make configuration for the SFP. See Creating Make Configuration (on page 606).</p> |
| Model | <p>Select the model for the SFP from the list. If the model does not exist for the SFP, click the plus icon (+) to create a model for the SFP. See Creating Model Configuration (on page 610).</p> |
| Bandwidth | Enter the bandwidth for the SFP. |
| Operating Distance | Enter the operating distance for the SFP. |
| Core Size | Enter the core size for the SFP. |
| Wave Length | Enter the wavelength for the SFP. |
| Fiber Type Unit | Select the fiber type from the list. |

| Field | Description |
|-----------------------|---|
| | <ul style="list-style-type: none">◦ MMF◦ SMF |
| Transmit Power Range | Enter the transmit power range for the SFP. |
| Receive Power Range | Enter the receive power range for the SFP. |
| Part Number | Enter the part number of the SFP. |
| SFP Signal Range (Km) | Enter the signal range in kilometer for the SFP. |
| SFP Nominal Bitrate | Enter the nominal bit rate for the SFP. |

5. Click **Create**.

A new SFP device profile is created on the Device Profile List page.

CPE Device Profile

The CPE device profile includes the following.

- Name
- ME Type
- Make
- Model
- Row
- Column
- Ports
- Creation Time
- Action

Creating CPE Device Profile

Prerequisites

Before you create a CPE device profile, you must create a make and model for the CPE device. See [Creating Make Configuration \(on page 606\)](#) and [Creating Model Configuration \(on page 610\)](#).

Perform the following steps to create CPE device profile.

1. Select **Profiles > Device Profile**.
The Device Profile List page appears.
2. Click on the **CPE** tab and click **Create**.
The CPE Device Profile Configuration page appears.
3. Complete the CPE device profile configuration according to the guidelines provided in the following table.

Table 241. CPE Device Profile Configuration

| Field | Description |
|------------------------|---|
| Name | Enter a unique name for the CPE device profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) ◦ Space |
| ME Type | Specifies the managed element type. This field is not editable. Example: CPE |
| Make | Select the make of the CPE from the list. |
| Model | Select the CPE model from the list. |
| Layout - Total Rows | Enter the total number of rows required for the CPE. |
| Layout - Total Columns | Enter the total number of columns required for the CPE. |

4. Click **Create**.

A new CPE device profile is created on the Device Profile List page.

Splitter Device Profile

The splitter device profile includes the following.

- Name
- ME Type
- Make
- Model
- Split Ratio
- Row
- Column
- Ports
- Creation Time
- Action

Creating Splitter Device Profile

Prerequisites

Before you create a splitter device profile, you must create a make and model for the device. See [Creating Make Configuration \(on page 606\)](#) and [Creating Model Configuration \(on page 610\)](#).

Perform the following steps to create a splitter device profile.

1. Select **Profiles > Device Profile**.

The Device Profile List page appears.

2. Click on the **SPLITTER** tab and click **Create**.

The SPLITTER Device Profile Configuration page appears.

3. Complete the splitter device profile configuration according to the guidelines provided in the following table.

Table 242. Splitter Device Profile Configuration

| Field | Description |
|------------------------|--|
| Name | Enter a unique name for the splitter device profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space |
| ME Type | Specifies the managed element type. This field displays the ME type as SPLITTER and it is not editable. Example: SPLITTER. |
| Make | Select the make of the splitter from the list. If the make does not exist for splitter, click the plus icon (+) to create a make configuration for the splitter. See Creating Make Configuration (on page 606) . |
| Model | Select the model of the splitter from the list. If the model does not exist for splitter, click the plus icon (+) to create a model for the splitter. See Creating Model Configuration (on page 610) . |
| Split Ratio | Enter the split ratio value for the splitter. The format must be two numeric integers separated by a colon (:). For example, 1:32 or 1:64. |
| Layout - Total Rows | Enter the total number of rows required for the device view. |
| Layout - Total Columns | Enter the total number of columns required for the device view. |

4. Click **Create**.

A new splitter device profile is created on the Device Profile List page.

BNG Device Profile

The BNG device profile includes the following.

- Name
- ME Type
- Make
- Model
- Row
- Ports
- Column
- Creation Time
- Action

Creating BNG Device Profile

Prerequisites

Before you create a BNG device profile, you must create a make and model for the BNG. See [Creating Make Configuration \(on page 606\)](#) and [Creating Model Configuration \(on page 610\)](#).

Perform the following steps to create a BNG device profile.

1. Select **Profiles > Device Profile**.
The Device Profile List page appears.
2. Click on the **BNG** tab and click **Create**.
The BNG Device Profile Configuration page appears.
3. Complete the BNG device profile configuration according to the guidelines provided in the following table.

Table 243. BNG Device Profile Configuration

| Field | Description |
|---------|--|
| Name | Enter a unique name for the BNG device profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space. |
| ME Type | Specifies the managed element type. This field displays the ME type as BNG and it is not editable. Example: BNG |

| Field | Description |
|------------------------|--|
| Make | Select the make for the BNG from the list. If the make does not exist for BNG, click the plus icon (+) to create a make configuration for the BNG. See Creating Make Configuration (on page 606) . |
| Model | Select the model for the BNG from the list. If the model does not exist for BNG, click the plus icon (+) to create a model for the BNG. See Creating Model Configuration (on page 610) . |
| Layout - Total Rows | Enter the total number of rows required for the device view. |
| Layout - Total Columns | Enter the total number of columns required for the device view. |

4. Click **Create**.

A new BNG device profile is created on the Device Profile List page.

Card Device Profile

The card device profile includes the following.

- Name
- ME Type
- Make
- Model
- Row
- Column
- Ports
- Creation Time
- Action

Creating Card Device Profile

Prerequisites

Before you create a card device profile, you must create a make and model for the card device. See [Creating Make Configuration \(on page 606\)](#) and [Creating Model Configuration \(on page 610\)](#).

The following card device profiles exist in RMS by default even after the RMS redeployment.

- RLT-3200C-Card
- RLT-1600X-Card
- RLT-3200G-Card
- RLT-1600G-Card
- RLT-1600C-Card
- Iskratel-G16-Card-DP



Note: Each CARD device profile contains Alarm port, NNI port, and PON port.

Perform the following steps to create a card device profile.

1. Select **Profiles > Device Profile**.

The Device Profile List page appears.

2. Click on the **CARD** tab and click **Create**.

The CARD Device Profile Configuration page appears.

3. Complete the card device profile configuration according to the guidelines provided in the following table.

Table 244. Card Device Profile Configuration

| Field | Description |
|-------------------------|---|
| Name | <p>Enter a unique name for the card device profile. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> Underscore (_) Hyphen (-) Space <p>Example: Radisys-1RU-AnyPON-PON-Card</p> |
| ME Type | <p>Specifies the managed element type. This field displays the ME type as CARD and it is not editable.</p> <p>Example: CARD</p> |
| Make | <p>Select the make for the card from the list. If the make does not exist for the card, click the plus icon (+) to create a make configuration for the card. See Creating Make Configuration (on page 606).</p> |
| Model | <p>Select the model for the card from the list. If the model does not exist for the card, click the plus icon (+) to create a model for the card. See Creating Model Configuration (on page 610).</p> |
| Layout - Total Rows | Enter the total number of rows required for the device view. |
| Layout - Total Columns | Enter the total number of columns required for the device view. |
| Technology Capabilities | <p>Specifies the technology supported by card device profile. For example, GPON or XGSPON.</p> <p>The default value is GPON.</p> |
| Advanced Details | |
| Card Image | Specifies the image for the card device. Click Choose File and select the card image. The supported values are. |

| Field | Description |
|----------------|---|
| | <ul style="list-style-type: none"> ◦ PNG ◦ JPEG |
| Alarm x-axis | Specifies the x-axis coordinates of alarm status in the device view. |
| Alarm y-axis | Specifies the y-axis coordinates of alarm status in the device view. |
| Power A x-axis | Specifies the x-axis coordinates of power A status in the device view. |
| Power A y-axis | Specifies the y-axis coordinates of power A status in the device view. |
| Power B x-axis | Specifies the x-axis coordinates of power B status in the device view. |
| Power B y-axis | Specifies the y-axis coordinates of power B status in the device view. |
| Status x-axis | Specifies the x-axis co-ordinates of the OLT status in the device view. |
| Status y-axis | Specifies the y-axis coordinates of the OLT status in the device view. |

4. Click **Create**.

A new card device profile is created on the Device Profile List page.

Rack Device Profile

The rack device profile includes the following.

- Name
- ME Type
- Make
- Model
- Total Slots
- Size
- Creation Time
- Action

Creating Rack Device Profile

Prerequisites

Before you create a rack device profile, you must create a make and model for the rack device. See [Creating Make Configuration \(on page 606\)](#) and [Creating Model Configuration \(on page 610\)](#).

Perform the following steps to create a rack device profile.

1. Select **Profiles > Device Profile**.

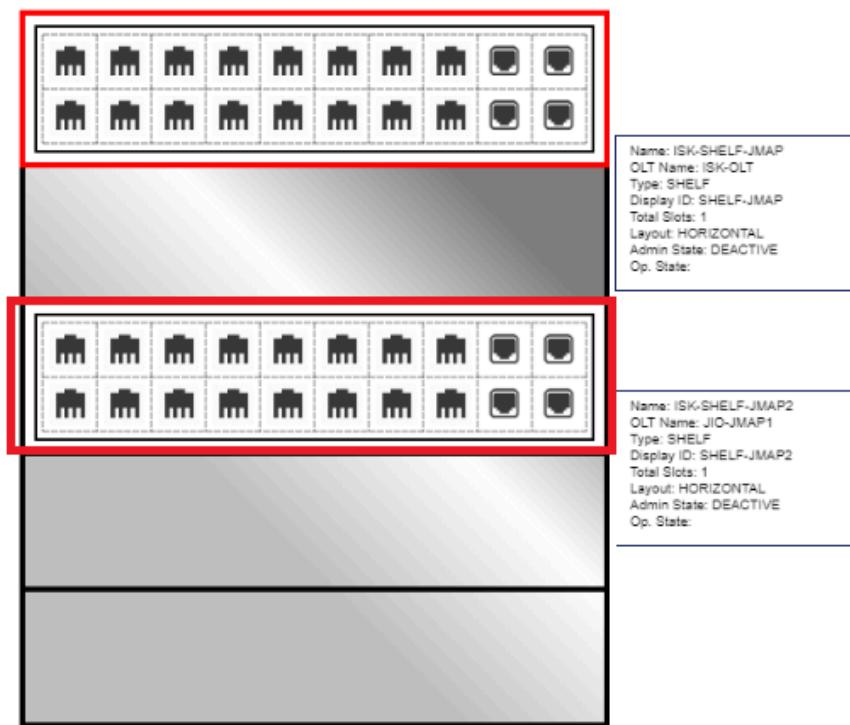
The Device Profile List page appears.

2. Click on the **RACK** tab and click **Create**.
The RACK Device Profile Configuration page appears.
3. Complete the rack device profile configuration according to the guidelines provided in the following table.

Table 245. Rack Device Profile Configuration

| Field | Description |
|-------------|--|
| Name | <p>Enter a unique name for the rack device profile. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space <p>Example: Iskratel-G16-Rack-DP</p> |
| ME Type | Specifies the managed element type. This field displays the ME type as RACK and it is not editable. Example: RACK |
| Make | Select the make for the rack from the list. If the make does not exist for rack, click the plus icon (+) to create a make configuration for the rack. See Creating Make Configuration (on page 606) . Example: Rack |
| Model | Select the model for the rack from the list. If the model does not exist for rack, click the plus icon (+) to create a model for the rack. See Creating Model Configuration (on page 610) . Example: Radisys-G16-Rack |
| Size (U) | Enter the size for the rack. |
| Total Slots | Enter the total number of slots that you want to create within the rack. Example: 2 |

The following figure shows the full rack view of size (U) 5 with two shelves assigned to the rack slot number 1 and 3, respectively.

Figure 89. Rack View

4. Click **Create**.

A new rack device profile is created for the selected device on the Device Profile List page.

Cable Profile

Cable Profile. Specifies the parameters configured for the cable device profile. The cable device profile includes the following.

- Name
- ME Type
- Make
- Model
- Row
- Column
- Creation Time
- Action

Creating Cable Profile

Prerequisites

Before you create a device profile, you must create a make and model for the cable. See [Creating Make Configuration \(on page 606\)](#) and [Creating Model Configuration \(on page 610\)](#).

Perform the following steps to create a cable profile.

1. Select **Profiles > Device Profile**.

The Device Profile List page appears.

2. Click on the **CABLE** tab and click **Create**.

The CABLE Device Profile Configuration page appears.

3. Complete the cable device profile configuration according to the guidelines provided in the following table.

Table 246. Cable Device Profile Configuration

| Field | Description |
|------------------------|---|
| Name | Enter a unique name for the cable device profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space |
| ME Type | Specifies the managed element type. This field displays the ME type as CABLE and it is not editable. Example: CABLE |
| Make | Select the make for the cable from the list. If the make does not exist for the cable, click the plus icon (+) to create a make configuration for the cable. See Creating Make Configuration (on page 606) . |
| Model | Select the model for the cable from the list. If the model does not exist for the cable, click the plus icon (+) to create a model for the cable. See Creating Model Configuration (on page 610) . |
| Layout - Total Rows | Enter the total number of rows required for the device view. |
| Layout - Total Columns | Enter the total number of columns required for the device view. |

4. Click **Create**.

A new cable device profile is created on the Device Profile List page for the selected device.



Note: When you modify the device profile, the changes do not apply to the managed elements that are already created using the profile. All new managed elements are updated with the new device profile changes.

To edit, clone, and delete the cable profile configuration, see [Common Operations \(on page 27\)](#).

Port Configuration

You can configure and view the following port configuration.

| Port Details | For more information, see |
|--------------------------------|--|
| PON and NNI Port configuration | PON and NNI Port Configuration (on page 528) |
| UNI Port configuration | UNI Port Configuration (on page 533) |

PON and NNI Port Configuration

You can configure and view the PON and NNI port for the OLT. The PON and NNI ports are configured as part of the CARD device profile.

Creating PON and NNI Port Configuration

You can configure the PON and NNI port in the CARD device profile.

Perform the following steps to configure the PON and NNI ports.

1. Select **Profiles > Device Profile**.
The Device Profile List page appears.
2. Navigate to the CARD, BNG, or CPE tab.
3. Click the **View/Create Port Details** icon from the **Ports** column.
The Port List [Device Port Profile - <Profile Name>] appears.
4. Click **Create**.

The Port Details Configuration page appears.

5. Complete the port configuration according to the guidelines provided in the following table.

Table 247. Port Detail Configuration

| Field | Description |
|-------------|---|
| Name | Enter a unique name for the port. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) The port can be either NNI or PON port. |
| Description | Enter the description about the port. |
| Port Number | Enter the port number for the device (ONT, BNG, Splitter, Card, or CPE) Example: 4 |

| Field | Description |
|--|---|
| Port Media | <p>Select the port media type from the list. The supported values are:</p> <ul style="list-style-type: none"> ◦ PON ◦ ETHERNET ◦ LTE ◦ VOICE PORT ◦ ALARM |
| | <p>If the port media type is selected as “PON”, the following fields are displayed. When you configure the port for the card and if the Port Media type is selected as PON, the “Enabled PON Encryption” and the “PON Encryption Key Interval” fields are displayed. This is applicable only for the CARD device profile.</p> |
| Enable PON Encryption | <p>Specifies PON encryption. The OLT supports the PON downstream unicast encryption. The PON encryption is enabled by default for all the PON ports and unicast services (at GEM port level) for the subscribers.</p> |
| PON Encryption Key Interval (milliseconds) | <p>Enter the PON encryption key exchange interval in milliseconds. The default value is 3600000 milliseconds (1 hour). If this field is configured as ‘0’, one-time key exchange is considered. However, for the security, always periodic key exchange is recommended.</p> |
| GPON Multicast Shaper Profile | <p>Select the multicast shaper profile. This field is applicable only for the PON port.</p> <p>This field is applicable for GPON and CPON port mode.</p> |
| XGSPON Multicast Shaper Profile | <p>Select the multicast shaper profile. This field is applicable only for the PON port.</p> <p>This field is applicable for Auto, XGSPON, and CPON port mode.</p> |
| Multicast Queue Priority | <p>Specifies the priority to be applied on the downstream multicast queue.</p> <p>The default value is 3.</p> <p>This field is applicable only for the PON port.</p> |
| Active IGMP Channels | <p>Specifies the active IGMP channels for the PON port.</p> <p>The supported value ranges from 0 to 11,648.</p> <p>The default value is 1024.</p> |
| GPON Downstream FEC | <p>Specifies whether the Forward Error Correction (FEC) is enabled in the downstream traffic for GPON port. This field is applicable for GPON and CPON port mode. The supported values are:</p> <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED |

| Field | Description |
|-----------------------|--|
| | The default value for GPON Downstream FEC is DISABLED. |
| XGSPON Downstream FEC | <p>Specifies whether the Forward Error Correction (FEC) is enabled in the downstream traffic for XGSPON port. This field is applicable for XGSPON and CPON port mode. The supported values are:</p> <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED <p>The default value for XGSPON Downstream FEC is ENABLED.</p> |
| DBA Mode | <p>Specifies the PON upstream scheduling of resources (TCONTs) for ONTs. The supported values are:</p> <ul style="list-style-type: none"> ◦ NORMAL ◦ EXTENDED <p>The default value is EXTENDED.</p> |
| Port Direction | <p>Select the port direction from the list. The supported values are:</p> <ul style="list-style-type: none"> ◦ UNI |
| Capacity | Enter the capacity of the port. Example: 1 |
| Capacity Type | <p>Select the capacity type from the list. The supported values are:</p> <ul style="list-style-type: none"> ◦ Megabit ◦ Gigabit |
| X Axis | It specifies the x-axis coordinates to show the port status in the device view. |
| Y Axis | It specifies the y-axis coordinates to show the port status in the device view. |
| Row Number | Enter the row number on which the port is positioned. This can be defined based on the total number of rows that you have configured on the CARD device profile. |
| Column Number | Enter the column number on which the port is positioned. This can be defined based on the total number of columns that you have configured on the CARD device profile. |
| Port Mode | <p>Select the port mode from the list. The supported values are:</p> <ul style="list-style-type: none"> ◦ Auto ◦ GPON ◦ XGSPON ◦ CPON <p>The default value is Auto.</p> |

| Field | Description |
|--------------------------------------|--|
| |  Note: <ul style="list-style-type: none"> ◦ If the port mode is Auto or CPON, the default value for GPON and XGSPON Downstream FEC is DISABLED and ENABLED respectively. ◦ If the port mode is GPON, the default value for GPON Downstream FEC is DISABLED. XGSPON Downstream FEC option is grayed out and cannot be selected. ◦ If the port mode is XGSPON, the default value for XGSPON Downstream FEC is ENABLED. GPON Downstream FEC option is grayed out and cannot be selected. |
| ONT Capacity | <p>Specifies the number of ONTs can be configured on the PON port based on the PON technology. The supported value ranges from 1 to 384.</p> <p>You cannot decrease the value for ONT capacity after configuration.</p> |
| GPON Alarm Profile | <p>Select the OLT port alarm profile from the list.</p> <p>This field is applicable for GPON and CPON port mode.</p> |
| XGSPON Alarm Profile | <p>Select the OLT port alarm profile from the list.</p> <p>This field is applicable for Auto, XGSPON, and CPON port mode.</p> |
| Maximum Logical Distance | <p>Specifies the maximal logical distance in kilometers between the ONU and the OLT on the PON port.</p> <p>The supported value ranges from 0 to 60.</p> <p>The default value is 20.</p> |
| Maximum Differential Reach | <p>Specifies the maximum distance in kilometers between the closest ONU to the farthest ONU from the OLT.</p> <p>The value ranges from 0 to 40.</p> <p>The default value is 20.</p> |
| SFP Alarm Profile | <p>Select the SFP alarm profile from the list.</p> |
| MTU Size | <p>Specifies the maximum transmission unit (MTU) size in bytes on the NNI port. The field is applicable for the NNI port.</p> <p>The supported value ranges from 68 to 9600 bytes.</p> <p>The default value is 9600 bytes.</p> |
| Periodic Rogue ONT Detection Control | <p>Select whether the periodic rogue ONT detection needs to be enabled. The supported values are.</p> <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED |

| Field | Description |
|---|---|
| | The default value is DISABLED. |
| Periodic Rogue ONT Detection Measurement Type | <p>Select the RSSI measurement window type. The supported values are.</p> <ul style="list-style-type: none"> ◦ SILENT-WINDOW. Detects and identifies an ONU that is responding to allocations belonging to another ONT and detects rogue ONT behavior. ◦ CUTOFF-WINDOW. Detects an ONT that stops the laser transmit later than it should, potentially interfering with the next allocation. <p>The default value is SILENT-WINDOW.</p> |
| Alloc Type to Scan | <p>Select the alloc ID type to scan. The supported values are.</p> <ul style="list-style-type: none"> ◦ UNUSED. AllocIDs that are currently not in use (not yet assigned to any ONTs). ◦ PREVIOUSLY-USED. AllocIDs that are used once and cleared. ◦ ALL. Scan both unused and previously used AllocIDs. <p>The default value is PREVIOUSLY-USED.</p> |
| Periodic Rogue ONT Detection Interval (in milliseconds) | <p>Enter the periodic rogue ONU detection procedure initiation interval in milliseconds. The value ranges from 1000 to 10000000.</p> <p>The default value is 1000.</p> |
| If the port media type is selected as “ETHERNET”, “LTE”, or “VOICE PORT”. The following fields are displayed. | |
| Port Direction | <p>Select the port direction from the list. The supported values are.</p> <ul style="list-style-type: none"> ◦ UNI ◦ NNI ◦ ANY |
| Capacity | <p>Enter the capacity of the port.</p> <p>Example: 1</p> |
| Capacity Type | <p>Select the capacity type from the list. The supported values are.</p> <ul style="list-style-type: none"> ◦ Megabit ◦ Gigabit |
| X Axis | <p>Specifies the x-axis coordinates for showing the status of the port in the device view.</p> |
| Y Axis | <p>Specifies the y-axis coordinates for showing the status of the port in the device view.</p> |
| Row Number | <p>Enter the row number on which the port is positioned. This can be defined based on the total number of rows that you have configured on the CARD device profile.</p> |

| Field | Description |
|---|--|
| Column Number | Enter the column number on which the port is positioned. This can be defined based on the total number of columns that you have configured on the CARD device profile. |
| ONT Capacity | Specifies the number of ONTs can be configured on the PON port based on the PON technology. The supported value ranges from 1 to 384. You cannot decrease the value for ONT capacity after configuration. |
| Alarm Profile | Select the OLT port alarm profile from the list. |
| If the port media type is selected as "ALARM" the following fields are displayed. | |
| Auto-negotiation | Specifies whether the auto-negotiation is enabled. |
| Capacity | Enter the capacity of the port. Example: 1 |
| Capacity Type | Select the capacity type from the list. The supported values are. <ul style="list-style-type: none"> ◦ Megabit ◦ Gigabit |
| X Axis | Specifies the x-axis coordinates for showing the status of the port in the device view. |
| Y Axis | Specifies the y-axis coordinates for showing the status of the port in the device view. |
| Row Number | Enter the row number on which the port is positioned. This can be defined based on the total number of rows that you have configured on the CARD device profile. |
| Column Number | Enter the column number on which the port is positioned. This can be defined based on the total number of columns that you have configured on the CARD device profile. |
| ONT Capacity | Specifies the number of ONTs can be configured on the PON port based on the PON technology. The supported value ranges from 1 to 384. You cannot decrease the value for ONT capacity after configuration. |

6. Click **Create**.

A new port (PON or NNI) is created on the Port List [Device Port Profile] page.

UNI Port Configuration

You can configure and view the UNI port for the ONT. The UNI port is configured as part of the ONT device profile.

Creating UNI Port Configuration

RMS adds UNI ports to CBAC as managed entities. The UNI port is added to the sub-service configuration. The UNI port number and UNI port ID coexist in the service configuration. If the UNI port number and UNI port ID are configured, then UNI port ID precedes the service configuration.

Perform the following steps to create a UNI port.

1. Select **Configuration > Profiles > Device Profile**.
The Device Profile List page appears.
2. Navigate to the ONT tab.
3. Click the **View/Create Port Details** (grid icon) under the **Ports** column on which you want to configure a UNI port.
The Port List [Device Port Profile - <ONT Name>] page appears.
4. Click **Create** and complete the UNI port configuration according to the guidelines provided in the following table.

Table 248. UNI Port Detail Configuration

| Field | Description |
|----------------|---|
| Name | Enter a unique name for the port. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">Underscore (_)Hyphen (-) |
| Description | Enter a meaningful description for the UNI port configuration. |
| Port Number | Enter the port number. Example: 4 |
| Port Direction | Select the port direction from the list. The supported value is UNI. |
| UNI Port Type | Select the UNI port type from the list. The supported values are. <ul style="list-style-type: none">VEIPPPTP-ETHERNETPPTP-POTSIP-HOSTIPv6-HOST |
| Capacity | Enter the capacity of the port. Example: 1 |
| Capacity Type | Select the capacity type from the list. The supported values are. |

| Field | Description |
|--|--|
| | <ul style="list-style-type: none"> ◦ Megabit ◦ Gigabit |
| Row Number | Enter the row number on which the port must be positioned. This can be defined based on the total number of rows that you have configured on the ONT device profile. |
| Column Number | Enter the column number on which the port must be positioned. This can be defined based on the total number of columns that you have configured on the ONT device profile. |
| MAC Limit | <p>Specifies the MAC learning depth attribute of the ME MAC bridge service profile on the ONU. This attribute specifies the maximum number of UNI MAC addresses to be learned by the bridge. The default value 0 specifies that there is no administratively imposed limit.</p> <p>The supported value ranges from 0 to 255.</p> <p>The default value is 0.</p> <p>This value can be modified when the ONT is in the deactivated state.</p> |
| When the UNI port type is selected as VEIP, the following fields are displayed. | |
| IP Host Instance | <p>Specifies the port ID string value of the IP host interface. Attaches the IP host interface with a VEIP interface.</p> <p> Note:</p> <ul style="list-style-type: none"> ◦ IP host instance must not be sent to CBAC for other UNI port type. ◦ When the UNI port type is not configured as VEIP, this attribute must be sent as nil to CBAC. ◦ CBAC sends the IP host instance attribute as nil during CLI synchronization when modified from the CLI. |
| When the UNI port type is selected as IP-HOST, the following fields are displayed. | |
| Choose Profile Type | <p>Select the profile type from the list. The supported values are.</p> <ul style="list-style-type: none"> ◦ IP Host ◦ PPPoE <p> Note: If the UNI port type is IP-HOST, the supported IP address is IPv4.</p> |

| Field | Description |
|--|--|
| When the profile type is selected as IP-Host, the following fields are displayed. | |
| Ip Address | Specifies the static IP address of the IP host interface. <ul style="list-style-type: none"> ◦ If DHCP is disabled, the ONT uses the static IP address. ◦ If DHCP is enabled, the ONT uses the dynamic IP address. |
| Ip Host Profile | Specifies the IP host profile that must be applied to the port. |
| When the profile type is selected as PPPoE, the following fields are displayed. | |
| PPPoE Profile | Select the applicable PPPoE profile from the list. |
| Service Name | Enter the service name. |
| User Name | Enter the username. |
| Password | Enter the password. |
| When the UNI port type is selected as IPv6-HOST, the following fields are displayed. | |
| Ip Address | Specifies the static IP address of the IP host interface. <ul style="list-style-type: none"> ◦ If DHCP is disabled, the ONT uses the static IP address. ◦ If DHCP is enabled, the ONT uses the dynamic IP address. |
| Ip Host Profile | Specifies the IP host profile that must be applied to the port. |

5. Click **Create**.

A new UNI port is created on the Port List [Device Port Profile] page.

Deleting UNI Port Configuration

Perform the following steps to delete a UNI port.

1. Select **Configuration > Profiles > Device Profile**.
The Device Profile List page appears.
2. Navigate to the ONT tab.
3. Click the **View/Create Port Details** (grid icon) under the **Ports** column on which you want to configure a UNI port.
The Port List [Device Port Profile - <ONT Name>] page appears.
4. Click the Delete icon under the Action column.
A confirmation message appears, indicating the status of the operation.

Authentication Profile

To access this page, click **Configuration** from the top right corner and then select **Profile > Authentication Profile** from the left-hand side of the menu.

RMS uses the Remote Authentication Dial In User Service (RADIUS) server to validate users who attempt to access the RMSapplication. RADIUS is a networking protocol that provides centralized authentication and authorization for user accounts.

You can configure a RADIUS server to authenticate and authorize users to log into RMS. When a user enters a username and password for login, RMS sends the username and password to the RADIUS server for login information verification and authentication.

If authentication is successful, the user can log in. The user is denied access if authentication is unsuccessful due to invalid credentials.

The RADIUS server authentication might return a reject response for the following reasons.

- The user accounts accessing RMS may not be configured on the RADIUS server.
- The user enters incorrect login credentials.

Creating Authentication Profile

Perform the following steps to create an authentication profile.

1. Select **Profiles > Authentication Profile > Create**.
The Authentication Profile Configuration page appears.
2. Complete the authentication profile configuration according to the guidelines provided in the following table.

Table 249. Authentication Profile Configuration

| Field | Description |
|--|---|
| Name | Enter a unique name for the authentication profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Type | Select the type of authentication profile from the list. The supported authentication methods are. <ul style="list-style-type: none">◦ RADIUS. Select RADIUS for specifying the radius server details for the authentication profile. This is used to authenticate the OLT security configuration by CBAC. |
| When the type is selected as RADIUS, the following fields are displayed. | |

| Field | Description |
|------------|--|
| Host Name | Enter a valid IP address for the RADIUS server. |
| Port | Enter the port number of the RADIUS server, which is exposed for accessing the server-client communication. The default value is 1812. |
| Secret Key | Enter the secret key, which is used to encrypt the password. |

3. Click **Create**.

A new authentication profile is created on the Authentication Profile List page.



Note: You cannot delete a RADIUS profile if the profile is associated with an active managed element. To delete a RADIUS profile, you must first dissociate the RADIUS profile from the managed element.

To edit, clone, and delete the Authentication profile configuration, see [Common Operations \(on page 27\)](#).

ACL Profile

To access this page, click **Configuration** from the top right corner and then select **Profile > ACL Profile** from the left-hand side of the menu.

RMS supports Access Control List (ACL) profiles, which include the configurations to add packet filtering through a set of specified ports in the OLT. ACL profiles are supported in RMS to ease the ACL configurations across OLT.

You can create ACL profiles for management and data path traffic. ACL is a set of Access Control Entries (ACEs) applied to the NNI and management interfaces. The packets are filtered based on the ACEs, and statistics are created for the number of packets matching each ACE.

ACL is applied on the interfaces while ACE defines the packet filtering criteria such as Match and Result/Action.

OLT implements ACLs on the management interface to prevent intrusion and DDoS attacks to provide a secure environment and proper functioning of the OLT. ACLs support preventing attacks from IP and MAC addresses outside the permitted devices. ACLs also support accepting requests from only the known IP and MAC addresses.

You can configure more than one ACL on the interface (physical LAG or management).

Management ACL defines access control policies to control management traffic. The management ACL configuration limits or allows traffic from a particular trusted network.

Creating ACL Profile

Perform the following steps to create an ACL profile.

1. Select **Profile > ACL Profile > Create**.
The ACL Profile Configuration page appears.
2. Complete the ACL profile configuration according to the guidelines provided in the following table.

Table 250. ACL Profile Configuration

| Field | Description |
|----------------|--|
| Name | Enter a unique name for the ACL profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Type | Specifies the type of ACE entries in the ACL profile. The supported types are. <ul style="list-style-type: none"> ◦ MAC ◦ IPv4 ◦ IPv6 ◦ MAC-IPv4 ◦ MAC-IPv6 ◦ MAC-IPv4-IPv6 |
| Management ACL | Specifies whether the ACL profile is a management ACL or a data path ACL. The supported values are. <ul style="list-style-type: none"> ◦ True. Specifies the management ACL, which is applied on the managed element level. ◦ False. Specifies the data path ACL, which is applied on the specified port (NNI or LAG). The default value is false. |
| Add ACE | You can create one or more ACEs for each ACL profile type. See Creating ACE Configuration (on page 540) . |

**Note:**

- Never deny or exclude the gateway IP of the OLT from the allowed list in the Management ACL. It can result in disconnection between the servers (NTP, SFTP, REPO, LOG, and RMS), and the OLT cannot be accessed remotely.
- In case of connection loss.
 - Connect to the OLT console or out-of-band and remove the ACL using the CLI command.
 - Recheck the OLT connectivity and perform reconciliation to remove the ACL configuration from RMS.

3. Click **Create**.

A new ACL profile is created on the ACL Profile List page.

ACE Configuration

An Access Control Entry (ACE) contains match criteria, action, and result (permit or deny) for the egress and ingress packets.

There are two possible actions for an ACE rule: allow and deny.

- If an ACE with 'allow' condition matches, the packet is allowed for further processing and the actions specified in the ACE are executed.
- If an ACE with 'deny' condition matches, the packet is dropped.

Creating ACE Configuration

Perform the following steps to create one or more ACEs.

1. Select **Profiles > ACL Profile > Create**.
The ACL Profile Configuration page appears.
2. Click **Add ACE**.
3. Complete the ACE configuration according to the guidelines provided in the following table.

Table 251. ACE Configuration

| Field | Description |
|-------|--|
| Name | Enter a unique name for ACE. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Type | Select the type of ACE configuration. This defines the packet fields used for the match criteria. The supported types are. <ul style="list-style-type: none">◦ MAC◦ IPv4◦ IPv6◦ MAC-IPv4◦ MAC-IPv6 <p> Note:</p> <ul style="list-style-type: none">◦ You can add the MAC ACE configuration when the ACL profile type is selected as “MAC”.◦ You can add the IPv4 ACE configuration when the ACL profile type is selected as “IPv4”. |

| Field | Description |
|---|---|
| |  <ul style="list-style-type: none"> ◦ You can add the MAC ACE configuration when the ACL profile type is selected as “IPv6”. ◦ You can add the MAC, IPv4, and MAC-IPv4 ACE configuration when the ACL profile type is selected as “MAC-IPv4”. ◦ You can add the MAC, IPv6, and MAC-IPv6 ACE configuration when the ACL profile type is selected as “MAC-IPv6”. ◦ You can add the MAC, IPv4, IPv6, MAC IPv4, and MAC-IPv6 ACE configuration when the ACL profile type is selected as “MAC-IPv4-IPv6”. |
| If the type is selected as “MAC”, the following fields are displayed. | |
| ACE MAC Configuration | |
| Priority | <p>Specifies the priority of an ACE within the ACL profile. The value ranges from 0 to 31.</p> <ul style="list-style-type: none"> ◦ Management ACL. A lower number indicates higher priority. The value 0 indicates the highest priority, and the value 31 indicates the least priority. ◦ Data Path ACL. A higher number indicates higher priority. The value 0 indicates the least priority, and the value 31 indicates the highest priority. <p>The default value is 31.</p> |
| Destination MAC | <p>Specifies the destination MAC address. The length is 6 bytes.</p> <p>Example: 0b:0a:95:9d:68:16</p> |
| Destination MAC Mask | <p>Enter the mask for the destination MAC address. The length is 6 bytes. The mask defines the bits in the MAC address that must be used, and the bits in the MAC address must be wild carded.</p> |
| Source MAC | <p>Enter the source MAC address. The length is 6 bytes.</p> <p>Example: e0:0c:12:d1:86:15</p> |
| Source MAC Mask | <p>Enter the mask for the source MAC address. The length is 6 bytes. The mask defines the bits in the MAC address that must be used, and the bits in the MAC address must be wild carded.</p> |
| Ether Type | <p>Enter the ether type. The length is 2 bytes. The supported values are.</p> <ul style="list-style-type: none"> ◦ 0x0800 ◦ 0x86DD ◦ 0x0806 |

| Field | Description |
|--|---|
| | <ul style="list-style-type: none"> ◦ 0x8863 ◦ 0x8864 |
| S vlan id | <p>Enter the service VLAN ID. The length is 12 bits. The value ranges from 2 to 4094. Example: 126</p> <p> Note: The values 2 and 4094 are reserved.</p> |
| C vlan id | <p>Enter the customer VLAN ID. The length is 12 bits. The value ranges from 2 to 4094. Example: 321</p> <p> Note: The values 2 and 4094 are reserved.</p> |
| S PCP | <p>Enter the service VLAN Priority Code Point (PCP) value. The length is 3 bits. The value ranges from 0 to 7. Example: 2</p> |
| C PCP | <p>Enter the customer VLAN PCP value. The length is 3 bits. The value ranges from 0 to 7. Example: 4</p> |
| Result | <p>Select whether to allow or deny the packet.</p> <ul style="list-style-type: none"> ◦ ALLOW. Accepts the packet for further processing. ◦ DENY. Discards the packet. |
| Alarm Profile | Select the ACE alarm profile associated with the ACE entry. |
| If the type is selected as IPv4 , the following fields are displayed. | |
| Priority | <p>Specifies the priority of an ACE within the ACL profile. The value ranges from 0 to 31.</p> <ul style="list-style-type: none"> ◦ Management ACL. A lower number indicates higher priority. The value 0 indicates the highest priority, and the value 31 indicates the least priority. ◦ Data Path ACL. A higher number indicates higher priority. The value 0 indicates the least priority, and the value 31 indicates the highest priority. <p>The default value is 31.</p> |

| Field | Description |
|-------------------------|--|
| |  Note: Multiple ACEs within the same ACL cannot have the same priority. |
| Source IP | Enter the source IP address. The length is 4 bytes. A standard valid IP address range is supported. Example: 1.1.1.1  Note: You can enter the IPv4 address based the ACE type that you have selected. |
| Source Subnet Mask | Enter the subnet mask for the source address. The value ranges from 0 to 128. |
| Destination IP | Enter the destination IP address. The length is 4 bytes. Standard valid IP address range is supported. Example: 2.2.2.2  Note: You can enter the IPv4 address based the ACE type that you have selected. |
| Destination Subnet Mask | Enter the subnet mask for the destination address. The value ranges from 0 to 128. |
| Flag DF | Enter the Do not Fragment (DF) flag. The length is 1 bit. The supported values are 0 and 1. Example: 1 |
| Flag MF | Enter the More Fragments (MF) flag. The length is 1 bit. The supported values are 0 and 1. Example: 0 |
| Protocol | Enter the transport protocol field of the IP header. The length is 1 byte. The supported values are. <ul style="list-style-type: none"> ◦ TCP ◦ UDP ◦ ICMP |
| DSCP | Enter the DSCP field of the IP header. The length is 6 bits. The value ranges from 0 to 63. Example: 1 |
| Source Port | Enter the source port of the IP header. The length is 2 bytes. |

| Field | Description |
|--|--|
| | <p>The value ranges from 0 to 65,535. Example: 1234</p> |
| Destination Port | <p>Enter the destination port of the IP header. The length is 2 bytes. The value ranges from 0 to 65,535. Example: 2048</p> |
| Result | <p>Select whether to allow or deny the packet.</p> <ul style="list-style-type: none"> ◦ ALLOW. Accepts the packet for further processing. ◦ DENY. Discards the packet. |
| Alarm Profile | Select the ACE alarm profile from the list. |
| <p>If the type is selected as IPv6, the following fields are displayed.</p> | |
| Priority | <p>Specifies the priority of an ACE within the ACL profile. The value ranges from 0 to 31.</p> <ul style="list-style-type: none"> ◦ Management ACL. A lower number indicates higher priority. The value 0 indicates the highest priority, and the value 31 indicates the least priority. ◦ Data Path ACL. A higher number indicates higher priority. The value 0 indicates the least priority, and the value 31 indicates the highest priority. <p>The default value is 31.</p> <p> Note: Multiple ACEs within the same ACL cannot have the same priority.</p> |
| Source IP | <p>Enter the source IP address. The length is 4 bytes. A standard valid IP address range is supported. Example: 1.1.1.1</p> <p> Note: You can enter the IPv6 address based the ACE type that you have selected.</p> |
| Source Subnet Mask | Enter the subnet mask for the source address. The value ranges from 0 to 128. |
| Destination IP | Enter the destination IP address. The length is 4 bytes. Standard valid IP address range is supported. Example: 2.2.2.2 |

| Field | Description |
|-------------------------|---|
| |  Note: You can enter the IPv6 address based the ACE type that you have selected. |
| Destination Subnet Mask | Enter the subnet mask for the destination address. The value ranges from 0 to 128. |
| Next Header | Specifies the type of extension header immediately following the IPv6 header. It indicates the protocols contained within the upper-layer packet such as TCP and UDP. |
| Traffic Classifier | Specifies the IPv6 DSCP value, which is the first six bits in the 8-bit traffic class field of the IPv6 header. |
| Source Port | Enter the source port of the IP header. The length is 2 bytes. The value ranges from 0 to 65,535. Example: 1234 |
| Destination Port | Enter the destination port of the IP header. The length is 2 bytes. The value ranges from 0 to 65,535. Example: 2048 |
| Result | Select whether to allow or deny the packet. <ul style="list-style-type: none"> ◦ ALLOW. Accepts the packet for further processing. ◦ DENY. Discards the packet. |
| Alarm Profile | Select the ACE alarm profile from the list. |

Deleting ACL Profile



Note: You cannot delete the ACL profile, if it is associated with the subscriber service.

You can delete an ACL profile configuration.

Perform the following steps to delete an ACL profile.

1. Select **Profiles > ACL Profile**.
The ACL Profile List page appears.
2. Select the **Delete** icon from the **Action** column.
An alert message appears, asking you to confirm the delete operation.
3. Click **Confirm** to delete the ACL profile.
A confirmation message appears, indicating the status of the delete operation.

ERPS Profile

To access this page, click **Configuration** from the top right corner and then select **Profile > ERPS Profile** from the left-hand side of the menu.

Ethernet Ring Protection Switching (ERPS) is a protection switching mechanism for Ethernet networks. It uses the G.8032 defined Ring Automatic Protection Switching (R-APS) protocol to protect Ethernet traffic in a ring topology.

The Ethernet ring consists of multiple Ethernet ring nodes. Each Ethernet ring node is connected to adjacent nodes using two independent ring links. ERPS uses a specific link to protect the entire ethernet ring, and the link is called Ring Protection Link (RPL).

Each Ethernet ring must contain at least two Ethernet ring nodes.

ERPS profiles allow ease of configuration and reduce the effort of repeating the same configuration across ERPS rings. You can create an ERPS profile and apply it on multiple nodes to repeat the common configurations across different rings.

Creating ERPS Profile

Perform the following steps to create an ERPS profile.

1. Select **Profiles > ERPS Profile > Create**.
The ERPS Profile Configuration page appears.
2. Complete the ERPS profile configuration according to the guidelines provided in the following table.

Table 252. ERPS Profile Configuration

| Field | Description |
|----------------|---|
| Name | Enter a unique name for the ERPS profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Control VLAN | Enter the ERPS profile control VLAN. The value ranges from 2 to 4094. |
| Data VLAN List | Enter the ERPS profile data VLAN list. The value ranges from 2 to 4094. |
| Mode | Specifies the mode of the ERPS ring protection. The supported values are. <ul style="list-style-type: none">◦ REVERTIVE◦ NON-REVERTIVE |
| East Port Role | Enter the ERPS east port role. The supported values are. |

| Field | Description |
|-----------------------------|--|
| | <ul style="list-style-type: none"> ◦ Ring Protection Link (RPL) ◦ NORMAL ◦ NEIGHBOUR ◦ NEXT-NEIGHBOUR |
| West Port Role | <p>Enter the ERPS west port role. The supported values are.</p> <ul style="list-style-type: none"> ◦ RPL ◦ NORMAL ◦ NEIGHBOUR ◦ NEXT-NEIGHBOUR |
| Guard Timer (ms) | <p>Enter the ERPS guard timer value in milliseconds. All the Ethernet ring nodes uses this time while changing the state. This timer blocks the latent outdated messages from causing unnecessary state changes. The value ranges from 10 ms to 2000 ms. The default value is 500 ms.</p> |
| Wait-to-Restore Timer (min) | <p>Enter the ERPS restore timer value in minutes.</p> <ul style="list-style-type: none"> ◦ After a signal failure, this timer verifies that the signal failure is not intermittent. ◦ After a forced switch or manual switch, this timer verifies that no background condition exists. <p>The value ranges from 1 to 12 minutes. The default value is 5 minutes.</p> |
| Hold off Times (ms) | <p>Enter the ERPS hold off timer value. This timer is used by the underlying Ethernet layer to filter out intermittent link faults. The value ranges from 0 to 10000 ms. The default value is 0 ms.</p> |
| Wait-to-Block Timer (ms) | <p>Enter the ERPS wait to block timer value. The default value is 5500 ms. The value ranges from 0 to 86400000 ms.</p> |
| R-APS Intervals (ms) | <p>Enter the ERPS R-APS interval value. The default value is 5000 ms. The value ranges from 10 to 3600000 ms.</p> |

3. Click **Create**.

A new ERPS profile is created on the ERPS Profile List page.

To edit, clone, and delete the ERPS profile configuration, see [Common Operations \(on page 27\)](#).

IP Host Profile

To access this page, click **Configuration** from the top right corner and then select **Profile > IP Host Profile** from the left-hand side of the menu.

The IP host profile contains attributes that enable the operator to assign the management IP address to the ONT on a virtual interface. This interface provides IP connectivity to voice service using POTS.

Field Descriptions

The following table describes the fields on the IP Host Profile page.

Table 253. IP Host Profile List

| Field | Description |
|---------------------|--|
| Name | Specifies the name of the IP host profile. |
| Type | Specifies the type of the IP host profile. |
| Enable DHCP | Specifies whether to enable DHCP. |
| Network Mask | Specifies the network mask of static IP address of the IP host interface. |
| Gateway | Specifies the gateway static IP address of the IP host interface. |
| Primary DNS | Specifies the primary DNS static IP address of the IP host interface. |
| Secondary DNS | Specifies the secondary DNS static IP address of the IP host interface. |
| ONT Identifier | Specifies the ONT identifier. |
| Relay Agent Options | Specifies one or more DHCP relay agent options. |
| IPv6 Options | Specifies whether to enable DHCPv6 and router solicitation. |
| Default Router | Specifies the default router IPv6 address of the IPv6 host interface. |
| On Link Prefix | Specifies the IPv6 prefix. |
| Creation Time | Specifies the date and time when the IP host profile was created. |
| Action | Specifies the action that you can perform on the IP host profile. The supported actions are. <ul style="list-style-type: none">• Edit• Clone• Delete |

Creating IP Host Profile

Perform the following steps to create an IP host profile.

1. Select **Profile > IP Host Profile > Create**.
The IP Host Profile Configuration page appears.
2. Complete the IP host profile configuration according to the guidelines provided in the following table.

Table 254. IP Host Profile Configuration

| Field | Description |
|----------------|--|
| Name | Enter a unique name for the IP host profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Type | Specifies the type of the IP host profile. Example: IPv4 or IPv6. |
| Enable DHCP | Specifies whether to enable DHCP. <ul style="list-style-type: none">◦ If this option is enabled, the IP interface of the ONT is learned dynamically.◦ If this option is disabled, the following options must be configured.<ul style="list-style-type: none">▪ Network Mask▪ Gateway |
| Network Mask | Enter the network mask static IP address of the IP host interface. This is mandatory if the Enable DHCP field is disabled. Example: 255.255.255.0 |
| Gateway | Enter the gateway static IP address of the IP host interface. This is mandatory if the Enable DHCP field is disabled. Example: 172.27.172.254 |
| Primary DNS | Enter the primary DNS static IP address of the IP host interface. This is applicable on the ONT, if the DHCP is disabled. Example: 172.27.173.101 |
| Secondary DNS | Enter the secondary DNS static IP address of the IP host interface. This is applicable on the ONT, if the DHCP is disabled. Example: 172.27.173.102 |
| ONU Identifier | Enter the ONU identifier, which is used (instead of MAC address) to retrieve the DHCP parameters. |

| Field | Description |
|---------------------|---|
| | The maximum length is 25 characters. Example: voice-service |
| Relay Agent Options | Enter one or more DHCP relay agent options. |
| IPv6 Options | <p>Specifies whether to enable DHCPv6 and router solicitation. The supported values are.</p> <ul style="list-style-type: none"> ◦ DHCPv6 ◦ Router-Solicitation ◦ DHCPv6andRouterSolicitation ◦ Disable <p>When it is configured as Disable, the IPv6 address from Add IPv6-Host interface API and all the following parameters must be configured.</p> <ul style="list-style-type: none"> ◦ default_router ◦ primary_dns ◦ secondary_dns ◦ on_link_prefix |
| Default Router | Specifies the default router IPv6 address of the IPv6 host interface. This is mandatory if the IPv6 Options parameter is disabled. |
| On Link Prefix | <p>Specifies the IPv6 prefix. The prefix must be in <i>prefixstring:/prefixlength</i> format, where, the prefix string is 16 bytes and prefix length is 1 byte.</p> <p>This is mandatory if the IPv6 Options parameter is disabled.</p> |

3. Click **Create**.

A new IP host profile is created on the IP Host Profile List page.

To edit, clone, and delete the IP host profile configuration, see [Common Operations \(on page 27\)](#).

MEP Profile

To access this page, click **Configuration** from the top right corner and then select **Profile > MEP Profile** from the left-hand side of the menu.

Create a Maintenance End Point (MEP) profile, add the profile to the MEP instance, and associate the MEP instance to the OLT.

Creating MEP Profile

Perform the following steps to create a MEP profile.

1. Select **Profiles > MEP Profile > Create**.
The MEP Profile Configuration page appears.
2. Complete the MEP profile configuration according to the guidelines provided in the following table.

Table 255. MEP Profile Configuration

| Field | Description |
|-----------------------|---|
| Name | <p>Enter a unique name for the MEP profile. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Association Name Type | <p>Specifies the maintenance association name type. The supported types are.</p> <ul style="list-style-type: none"> ◦ Character-string ◦ Unsigned-integer |
| Association Name | <p>Specifies the maintenance association name.</p> <ul style="list-style-type: none"> ◦ If the association name type is selected as 'character-string', then the association name type must be alphabets or alphanumeric string. The name length must be 1 to 45 characters. <p>The following special characters are supported.</p> <ul style="list-style-type: none"> ▪ Exclamation Mark (!) ▪ At Sign (@) ▪ Hash or Pound (#) ▪ Dollar (\$) ▪ Percentage (%) ▪ Caret (^) ▪ Ampersand (&) ▪ Asterisk (*) ▪ Hyphen (-) ▪ Underscore (_) ▪ Vertical Bar or Pipe () ▪ Forward Slash (/) ▪ Period or Dot (.) ▪ Comma (,) ▪ Colon (:) ▪ Semicolon (;) |

| Field | Description |
|-------------------|---|
| | <ul style="list-style-type: none"> ▪ Double Quote ("") ▪ Single Quote ('') ◦ If the association name type is selected as 'unsigned-integer', then the association name type must be Uint16. The value ranges from 0 to 65,535. |
| CCM Interval Unit | <p>Specifies the unit for CCMs interval. The supported values are.</p> <ul style="list-style-type: none"> ◦ Milliseconds ◦ Seconds ◦ Minutes <p>The default value is seconds.</p> |
| CCM Interval | <p>Specifies the interval at which CCMs are sent. The supported values are.</p> <ul style="list-style-type: none"> ◦ 3.3, 10, and 100 (If the ccm interval unit is in milliseconds) ◦ 1 and 10 (If the ccm interval unit is in seconds) ◦ 1 and 10 (If the ccm interval unit is in minutes) <p>The default value is 1.</p> |
| Remote MEP ID | <p>Specifies the remote MEP ID.</p> <p>The value ranges from 1 to 8191.</p> |
| Local MEP ID | <p>Specifies the local MEP ID.</p> <p>The value ranges from 1 to 8191.</p> |
| Control VLAN | <p>Specifies the control VLAN ID of the MEP.</p> <p>The value ranges from 2 to 4094.</p> |
| MD Level | <p>Specifies the maintenance domain level.</p> <p>The value ranges from 0 to 7.</p> <p>The default value is 7.</p> |

3. Click **Create**.

A new MEP profile is created on the MEP Profile List page.



Note: You cannot delete the MEP profile if it is associated with any OLT.

To edit, clone, and delete the MEP profile configuration, see [Common Operations \(on page 27\)](#).

NTP Profile

To access this page, click **Configuration** from the top right corner and then select **Profile > NTP Profile** from the left-hand side of the menu.

The Network Time Protocol (NTP) profile is a global configuration and must be attached to the OLT profile. You can attach the NTP profile during the "Add OLT" or "Update OLT" operation. You can also update the NTP profile already attached to some OLTs.

The NTP client in OLT consumes the configuration and runs the NTP protocol to synchronize its clock status based on the time reported by the peer NTP servers.

The NTP Server details (NTP profile) are configurable. The operator can also specify the preference for the NTP server, which is used when multiple NTP servers report almost simultaneously. The NTP servers must be IPv4, IPv6, or FQDN.

RMS allows you to configure a maximum of five NTP servers and a minimum of one NTP server for each NTP profile.

- The OLT reports the "NTP Server Not reachable" alarm if the configured server is not reachable for the last eight poll intervals.
- The OLT should report an "NTP Clock Out of Sync" alarm if the configured servers are not reachable for the last 15 minutes.

During the OLT provisioning, the operator needs to manually enter the server details in *ntp-client.conf* and restart the NTP service.

Creating NTP Profile

Perform the following steps to create a NTP profile.

1. Select **Profiles > NTP Profile > Create**.
The NTP Profile Configuration page appears.
2. Complete the NTP profile configuration according to the guidelines provided in the following table.

Table 256. NTP Profile Configuration

| Field | Description |
|--------|--|
| Name | Enter a unique name for the NTP profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Server | |

| Field | Description |
|-----------|--|
| Host | Specifies the IP address (IPv4 or IPv6) of the NTP server or FQDN of the NTP server. |
| Preferred | Specifies if the NTP server host is the preferred server in the NTP server pool. This host must be chosen for synchronization among a set of correctly operating hosts. |

3. Click **Create**.

A new NTP profile is created on the NTP Profile page.



Note: You cannot delete the NTP profile if it is associated with any OLT.

To edit, clone, and delete the NTP profile configuration, see [Common Operations \(on page 27\)](#).

Circuit ID Format

To access this page, click **Configuration** from the top right corner and select **Profiles > Circuit ID Format** from the left-hand side of the menu.

RMS supports the configuration of circuit ID for each sub-service.



Note: Circuit ID is assumed to be constructed as per the specified circuit ID format. It is highly recommended to test the constructed circuit ID from the format before deployment. There is no validation on the circuit ID as different operators may have their own recommended way of constructing the circuit ID.

Creating Circuit ID Format

Perform the following steps to create a circuit ID format.

1. Select **Profiles > Circuit ID Format > Create**.
The Circuit ID Format Configuration appears.
2. Complete the configuration according to the guidelines provided in the following table.

Table 257. Circuit ID Format Configuration

| Field | Description |
|-------|---|
| Name | Enter a unique name for the circuit ID. You can use any number of alphanumeric characters. Only the following special characters are supported. |

| Field | Description |
|-------|--|
| | <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) ◦ Space. |

| Field | Description |
|-------|--|
| | <ul style="list-style-type: none"> ◦ Circuit ID format. <p>gw,{{subscriber_display_id}} {{olt_name}} ge {{ont_id}}/{{ont_slot_no}}/{{ont_port_no}}@{{shelf_no}}/{{slot_no}}/{{port_no}}.xgsp</p> <p>Constructed circuit ID. For example: gw,STI-0689090-7 olt1.prodtest ge 8/1/1@1/2/1.xgsp</p> <p>Where,</p> <ul style="list-style-type: none"> ◦ Circuit ID format. {{olt_name}}#rack={{rack_no}}/shelf={{shelf_no}} / port={{port_no}}/{{ont_id}} <p>Constructed circuit ID. olt1#rack=1/shelf=1 /port=01/1</p> <ul style="list-style-type: none"> ◦ Circuit ID format. OLT_Name={{olt_name}}#Rack_No={{rack_no}}/Shelf_No={{shelf_no}}/Slot_No={{slot_no}}/P ON_Port_No={{port_no}}/ONT_No={{ont_id}}/ONT_Card_No={{ont_card}}/UNI_Port_No={{ont_port_no}} <p>Constructed circuit ID.</p> <p>OLT_Name=olt235#Rack_No=1/Shelf_No=1/Slot_No=01/PON_Port_No=24/ONT_No=10/ONT_Card_No=1/UNI_Port_No=1</p> <ul style="list-style-type: none"> ◦ olt_name. Specifies the OLT assigned on the ONT. ◦ subscriber_name. Specifies the name of the subscriber. ◦ subscriber_display_id. Specifies the display ID of the subscriber. ◦ rack_no. Specifies the rack number. ◦ shelf_no. Specifies the shelf number. ◦ slot_no. Specifies the slot number. ◦ ont. The ont number generated by the RMS. ◦ shelf. The OLT shelf in our case it is always 1. ◦ slot. The OLT slot in our case it is always 1. ◦ port. The PON port number. ◦ port_no. Specifies the PON port number of the OLT port. ◦ ont_id. Specifies the ONT number. This is auto generated once you create the ONT configuration. Click the Edit button on the corresponding ONT to view the ONT ID. For more information, see Common Operations (on page 27). ◦ ont_card. slot_no present in the ONT object, which is captured from the ONT device profile. |

| Field | Description |
|-------|---|
| | <ul style="list-style-type: none"> ◦ ont_port_no. Specifies the ONT port number and this is available on the service once the UNI port definition is available. ◦ ont_slot_no. Specifies the ONT slot number. ◦ UNI_Port_No. Specifies the UNI port number. <p> Note: You must specify the values for all the variables to create a valid constructed circuit ID.</p> |

3. Click **Create**.

A new circuit ID is created on the Circuit ID Format List page.

To edit, clone, and delete the Circuit ID format configuration, see [Common Operations \(on page 27\)](#).

Remote ID Profile

To access this page, click **Configuration** from the top right corner and select **Profiles > Remote ID Profile** from the left-hand side of the menu.

RMS allows you to create a remote ID template in the remote ID profile, which can then be attached to the service or VNet profile.

- If the remote ID profile is attached to the VNet profile, then the generation of remote ID is automated for all the services referred to the VNet profile.
- If the remote ID profile is attached to the service, it takes precedence over the VNet profile (if configured), and the remote ID is generated only for this service.

The remote ID profile can be configured in the following ways.

- Configured as a local profile specific to the OLT from the CBAC CLI
- Configured as global profile for all the OLTs or local profile specific to OLT from the RMS GUI



Note:

- An update of the remote ID is not supported. A user can either create a new remote ID profile and attach it to the service or create a new VNet profile using this remote ID profile and attach the new VNet profile to the service.
- Global VNet profile cannot refer to local remote ID profile.
- MAC address cannot be combined with any other template or string, and this is to maintain the backward compatibility with the Remote ID type **MAC_ADDRESS**.
- A user can configure the Enterprise number in (**Configuration > OLT**), which can be added to the DHCPv6 Remote ID option.
- For the WHDVR use case, the first added port adds the **ont_port_no**.

Creating Remote ID Profile

Perform the following steps to create a remote ID profile.

1. Select **Profiles > Remote ID Profile > Create.**

The Remote ID Profile Configuration appears.

2. Complete the configuration according to the guidelines provided in the following table.

Table 258. Remote ID Profile Configuration

| Field | Description |
|----------|--|
| Name | <p>Enter a unique name for the remote ID profile. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Template | <p>Enter the template for the remote ID profile.</p> <p>The following variables are supported to create a remote ID template.</p> <ul style="list-style-type: none">◦ {{olt_name}}◦ User_String◦ {{olt_name}}-User_String◦ {{olt_name}}-{{port_no}}-{{ont_name}}-{{ont_port_type}}-{{ont_port_no}}◦ {{olt_name}}-{{port_no}}-{{ont_name}}◦ {{olt_name}}-User_string-{{ont_name}}◦ {{olt_name}}-{{ont_serial_no}}◦ {{mac_address}} <p>Example template; RLT-{{olt_name}}/{{port_no}}/{{ont_name}}-{{ont_port_type}}-{{ont_port_no}}</p> <p> Note: Do not use curly braces in plain user string data.</p> |

3. Click **Create**.

A new remote ID profile is created on the Remote ID Profile List page.

TACACS Profile

To access this page, click **Configuration** from the top right corner and then select **Profile > TACACS Profile** from the left-hand side of the menu.

The Terminal Access Controller Access Control System (TACACS) is a networking protocol that enables the Authentication, Authorization, and Accounting (AAA) of users attempting to gain access to the OLT, RMS VMs, log server VMs, NTP server VMs, SFTP server VMs, repository server VMs, RMS application, and CBAC. TACACS is a remote authentication and authorization mechanism. A TACACS client (OLT, RMS application, and CBAC) authenticates the users with the configured TACACS server and authorizes all operations against the role configured in the TACACS server.

The TACACS profile defines the details of the TACACS servers such as IP, Port, and the Secret key. When the TACACS server is not reachable, then the authentication and authorization fall back to the local authentication.



Note:

- TACACS can be configured on the OLT, even if it is not enabled on the RMS application or CBAC.
- Only a user with an admin role can configure RMS authentication settings.
- RMS allows only one TACACS server to be configured for the RMS application and the TACACS profile.
- An alarm is raised in RMS when a TACACS server from the CBAC or OLT is unreachable.
- The alarm is reported in the **RMS > Faults** page if the TACACS-SERVER-CONNECTIVITY-LOST alarm is triggered from CBAC when the TACACS server connectivity is lost.
- Single sign-on for CBAC CLI is not supported for users authenticated through TACACS.
- For proper RMS and CBAC functionalities, TACACS+ authentication must be enabled on RMS and all the CBACs. Both RMS and CBAC must communicate with the same TACACS+ server. If different TACACS+ servers are configured for RMS and CBAC, they must have the same user configuration.
- If TACACS+ is disabled on RMS, ensure it is disabled across all CBACs managed by RMS
- The super admin user (admin or pajmapuser) is always authenticated locally, even if TACACS+ is enabled on RMS
- RMS security settings is only applicable to local users and not to users authenticated through TACACS+ server.
- If RMS cannot reach the TACACS+ server for authentication, it authenticates the user locally.

Creating TACACS Profile

Perform the following steps to create a TACACS profile.

1. Select **Profiles > TACACS Profile > Create**.

The TACACS Profile Configuration page appears.

2. Complete the TACACS profile configuration according to the guidelines provided in the following table.

Table 259. TACACS Profile Configuration

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the TACACS security profile. You can use 128 alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Enable Accounting | Specifies whether TACACS accounting on RMS is enabled or disabled. Enable this option to push the CBAC accounting (audit) logs to the configured TACACS hosts. This option is disabled by default. |
| Servers | |
| Host | Specifies the IP address or Fully Qualified Domain Name (FQDN) of the TACACS server. |
| Port | Specifies the port number of the TACACS server, which is exposed to access the server-client communication. The default value is 49. The supported value ranges from 0 to 65,535. |
| Secret key | Specifies the secret key, which is used to encrypt the payload. The maximum length of the secret key must not exceed 64 characters. |

3. Click **Create**.

A new TACACS profile is created on the TACACS Profile page.

To edit, clone, and delete the TACACS profile configuration, see [Common Operations \(on page 27\)](#).

Alarm Soak Profile

To access this page, click **Configuration** from the top right corner of the page and then select **Profile > Alarm Soak Profile** from the left-hand side of the menu.

An alarm soak allows the system to not report alarms to the operator if they are raised and cleared within the defined time limit.

In CBAC, all management component managers send the alarm to telemetry after performing alarm correlation. Once soaking is done based on the alarm condition, the alarm is reported to RMS.

The following is the usage of alarm soaking at OLT.

1. It helps not to report false alarms due to intermittent failure and report the correct alarm to RMS.
2. Reduces reporting of unwanted alarms that get raised and cleared immediately.
3. Helps OSS auto ticketing system to raise tickets only for the valid alarms.

The alarm soaking is done at the OLT based on the following configurable parameters.

- **Alarm Raise Soak Time.** If the alarm is raised and stays for at least this time, the alarm indication is sent to RMS.
- **Alarm Clear Soak Time.** After the alarm is raised, if it is cleared and stays cleared for at least this time, the alarm indication is sent to RMS.

Creating Alarm Soak Profile

Perform the following steps to create an alarm soak profile.

1. Select **Profiles > Alarm Soak Profile > Create.**
The Alarm Soak Profile Configuration page appears.
2. Complete the alarm soak profile configuration according to the guidelines provided in the following table.

Table 260. Alarm Soak Profile Configuration

| Field | Description |
|----------------------------------|---|
| Name | Enter a unique name for the alarm soak profile. The following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Global Default Soak Period Raise | Specifies the soak duration before raising the alarm. The default value is 2.5. The supported value ranges from 0 to 3600. |
| Global Default Soak Period Clear | Specifies the soak duration before clearing the reported alarm. The default value is 10. The supported value ranges from 0 to 3600. |
| Alarms | Specifies the list of supported alarms. |
| Resource Type | Specifies resource type if the same alarm name is used for multiple resource types. This field is applicable if the same alarm name is used for multiple resource types. The same soak period configuration is applied for all resource types if this field is not provided. For example: Name: LOSS-OF-SIGNAL resource_type: ME-PORT/ONT |

| Field | Description |
|-------------------------|--|
| Soak Raise Period (Sec) | Enter the value to update the field for that specific alarm other than Global Default Soak Period Raise . |
| Soak Clear Period (Sec) | Enter the value to update the field for that specific alarm other than Global Default Soak Period Clear . |

3. Select the applicable checkbox for the alarms.

4. Click **Create**.

A new alarm soak profile is created on the Alarm Soak Profile page.

To edit, clone, and delete the alarm soak profile configuration, see [Common Operations \(on page 27\)](#).

PON Profiles

Create and manage Passive Optical Network (PON) profiles such as bandwidth profile, shaper profile, Multicast VLAN (MVLAN) profile, multicast group, Class of Service Queues (CoSQ) profile, Virtual Network (VNet) profile, policer profile, and storm control profile.



Note: When you create a service profile name, the profile name can contain a special character underscore (_).

Bandwidth Profile

To access this page, click **Configuration** from the top right corner of the page and then select **PON Profile** > **Bandwidth Profile** from the left-hand side of the menu.

A bandwidth profile enforces the limit on the bandwidth utilization of a service configured for a subscriber.

You can create bandwidth profiles for HSIA, VoIP, and IPTV services. Bandwidth profiles are created for both residential and enterprise services. Based on the subscriber's chosen service plan, the respective bandwidth profile is applied to the subscriber when the subscriber is activated.

The bandwidth utilization includes the Committed Information Rate (CIR), Assured Information Rate (AIR), Excess Information Rate (EIR), and delay tolerance values for service.

CBAC supports type 1, type 2, type 3, type 4, and type 5 TCONT with Assured Information Rate (AIR) values as follows.

- CIR=AIR=EIR> 0 -> TCONT Type 1
- CIR=0, AIR=EIR > 0 -> TCONT Type 2
- CIR=0, AIR>0, EIR>AIR -> TCONT Type 3
- CIR=AIR=0, EIR>0 -> TCONT Type 4
- 0<CIR<AIR<EIR ->TCONT Type 5

You can configure different bandwidth parameters such as CIR, AIR, and EIR, which characterize service as fixed, best effort, or assured as per the type of Tcont1 to 5. For example, the services HSIA and IPTV are treated as best efforts. The parameters CIR and delay tolerance are used to control the latency for a particular service to be less than 1.5 ms.

RMS allows you to create a null bandwidth profile. You can configure the CIR, AIR, and EIR values as zero.

Field Descriptions

The following table describes the fields on the Bandwidth Profile page.

Table 261. Bandwidth Profile List

| Field | Description |
|-----------------------------------|--|
| Name | Specifies the name of the bandwidth profile. |
| Committed Information Rate (Kbps) | Specifies the Committed Information Rate (CIR) in kilobits per second. The configurable value ranges from 0, 255Kbps \geq 10 Gbps. |
| Assured Information Rate (Kbps) | Specifies the Assured Information Rate (AIR) in kilobits per second. The configurable value ranges from 0, 255Kbps \geq 10 Gbps. |
| Excess Information Rate (Kbps) | Specifies the Excess Information Rate (EIR) in kilobits per second. The configurable value ranges from 0, 255Kbps \geq 10 Gbps. |
| Delay Tolerance | Specifies the frequency at which the containers (T-CONT) are allocated to ensure that the required user quality of experience (QoE) for the user is achieved. |
| Creation Time | Specifies the date and time when the bandwidth profile was created. |
| Action | Specifies the action that you can perform on the bandwidth profile. The supported actions are. <ul style="list-style-type: none"> • Edit • Clone • Delete |

**Note:**

- By default, the values of CIR, AIR, and EIR are in Kbps.
- If the value of CIR, AIR, and EIR are in Gbps, the value ranges from 0 to 10 Gbps.
- The value of CIR \leq AIR \leq EIR.

Creating Bandwidth Profile

Perform the following steps to create a bandwidth profile.

1. Select **PON Profile > Bandwidth Profile > Create**.
The Bandwidth Profile Configuration page appears.
2. Complete the bandwidth profile configuration according to the guidelines provided in the following table.

Table 262. Bandwidth Profile Configuration

| Field | Description |
|-----------------------------------|---|
| Name | Enter a unique name for the bandwidth profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Committed Information Rate (Kbps) | Enter the Committed Information Rate (CIR) in kilobits per second. The guaranteed traffic rate is committed to the subscriber with specific SLA parameters. 0, 256Kbps<=CIR (1.25 Gbps for GPON) 0, 256Kbps<=CIR (10 Gbps for XGS-PON) Example: 256 |
| Assured Information Rate (Kbps) | Enter the Assured Information Rate (AIR) in kilobits per second. 0, 256Kbps<=CIR (1.25 Gbps for GPON) 0, 256Kbps<=CIR (10 Gbps for XGS-PON) Example: 256 |
| Excess Information Rate (Kbps) | Enter the Excess Information Rate (EIR) in kilobits per second. The maximum traffic rate that the subscriber can receive above the CIR traffic is subject to bandwidth availability. 0, 256Kbps<=CIR (1.25 Gbps for GPON) 0, 256Kbps<=CIR (10 Gbps for XGS-PON) Example: 256 <div style="margin-top: 10px;">  Note: The EIR value must be greater than the AIR value. </div> |
| Delay Tolerance (No of Frames) | Specifies the frequency at which the transmission containers (T-CONT) are allocated to ensure that the required user quality of experience (QoE) for the user is achieved. An operator can ensure that the user experience is not compromised by controlling the maximum latency between two consecutive grants at the OLT. The supported value ranges from 0 to 128. The unit is in the number of bandwidth frames. The default value is zero if not configured. The value zero means that no specific latency is required for the service. |

3. Click **Create**.

A new bandwidth profile is created on the Bandwidth Profile List page.



Note:



- When you update the bandwidth profile, RMS sends an update bandwidth profile request to CBAC.
- You cannot delete the bandwidth profile if the profile is associated with the subscriber or the subscriber service.

To edit, clone, and delete the bandwidth profile configuration, see [Common Operations \(on page 27\)](#).

Shaper Profile

To access this page, click **Configuration** from the top right corner of the page and then select **PON Profile > Shaper Profile** from the left-hand side of the menu.

The shaper profile includes Committed Information Rate (CIR), Committed Burst Size (CBS), and Excess Information Rate (EIR) values for service.

RMS allows you to create a null shaper profile. You can configure the CIR, CBS, and EIR values as zero.

Field Descriptions

The following table describes the fields on the Shaper Profile page.

Table 263. Shaper Profile List

| Field | Description |
|-----------------------------------|---|
| Name | Specifies the name of a shaper profile. |
| Committed Information Rate (Kbps) | Specifies the Committed Information Rate (CIR) in kilobits per second. The configurable value ranges from 0 Kbps >= 10 Gbps. |
| Excess Information Rate (Kbps) | Specifies the Excess Information Rate (EIR) in kilobits per second. The configurable value ranges from 0 Kbps >= 10 Gbps. |
| Committed Burst Size (KB) | Specifies the committed burst size. |
| Creation Time | Specifies the date and time when the shaper profile was created. |
| Action | Specifies the action that you can perform on the shaper profile. The supported actions are. <ul style="list-style-type: none">• Edit• Clone• Delete |



Note:



- By default, the values of CIR and EIR are in Kbps.
- If the value of CIR and EIR are in Gbps, the value ranges from 0 to 10 Gbps.
- The value of CIR <=EIR.

Creating Shaper Profile

Perform the following steps to create a shaper profile.

1. Select **PON Profile > Shaper Profile > Create**.
The Shaper Profile Configuration page appears.
2. Complete the shaper profile configuration according to the guidelines provided in the following table.

Table 264. Shaper Profile Configuration

| Field | Description |
|-----------------------------------|--|
| Name | Enter a unique name for the shaper profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Committed Information Rate (Kbps) | The Committed Information Rate (CIR) is the minimum guaranteed rate for traffic that the ONT provides for the particular Ethernet service. CIR defines the average rate in bytes of packets up to which the network delivers and meets the performance objectives defined by the Class of Service (CoS) service attribute. The configurable value ranges from 0 Kbps >= 10 Gbps. The CIR value must be >= 0. The unit is in kilobits per second. |
| Excess Information Rate (Kbps) | Enter the Excess Information Rate (EIR). EIR is the maximum allowed traffic during non-busy times without any guarantee. The unit is in kilobits per second. The configurable value ranges from 0 Kbps >= 10 Gbps.  Note: The EIR value must be >=0 or EIR>=CIR. |
| Committed Burst Size (KB) | Enter the committed burst size in kilobytes. CBS limits the maximum number of bytes available for a burst of packets sent at the UNI speed to remain CIR-conformant. The CBS value must be >= 0 (0 to 10000000). The unit is in kilobytes. |

3. Click **Create**.

A new shaper profile is created on the Shaper Profile List page.



Note:

- When you update the shaper profile, RMS sends an updated shaper profile request to CBAC.
- You cannot delete the shaper profile if the profile is associated with the subscriber or the subscriber service.
- By default, the values of CIR and EIR are in Kbps.
- If the value of CIR and EIR are in Gbps, the value ranges from 0 to 10 Gbps.
- The value of CIR <=EIR.

To edit, clone, and delete the shaper profile configuration, see [Common Operations \(on page 27\)](#).

MVLAN Profile

To access this page, click **Configuration** from the top right corner of the page and then select **PON Profile > MVLAN Profile** from the left-hand side of the menu.

Configure the Multicast (MVLAN) profile for each subscriber. Multicast traffic reaches the subscriber only if the traffic is sent through the configured MVLAN.



Note: You can create one or more MVLAN profiles in RMS.

Creating MVLAN Profile

Prerequisites

Before you create an MVLAN profile, you must create a multicast group. See [Creating Multicast Group \(on page 27\)](#).

Perform the following steps to create an MVLAN profile.

1. Select **PON Profile > MVLAN Profile > Create**.

The MVLAN Profile Configuration page appears.

2. Complete the MVLAN profile configuration according to the guidelines provided in the following table.

Table 265. MVLAN Profile Configuration

| Field | Description |
|-------|--|
| Name | Enter a unique name for the MVLAN profile. You can use any number of alphanumeric characters. Only the following special characters are supported. |

| Field | Description |
|-------------------------------------|---|
| | <ul style="list-style-type: none"> Underscore (_) Hyphen (-) |
| VLAN ID | Enter the VLAN ID for downstream multicast service. Example: 4000 |
| PON VLAN | Enter the PON VLAN ID where the multicast traffic is translated on the OLT. The value ranges from 2 to 4094. |
| Multicast Groups | <p>Select the list of IP addresses allowed for multicast traffic. The following IP addresses are supported.</p> <ul style="list-style-type: none"> 239.1.1.1 239.1.1.2 239.1.1.3 to 239.1.1.255 <p>The static group can be configured using the key static in the group configuration. For the static group, the static joins are sent prior to the multicast server to foster the multicast services for the subscribers.</p> |
| One group per channel | Enable this option for the group creation logic. If this is enabled, specifies one channel corresponding to one group at the OLT. This field is enabled by default. |
| Active IGMP Channels per Subscriber | Enter the maximum number of active channels per subscriber. The default value is 100. The value ranges from 3 to 192. |

3. Click **Create**.

A new MVLAN profile is created on the MVLAN Profile List page.



Note:

- You can modify the parameters that you configure for an MVLAN profile, except for the following fields.
 - ID
 - Name
 - VLAN ID
 - PON VLAN
- If you want to modify any of the above fields, create a new MVLAN profile and associate it with the subscribers. You can update the static and dynamic IP lists only if the configured IPs



- are less than or equal to 2048. If the IPs count is greater than 2048 then the system rejects the update to the static and dynamic IPs.
- You can delete the MVLAN profile only when the service is not in use or the profile is not associated with the service configuration.

To edit, clone, and delete the MVLAN profile configuration, see [Common Operations \(on page 27\)](#).

COSQ Profile

To access this page, click **Configuration** from the top right corner of the page and then select **PON Profile > COSQ Profile** from the left-hand side of the menu.

The Class of Service Queues (CoSQ) Profile describes the scheduling configuration, DSCP to p-bit mapping, and discard configuration.

- A scheduling configuration includes the scheduling policy, weight, and priority.
- A discard configuration includes the discard policy, max queue size, maximum and minimum threshold value, and maximum probability value.

You can configure the packet queues for each TCONT, the GEM ports for each packet queue, the p-bits allowed for each GEM port, and the DSCP to p-bit marking for the upstream traffic. It also supports the default p-bit marking for untagged traffic. CoSQ profile also supports p-bit remaking configurations in both upstream and downstream traffic.

Creating COSQ Profile

Perform the following steps to create a COSQ profile.

1. Select **PON Profile > COSQ Profile > Create**.
The COSQ Profile Configuration page appears.
2. Complete the COSQ profile configuration according to the guidelines provided in the following table.

Table 266. COSQ Profile Configuration

| Field | Description |
|-------|---|
| Name | Enter a unique name for the COSQ profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| DSCP | Enter the default DSCP pbit value that needs to be marked. This applies to DSCP values that are not mentioned in the "dscp" field. The value ranges from 0 to 7. |

| Field | Description |
|---|---|
| | <p>The value 0 is the lowest precedence and the value 7 is the highest precedence.</p> <p> Note: This field is disabled if you select Ether Type.</p> |
| Ether Type | <p>Enter the default ether type pbit value that needs to be marked. This applies to Ethertype values that are not mentioned in the "Ether Type" field.</p> <p>The value ranges from 0 to 7.</p> <p> Note: This field is disabled if you select DSCP.</p> |
| Configure Packet Queue | |
| Scheduler Config Policy | <p>Select the scheduler configuration policy from the list. The supported values are.</p> <ul style="list-style-type: none"> ◦ Weighted Round Robin. In WRR mode, the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight, the more frames are sent). The queues are serviced until their quota is used and then another queue is serviced. ◦ Strict Priority. Egress traffic from the highest priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue is transmitted, which provides the highest level of priority of traffic to the highest numbered queue. The priority sets the order in which queues are serviced, starting with queue 8 (the highest priority queue) and going to the next lower queue when each queue is completed. |
| If the scheduler config policy is selected as "Weighted Round Robin", you must enter scheduler config weight value. | |
| Scheduler Config Weight | <p>Enter the scheduler configuration weight.</p> <p>The value ranges from 0 to 100.</p> |
| If the scheduler config policy is selected as "Strict Priority", you must enter scheduler configuration priority value. | |
| Scheduler Config Priority | <p>Enter the scheduler configuration priority value.</p> <p>The value ranges from 0 to 7.</p> |
| Discard Config Policy | Select the packet discard policy followed in the access network. The supported values are. |

| Field | Description |
|---------------------------------------|--|
| | <ul style="list-style-type: none"> • Tail Drop. In tail drop, when the queue is filled to its maximum capacity, the newly arriving packets are dropped until the queue has enough room to accept the incoming traffic. • Random Early Detection (RED). The RED preemptively drops packets before the buffer becomes completely full. It uses predictive models to decide which packets to drop. • Weighted Random Early Detection (WRED). The weighted RED supports different probabilities for different priorities (IP precedence and DSCP) and/or queues. |
| Discard Config Maximum Queue Size | <p>Enter the maximum size of the packet queue. The unit is in packet count. This field is used when the discard policy is selected as Tail Drop. The value depends on the available memory as to how many packets the queue can take. The default value is auto. Otherwise, it takes the size of the queue.</p> |
| Discard Config Minimum Threshold | <p>Enter the minimum threshold value for the packet queue. This field is configured only when the discard policy is selected as RED or WRED. The unit is in packet count.</p> |
| Discard Config Maximum Threshold | <p>Enter the maximum threshold value for the packet queue. This field is configured only when the discard policy is selected as RED or WRED. The unit is in packet count.</p> |
| Discard Config Maximum Probability | <p>Enter the maximum probability value for the packet queue. This field configured only when the discard policy is selected as RED or WRED. The unit is in percentage. The value ranges from 0 to 100.</p> |
| Traffic Class Config | Click on the Traffic Class Config option to add the traffic class configuration. |
| Allowed Pbits | <p>Specifies the list of allowed p-bits. The values of all pbits mentioned in the "default_dscp_pbit_marking" and "pbit" fields must be specified in this field. Any other value other than the pbit would be for non-dscp-to-pbit packets. Example: 1 2 3 The pbits configured in allowed the pbits are allowed in the data path. In addition to this, the allowed pbits can be used to configure pbit remarking. Example: 0-7:2</p> |

| Field | Description |
|-------------------|---|
| | <ul style="list-style-type: none"> ◦ If the pbit remarking is configured in the upstream CoSQ profile, the traffic that comes from RG with any pbit (0-7) is remarked to pbit 2. ◦ If the pbit remarking is configured in the downstream CoSQ profile, the traffic comes from BNG with any pbit (0-7) is remarked to pbit 2. <p>Example: 1:2</p> <ul style="list-style-type: none"> ◦ If the pbit remarking is configured in the upstream CoSQ profile, the traffic that comes from RG with pbit 1 is remarked to pbit 2. ◦ If the pbit remarking is configured in the downstream CoSQ profile, it becomes invalid. <p> Note: Only any pbit to the single pbit is allowed in the downstream CoSQ profile.</p> <p>You can delete the traffic class configuration using the Delete icon.</p> |
| DSCP Pbit Marking | <p>Click on the DSCP Pbit Marking to add the DSCP to p-bit mapping configuration. You can add one or more DSCP pbit marking configuration. When you click on this field, the “DSCP” and “PBIT” fields are displayed.</p> <p>You can delete the DSCP pbit marking configuration using the Delete icon.</p> <p> Note:</p> <ul style="list-style-type: none"> ◦ A user can configure one or more DSCP mappings for each PBIT for each queue. ◦ This field is disabled if you select Ethertype Pbit Marking. |
| DSCP | <p>Specifies the DSCP values associated with packet queues. The associated value can be a range or an individual DSCP value. The maximum value allowed is 63.</p> <p>Example: ["0-5", "8-12", and "16"]</p> <p>The supported value ranges from 0 to 63.</p> <p> Note: You must use the hyphen (-) to specify the range.</p> |

| Field | Description |
|------------------------|---|
| PBIT | <p>Specifies the priority bit associated with packet queues. The value ranges from 0 to 7. The value 0 indicates the lowest PBIT and the value 7 indicates the highest PBIT.</p> <p>Example: 0</p> |
| Ethertype Pbit Marking | <p>Click on the Ethertype Pbit Marking to add the Etheretype to p-bit mapping configuration. You can add one or more Etheretype pbit marking configuration. When you click on this field, the “Etheretype” and “PBIT” fields are displayed.</p> <p>You can delete the Etheretype pbit marking configuration using the Delete icon.</p> <p> Note:</p> <ul style="list-style-type: none"> ◦ A user can configure one or more Etheretype mappings for each PBIT for each queue. ◦ This field is disabled if you select DSCP Pbit Marking. |
| Ethertype | <p>Specifies the Etheretype values associated with packet queues. The supported values are.</p> <ul style="list-style-type: none"> ◦ ARP. Enables CBAC to use the same pbit for IPoE and IPv6 internally. ◦ IPoE. Enables CBAC to use the same pbit for ARP and IPv6 internally. ◦ IPv6. Enables CBAC to use the same pbit for ARP and IPoE internally. ◦ PPPoE. Other strings are not allowed to be configured. |
| PBIT | <p>Specifies the priority bit associated with packet queues. The value ranges from 0 to 7. The value 0 indicates the lowest PBIT and the value 7 indicates the highest PBIT.</p> <p>Example: 0</p> |

3. Click **Create**.

A new COSQ profile is created on the COSQ Profile List page.



Note:

- When you update the COSQ profile, RMS sends an update COSQ profile request to CBAC.
- You cannot delete the CoSQ profile if the profile is associated with the subscriber or the subscriber service.

To edit, clone, and delete the COSQ profile configuration, see [Common Operations \(on page 27\)](#).

VNet Profile

To access this page, click **Configuration** from the top right corner and then select **PON Profile > VNet Profile** from the left-hand side of the menu.

The Virtual Network (VNet) profile captures the VLAN service model.

VNet profile helps achieve multiple deployment scenarios such as residential, enterprise, and service types. It is a way of specifying how the subscriber service is realized end-to-end in terms of VLAN.

CBAC supports VNet profiles on a per-subscriber basis and not a system-wide configuration. RMS supports the VNet profile per sub-service or can share the same VNet across services in the N:1 model.

RMS supports ARP and DHCP-based MAC learning for N:1 VLAN services, and the subscriber traffic flows end-to-end only when the respective MAC learning cycle is completed successfully.

Services such as HSIA, VOIP, IPTV, and VoD can be configured using the VLAN IDs such as Service VLAN ID (SVLAN), Customer VLAN ID (CVLAN), Q-VID (UNI-VLAN), and VLAN controls in the VNet profile.

VLAN CONTROL

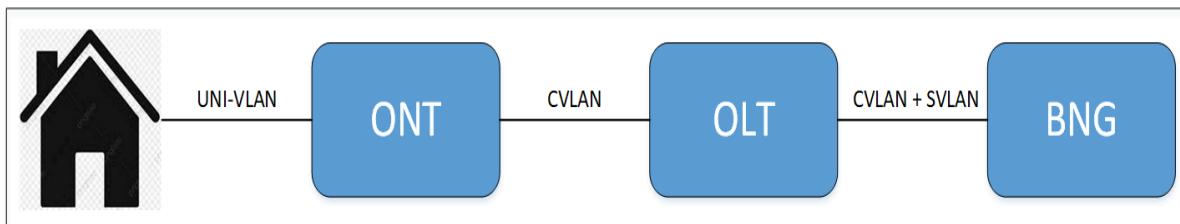
VLAN control explains about the VLAN translations happening at different level within the network. CBAC supports the following VLAN control models.

- [ONU_CVLAN_OLT_SVLAN \(on page 575\)](#)
- [OLT_CVLAN_OLT_SVLAN \(on page 576\)](#)
- [ONU_CVLAN_ONU_SVLAN \(on page 576\)](#)
- [ONU_CVLAN \(on page 576\)](#)
- [OLT_SVLAN \(on page 577\)](#)
- [NONE \(on page 577\)](#)

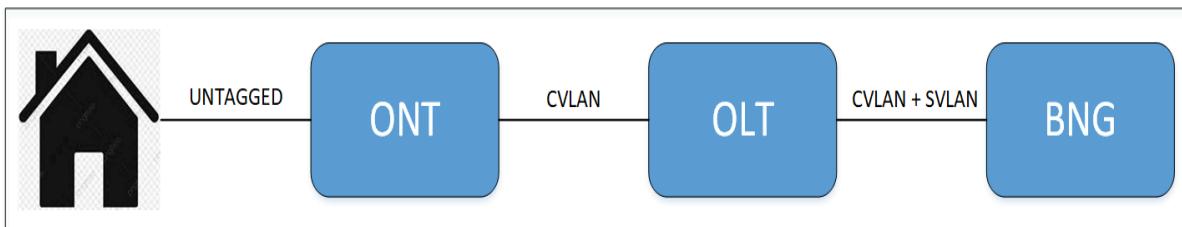
ONU_CVLAN_OLT_SVLAN

For the tagged traffic, ONU translates UNI VLAN to CVLAN and the OLT adds the SVLAN to the packet.

Figure 90. ONU CVLAN OLT SVLAN TAGGED

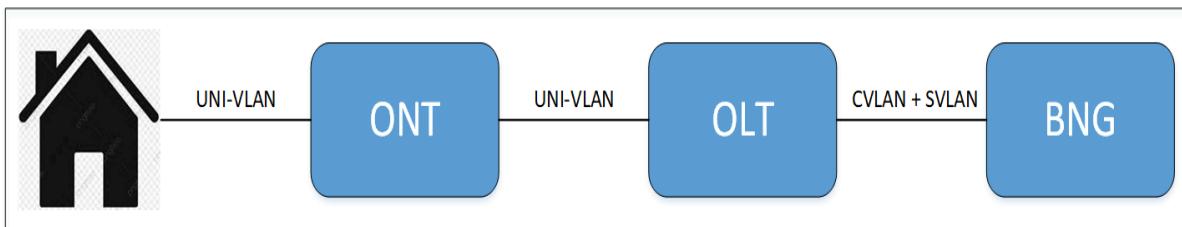


For the untagged traffic, ONU adds CVLAN and the OLT adds the SVLAN to the packet.

Figure 91. ONU CVLAN OLT SVLAN UNTAGGED

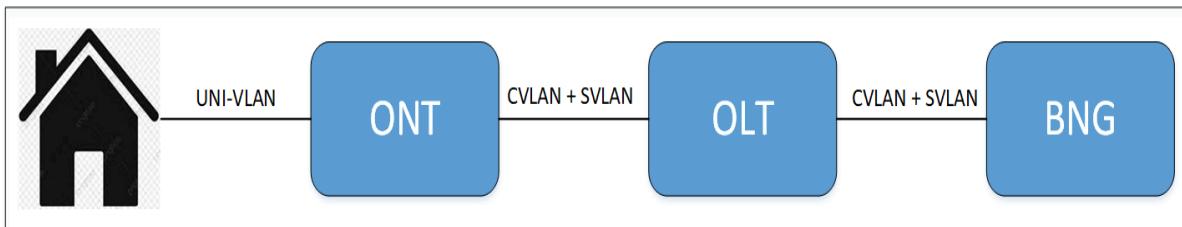
OLT_CVLAN_OLT_SVLAN

For the tagged traffic, ONU transparently forwards the traffic and the OLT translates UNI-VLAN to CVLAN and adds SVLAN to the packet.

Figure 92. OLT CVLAN OLT SVLAN TAGGED

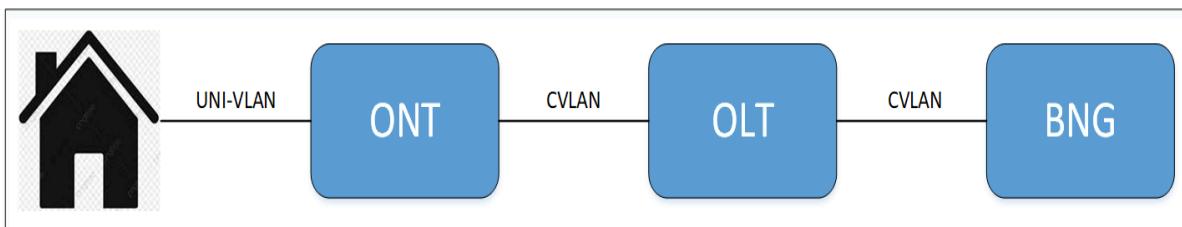
ONU_CVLAN_ONU_SVLAN

For the tagged traffic, ONU replaces the UNI-VLAN with CVLAN and the ONU adds SVLAN.

Figure 93. ONU CVLAN ONU SVLAN TAGGED

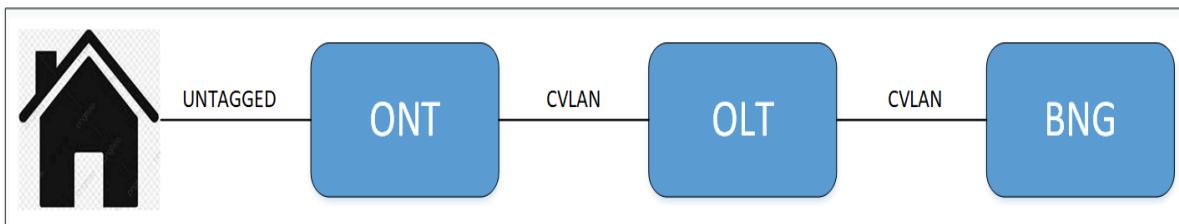
ONU_CVLAN

For the tagged traffic, ONU translates UNI-VLAN to CVLAN and the OLT transparently forwards the packet.

Figure 94. ONU CVLAN TAGGED

For the untagged traffic, ONU adds CVLAN, adds p-bit based on the CoSQ profile, and the OLT transparently forwards the packet.

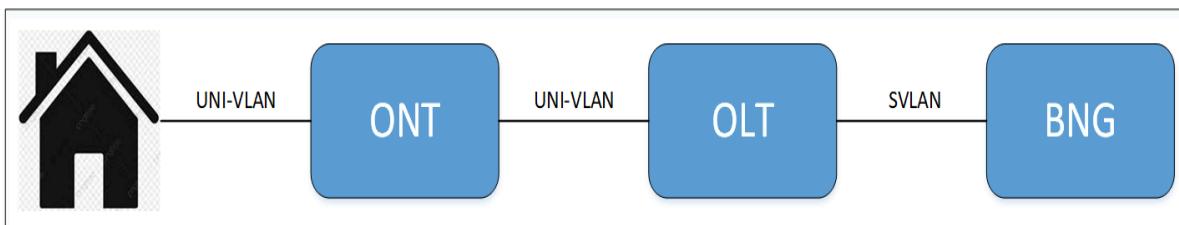
Figure 95. ONU CVLAN UNTAGGED



OLT_SVLAN

For the tagged traffic, ONU transparently forwards the packet and the OLT translates UNI-VLAN to SVLAN.

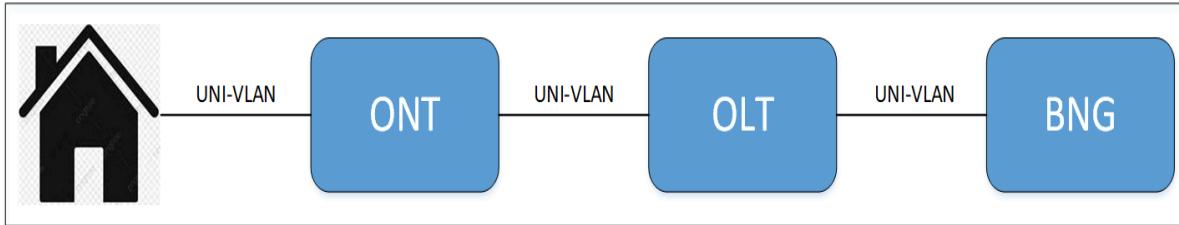
Figure 96. OLT SVLAN TAGGED



NONE

For tagged traffic, ONU and OLT passes through the UNI-VLAN as is to BNG.

Figure 97. NONE TAGGED



Creating VNet Profile

Perform the following steps to create a VNet profile.

1. Select **PON Profile > VNet Profile > Create**.
The VNet Profile Configuration page appears.
2. Complete the VNet profile configuration according to the guidelines provided in the following table.

Table 267. VNet Profile Configuration

| Field | Description |
|------------------------------|---|
| Name | <p>Enter a unique name for the VNet profile. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| SVLAN | Enter the subscriber's S-Tag value. The supported value ranges from 2 to 4094. |
| CVLAN | Enter the subscriber's C-Tag value. The supported value ranges from 2 to 4094. |
| Encapsulation | <p>Select the type of access protocol used to establish the access link. The supported values are.</p> <ul style="list-style-type: none"> ◦ IPoE ◦ PPPoE ◦ PPPoE-IA <p>The default value is IPoE.</p> <p> Note: When this field value is selected as PPPoE-IA, the Remote-ID Type field value in the service configuration can be selected as Custom or left blank.</p> |
| ONT Ethertype Classification | Specifies the ONT ethernet classification. The supported value is. |
| MAC Learning Type | Select the type of method to be used to learn the device MAC address. For more information on MAC Learning Type, see Table 268: MAC Learning Type (on page 580) . |
| Uni VLAN | <p>Specifies the UNI VLAN ID.</p> <p>The supported value ranges from 0 to 4094.</p> <p> Note:</p> |

| Field | Description |
|------------------------|---|
| |  <ul style="list-style-type: none"> ◦ The value uni_vlan=0 indicates the priority tagged packet classification, which is a valid value. ◦ When uni_vlan is configured, ONU is programmed to accept the tagged traffic on the UNI port with VLAN as UNI VLAN. ◦ When uni_vlan is not configured, it is considered as an untagged packet configuration for the subscriber. |
| Uni VLAN Range End | <p>Specifies the end UNI vlan for L2VPN subscriber VLANs range. The Uni VLAN field is mandatory when this field is configured. The value ranges from 2 to 4094.</p> <p>The value of Uni VLAN Range End must be greater than the Uni VLAN value.</p> <p> Note: When Uni VLAN Range End is configured CVLAN and Uni VLAN must be same.</p> |
| Vlan Control | <p>Specifies the VLAN tagging to be supported at the ONU and OLT. The supported values are.</p> <ul style="list-style-type: none"> ◦ ONU_CVLAN_OLT_SVLAN ◦ OLT_CVLAN_OLT_SVLAN ◦ ONU_CVLAN ◦ OLT_SVLAN ◦ ONU_CVLAN_ONU_SVLAN ◦ NONE <p>For more information, see Table 270: VLAN Tagging (on page 582).</p> |
| Allow Transparent VLAN | <p>Specifies the configuration to allow the transparent VLAN from RG. Indicates that the upstream traffic needs to be classified based on the Ether type. The supported values are.</p> <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED <p>When set to "ENABLED", the traffic from RG is passed transparently.</p> |
| CoSQ Profile | <p>Select the CoSQ profile from the list.</p> <p>When this field is configured in the Vnet Profile, the allowed pbits in the CoSQ profile are used for downstream control IPv6 solicit message and downstream ARP request message to remark the pbits.</p> |
| SVLAN TPID | <p>Specifies the TPID that must be used with S-Tag. The supported values are.</p> |

| Field | Description |
|-------------------|--|
| | <ul style="list-style-type: none"> ◦ 0x88A8 ◦ 0x8100 <p>The default value is 0x8100.</p> |
| PON Hair Pinning | <p>Specifies whether the PON hair pinning is enabled for the VLAN model. The supported values are.</p> <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED <p>The default value is DISABLED.</p> |
| Remote Id Profile | Specifies the Remote ID profile name to be used to generate the Remote ID string in DHCP relay and PPPoE Intermediate Agent. |

Table 268. MAC Learning Type

| Field | Description |
|-------------------|---|
| MAC Learning Type | <p>Select the method to be used to learn the device MAC address. If the encapsulation type is selected as IPoE, the following values are supported.</p> <ul style="list-style-type: none"> ◦ NONE. CBAC does not learn MAC addresses; the MAC anti-spoofing is disabled unless the user provides a CPE MAC. The DHCP relay agent is disabled. ◦ DHCP. MAC addresses are learned dynamically along with IP addresses obtained through DHCP. The MAC anti-spoofing is enabled, and the DHCP relay agent is enabled. ◦ ARP. MAC addresses are learned dynamically when devices communicate through ARP. The MAC anti-spoofing is enabled, and the DHCP relay agent is disabled. ◦ DHCP ALLOW RELEARN. Allows MAC relearning based on DHCP; the CPE device/MAC can be updated. The MAC anti-spoofing is enabled, and the DHCP relay agent is enabled. ◦ ARP ALLOW RELEARN. Allows MAC relearning based on ARP; the CPE device/MAC can be updated. The MAC anti-spoofing is enabled, and the DHCP relay agent is disabled. ◦ DHCP IP ANTISPOOFING NO MAC. IP addresses are learned based on DHCP; the IP-based anti-spoofing is enabled. The DHCP relay agent is enabled. ◦ DHCP IP ANTISPOOFING MAC. IP addresses and MAC addresses are learned based on DHCP; the IP and MAC-based anti-spoofing is enabled. The DHCP relay agent is enabled. |

| Field | Description |
|-------|---|
| | <ul style="list-style-type: none"> • DHCP NO MAC. CBAC learns the MAC addresses from DHCP, but MAC anti-spoofing is disabled. The DHCP relay agent is enabled. • ARP NO MAC. CBAC learns MAC addresses from ARP, but MAC anti-spoofing is disabled. The DHCP relay agent is disabled. <p>The following values are supported if the encapsulation type is selected as PPPoE.</p> <ul style="list-style-type: none"> • NONE. CBAC does not learn MAC addresses; the MAC anti-spoofing is disabled unless the user provides a CPEMAC. The DHCP relay agent is disabled. <p>The following values are supported if the encapsulation type is selected as PPPoE-IA.</p> <ul style="list-style-type: none"> • PPPoE. The MAC addresses are learned dynamically within a Point-to-Point Protocol over Ethernet (PPPoE) context. The MAC anti-spoofing is enabled, and the PPPoE-IA intermediate agent is enabled. • NONE. CBAC does not learn MAC addresses; the MAC anti-spoofing is disabled unless the user provides a CPEMAC. The DHCP relay agent is disabled. |

| MAC Learning Type | DHCP-Relay V4 and V6 | MAC Anti Spoofing | IP Antispoofing | Allow Change of CPE Device/MAC |
|------------------------------|----------------------|---|-----------------|--------------------------------|
| None | NO | YES (If CPE MAC is configured), else NO | NO | YES |
| DHCP | YES | YES - From Learnt MAC (MAC from DHCP) | NO | NO |
| ARP | NO | YES | NO | NO |
| DHCP_RELEARN | YES | YES | NO | YES |
| ARP_RELEARN | NO | YES | NO | YES |
| DHCP_NO_MAC | YES | NO | NO | YES |
| ARP_NO_MAC | NO | NO | NO | YES |
| DHCP_IP_ANTISP_OOFING_NO_MAC | YES | NO | YES | YES |
| DHCP_IP_ANTISP_OOFING_MAC | YES | YES | YES | YES |

Table 269. PPPoE Behaviour

| Encapsulation | Mac Learning | Intermediate Agent | Mac anti-spoofing |
|---------------|--------------|--------------------|-------------------|
| PPPoE | None | No | No |
| PPPoE-IA | None | Yes | No |
| PPPoE-IA | PPPoE | Yes | Yes |

Table 270. VLAN Tagging

| vlan_control | Case | Packet Egress Uplink and Ingress Downlink |
|---------------------|--|---|
| ONU_CVLAN_OLT_SVLAN | ONU replaces the UNI-VLAN with CVLAN and the OLT adds SVLAN (Tagged traffic from RG). ONU adds the CVLAN and OLT adds SVLAN (Untagged traffic from RG). | Double Tagged packet |
| OLT_CVLAN_OLT_SVLAN | ONU passes through the UNI-VLAN to the OLT and the OLT replaces the UNI-VLAN with CVLAN and adds the SVLAN (Tagged traffic from RG). | Double Tagged packet |
| ONU_CVLAN_ONU_SVLAN | ONU replaces the UNI-VLAN with CVLAN and the ONU adds SVLAN. | Single Tagged packet |
| ONU_CVLAN | ONU replaces the UNI-VLAN with CVLAN (Tagged traffic from RG) and the OLT does not add any tag. ONU adds the CVLAN (Untagged traffic from RG) and OLT does not add any tag. | Single Tagged packet |
| OLT_SVLAN | ONU passes through the packet and the OLT adds the SVLAN Only. | Single Tagged packet |
| NONE | ONU and OLT passes through the UNI-VLAN to BNG (Tagged traffic from RG). | Single Tagged packet |

3. Click **Create**.

A new VNet profile is created on the VNet Profile List page.



Note: You cannot delete the Vnet profile if the profile is associated with a service.

To edit, clone, and delete the VNet profile configuration, see [Common Operations \(on page 27\)](#).

IGMP Profile

To access this page, click **Configuration** from the top right corner of the page and then select **PON Profile** > **IGMP Profile** from the left-hand side of the menu.

Internet Group Management Protocol (IGMP) is the network configuration for the IGMP proxy application. Each MVLAN profile configured on the OLT must be associated with IGMP profile information for IGMP proxy functionality.

Field Descriptions

The following table describes the fields on the IGMP Profile List page.

Table 271. IGMP Profile List

| Field | Description |
|---------------------|--|
| Name | Specifies the unique name of the IGMP profile. |
| Unsolicited Timeout | Specifies the time interval (in seconds) between the IGMP proxy application membership report messages to receive multicast service for a group or channel. |
| Max Response | Specifies the maximum response time (in seconds), which is used to calculate the max response code inserted into the periodic IGMP queries. |
| Keep Alive Interval | Specifies the time interval (in seconds) between the IGMP General Membership Queries^a (on page 584) / IGMP Group Specific Queries^b (on page 584) sent by the IGMP proxy application. |
| Keep Alive Count | Specifies the number of IGMP General Membership Queries^a (on page 584) / IGMP Group Specific Queries^b (on page 584) sent before the IGMP application assumes that there are no local members. |
| Last Query Interval | Specifies the time interval (in seconds) between the IGMP General Membership Queries^a (on page 584) / IGMP Group Specific Queries^b (on page 584) sent by the IGMP proxy before it assumes that there are no local members for a group. |
| Last Query Count | Specifies the number of IGMP General Membership Queries^a (on page 584) / IGMP Group Specific Queries^b (on page 584) sent before the IGMP application assumes that there are no local members. |
| Fast Leave | Specifies whether the IGMP application needs to send IGMP Group-Specific Queries^b (on page 584) to the individual member in the group when the leave message is received. |
| Periodic Query | Specifies if the IGMP application needs to perform periodic queries. |

Table 271. IGMP Profile List (continued)

| Field | Description |
|------------------------|---|
| IGMP Cos | Specifies the priority bit value in the IGMP packet. |
| RA Uplink | Specifies if the IGMP application needs to add a route alert (IgmpReport, Igmpjoin, and Igmpleave) packet into the uplink packets. |
| RA Downlink | Specifies if the IGMP application needs to add a route alert (IgmpQuery) packet into the downlink packets. |
| IGMP Version to Server | Specifies the IGMP report version number to be sent to the multicast server or Broadband Network Gateway (BNG). |
| Creation Time | Specifies the date and time when the IGMP profile was created. |
| Action | Specifies the action that you can perform on the IGMP profile. The supported actions are. <ul style="list-style-type: none"> • Edit • Clone • Delete |

IGMP General Membership Queries^a. The IGMP query sent to all system groups (224.0.0.1). IGMP general queries are destined to the address 224.0.0.1 (all systems on a subnet).

IGMP Group Specific Queries^b. The IGMP query sent to individual members subscribed to a specific multicast group. IGMP group-specific queries are destined to the group IP address for which the device is querying.

Creating IGMP Profile

Perform the following steps to create an IGMP profile.

1. Select **PON Profile > IGMP Profile > Create**.
The IGMP Profile Configuration page appears.
2. Complete the IGMP profile configuration according to the guidelines provided in the following table.

Table 272. IGMP Profile Configuration

| Field | Description |
|-------|--|
| Name | Enter a unique name for the IGMP profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |

| Field | Description |
|------------------------|---|
| Max Response | <p>Enter the maximum response time (in seconds), which is used to calculate the max response code inserted into the periodic IGMP queries.</p> <p>The value ranges from 5 to 12 seconds.</p> <p>The minimum value is 5 seconds, and the maximum value is 12 seconds.</p> <p>The default value is 10 seconds.</p> |
| Unsolicited Timeout | <p>Enter the time interval (in seconds) between the IGMP proxy application membership report messages to receive multicast service for a group or channel.</p> <p>The minimum value must be \geq “Max Response” value.</p> <p>The maximum value is 255 seconds.</p> <p>The default value is 12 seconds.</p> |
| Keep Alive Interval | <p>Enter the time interval (in seconds) between the IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent by the IGMP proxy application.</p> <p>The minimum value must be \geq “Max Response” value.</p> <p>The maximum value is 255 seconds.</p> <p>The default value is 120 seconds.</p> |
| Keep Alive Count | <p>Enter the number of IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent before the IGMP application assumes that there are no local members.</p> <p>The value ranges from 1 to 255.</p> <p>The default value is 3.</p> |
| Last Query Interval | <p>Enter the time interval (in seconds) between the IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent by the IGMP proxy before it assumes that there are no local members for a group.</p> <p>The minimum value must be \geq “Max Response” value.</p> <p>The minimum value is 1 second.</p> <p>The maximum value is 255 seconds.</p> <p>The default value is 12 seconds.</p> |
| Last Query Count | <p>Enter the number of IGMP General Membership Queries^a / IGMP Group Specific Queries^b sent before the IGMP application assumes that there are no local members.</p> <p>The value ranges from 1 to 255.</p> <p>The default value is 2.</p> |
| IGMP Cos | <p>Enter the priority bit value in the IGMP packet.</p> <p>The value ranges from 0 to 7.</p> <p>The default value is 7.</p> |
| IGMP Version to Server | <p>Enter the IGMP report version number to be sent to the multicast server or Broadband Network Gateway (BNG).</p> <p>Example: v3.</p> |

| Field | Description |
|--------------------|---|
| MLD Version Server | Specifies the MLD version. The supported values are. <ul style="list-style-type: none"> ◦ v1 ◦ v2 The default value is v2. |
| Fast Leave | Enable this option if the IGMP application needs to send IGMP Group-Specific Queries ^b to the individual member in the group when the leave message is received. |
| Periodic Query | Enable this option if the IGMP application needs to perform periodic queries. <ul style="list-style-type: none"> ◦ Enable. Enables the IGMP application to perform periodic queries. ◦ Disable. May cause the ONU to delete the IGMP routing table. |
| RA Uplink | Enable this option if the IGMP application needs to add a route alert (IgmpReport, Igmpjoin, and Igmpleave) packet into the uplink packets. |
| RA Downlink | Enable this option if the IGMP application needs to add a route alert (IgmpQuery) packet into the downlink packets. |

IGMP General Membership Queries^a. The IGMP query sent to all system groups (224.0.0.1). IGMP general queries are destined to the address 224.0.0.1 (all systems on a subnet).

IGMP Group Specific Queries^b. The IGMP query sent to individual members subscribed to a specific multicast group. IGMP group-specific queries are destined to the group IP address for which the device is querying.

3. Click **Create**.

A new IGMP profile is created on the IGMP Profile List page.



Note: You can delete the IGMP profile only if it is not associated with the multicast configuration.

To edit, clone, and delete the IGMP profile configuration, see [Common Operations \(on page 27\)](#).

Policer Profile

To access this page, click **Configuration** from the top right corner of the page and then select **PON Profile** > **Policer Profile** from the left-hand side of the menu.

Policer profile configures the traffic rate supported by the storm control profile that is Committed Information Rate (CIR), and Committed Burst Size (CBS).

Creating Policer Profile

Perform the following steps to create a policer profile.

1. Select **PON Profile > Policer Profile > Create**.
The Policer Profile Configuration page appears.
2. Complete the policer profile configuration according to the guidelines provided in the following table.

Table 273. Policer Profile Configuration

| Field | Description |
|---------------------------|--|
| Name | Enter a unique name for the policer profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">Underscore (_)Hyphen (-) |
| Add Policer Config | |
| CIR (Kbps) | Enter the Committed Information Rate (CIR). The unit is in kilobits per second. The supported value ranges from 1 to 500000 Kbps. |
| CBS (KB) | Enter the Committed Burst Size (CBS). The unit is in kilo bytes. The supported value ranges from 0 to 32000 KB. |
| Traffic type | Enter the type of traffic. The supported values are. <ul style="list-style-type: none">BroadcastMulticastUnknown Unicast |

3. Click **Create**.

A new policer profile is created on the Policer Profile List page.

To view, clone, and delete the Policer profile configuration, see [Common Operations \(on page 27\)](#).

Storm Control Profile

To access this page, click **Configuration** from the top right corner of the page and then select **PON Profile > Storm Control Profile** from the left-hand side of the menu.

Storm control prevents excessive traffic and enhances network performance. A traffic storm occurs when packets flood the device and create excessive traffic. The network performance degrades due to excessive traffic.

The traffic broadcast, multicast, and unknown unicast suppression feature prevent the device from being disrupted by storm on physical interfaces.

Creating Storm Control Profile

Perform the following steps to create a storm control profile.

1. Select **PON Profile > Storm Control Profile > Create**.
The Storm Control Profile Configuration page appears.
2. Complete the storm control profile configuration according to the guidelines provided in the following table.

Table 274. Storm Control Profile Configuration

| Field | Description |
|-----------------|--|
| Name | Enter a unique name for the storm control profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| VLAN | Specifies the outer-tag value of the subscriber. The supported value ranges from 2 to 4094. |
| I-VLAN | Specifies the inner-tag value of the subscriber. The supported value ranges from 2 to 4094. |
| Priority | Enter the priority of the storm control profile. The supported value ranges from 0 to 4000. The default value is 0. |
| Policer Profile | Specifies the name of the policer profile. |

3. Click **Create**.

A new storm control profile is created on the Storm Control Profile List page.

To view, clone, and delete the Storm Control Profile configuration, see [Common Operations \(on page 27\)](#).

Voice Service Profiles

Create and manage voice service profiles such as Plain Old Telephone Service (POTS), IP host profile, SIP Agent Profile, SIP User Data Profile, network dial plan profile, VoIP service information profile, VoIP media information profile, RTP information profile, and VoIP App Service Profile.

POTS Profile

To access this page, click **Configuration** from the top right corner of the page and then select **Voice Service Profile > POTS Profile** from the left-hand side of the menu.

The Plain Old Telephone Service (POTS) profile contains the attributes specific to the POTS physical interface, which is the type of telephone connected to the ONT. This profile provides a configuration option to configure the waiting period before signaling the intrusion alert security systems.

Creating POTS Profile

Perform the following steps to create a POTS profile.

1. Select **Voice Service Profile > POTS Profile > Create**.
The POTS Profile Configuration page appears.
2. Complete the POTS profile configuration according to the guidelines provided in the following table.

Table 275. POTS Profile Configuration

| Field | Description |
|-----------|---|
| Name | Enter a unique name for the POTS profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-) |
| Impedance | Enter the impedance for the POTS port. The supported value ranges from 0 to 4. The default value is 0. |
| Rx Gain | Enter the gain value for the received signal. The supported value ranges from -120 to 60. The direction of the affected signal is from D to A, towards the telephone set. The default value is 0. |
| Tx Gain | Enter the gain value for the transmitted signal. The supported value ranges from -120 to 60. The direction of the affected signal is from A to D direction, towards the telephone set. |

| Field | Description |
|----------------------|---|
| | The default value is 0. |
| POTS Holdover Time | Enter the POTS holdover time. This field determines the time during which the POTS loop voltage is held up when a Loss of Signal (LOS) or soft switch is detected. After the specified time elapses, the ONT drops the loop voltage and may cause the intrusion or fire alarms to go active. The value ranges from 0 to 65535. |
| Nominal Feed Voltage | Enter the designed nominal feed voltage of the POTS loop. The supported value ranges from 0 to 255. The default value is 0. |

3. Click **Create**.

A new POTS profile is created on the POTS Profile page.



Note: You cannot delete the POTS profile if it is associated with any OLT.

To edit, clone, and delete the POTS profile configuration, see [Common Operations \(on page 27\)](#).

SIP Agent Profile

To access this page, click **Configuration** from the top right corner of the page and then select **Voice Service Profile > SIP Agent Profile** from the left-hand side of the menu.

The SIP agent profile contains attributes that enable the operator to provision the SIP server parameters. The SIP client in the ONT uses these parameters to contact the SIP server in the network through the IP host interface.

Creating SIP Agent Profile

Perform the following steps to create a SIP agent profile.

1. Select **Voice Service Profile > SIP Agent Profile > Create**.
The SIP agent profile Configuration page appears.
2. Complete the SIP agent profile configuration according to the guidelines provided in following table.

Table 276. SIP Agent Profile Configuration

| Field | Description |
|-------|--|
| Name | Enter a unique name for the SIP agent profile. You can use any number of alphanumeric characters. Only the following special characters are supported. |

| Field | Description |
|-------------------------------|---|
| | <ul style="list-style-type: none"> Underscore (_) Hyphen (-) |
| Registrar Address | Enter the registrar address. This can be an IP address, resolved name, or FQDN. Example: 10.1.1.1, www.server1.com, or server1 |
| Proxy Server Address | Enter the proxy server address. This can be an IP address, resolved name, or FQDN. Example: 10.1.1.1, www.server1.com, or server1 |
| Outbound Proxy Server Address | Enter the outbound proxy server address. This can be an IP address, resolved name, or FQDN. Example: 10.1.1.1, www.server1.com, or server1 |
| Primary DNS | Enter the primary DNS IP or hostname. |
| Secondary DNS | Enter the secondary DNS IP or hostname. |
| Reg Exp Time | Enter the IP or hostname SIP registrar expiry time in seconds. The value ranges from 0 to 4294967295. The default value is 3600 seconds. Example: 3600 seconds |
| Re-registrar Head Start Time | Enter the SIP re-registrar head start time in seconds. The value ranges from 0 to 4294967295. The default value is 360 seconds. Example: 360 seconds |
| Host Part URI | Enter the host part URI or IP address. Following is the example URI that can accept different values. http://server1.com, https://172.27.172.10/xxx/profile1/usr/bin/profile1 |
| Soft Switch | Enter the SIP gateway soft switch vendor. The format is four ASCII code alphabetic characters [A..Z]. Example: A |

3. Click **Create**.

A new SIP agent profile is created on the SIP Agent Profile List page.

To edit, clone, and delete the SIP agent profile configuration, see [Common Operations \(on page 27\)](#).

SIP User Data Profile

To access this page, click **Configuration** from the top right corner of the page and then select **Voice Service Profile > SIP User Data Profile** from the left-hand side of the menu.

The SIP user data profile defines attributes related to voice mail configuration and is used in conjunction with a VoIP line service. It is an optional profile for ONUs that supports VoIP SIP services. The SIP user data profiles are created and deleted by OLT over OMCI. This profile is required for each POTS UNI port using the SIP protocol and configured by the OMCI.

Creating SIP User Data Profile

Perform the following steps to create a SIP user data profile.

1. Select **Voice Service Profile > SIP User Data Profile > Create**.

The SIP User Data Profile Configuration page appears.

2. Complete the SIP user data profile configuration according to the guidelines provided in the following table.

Table 277. SIP User Data Profile Configuration

| Field | Description |
|----------------------------------|--|
| Name | Enter a unique name for the SIP user data profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-) |
| Voicemail Server SIP URI | Specifies the voicemail server SIP URI. The SIP URI can be provided as a URI, IP address, or a local host file system path. Examples: <ul style="list-style-type: none">• URIs: http://server1.com, https://172.27.172.10/xxx/profile1, and /usr/bin/profile1• IP address: 172.21.172.10 |
| Voicemail Expiry Sub Time (secs) | Specifies the voicemail expiry sub time. The value ranges from 0 to 4294967295. The default value is 3600 seconds. |
| Release Timer (secs) | Specifies the release timer. The value ranges from 0 to 255. The default value is 10 seconds. |
| ROH Timer (secs) | Specifies the ROH timer. The value ranges from 0 to 255. The default value is 255. |

3. Click **Create**.

A new SIP user data profile is created on the SIP User Data Profile List page.

To edit, clone, and delete the SIP user data profile configuration, see [Common Operations \(on page 27\)](#).

Network Dial Plan Profile

To access this page, click **Configuration** from the top right corner of the page and select **Voice Service Profile > Network Dial Plan Profile** from the left-hand side of the menu.

The network dial plan profile contains attributes that enable the operator to provision the ONT with the dial plan used in their voice network. This plan tells the ONT how to interpret the digits entered by the user on an analog phone.

Creating Network Dial Plan Profile

Perform the following steps to create a network dial plan profile.

1. Select **Voice Service Profile > Network Dial Plan Profile > Create**.
The Network Dial Plan Profile Configuration page appears.
2. Complete the network dial plan profile configuration according to the guidelines provided in the following table.

Table 278. Network Dial Plan Profile Configuration

| Field | Description |
|----------------------------|---|
| Name | Enter a unique name for the network dial plan profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-) |
| Dial Plan Table Size | Enter the size of the dial plan. The value ranges from 1 to 65,535. Example: 1 |
| Critical Dial Timeout | Enter the critical dial timeout in ms. The value ranges from 0 to 65,535. The default value is 4000ms. |
| Partial Dial Timeout | Enter the partial dial timeout in ms. The value ranges from 0 to 65,535. The default value is 16000ms. |
| Format | Enter the format of dial plan. The value ranges from 0 to 3. <ul style="list-style-type: none">• 0. Not defined.• 1. ITU-T H.248 format.• 2. NCS format.• 3. Vendor-specific format. |
| Add Dial Plan Table | |
| Dial Plan ID | Specifies the dial plan entry. The value ranges from 1 to 255. Example: 1 |

| Field | Description |
|-------|---|
| Token | <p>Specifies the dial plan pattern. The supported values are alphanumeric characters with special characters.</p> <p> Note: The maximum length of the token is 28 bytes (characters).</p> <p>Example: 90[1-3]1x.T</p> <ul style="list-style-type: none"> • T. Indicates timer expiry. • x. Indicates the DTMF digits from 0 to 9. • (-). A hyphen Indicates a range of the number. <ul style="list-style-type: none"> ◦ Example, [1-3] indicates numbers range from 1 to 3. • (.). A period indicates that the number can be repeated zero or more times. <ul style="list-style-type: none"> ◦ Example, 90[1-3]x. indicates that it matches 9011, 9021, 9031, 90111, 90112, 90211, 90212 and so on. • . Indicates a separator in the token. <p> Note:</p> <ul style="list-style-type: none"> • The system cannot parse the separator () in the token for R3.x.x. You must create multiple dial plans for R3.x.x. For more information, see Table 279: Dial Plan Token Format (on page 594). • The system stops collecting digits on the smallest string it matches that does not have a T. For example, if you have configured two dial plans, xxxx and xxxxxxxx. The system stops at the fifth and never goes to the eighth digit. So you must set up the dial plan as xxxxT and xxxxxxxx. |

The following table list the format for dial plan token.

Table 279. Dial Plan Token Format

| Dial Plan ID | Token | Supported or Not Supported |
|--------------|-------------|----------------------------|
| 1 | xxxxxxxxxxT | Supported |
| 2 | 1xxxxxxxxxx | Supported |
| 3 | xxxxxxT | Supported |
| 4 | *xx | Supported |

| Dial Plan ID | Token | Supported or Not Supported |
|--------------|--|----------------------------|
| 5 | xxxT | Supported |
| 6 | 0T 00T [1-7]xxx 8xxxxxxxx #xxxxxxxx *xx 91xxxxxxxxxx 9011x.T | Not Supported |

3. Click **Create**.

A new network dial plan profile is created on the Network Dial Plan Profile page.

To edit, clone, and delete the network dial plan profile configuration, see [Common Operations \(on page 27\)](#).

VoIP Service Info Profile

To access this page, click **Configuration** from the top right corner of the page and select **Voice Service Profile > VoIP Service Info Profile** from the left-hand side of the menu.

The VoIP service information profile describes the voice service function parameters. This profile manages the tones patterns and tone events played on the analog phone, ringing patterns, jitter target, and DTMF digit duration.

Creating VoIP Service Info Profile

Perform the following steps to create a VoIP service information profile.

1. Select **Voice Service Profile > VoIP Service Info Profile > Create**.
The VoIP Service Info Configuration page appears.
2. Complete the VoIP service information configuration according to the guidelines provided in the following table.

Table 280. VoIP Service Info Profile Configuration

| Field | Description |
|-------------------|--|
| Name | Enter a unique name for the VoIP service information profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) |
| Announcement Type | Specifies the announcement type. The supported values are. <ul style="list-style-type: none"> • 0x01-Silence • 0x02-Reorder_tone • 0x03-Fast_busy |

| Field | Description |
|------------------------|---|
| | <ul style="list-style-type: none"> • 0x04-Voice_announcement • 0xFF-Not_specified <p>The default value is 0xFF- Not_specified.</p> |
| Jitter Target | <p>Specifies the jitter target.</p> <p>The value ranges from 0 to 65,535.</p> |
| Jitter Buffer Max | <p>Specifies the maximum jitter buffer.</p> <p>The value ranges from 0 to 65,535.</p> |
| PSTN Protocol | <p>Specifies the Public Switched Telephone Network (PSTN) protocol.</p> <p>The PSTN protocol represents the country code that must be configured on the ONU.</p> <p>To view the list of country codes, refer to the https://countrycode.org/.</p> <p>For example-</p> <ul style="list-style-type: none"> • 91- India • 1- United States • 44- United Kingdom, and so on. <p>The default value is 1.</p> |
| Echo Cancel Indication | Specifies the echo cancel indication. |

3. Click **Create**.

A new VoIP service information profile is created on the VoIP Service Info Profile page.

To edit, clone, and delete the VoIP service info profile configuration, see [Common Operations \(on page 27\)](#).

VoIP Media Info Profile

To access this page, click **Configuration** from the top right corner of the page and select **Voice Service Profile > VoIP Media Info Profile** from the left-hand side of the menu.

The VoIP media information profile configures the voice encoding for the voice service. The encodings of FAX codecs are implemented as per the operator's requirement. A user can direct the ONT to negotiate the codec profile based on the order or preference specified in the VoIP Media Info Profile. This profile is used in the session description protocol offer or answer by the ONT to negotiate the codec for the media.

Creating VoIP Media Info Profile

Perform the following steps to create a VoIP media information profile.

1. Select **Voice Service Profile > VoIP Media Info Profile > Create**.
The VoIP Media Info Profile Configuration page appears.
2. Complete the VoIP media information according to the guidelines provided in the following table.

Table 281. VoIP Media Info Profile Configuration

| Field | Description |
|------------------------------|--|
| Name | Enter a unique name for the VoIP media information profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) |
| Fax Mode | Specifies the fax mode. The supported values are. <ul style="list-style-type: none"> • 0. Passthru • 1. ITU-T_T.38 |
| OOB DTMF | Specifies the Out of Band (OOB) Dual Tone Multi Frequency (DTMF). The supported values are 0 and 1. |
| First Preference | |
| Codec | Specifies the codec for the first order selection. The value ranges from 0 to 18. |
| Packet Period Selection (ms) | Specifies the packet selection period for the first order selection in milliseconds. The default value is 10. The value ranges from 10 to 30. |
| Silence Suppression | Specifies the silence suppression for the first order selection. The supported values are 0 and 1. |
| Second Preference | |
| Codec | Specifies the codec for the second order selection. The value ranges from 0 to 18. |
| Packet Period Selection (ms) | Specifies the packet selection period for the second order selection in milliseconds. The default value is 10. The value ranges from 10 to 30. |
| Silence Suppression | Specifies the silence suppression for the second order selection. The supported values are 0 and 1. |
| Third Preference | |
| Codec | Specifies the codec for the third order selection. |

| Field | Description |
|------------------------------|--|
| | The value ranges from 0 to 18. |
| Packet Period Selection (ms) | Specifies the packet selection period for the third order selection in milliseconds. The default value is 10. The value ranges from 10 to 30. |
| Silence Suppression | Specifies the silence suppression for the third order selection. The supported values are 0 and 1. |
| Fourth Preference | |
| Codec | Specifies the codec for the fourth order selection. The value ranges from 0 to 18. |
| Packet Period Selection (ms) | Specifies the packet selection period for the fourth order selection in milliseconds. The default value is 10. The value ranges from 10 to 30. |
| Silence Suppression | Specifies the silence suppression for the fourth order selection. The supported values are 0 and 1. |

3. Click **Create**.

A new VoIP media information profile is created on the VoIP Media Info Profile page.

To edit, clone, and delete the VoIP media info profile configuration, see [Common Operations \(on page 27\)](#).

RTP Info Profile

To access this page, click **Configuration** from the top right corner of the page and select **Voice Service Profile > RTP Info Profile** from the left-hand side of the menu.

The Real-time Transport Protocol (RTP) profile configures the ONUs RTP parameters during the VoIP session. The parameters include DSCP marking of RTP packets and events supported in the RTP, such as Dual Tone Multi Frequency (DTMF), tones, and Channel Associated Signaling (CAS).

Creating RTP Info Profile

Perform the following steps to create a RTP information profile.

1. Select **Voice Service Profile > RTP Info Profile > Create**.
The Network Dial Plan Profile Configuration page appears.
2. Complete the RTP information profile configuration according to the guidelines provided in the following table.

Table 282. RTP Info Profile Configuration

| Field | Description |
|------------------|---|
| Name | Enter a unique name for the RTP information profile. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> Underscore (_) Hyphen (-) |
| Local Port Min | Specifies the minimum local port. The value ranges from 0 to 65,535. |
| Local Port Max | Specifies the maximum local port. The value ranges from 0 to 65,535. The value for local port max must be greater than local port min. |
| DSFP Mark | Specifies the DSFP mark. The value ranges from 0 to 63. |
| Piggyback Events | Specifies the piggyback events. The supported values are 0 and 1. |
| Tone Events | Specifies the tone events. The supported values are 0 and 1. |
| DTMF Events | Specifies the Dual Tone Multi Frequency (DTMF) events. The supported values are 0 and 1. |
| CAS Events | Specifies the Channel Associated Signaling (CAS) events. The supported values are 0 and 1. |

3. Click **Create**.

A new RTP information profile is created on the RTP Info Profile page.

To edit, clone, and delete the RTP info profile configuration, see [Common Operations \(on page 27\)](#).

VoIP App Service Profile

To access this page, click **Configuration** from the top right corner of the page and select **Voice Service Profile > VoIP App Service Profile** from the left-hand side of the menu.

The VoIP application service profile defines attributes of calling features used with a VoIP line service and is optional for ONUs that support VoIP services. OLT or CBAC can create or delete this profile through OMCI.

The VoIP application service profile supports the following capabilities.

- 3-way calling
- Call forwarding
- Call transfer
- Call waiting
- Caller ID display

Creating VoIP Application Service Profile

Perform the following steps to create a VoIP application service profile.

1. Select **Voice Service Profile > VoIP App Service Profile > Create**.
The Network Dial Plan Profile Configuration page appears.
2. Complete the RTP information profile configuration according to the guidelines provided in the following table.

Table 283. VoIP Application Service Profile Configuration

| Field | Description |
|-----------------------|--|
| Name | <p>Enter a unique name for the VoIP application service profile. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none">• Underscore (_)• Hyphen (-) |
| Caller ID Features | <p>Specifies the caller ID features. The supported values are.</p> <ul style="list-style-type: none">• 0x00-Disable• 0x01-Calling_number• 0x02-Calling_name• 0x04-CID_blocking• 0x08-CID_number• 0x10-CID_name• 0x20-Anonymous_CID_blocking <p> Note: You can select "0x00-Disable" or multiple options of call ID features.</p> |
| Call Waiting Features | <p>Specifies the call waiting features. The supported values are.</p> <ul style="list-style-type: none">• 0x00-Disable• 0x01-Call_waiting• 0x02-Caller_ID_announcement |

| Field | Description |
|----------------------------|--|
| |  Note: You can select "0x00-Disable" or multiple options of call waiting features. |
| Call Transfer Features | <p>Specifies the call transfer features. The supported values are.</p> <ul style="list-style-type: none">• 0x0000-Disable• 0x0001-3way• 0x0002-Call_transfer• 0x0004-Call_hold• 0x0008-Call_park• 0x0010-Do_not_disturb• 0x0020-Flash_on_emergency_service_call• 0x0040-Emergency_service_originating_hold• 0x0080-6way  Note: You can select "0x0000-Disable" or multiple options of call transfer features. |
| Call Presentation Features | <p>Specifies the call presentation features. The supported values are.</p> <ul style="list-style-type: none">• 0x0000-Disable• 0x0001-Message_waiting_indication_splash_ring• 0x0002-Message_waiting_indication_special_dial_tone• 0x0004-Message_waiting_indication_visual_indication• 0x0008-Call_forwarding_indication  Note: You can select "0x0000-Disable" or multiple options of call presentation features. |
| Direct Connect | <p>Specifies the direct connect. The supported values are.</p> <ul style="list-style-type: none">• 0x00-Disable• 0x01-Direct_connect_feature_enabled• 0x02-Dial_tone_feature_delay_option  Note: You can select "0x00-Disable" or multiple options of direct connect features. |

| Field | Description |
|------------------------|---------------------------------------|
| Direct Connect URI | Specifies the direct connect URI. |
| Bridged Line URI | Specifies the bridge line URI. |
| Conference Factory URI | Specifies the conference factory URI. |

3. Click **Create**.

A new VoIP application service profile is created on the VoIP Application Service Profile page.

To edit, clone, and delete the VoIP application service profile configuration, see [Common Operations \(on page 27\)](#).

Settings

You can create and manage email notification, device template, Zero Touch Provisioning (ZTP), site group type, make, model, alarm severity, and RMS default settings.

Email Notification

To access this page, click **Configuration** from the top right corner of the page and select **Settings > Email Notification** from the left-hand side of the menu.

Configure an email notification to notify the users about the alarms reported in RMS. You can also specify the severity level of alarms, alarm type, and how frequently the alarms must be notified to the users.

Field Descriptions

The following table describes the fields on the Email Notification List page.

Table 284. Email Notification List

| Field | Description |
|---------------|---|
| Name | Specifies the name of the email notification. |
| Type | Specifies the type for which you want to generate the email notifications. |
| Recipients | Displays the recipients list. |
| Frequency | Specifies how frequently the email notifications must be sent to the users. |
| Severity | Specifies the severity of an alarm. |
| Alarm Status | Specifies the status of an alarm. |
| Creation Time | Specifies the date and time when the email notification was created. |
| Action | Specifies the action that you can perform on the email notification. The supported actions are. <ul style="list-style-type: none">• Edit• Clone• Delete |

Creating E-Mail Notification

Perform the following steps to create an email notification.

1. Select **Configuration > Settings > Email Notifications > Create**.
The Email Notification page appears.
2. Complete the email notification configuration according to the guidelines provided in the following table.

Table 285. Email Notification Configuration

| Field | Description |
|--------------|--|
| Name | Enter a unique name for the email notification. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-)• Space |
| Type | Select the type for which you want to generate the email notifications. The supported values are. <ul style="list-style-type: none">• ME• SITE GROUP• ME GROUP |
| Recipients | Enter one or more e-mail addresses of the users. |
| Frequency | Select the frequency that how often the email notifications must be sent to the distribution list. The supported values are. <ul style="list-style-type: none">• Immediate• Hourly• Daily |
| Severity | Select the severity of an alarm. The supported values are. <ul style="list-style-type: none">• Critical• Major• Minor• Indeterminate• Warning For example, email notifications are sent to the user as per the selected severity. If you have selected the value “Critical”, email notifications are sent to users only for alarms with the critical severity level. |
| Alarm Status | Select the status of an alarm. <ul style="list-style-type: none">• Open• Cleared• All |

| Field | Description |
|-------|---|
| | For example, if you have selected the value as “All”, email notifications are sent to users for alarms with status open, acknowledged, and cleared. |

3. Click **Create**.

A new email notification is created on the Email Notifications List page.



Note: You can delete an email notification configuration.

To edit, clone, and delete the Email notification configuration, see [Common Operations \(on page 27\)](#).

Make

To access this page, click **Configuration** from the top right corner of the page and then select **Settings > Make** from the left-hand side of the menu.

The make and model categorize managed elements. The make specifies the manufacturer of the managed element, for example, Iskratel, Hisene, Radisys, and so on.

The model specifies the product name, for example, Lumia_SI6000_ASXvOLT, and so on.

You can create a make for the managed elements such as OLT, ONT, CPE, splitter, card, rack, BNG, SFP, and cable.

The following Makes exist in RMS by default even after the RMS redeployment.

- Radisys

Field Descriptions

The following table describes the fields on the Make List page.

Table 286. Make List

| Field | Description |
|-------|--|
| Name | Specifies the name of the manufacturer. |
| OLT | Specifies whether the manufacturer supplies the OLT. <ul style="list-style-type: none">• Tick mark (✓). Specifies that the manufacturer supplies the OLT.• Cross mark (x). Specifies that the manufacturer does not supply the OLT. |
| ONT | Specifies whether the manufacturer supplies the ONT. <ul style="list-style-type: none">• Tick mark (✓). Specifies that the manufacturer supplies the ONT.• Cross mark (x). Specifies that the manufacturer does not supply the ONT. |

Table 286. Make List (continued)

| Field | Description |
|---------------|--|
| CPE | Specifies whether the manufacturer supplies the CPE. <ul style="list-style-type: none"> Tick mark (✓). Specifies that the manufacturer supplies the CPE. Cross mark (x). Specifies that the manufacturer does not supply the CPE. |
| BNG | Specifies whether the manufacturer supplies the BNG. <ul style="list-style-type: none"> Tick mark (✓). Specifies that the manufacturer supplies the BNG. Cross mark (x). Specifies that the manufacturer does not supply the BNG. |
| SPLITTER | Specifies whether the manufacturer supplies the splitter. <ul style="list-style-type: none"> Tick mark (✓). Specifies that the manufacturer supplies the splitter. Cross mark (x). Specifies that the manufacturer does not supply the splitter. |
| CARD | Specifies whether the manufacturer supplies the card. <ul style="list-style-type: none"> Tick mark (✓). Specifies that the manufacturer supplies the card. Cross mark (x). Specifies that the manufacturer does not supply the card. |
| RACK | Specifies whether the manufacturer supplies the rack. <ul style="list-style-type: none"> Tick mark (✓). Specifies that the manufacturer supplies the rack. Cross mark (x). Specifies that the manufacturer does not supply the rack. |
| SFP | Specifies whether the manufacturer supplies the SFP. <ul style="list-style-type: none"> Tick mark (✓). Specifies that the manufacturer supplies the SFP. Cross mark (x). Specifies that the manufacturer does not supply the SFP. |
| CABLE | Specifies whether the manufacturer supplies the cable. <ul style="list-style-type: none"> Tick mark (✓). Specifies that the manufacturer supplies the cable. Cross mark (x). Specifies that the manufacturer does not supply the cable. |
| Creation Time | Specifies the date and time when the make was created. |
| Action | Specifies the action that you can perform on the device model. The supported actions are. <ul style="list-style-type: none"> Edit Clone Delete |

Creating Make Configuration

You can create a make for the managed elements such as OLT, ONT, CPE, Splitter, Card, Rack, SFP, and Cable.

Perform the following steps to create a make for the managed element.

1. Select **Settings > Make > Create**.
The Make Configuration page appears.
2. Complete the service provider configuration according to the guidelines provided in the following table.

Table 287. Make Configuration

| Field | Description |
|----------|---|
| Name | <p>Enter a unique name of the manufacturer who supplied the managed element. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none">• Underscore (_)• Hyphen (-)• Space <p>Example: Rack</p> |
| OLT | <p>Specifies whether the specified manufacturer supplies the OLT. The supported values are.</p> <ul style="list-style-type: none">• Yes• No |
| ONT | <p>Specifies whether the specified manufacturer supplies the ONT. The supported values are.</p> <ul style="list-style-type: none">• Yes• No |
| CPE | <p>Specifies whether the specified manufacturer supplies the CPE. The supported values are.</p> <ul style="list-style-type: none">• Yes• No |
| SPLITTER | <p>Specifies whether the specified manufacturer supplies the splitter. The supported values are.</p> <ul style="list-style-type: none">• Yes• No |
| BNG | <p>Specifies whether the specified manufacturer supplies the BNG. The supported values are.</p> <ul style="list-style-type: none">• Yes• No |
| CARD | <p>Specifies whether the specified manufacturer supplies the card. The supported values are.</p> |

| Field | Description |
|-------|---|
| | <ul style="list-style-type: none">• Yes• No |
| RACK | Specifies whether the specified manufacturer supplies the rack. The supported values are. <ul style="list-style-type: none">• Yes• No |
| SFP | Specifies whether the specified manufacturer supplies the SFP. The supported values are. <ul style="list-style-type: none">• Yes• No |
| CABLE | Specifies whether the specified manufacturer supplies the cable. The supported values are. <ul style="list-style-type: none">• Yes• No |

3. Click **Create**.

A new make is created on the Make List page.



Note: You cannot modify the name of the manufacturer.

To edit, clone, and delete the make configuration, see [Common Operations \(on page 27\)](#).

Model

To access this page, click **Configuration** from the top right corner of the page and then select **Settings > Model** from the left-hand side of the menu.

Managed elements are categorized by the make and model. The model specifies the product name. For example, Lumia_SI6000.

You can create a model name for the managed elements such as OLT, ONT, CPE, splitter, BNG, card, rack, SFP, and cable.

The following models for the OLT exist in RMS by default even after the RMS redeployment.

- RLT-3200C (Part number of the OLT)
- RLT-1600X (Part number of the OLT)
- RLT-1600G (Part number of the OLT)
- RLT-1600C (Part number of the OLT)
- RLT-3200G (Part number of the OLT)

**Note:**

- RLT-1600G supports four NNI ports.
- RLT-1600X and RLT-1600C support six NNI ports.
- RLT-3200G supports ten NNI ports.
- RLT-3200C supports twelve NNI ports.
- The OLT supports GPON/XGS-PON board technology. The number of NNI ports depends on the platform variant rather than the OLT board technology. The user must select the RLT-1600X model while creating the OLT if the platform variant is GPON/XGS-PON.

The following device profiles exist in RMS even after the RMS redeployment. You create CARD configuration using the following device profiles with appropriate OLT models.

- RLT-3200C-Card
- RLT-1600C-Card
- RLT-1600G-Card
- RLT-3200G-Card
- RLT-1600X-Card

Field Descriptions

The following table describes the fields on the Model List page.

Table 288. Model List

| Field | Description |
|---------------|---|
| Name | Specifies the name of the device model. Example: Radisys-GPON-Rack |
| Device Type | Specifies the device type. Example: Rack |
| Make | Specifies the make name of the device. Example: Radisys |
| Total Device | Specifies the total number of devices of the particular manufacturer. Example: 4 |
| Action | Specifies the action that you can perform on the device model. The supported actions are. <ul style="list-style-type: none">• Edit• Clone• Delete |
| Creation Time | Specifies the date and time when the model configuration was created. |

Creating Model Configuration

You can create a model for the managed elements such as OLT, ONT, CPE, Splitter, Card, Rack, SFP, and Cable.



Note: Before you create a model for the managed element, you must create a make for the managed element. See [Creating Make Configuration \(on page 606\)](#).

You can create model configuration for the following resources.

- OLT
- ONT
- CPE
- BNG
- Splitter
- Card
- Rack
- SFP
- Cable

Perform the following steps to create a model configuration.

1. Select **Settings > Model > Create**.
The Model Configuration page appears.
2. Complete the model configuration according to the guidelines provided in the following table.

Table 289. Model Configuration

| Field | Description |
|-------|--|
| Name | Enter a unique name for the device model configuration. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-)• Space Example: Radisys-GPON-Rack |
| Type | Select the type of the device for which you want to create the model configuration. The supported types are. <ul style="list-style-type: none">• OLT• ONT• CPE |

| Field | Description |
|-------|---|
| | <ul style="list-style-type: none"> • SPLITTER • BNG • CARD • RACK • SFP • CABLE <p>Example: RACK</p> |
| Make | <p>Enter the make configuration for the device. If the make configuration does not exist, click the + icon to create a make configuration for the device. See Creating Make Configuration (on page 606).</p> <p>Example: Rack</p> |

3. Click **Create**.

A new device model is created on the Model List page.

To edit, clone, and delete the model configuration, see [Common Operations \(on page 27\)](#).

Model Version

To access this page, click **Configuration** from the top right corner of the page and then select **Settings > Model Version** from the left-hand side of the menu.

You can use this page to view the current software version of the device model and add the new version for the device model. You must specify this version when you upgrade the software of the device.

Field Descriptions

The following table describes the fields on the Model Version List page.

Table 290. Model Version List

| Field | Description |
|----------------|---|
| Device Type | Specifies the device type. |
| Make | Specifies the make name of the device. Example: Radisys |
| Model | Specifies the model name of the device. |
| Version | Specifies the software version of the device. |
| Image Location | Specifies the URL of the firmware image. Example: SFTP/HTTPS |

Table 290. Model Version List (continued)

| Field | Description |
|-----------------|---|
| Equipment ID | Specifies the equipment ID of the ONT. |
| CRC-32 Checksum | Specify the CRC value of the image. |
| Image Size | Specifies the image size in bytes. |
| MD 5 CheckSum | Specifies the checksum string to validate the integrity of the file. |
| Action | Specifies the action that you can perform on the device model. The supported actions are. <ul style="list-style-type: none"> • Edit • Clone • Delete |

Creating Model Version Configuration

You can create a model version for the managed elements such as OLT and ONT.



Note: Before you create a model version for the managed element, you must create a make for the managed element. See [Creating Make Configuration \(on page 606\)](#).

You can create model configuration for the following resources.

- OLT
- ONT

Perform the following steps to create a model version configuration.

1. Select **Settings > Model Version > Create**.
The Model Version Configuration page appears.
2. Complete the model configuration according to the guidelines provided in the following table.

Table 291. Model Version Configuration

| Field | Description |
|---------|---|
| Type | Select the type of the device for which you want to create the model version configuration. The supported types are. <ul style="list-style-type: none"> • OLT • ONT |
| Make ID | Select the make ID for the device. If the make configuration does not exist, see Creating Make Configuration (on page 606) . |

| Field | Description |
|--|--|
| Model ID | Select the model ID of the device. If the model configuration does not exist, see Creating Model Configuration (on page 610) . |
| Version | Enter the software version of the device. |
| Image Location | <p>Enter the image location where the new software version is stored.</p> <p>Example: If the image version is v10x and the image name is Rxxxx-B-TW R01B01xxxxxxxx.squashfs.upf, the image path is http://172.27.x.x/v10x/Rxxxx-B-TWR01B01xxxxxxxx.squashfs.upf, where 172.27.x.x is the web/HTTP server.</p> <p> Note:</p> <ul style="list-style-type: none"> • If the image location is web/HTTP server, the image must be placed in the <code>/var/www/html/<version>/<image name></code> directory. • If the image location is artifact repository server, the image must be placed in the <code>sftp://172.27.x.x/v10x/Rxxxx-B-TWR01B01xxxxxxxx.squashfs.upf</code>, where 172.27.x.x is the artifact repository server. • If the image location is artifact repository server, enter the artifact SFTP username and artifact SFTP password in the following path Configuration > Controller > Edit Controller Configuration > Settings > SDPON Settings. |
| If the device type is selected as ONT , the following fields are displayed. | |
| Equipment ID | Enter the equipment ID of the ONT. |
| Image Size (in bytes) | Enter the image size in bytes. |
| CRC-32 CheckSum | <p>Enter the checksum of the image (Crc-32). The supported length is 8 character. Example: ab217d9b</p> |
| If the device type is selected as OLT , the following fields are displayed. | |
| MD5-CheckSum | Enter the checksum string of the OLT file. |

3. Click **Create**.

A new model version is created on the Model Version List page.

To edit, clone, and delete the model version configuration, see [Common Operations \(on page 27\)](#).

ONT Firmware Information

To access this page, click **Configuration** from the top right corner of the page and then select **Settings > ONT Firmware Information** from the left-hand side of the menu.

You can use this page to view the global configuration table with the ONU make, model, and the firmware details such as firmware version, image URL, and image size.

Field Descriptions

The following table describes the fields on the ONT Firmware Information Table page.

Table 292. ONT Firmware Information Table

| Field | Description |
|--------------------------|---|
| Name | Specifies the ONT firmware name. |
| Version | Specifies the ONT firmware version. |
| Make | Specifies the make of the ONT. |
| Model | Specifies the model of the ONT. |
| Equipment ID | Specifies the equipment ID of the ONT. |
| Scheduled Upgrade | Specifies the scheduled upgrade day, time, and meridian. |
| Current Firmware Version | Specifies the current firmware version of the ONT. |
| Rule Enabled | Specifies whether the rule entry is enabled or disabled. |
| Creation Time | Specifies the date and time when the ONT firmware was created. |
| Action | Specifies the action that you can perform on the ONT firmware. The supported actions are. <ul style="list-style-type: none">• Edit• Clone• Delete |

Creating ONT Firmware Information

Perform the following steps to create ONT firmware information configuration.

1. Select **Settings > ONT Firmware Information > Create**.
The ONT Firmware Information Configuration page appears.
2. Complete the application configuration according to the guidelines provided in the following table.

Table 293. ONT Firmware Information Configuration

| Field | Description |
|--------------------------|--|
| Make | Select the make of the ONT. If the make configuration does not exist, see Creating Make Configuration (on page 606) . |
| Model | Select the model of the ONT. If the model configuration does not exist, see Creating Model Configuration (on page 610) . |
| Equipment ID | Select the equipment ID of the ONT. |
| Model Version | Select the ONT model version. For more details, see Creating Model Version Configuration (on page 612) . |
| Current Firmware Version | Enter the current firmware version of the ONT. The following fields are mandatory if the current firmware version field is configured. <ul style="list-style-type: none">• Make• Model• Equipment ID |
| Rule Enabled | Specifies whether the rule entry is enabled or disabled. The supported values are. <ul style="list-style-type: none">• True• False |
| Scheduled Upgrade | Specifies the time at which ONT firmware is upgraded automatically. |
| Day | Select the day in a week you want to set the automatic ONT firmware upgrade. The supported values are. <ul style="list-style-type: none">• Sunday• Monday• Tuesday• Wednesday• Thursday• Friday• Saturday |
| Time | Select the time that you want to set the automatic ONT firmware upgrade. The supported value ranges from 1 to 12. |
| Meridian | Specify the median at which you want to set the automatic ONT firmware upgrade. The supported values are. |

| Field | Description |
|-------|---|
| | <ul style="list-style-type: none">• AM• PM |

3. Click **Create**.

A new ONT Firmware Information is created on the ONT Firmware Information Table page.

To edit, clone, and delete the ONT firmware information configuration, see [Common Operations \(on page 27\)](#).

Alarm Severity

To access this page, click **Configuration** from the top right corner of the page and then select **Settings > Alarm Severity** from the left-hand side of the menu.

You can use this page to change the severity of the alarm reported to RMS. For example, if the controller reports some alarm with the severity level as CRITICAL, that can be changed to MAJOR using this page. RMS overrides the severity with the configured severity upon receiving the alarm from the controller.

Field Descriptions

The following table describes the fields on the Alarm Severity page.

Table 294. Alarm Severity

| Field | Description |
|------------|---|
| Alarm Name | Specifies the name of the alarm. |
| Severity | Specifies the severity level of an alarm. |
| Action | Specifies the action that you can perform on the alarm. The supported action is. <ul style="list-style-type: none">• Edit |

Editing Alarm Severity

You can edit the severity of the existing alarm.



Note: You cannot modify the name of the alarm.

Perform the following steps to modify the severity of an existing alarm.

1. Select **Settings > Alarm Severity**.

The Alarm Severity page appears.

2. Select the Edit Alarm Severity icon from the **Action** column.
The Alarm Severity Configuration page appears.
3. Select the severity from the Severity list.
4. Click **Save**.
The alarm is updated with the new severity level and the confirmation message is displayed.

File Storage

To access this page, click **Configuration** from the top right corner of the page and select **Settings > File Storage** from the left-hand side of the menu.

SSH File Transfer Protocol (SFTP) servers are used to upload the backup configuration and restore the backup configuration for the following functions.

- OLT software upgrade
- CBAC software upgrade
- OLT database backup and restore
- Controller database backup and restore
- RMS database backup and restore



Note: You can use different SFTP servers for backup and restore functions. This is optional.

Field Descriptions

The following table describes the fields on the File Storage page.

Table 295. File Store List

| Field | Description |
|---------------|---|
| Name | Specifies the name of the SFTP server. |
| SFTP Username | Specifies the username of the SFTP server. |
| SFTP Filepath | Specifies the file path of the SFTP server. |
| SFTP IP | Specifies the IP address of the SFTP server. |
| Port | Specifies the port number of the SFTP server. |
| Creation Time | Specifies the date and time when the SFTP server was created. |
| Action | Specifies the action that you can perform on the SFTP server. |

Creating File Store Configuration

Perform the following steps to create a file storage.

1. Select **Settings > File Storage > Create**.
The File Storage Configuration page appears.
2. Complete the application configuration according to the guidelines provided in the following table.

Table 296. File Store Configuration

| Field | Description |
|----------------|--|
| Name | Enter a unique name for the file storage. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-)• Space |
| Protocol | Select the protocol from the list. The supported value is SFTP. |
| SFTP Username | Enter a valid username for the SFTP server. |
| SFTP Password | Enter a valid password for the SFTP server. |
| SFTP File Path | Enter the SFTP file path where you want to save the backed-up configuration. Example: /home/sdponmp/  Note: If the SFTP server redundancy is implemented, <ul style="list-style-type: none">• The file path must be <i>/mnt/sftpstore/</i>.• The old backup files must be available on the SFTP server in the previous backup location (example, <i>/home/sdponmp/backup_file.zip</i>).• The old backup files are not maintained by Ceph unless manually copied to <i>/mnt/sftpstore/</i>. |
| SFTP IP | Enter the IP address of the SFTP server. Example: 172.27.173.132 |
| SFTP Port | Enter the port number for the SFTP server. Example: 22, 31840 |

3. Click **Create**.

A new file storage is created on the File Storage List page.

To edit, clone, and delete the file storage configuration, see [Common Operations \(on page 27\)](#).

Alarm Suppression

RMS allows to suppress the alarm of the RMS resources for the specified time interval or forever. This option is helpful in cases where the devices are under maintenance or some known issues exist with them. This feature prevents an indication of the alarm to the operators.

You can suppress the alarms reported for the particular managed element, particular port (NNI, PON, or Alarm), and the ME group.

Tasks

You can perform the following tasks using this page.



Note: To display all the columns on the page, click the **Restore to Default Settings** option.

- Create an alarm suppression configuration. See [Creating Alarm Suppression Configuration \(on page 620\)](#).
- Edit, delete, and monitor an alarm suppression. See [Editing, Deleting, and Monitoring Alarm Suppression Configuration \(on page 622\)](#).

Field Descriptions

The following table describes the fields on the Alarm Suppression page.

Table 297. Alarm Suppression List

| Field | Description |
|-------------|--|
| Name | Specifies the name of the alarm suppression. |
| Type | Specifies the type of the resource. |
| Device Type | Specifies the device type. |
| Device | Specifies the device name. |
| Fault | Specifies the list of faults that are suppressed for the particular resource. |
| Start Time | Specifies the date from when the alarm suppression starts for the device. |
| End Time | Specifies the date when the alarm suppression ends for the device. |
| Forever | Displays the following symbols. <ul style="list-style-type: none">• Tick mark (✓). If the alarm suppression is created forever. |

Table 297. Alarm Suppression List (continued)

| Field | Description |
|---------------|---|
| Creation Time | Specifies the date and time when the alarm suppression was created. |
| Action | Specifies the action that you can perform on the subscriber. The supported actions are. <ul style="list-style-type: none"> • Edit • Delete • Monitor |

Creating Alarm Suppression Configuration

Perform the following steps to create an alarm suppression.

1. Select **Settings > Alarm Suppression > Create**.
The Alarm Suppression Configuration page appears.
2. Complete the application configuration according to the guidelines provided in the following table.

Table 298. Alarm Suppression Configuration

| Field | Description |
|--|--|
| Name | Enter a unique name for the alarm suppression. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) • Space |
| Type | Select the resource type for which you want to suppress the alarms. The supported types are. <ul style="list-style-type: none"> • ME • ME PORT • ME GROUP • CONTROLLER Example: OLT |
| If the type is selected as ME , the following fields are displayed. | |
| Device Type | Select the device type for which you want to suppress the alarms. Example: OLT |
| Device | Enter the name of the device. |

| Field | Description |
|--|--|
| | Example: olt-136 |
| Fault | Select one or more faults you want to block for the particular device. The list displays the faults related to OLT, ONT, port, and LAG. If you select the “All” option, all the faults reported for the device are blocked.  Note: Fault is not a mandatory field. If the fault value is not selected, all the faults for the selected device and device type are suppressed. |
| If the type is selected as ME Port , the following fields are displayed. | |
| Parent Device | Enter the parent device name of the port. |
| Port | Select the PON, NNI, or Alarm ports from the list. |
| Fault | Select one or more faults that you want to block for the particular port. The list displays the faults related to the ME port. If you select the “All” option, all the faults reported for the port are blocked.  Note: Fault is not a mandatory field. If the fault value is not selected, all the faults for the selected parent device and port are suppressed. |
| If the type is selected as ME Group , the following fields are displayed. | |
| ME Group | Select the ME group from the list. |
| Fault | Select one or more faults that you want to block for the particular ME group. The list displays the faults related to the ME group. If you select the “All” option, all the faults reported for the ME group are blocked.  Note: Fault is not a mandatory field. If the fault value is not selected, all the faults related to ME group are suppressed. |
| If the type is selected as CONTROLLER , the following fields are displayed. | |
| Device | Select the device name from the list. |
| Fault | Select one or more faults that you want to block for the particular device. The list displays the faults related to the controller. If you select the “All” option, all the faults reported for the device are blocked. |

| Field | Description |
|---------|---|
| |  Note: Fault is not a mandatory field. If the fault value is not selected, all the faults for the selected device are suppressed. |
| Forever | Select this option if you want to suppress the alarms of the particular resource forever. |

3. Click **Create**.

A new alarm suppression is created on the Alarm Suppression List page.

Editing, Deleting, and Monitoring Alarm Suppression Configuration

You can modify the parameters configured for the alarm suppression.

Perform the following steps to modify the alarm suppression configuration.

1. Select **Settings > Alarm Suppression**.

The Alarm Suppression List page appears.

2. Select the Edit icon from the **Action** column.

The Alarm Suppression Configuration page appears.

3. Modify the parameters as needed.

4. Click **Save** to save the changes.

A confirmation message appears, indicating the status of the edit operation.

Perform the following steps to delete the alarm suppression configuration.

1. Select **Settings > Alarm Suppression**.

The Alarm Suppression List page appears.

2. Click the Delete icon from the **Action** column.

An alert message appears, asking you to confirm the delete operation.

3. Click **Confirm** to delete the configuration.

A confirmation message appears, indicating the status of the delete operation.

Perform the following steps to monitor the alarm suppression configuration.

1. Select **Settings > Alarm Suppression**.

The Alarm Suppression List page appears.

2. Select the monitor icon from the **Action** column.

The Alarm Suppression Details page appears.

3. You can monitor the basic alarm information.

Others

To access this page, click **Configuration** from the top right corner and then select **Settings > Others** from the left-hand side of the menu.

RMS default settings include RMS time zone, data retention days for audit logs, alarm data, event data, and activity logs. You can also configure event settings, user settings, and threshold value settings for current alarm table records, events table records, historic alarms table records, device table records, email settings, and re-branding.

Field Descriptions

The following table describes the fields on the Others page.

Table 299. Others

| Field | Description |
|------------------------------|---|
| Timezone and API Keys | |
| Time Zone | Specifies the time zone for the RMS environment. |
| Google API Key | Enter the google map license key. |
| Authentication | |
| Authentication Type | Specifies the type of the authentication. The supported authentication types are: <ul style="list-style-type: none">• Local. User accounts are maintained locally in the RMS database, and users are authenticated and authorized by RMS.• TACACS. RMS users are authenticated through a configured TACACS server. If the TACACS server becomes unreachable, the authentication is performed using the local authentication. |
| TACACS | |
| Enable Accounting | Specifies whether TACACS accounting on RMS is enabled or disabled. Enable this option to push the RMS accounting (audit) logs to the configured TACACS host. This option is disabled by default. |
| Servers | |

Table 299. Others (continued)

| Field | Description |
|------------|---|
| Host | Specifies the IP address or Fully Qualified Domain Name (FQDN) of the TACACS server. |
| Port | Specifies the port number of the TACACS server, which is exposed to access the server-client communication. The default value is 49. The supported value ranges from 0 to 65,535. |
| Secret key | Specifies the secret key, which is used to encrypt the payload. The maximum length of the secret key must not exceed 64 characters. |

Data Retention



Note: Data purge for all the items mentioned in the **Data Retention** page is triggered by a scheduled job. **Data Purge Frequency** and **Data Purge Interval** fields define the schedule of this job.

| | |
|---------------------------|--|
| Audit Log (days) | Enter the number of days to retain the audit logs. The audits logs are purged after the specified number of days. The default value is 180 days. |
| KPI Data (days) | Enter the number of days to retain the KPIs. The KPIs are purged after the specified number of days. The default value is 5 days. |
| Event Data (days) | Enter the number of days to retain the events. The events are purged after the specified number of days. The default value is 180 days. |
| Activity Log (days) | Enter the number of days to retain the activity logs. The activity logs are purged after the specified number of days. The default value is 180 days. |
| Current Fault Data (days) | Enter the number of days to retain the current alarms. The current alarms are purged after the specified number of days. The default value is 180 days. |
| Cleared Fault Data (days) | Enter the number of days to retain the cleared alarms. The cleared alarms are purged after the specified number of days. The default value is 180 days. |

Table 299. Others (continued)

| Field | Description |
|-------------------------|--|
| |  Note: It is recommended to select Cleared Fault Data as 14 days to retain the cleared alarms in the RMS database. |
| PM KPI Files (days) | Select the checkbox if you want to purge the KPI performance files after a specified number of days. Enter the number of days to retain the KPI performance related files in the SFTP server. The default value is 180 days. |
| DB Backup Files (days) | Select the checkbox if you want to purge the RMS backup files after a specified number of days. Enter the number of days to retain the RMS backup files in the SFTP server. The default value is 180 days. |
| OLT Backup Files (days) | Select the checkbox if you want to purge the OLT backup files after the specified number of days. Enter the number of days to retain the OLT backup files in the SFTP server. The default value is 180 days. |
| Data Purge Frequency | Select the periodicity for data (audit logs, alarms, events, and health card information) purge from the list. You can either specify the value in hours or minutes. The default value is Hour. |
| Data Purge Interval | Select the data purge interval. For example, if you specified a periodicity in hours, enter the number of hours after which the purge must recur. |
| Auto Discovery | |
| Kafka Username | Enter the kafka username. |
| Kafka Password | Enter the kafka password. |
| Kafka Port | Enter the Kafka port number for the CBAC controller. |
| REST Port | Enter the REST server port number. |
| Log Server | Enter the log server for the controller. |
| Enable OLT Blacklisting | Select this option to blacklist the OLT. Blacklisted OLT appears on the Monitor > Inventory > Blacklisted ME > OLT page. By default, this option is disabled. |
| Event | |

Table 299. Others (continued)

| Field | Description |
|--|---|
| Discovered data Precedence | <p>Enable this option to specify that the discovered data information has higher precedence over the configured information.</p> <ul style="list-style-type: none"> • Enable. Indicates that the discovered data takes precedence over the configured data for events. The configured data is overridden/ignored in specific cases. • Disable. Indicates that the configured data takes higher precedence. By default, this option is disabled. |
| Auto Upgrade Controller | Enable this option if you want to upgrade software of the controller. If this option is enabled, the software upgrade of the controller triggers automatically. The software upgrade is triggered upon receiving the new software version available in the notification. |
| Fault | |
| Alarm Summary Update Frequency | <p>Select the frequency that how often the fault summary must be updated. The supported values are.</p> <ul style="list-style-type: none"> • HOUR • MINUTE |
| Alarm Summary Update Interval | Enter the update interval for the fault summary. |
| User Accounts | |
| Third Party Account Expiry Duration (days) | Enter the expiry duration (in days) for third-party user accounts. The default value is 180 days. |
| Deactivate Account (days) | Enter the duration (in days) to deactivate the user accounts. The default value is 60 days. |
| User Session Duration (minutes) | <p>Enter the lock out time duration (in minutes) for user accounts. This feature prevents unauthorized users from accessing the RMS application. The default value is 10 minutes. This can be set for all the user accounts except the admin and the superuser.</p> <p> Note: Only the security administrator can configure and modify this value.</p> |
| Allow Multiple Sessions | Select this option to allow users to open multiple RMS sessions. By default, this check box is selected, and the user is allowed to open multiple sessions. |

Table 299. Others (continued)

| Field | Description |
|-------------------------------------|--|
| New User Inactivity Duration (days) | Enter the probation period (in days) for the new user. A new user has to login to the RMS application within this time. Otherwise, the user account is deactivated. |
| Threshold | You can configure the threshold value to display the alarms, events, devices in the table. |
| Current Alarms - Maximum size | Enter the threshold value to display the number of faults in the current fault table. The CURRENT-ALARM-TABLE-SIZE-EXCEEDED alarm is raised when the configured threshold value is reached. The default value is 1000000. |
| Cleared Alarms - Maximum size | Enter the threshold value to display the number of faults in the historic alarm table. The HISTORICAL-ALARM-TABLE-SIZE-EXCEEDED alarm is raised when the configured threshold value is reached. The default value is 1000000. |
| Events - Maximum size | Enter the threshold value to display the number of events in the event table. The EVENT-TABLE-SIZE-EXCEEDED alarm is raised when the configured threshold value is reached. The default value is 1000000. |
| Devices - Maximum size | Enter the threshold value to display the number of devices in the event table. The INVENTORY-TABLE-SIZE-EXCEEDED alarm is raised when the configured threshold value is reached. The default value is 1000000. |
| Email | RMS allows you to configure e-mail alerts to receive notifications on any activities in your network. The send email feature uses the mail server settings configured as the default setting for email alerts across RMS. After you log in to the RMS application, configure an Simple Mail Transfer Protocol (SMTP) e-mail server. The SMTP server is the local server that forwards your e-mail to the destination server. |
| SMTP Server | Enter the hostname for the SMTP server. |
| SMTP Port | Enter the port number for the SMTP server. |
| SMTP Username | Enter a valid username for the SMTP server. |
| SMTP Password | Enter a password for the SMTP server. |
| Admin Email Address | Enter a valid e-mail address for the admin user. If the Admin Email Address is configured, the e-mail is sent (Admin Email Address in CC) to the user accounts when the following operations are performed in RMS. |

Table 299. Others (continued)

| Field | Description |
|---------------------|--|
| | <ul style="list-style-type: none"> • Account deactivated • Account deleted • Account locked • Account expired • Password expired • Password about to expire recurring mail |
| Enable START TLS | Enable Transport Layer Security (TLS) protocol to ensure that the e-mail messages are transmitted over an encrypted channel. |
| Enable SSL | Enable the Secure Sockets Layer (SSL) protocol to ensure that the e-mail messages are transmitted over an encrypted channel. |
| Rebranding | You can use this option to re-brand the application settings. |
| Product Name | Enter the application name that appears on the top-left corner of the application. Example: RMS |
| Short Name | Enter the short name of the application that appears on the left-side menu breadcrumb. Example: RMS |
| Copyright | Enter the copyright information that appears on the left-below of the application. |
| Copyright URL | Enter the copyright URL to which the user needs to be taken to view the copyright information. |
| Application Favicon | <p>Upload an image for the favicon that appears on the browser when the user opens the application.</p> <p>The supported image extension is .ico, and the image size must be less than 16000 KB.</p> |
| Application Logo | <p>Upload an image for the logo that appears on the top-left corner of the application.</p> <p>The application logo supports all image extensions except .ico, and the image size must be less than 16000 KB.</p> |
| System Logs | |
| Server | Enter the hostname for the syslog server. |
| Port | Enter the port number for the syslog server. |
| Protocol | <p>Select the syslog protocol. The supported value is.</p> <ul style="list-style-type: none"> • UDP |

Table 299. Others (continued)

| Field | Description |
|-----------------------------|--|
| Backup Configuration | |
| Name | <p>Select one or more data that you want to include in the RMS backup configuration. The supported values are.</p> <ul style="list-style-type: none"> • Config • KPI • Audit Log • Event Data • Cleared Faults • Open Faults • Mac Dump • Activity Log <p>By default, only the Config data is selected.</p> <p>If the user selects the other options, the following warning messages appears.</p> <p> Warning: This impacts backup time and size of backup and other mongo DB operations running in parallel.</p> |

Filter Expression

To access this page, click **Configuration** from the top right corner of the page and select **Settings > Filter Expression** from the left-hand side of the menu.

Create a filter expression with the severity criteria (warning, minor, major, critical, and indeterminate). The filter expression is used in the forwarding policy. See [Forwarding Policy \(on page 631\)](#).

Field Descriptions

The following table describes the fields on the Filter Expression page.

Table 300. Filter Expression

| Field | Description |
|------------|--|
| Name | Specifies the name of the filter expression. |
| Field Name | Specifies the field name. |

Table 300. Filter Expression (continued)

| Field | Description |
|---------------|--|
| Field Value | Specifies the field value. |
| Creation Time | Specifies the date and time when the filter expression was created. |
| Action | Specifies the action that you can perform on the filter expression. The supported actions are. <ul style="list-style-type: none"> Clone Delete |

Creating Filter Expression

Perform the following steps to create a filter expression.

1. Select **Settings > Filter Expression > Create**.
The Filter Expression page appears.
2. Complete the filter expression configuration according to the guidelines provided in the following table.

Table 301. Filter Expression Configuration

| Field | Description |
|-------------|--|
| Name | Enter a unique name for the filter expression. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> Underscore (_) Hyphen (-) Space |
| Field Name | Select the field name. The supported value is severity. |
| Field Value | Select the field value. You can select one or more values. The supported values are. <ul style="list-style-type: none"> Critical Major Minor Indeterminate Warning |

3. Click **Create**.
A new filter expression is created on the Filter Expression page.

To clone and delete the filter expression configuration, see [Common Operations \(on page 27\)](#).

Forwarding Policy

To access this page, click **Configuration** from the top right corner of the page and select **Settings > Forwarding Policy** from the left-hand side of the menu.

A forwarding policy is added with filter expression to create filter criteria for the Java Message Service (JMS) queue. A new JMS topic is created once the forwarding policy is configured. Alarms are sent to different topics as per the severity filter criteria. The Northbound Alarm Service (NAS) application publishes the alarms, and the operator retrieves the alarms.

Field Descriptions

The following table describes the fields on the Forward Policy page.

Table 302. Forward Policy

| Field | Description |
|-----------------|--|
| Name | Specifies the name of the forward policy. |
| Forwarding Type | Specifies the forwarding type. The default value is JMS. |
| Topic Name | Specifies the topic name. |
| Creation Time | Specifies the date and time when the forward policy was created. |
| Action | Specifies the action that you can perform on the forward policy. The supported actions are. <ul style="list-style-type: none">CloneDelete |

Creating Forwarding Policy

Before you create a forwarding policy, you must create a filter expression. See [Creating Filter Expression \(on page 630\)](#).

Perform the following steps to create a forwarding policy.

1. Select **Settings > Forwarding Policy > Create**.
The Forward Policy page appears.
2. Complete the forward policy configuration according to the guidelines provided in the following table.

Table 303. Forwarding Policy Configuration

| Field | Description |
|-----------------|---|
| Name | Enter a unique name for the forward policy. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-)• Space |
| Forwarding Type | Specifies the forwarding type. The supported value is JMS. |
| Topic Name | Specifies the topic name. |
| Filters | Specifies the filter name. |

3. Click **Create**.

A new forward policy is created on the Forward Policy page.

To clone and delete the forward policy configuration, see [Common Operations \(on page 27\)](#).

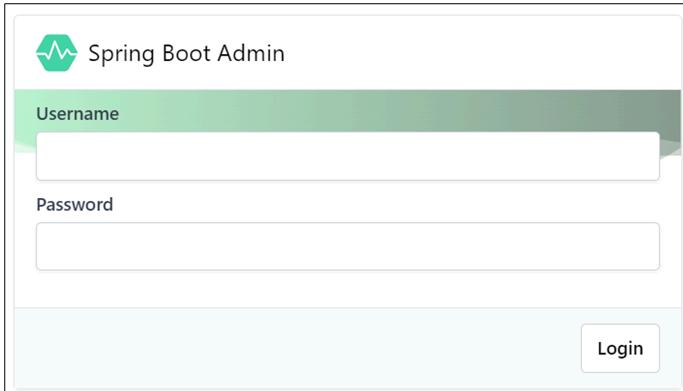
Logging Configuration

To access this page, click **Configuration** from the top right corner of the page and select **Settings > Logging Configuration** from the left-hand side of the menu.

Using the **Sprint Boot Admin** application, users can change the log level of any microservice at the class and package levels. The default log level is **Debug**.

1. Click on the **Logging Configuration Web Application**.

The Spring Boot Admin (SBA) application login page appears.

Figure 98. SPA Login

The screenshot shows the login interface for the Spring Boot Admin application. At the top left is a green circular icon with a white line graph. To its right, the text "Spring Boot Admin" is displayed. Below this is a horizontal input field with a green header labeled "Username". Underneath is another horizontal input field with a green header labeled "Password". At the bottom right of the form is a rectangular "Login" button.

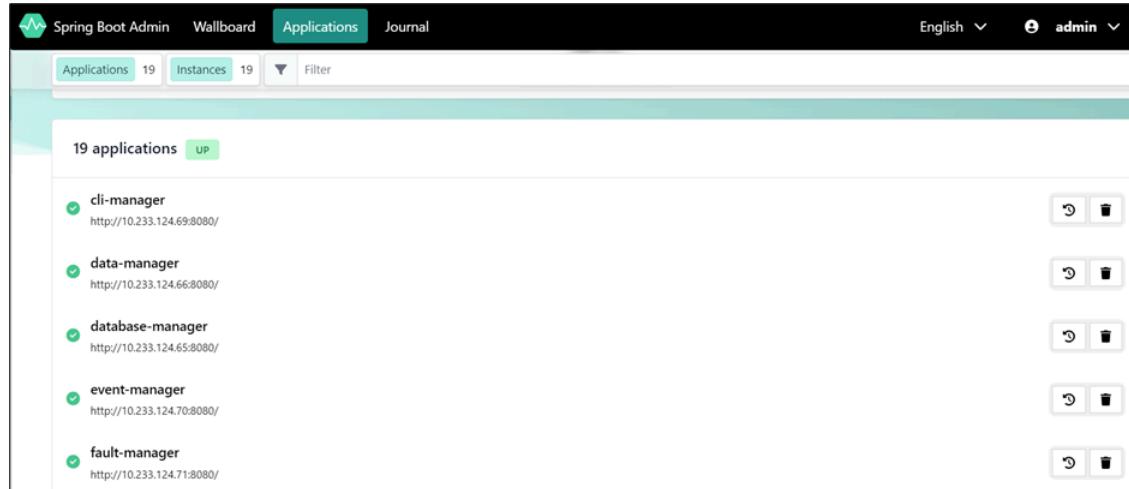
2. Log into the SPA application.

The default username and password are **admin/ADmin@123**.

3. Click **Login**.

The **Sprint Boot Admin** page appears with the list of RMS microservices.

Figure 99. SPA Page



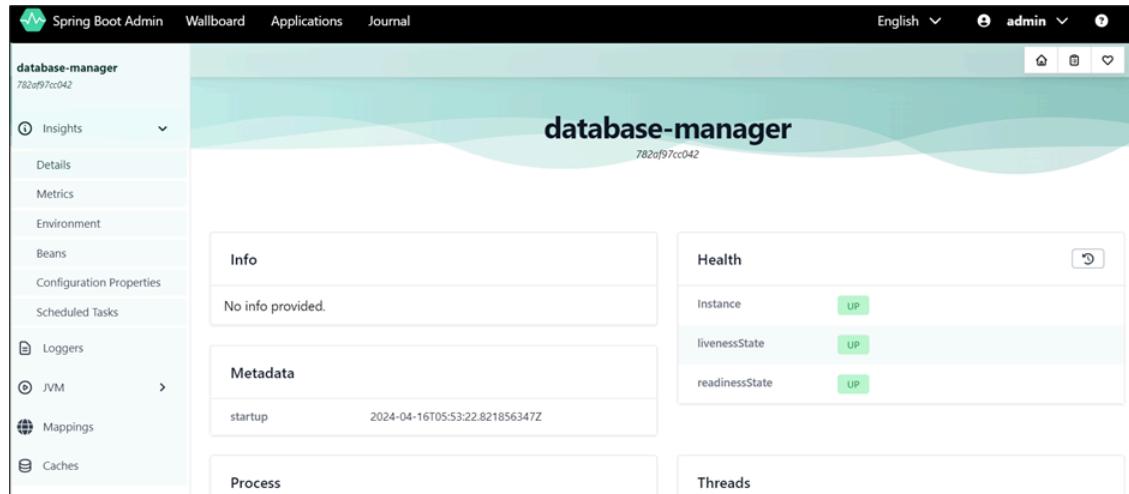
19 applications **UP**

- cli-manager
http://10.233.124.69:8080/
- data-manager
http://10.233.124.66:8080/
- database-manager
http://10.233.124.65:8080/
- event-manager
http://10.233.124.70:8080/
- fault-manager
http://10.233.124.71:8080/

4. Double-click on the check box icon of any microservice.

The microservice details page appears.

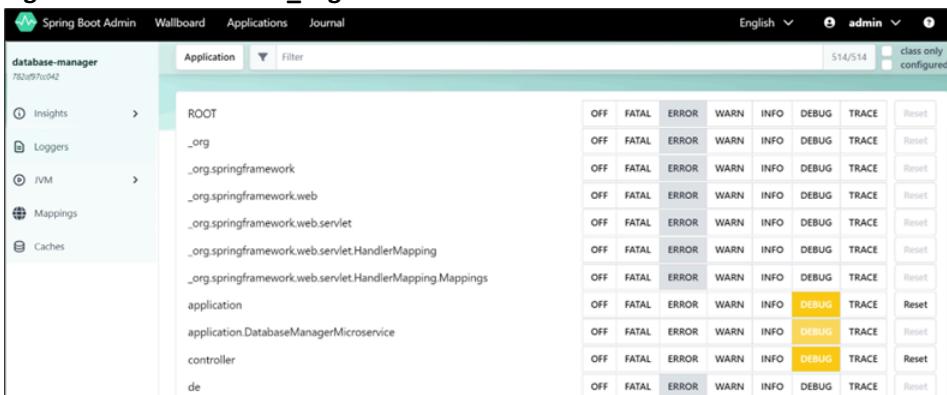
Figure 100. Details of Microservice



5. Click **Loggers** from the left pane.

The list of microservices with log levels is displayed, and the log level is set for each microservice.

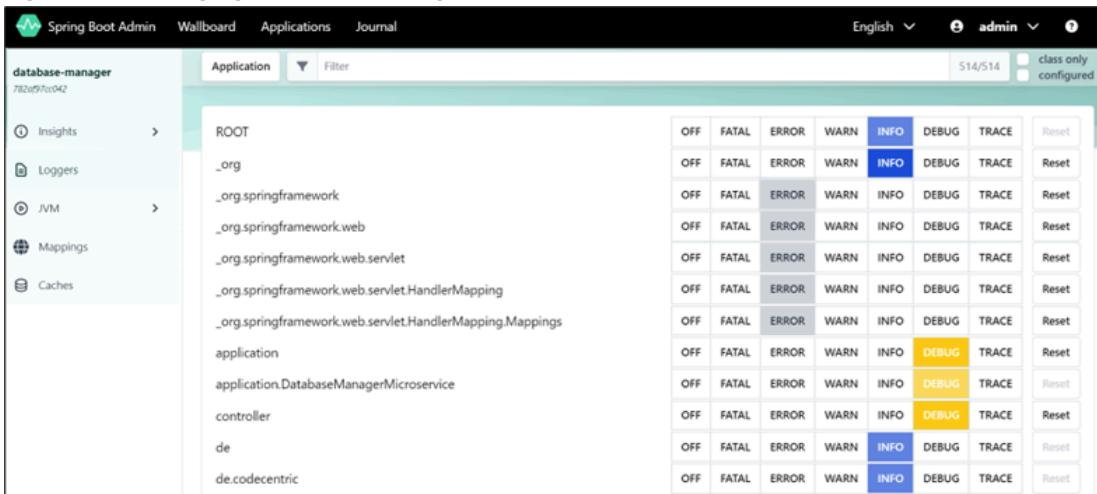
6. To change the log level for any microservices, click on the microservice's log level you want to set. For example, the log levels for **ROOT** and **_org** are set to **ERROR** in the following figure.

Figure 101. Microservice_Log Level

The screenshot shows the Spring Boot Admin interface for the 'database-manager' application. The left sidebar includes 'Insights', 'Loggers', 'JVM', 'Mappings', and 'Caches'. The 'Loggers' section is expanded, showing a tree structure with 'ROOT', '_org', and several Spring framework sub-components like '_org.springframework.web' and '_org.springframework.web.servlet'. The log level configuration table on the right shows the following settings:

| | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
|--|-----|-------|-------|------|------|-------|-------|
| ROOT | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| _org | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| _org.springframework | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| _org.springframework.web | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| _org.springframework.web.servlet | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| _org.springframework.web.servlet.HandlerMapping | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| _org.springframework.web.servlet.HandlerMapping.Mappings | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| application | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| application.DatabaseManagerMicroservice | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| controller | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| de | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |

7. If you want to change the log level for **ROOT** and **_org** to **INFO**, click on **INFO**, and the log level is changed to **INFO**, as shown in the figure below.

Figure 102. Changing Microservice Log Level

The screenshot shows the Spring Boot Admin interface for the 'database-manager' application. The left sidebar includes 'Insights', 'Loggers', 'JVM', 'Mappings', and 'Caches'. The 'Loggers' section is expanded, showing a tree structure with 'ROOT', '_org', and several Spring framework sub-components like '_org.springframework.web' and '_org.springframework.web.servlet'. The log level configuration table on the right shows the following settings:

| | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
|--|-----|-------|-------|------|------|-------|-------|
| ROOT | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| _org | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| _org.springframework | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| _org.springframework.web | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| _org.springframework.web.servlet | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| _org.springframework.web.servlet.HandlerMapping | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| _org.springframework.web.servlet.HandlerMapping.Mappings | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| application | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| application.DatabaseManagerMicroservice | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| controller | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| de | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |
| de.codecentric | OFF | FATAL | ERROR | WARN | INFO | DEBUG | TRACE |

Protection

Type-B Protection Pair

To access this page, click **Configuration** from the top right corner of the page and select **Protection > Type-B Protection Pair** from the left-hand side of the menu.

- Single Shelf
- Cross Shelf

Single Shelf Protection Pair

Single shelf type B protection protects a PON interface on the same shelf. Only PON interface failures are protected since the OLT is not a modular chassis and has all the PON interfaces on a single pizza box. PON interface failures include failures between the active PON and primary splitter and PON SFP failures.

- CBAC and OLT support the type B 1:1 PON protection on the same ODN connected to two different PON ports of an OLT using a 2:N splitter. The PON protection protects the connectivity of the subscribers to the network in the event of failures in the ODN.
- CBAC and OLT support fast and reliable real-time mirroring of the ONU configuration data and transient (run-time) data between the active and standby ports to enable quick switchover during the failure of an active port.
- CBAC supports automatic switchover for the type-B protection pair when the active port goes DOWN.
- CBAC and OLT also support type-B protection manual or forced switchover to carry out the planned maintenance activity and control outages.

RMS allows creating Type B protection pair only when both primary and secondary PON ports are configured, and the ports admin state is “DISABLED”.

RMS denies the type-B protection pair creation for the following scenarios.

- If the primary or the secondary PON port is not configured
- If the primary or the secondary PON port admin state is ENABLED
- If the “Create PON protection pair” request is invalid with the missing attributes
- If the primary or the secondary PON port is already part of an existing type-B protection pair
- If the ONTs are already added to the designated secondary port

Cross Shelf Protection Pair

Cross shelf type B protection protects a PON interface across two different shelves at two different sites. Cross shelf type B protects PON interface failure, OLT isolation (if both east and west NNI interfaces go down), OLT restart, and OLT failure.

CBAC supports the dual homing PON protection on the same ODN connected to two PON ports from two different OLTs, that are served by two different CBAC controllers using a 2:N splitter. The dual homing PON protection protects the connectivity of the subscribers to the network in the event of failures in the ODN, such as PON interface failure, OLT isolation, OLT restart, and OLT failure.

Adding type-B protection to an existing PON port with active subscribers does not affect the services on the PON port. The newly added secondary PON port to the type-B protection group must be in a deactivated or disabled state without any subscriber configuration.



Note: This is applicable only to type-B dual-homing protection.

RMS performs the configuration procedures on the CBAC controller serving as the primary PON port (For example, CBAC-A) and consumes the alarms, events, and KPIs from either of the CBAC controllers. The messages contain a unique northbound message ID for ONU and service.

The CBAC-A (primary PON port) performs the mirroring of the configuration data (ONU provisioning, subscriber, and services provisioning) towards CBAC-B (secondary PON port).

- Dual homing PON protection on two PON ports of two different OLTs served by two different CBAC controllers, using a 2:N splitter.
- The CBAC controller serving the active-working port mirrors the following transient data (run-time) data between the active and standby controller to enable quick switchover during the failure of an active controller.
 - ONU context updates (ONU_ID, UNI ports, and MIB data)
 - ONU operational state changes, ONU alarms, AES key, registration ID, ONU ranging time, password, and ITU-T key updates
 - Alloc_ID and GEM port provisioning
 - DHCP and IGMP updates
- CBAC supports automatic switchover for dual home protection when the active port's operation status is DOWN.
- CBAC supports dual home protection manual or forced switchover to carry out the planned maintenance activity and control outages.

Field Descriptions

The following table describes the fields on the Type-B Protection Pair List page.

Table 304. Type B-Protection Pair List

| Field | Description |
|---------------------|---|
| SINGLE SHELF | |
| Name | Specifies the unique name of the protection pair. |
| OLT | Specifies the name of the OLT. |

Table 304. Type B-Protection Pair List (continued)

| Field | Description |
|---|--|
| Primary Port | Specifies the primary port of the protection pair. |
| Primary Port Protection State | Specifies the primary port protection state. Example: ACTIVE-WORKING |
| Primary Port Protection Operational State | Specifies the operational state of primary port protection. |
| Secondary Port | Specifies the secondary port of the protection pair. |
| Secondary Port Protection State | Specifies the secondary port protection state. Example: ACTIVE-STANDBY |
| Secondary Port Protection Operational State | Specifies the operational state of secondary port protection. |
| Creation Time | Specifies the date and time when the single shelf type-B protection pair was created. |
| Action | Specifies the action performed on the single shelf protection pair. <ul style="list-style-type: none"> • Create • Delete |
| CROSS SHELF | |
| Primary | |
| Name | Specifies the name of the cross shelf protection pair. |
| OLT | Specifies the name of the primary OLT. |
| Port | Specifies the primary port. |
| Port Protection State | Specifies the state of the primary port. |
| Primary Port Protection Operational State | Specifies the operational state of primary port protection. |
| Secondary | |
| OLT | Specifies the name of the secondary OLT. |
| Port | Specifies the secondary port. |
| Port Protection State | Specifies the state of the secondary port. |

Table 304. Type B-Protection Pair List (continued)

| Field | Description |
|---|---|
| Secondary Port Protection Operational State | Specifies the operational state of secondary port protection. |
| Creation Time | Specifies the date and time when the cross shelf type-B protection pair was created. |
| Action | Specifies the action performed on the cross shelf protection pair. <ul style="list-style-type: none"> • Create • Delete |

Creating Type-B Protection Pair

You can create a type-B protection pair for both single and cross shelf.

- When a single shelf protection pair is created, the protection state of the primary PON port is “ACTIVE-WORKING” (after activation), and the protection state of the secondary PON port is “ACTIVE-STANDBY”.
- When a cross shelf protection pair is created, the protection state of the primary OLT is “ACTIVE-WORKING” (after activation), and the protection state of the secondary OLT is “ACTIVE-STANDBY”.

Perform the following steps to create a type-B protection pair.

1. Select **Configuration > Protection > Type-B Protection**.
The Type-B Protection Pair List page appears.
2. Select **SINGLE SHELF** or **CROSS SHELF** tab.
3. Click **Create**.
The Type-B Single Shelf Configuration/Type-B Cross Shelf Configuration page appears.
4. Complete the template configuration according to the guidelines provided in the following table.

Table 305. Creating Type-B Configuration

| Field | Description |
|---------------------|---|
| SINGLE SHELF | |
| Name | Enter a unique name for the single shelf protection pair. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) • Space |

| Field | Description |
|------------------------|--|
| Protection Type | Displays the protection type as SINGLE SHELF. |
| Revertive Mode Timeout | <p>Specifies the revertive mode timeout value in minutes. The default value is 0.</p> <p>The absence of this parameter or if the value is set to 0, signifies that the revertive mode is disabled. RMS displays the revertive mode as disabled in the configuration page.</p> <p>The value ranges from 0 to 128.</p> |
| OLT | <p>Enter the OLT name, whose PON ports are associated in the PON protection pair.</p> <p> Note: You must activate the OLT before you add the OLT in the protection pair.</p> |
| Primary Port | <p>Select the primary port, which is associated with the PON protection pair.</p> <p> Note: You must activate the primary PON port after the creation of the protection pair.</p> |
| Secondary Port | Select the secondary port, which is associated with the PON protection pair. |
| CROSS SHELF | |
| Name | <p>Enter a unique name for the cross shelf protection pair. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> Underscore (_) Hyphen (-) Space |
| Protection Type | Displays the protection type as CROSS SHELF. |
| Revertive Mode Timeout | <p>Specifies the revertive mode timeout value in minutes. The default value is 0.</p> <p>The absence of this parameter or if the value is set to 0, signifies that the revertive mode is disabled. RMS displays the revertive mode as disabled in the configuration page.</p> <p>The value ranges from 0 to 128.</p> |

| Field | Description |
|----------------|---|
| Primary OLT | Enter the primary OLT name, whose PON port is associated in the PON protection pair. |
| Primary Port | Select the primary PON port, which is associated with the PON protection pair.  Note: Both enabled and disabled PON ports are displayed in the list. |
| Secondary OLT | Enter the secondary OLT name, whose PON port is associated in the PON protection pair. |
| Secondary Port | Select the secondary PON port, which is associated with the PON protection pair.  Note: Only disabled PON ports are displayed in the list. |

5. Click **Create**.

A new type-B protection pair is created on the Type-B Protection Pair List page.

Deleting Type-B Protection Pair

You can delete the type-B protection pair only when the primary PON port admin state is “DEACTIVE” and associated ONTs are deleted.

Perform the following steps to delete a type-B protection pair.

1. Select **Configuration > Protection > Type-B Protection Pair**.
The Type-B Protection Pair List page appears.
2. Click the Delete icon from the **Action** column.
An alert message appears, asking you to confirm the delete operation.
3. Click **Confirm** to delete the protection pair.
A confirmation message appears, indicating the status of the delete operation.

Manual Switchover

RMS supports the manual switchover operation on the type-B protection pair. To carry out the planned maintenance activity and control outage, an operator can manually switch traffic from an active PON port to the standby PON port.

Perform the following steps for the manual switchover.

1. Select **Configuration > Protection > Type-B Protection Pair**.

The Type-B Protection Pair List page appears.

2. Click on the three dots () corresponding to the protection pair that you want to perform the manual switchover and click the **Manual/Force Switchover** option.

The protection state of the primary PON port changes to “ACTIVE-STANDBY” and the protection state of the secondary PON port changes to “ACTIVE-WORKING”.

Auto Switchover

OLT supports the auto switchover operation on the type-B protection pair. OLT performs the auto switchover only when the operational state of the active port goes DOWN and the protection state is updated in RMS.

Perform the following steps for the auto switchover.

1. Select **Configuration > Protection > Type-B Protection Pair**.

The Type-B Protection Pair List page appears.

2. Remove fiber of active working PON port from the protection pair.

3. Click on the three dots () corresponding to the protection pair that you want to perform the auto switchover and click the **Auto Switchover** option.

The protection state of the primary PON port changes to “ACTIVE-STANDBY” and the protection state of the secondary PON port changes to “ACTIVE-WORKING”.

Policy

To access this page, click **Configuration** from the top right corner of the page and select **Policy > PM Collection Policy** from the left-hand side of the menu.

RMS allows you to create a default Performance Monitoring (PM) collection policy to collect the KPI information of the OLT. This enables the system administrator to configure the default periodicity interval to retrieve the OLTs historical and live KPIs.

You can either use a default PM collection policy if the policy suits your specific requirements or customize the policy to meet your particular requirements. You can also create your PM policy.

Select the table columns that you want to display on the **PM Collection Policy List** page. Clear the table columns that are not required to be displayed on the page.

Creating PM Collection Policy

Perform the following steps to create a policy.



Note: Before creating a PM policy, you must create a file storage to store the OLT KPIs. See [Creating File Store Configuration \(on page 618\)](#).

1. Select **Configuration > Policy > PM Collection Policy**.

The PM Collection Policy page appears.

2. Complete the configuration according to the guidelines provided in the following table.

Table 306. PM Collection Policy Configuration

| Field | Description |
|-----------------|---|
| Name | Enter a unique name for the policy. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-)• Space |
| Resource Type | Select the resource type from the list. The resource type is OLT. |
| Collection Type | Select the collection policy type from the list. The following type of policies are supported to retrieve the OLT KPIs. You can select one or more values from the list. <ul style="list-style-type: none">• Historical-15-minute• Instant-15-minute |

| Field | Description |
|-----------|---|
| | <ul style="list-style-type: none">Instance-1-hourInstant-1-day <p>If you want to select all the above options, select the All option.</p> |
| Filestore | Select the file storage to store the OLT KPIs. |

3. Click **Create**.

A new PM collection policy is created on the PM Collection Policy List page.

Maintenance

To access this page, click **Configuration** from the top right corner of the page and select **Maintenance > Task** from the left-hand side of the menu.

RMS allows you to create and manage task to perform the following operations.

- OLT Software Upgrade
- Reports (Fault and performance summary)
- EMS Database Backup (Mongo DB)
- OLT or Controller Backup
- Restore OLT and Controller
- Controller Software Upgrade
- ONT Firmware Upgrade
- ONT Bulk Firmware Upgrade
- OLT Firmware Upgrade
- Inventory Collection
- Service Collection
- Fault Collection
- Event Collection
- Audit Log Collection
- Configuration Update (Single and Bulk OLT)
- Bulk Port Modification
- OLT Reboot
- PON Port Migration
- Banner Update



Note: If a task is scheduled for a later date and time, it is never marked as completed because it runs in frequency, and once it is executed and completed, it moves again to the scheduled state. You can view the executed task on the monitor page. See [Monitoring Task Details \(on page 252\)](#).

Field Descriptions

The following table describes the fields on the Task List page.

Table 307. Task List

| Field | Description |
|-------|---|
| Name | Specifies the name of the task. |
| Type | Specifies the type of task. Example: Inventory Collection |

Table 307. Task List (continued)

| Field | Description |
|----------------|--|
| Status | <p>Specifies the status of the task. The supported statuses are:</p> <ul style="list-style-type: none"> • CREATED. Tasks that are created and not yet executed. • RUNNING. Tasks that are currently running. • COMPLETED. Tasks that are executed successfully. • SCHEDULED. Tasks that are scheduled for execution for a later date and time. <p>To update the status, click the Refresh icon on the page.</p> |
| Description | <p>Specifies the short description about the task.</p> <p>Example: Generate Inventory Collection Report</p> |
| Creation At | <p>Specifies the date and time when the task was created.</p> <p>Example: Jul 2, 2020, 3:05:45 PM</p> |
| Scheduled Day | Specifies the scheduled day of the task. |
| Scheduled Date | Specifies the scheduled date of the task. |
| Scheduled Time | Specifies the scheduled time of the task. |
| Frequency | Specifies the frequency of the task. |
| Action | <p>Specifies the action that you can perform on the task. The supported actions are:</p> <ul style="list-style-type: none"> • Delete • Update |

Creating Task Configuration

You can use this page to create the tasks to perform the following operations.

| Operations | For more information, see |
|----------------------------|---|
| OLT software upgrade | Creating Task for Single or Bulk OLT Software Upgrade (ONL or OLT BINS) (on page 647) |
| RMS database backup | Creating Task for EMS Database Backup (on page 659) |
| Report generation | Creating Task for Report Generation (on page 656) |
| OLT and controller backup | Creating Task for Controller or OLT Backup (on page 661) |
| OLT and controller restore | Creating Task for Controller or OLT Restore (on page 667) |

| Operations | For more information, see |
|--|--|
| Controller software upgrade | Creating Task for Single or Bulk Controller Software Upgrade (on page 669) |
| ONT firmware upgrade | Creating Task for ONT Firmware Upgrade (on page 674) |
| ONT bulk firmware upgrade | Creating Task for ONT Bulk Firmware Upgrade (on page 681) |
| OLT Firmware Upgrade | Creating Task for OLT Firmware Upgrade (on page 687) |
| Inventory collection | Creating Task for Inventory Collection (on page 689) |
| Service collection | Creating Task for Service Collection (on page 693) |
| Fault Collection | Creating Task for Fault Collection (on page 696) |
| Event Collection | Creating Task for Event Collection (on page 700) |
| Audit Log Collection | Creating Task for Audit Log Collection (on page 705) |
| Bulk Port Modification | Creating Task for Bulk Port Modification (on page 710) |
| Configuration update (single and bulk OLT) | Creating Task for Configuration Update (on page 716) |
| Reboot | Creating Task for OLT Reboot (on page 720) |
| PON Port Migration | Creating Task for PON Port Migration (on page 721) |
| Banner Update | Creating Task for Banner Update (on page 724) |

Perform the following steps to create a task.

1. Select **Maintenance > Task**.
The Task List page appears.
2. Complete the task configuration according to the guidelines provided in the following table.

Table 308. Task Configuration

| Field | Description |
|-------|--|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) |
| Type | Select the type of task from the list. The supported tasks are. <ul style="list-style-type: none"> • OLT Software Upgrade • Reports • EMS Database Backup |

| Field | Description |
|-------------------|---|
| | <ul style="list-style-type: none"> • OLT/Controller Backup • Restore • Controller Software Upgrade • ONT Firmware Upgrade • Inventory Collection • Service Collection • Fault Collection • Configuration Update • Reboot • PON Port Migration |
| Short Description | Enter a meaningful short description for the task. |

3. Click **Create**.

A new task is created on the Task List page.

Creating Task for Single or Bulk OLT Software Upgrade (ONL or OLT BINS)

When many OLTs are deployed in a network, and a limited number of subscribers are connected to the OLT, it is not an efficient way to upgrade each OLTs software by physically accessing it.

CBAC enables the OLT software upgrade remotely from RMS. CBAC in conjunction with the OLT, ensures the software upgrade, where the OLT downloads the latest software package, upgrades the software on the OLT, and ensures that all services are served by the OLT are resumed to all the subscribers. This feature enables the operator to upgrade the software of all the OLTs that belong to the same make and model at the same time.

The OLT software is divided into multiple layers, such as Network Operating System (NOS), the application layer, firmware, and it supports the upgrade of all these components.

The NOS layer changes very often compared to the application layer. The change in the NOS layer consumes more time to upgrade as it involves a reboot of the latest image. The OLT application layer supports In-Service Software Upgrade (ISSU) for most cases.

RMS supports bulk upgrades of OLT. The OLT software upgrade (ONL or OLT BINS) is a three-step upgrade process involving the following.

- Download the OLT software to the OLT first from a centralized location.
- Activate the downloaded software on the OLT.
- Commit the software to the OLT.

The upgrade process allows backing out from an upgrade and returning to the previous version of the software.

The status of OLT software upgrade is marked COMPLETED by RMS when the upgrade request is initiated successfully for all the selected devices in the task.

OLT also has auto-recovery procedures in the event of upgrade fail during activation. After three unsuccessful attempts if the OLT does not come up with the new release, it goes back to the previous release automatically and notifies the upgrade failure as an alarm.

You can also perform on-demand upgrade of the OLT software from RMS. For more information, see [Upgrade the OLT Software \(ONL or OLT BINS\) \(on page 388\)](#).



Note: Before you upgrade the software, you can verify the current version of the OLT software (ONL) from the **Monitor > Inventory > OLT** page.

Prerequisites

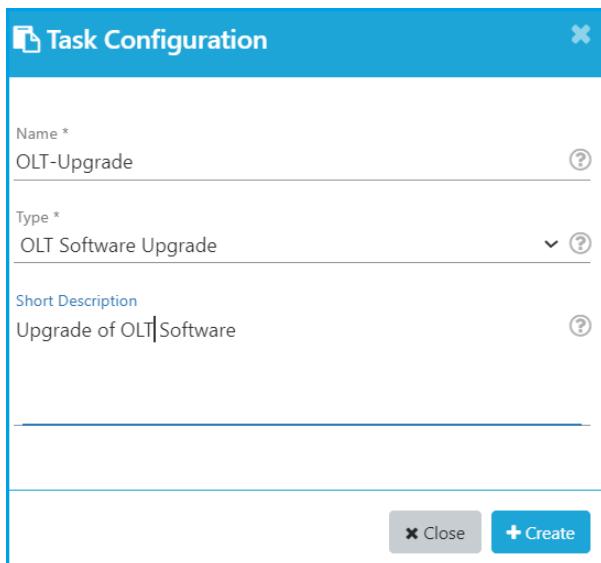
The following prerequisites must be fulfilled before creating task for OLT software upgrade.

- Create model version configuration. For more details, see [Creating Model Version Configuration \(on page 612\)](#).
- The user must upgrade the controller software first and then proceed with OLT software upgrade. For more details, see [Creating Task for Single or Bulk Controller Software Upgrade \(on page 669\)](#).
- If the upgrade is only for the OLT applications, ensure that the OLT is upgraded to the latest version before upgrading the OLT (ONL or OLT BINS) image.
- Create a site group and the OLT must be part of the site group. For more details, see [Creating Site Group Configuration \(on page 290\)](#).

Perform the following steps to create a task for the OLT software upgrade (ONL or OLT BINS).

1. Select **Maintenance > Task**.
The Task List page appears.
2. Click **Create**.
The Task Configuration page appears.

Figure 103. OLT Upgrade Task



3. Complete the task configuration according to the guidelines provided in the following table.

Table 309. Software Upgrade Task Configuration

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-) |
| Type | Select the task type as “OLT Software Upgrade” under OLT . |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.

The ME Software Upgrade page appears.

Figure 104. ME Software Upgrade

CONFIGURE

SELECT DEVICES

CONFIGURE EXECUTION

TASK COMPLETE

Type *
OLT

Make *
Radisys

Model
RLT-3200G

Select Actions : ?

Download Software
Version *
RLT-3200G-ver-RLT.1.17.42

Activate Software

Commit Software

Rollback Software

Next

5. Complete the configuration according to the guidelines provided in the following table.

Table 310. Managed Element Software Upgrade Task

| Field | Description |
|------------------------|--|
| Configure | |
| Type | Select the device type. Example: OLT |
| Make | Select the make from the list. Example: Iskratel or Radisys |
| Model | Select the model from the list. Example: openolt |
| Select Actions: | You must select all the following options at the same time. <ul style="list-style-type: none">• Download Software. You must select the software version of the OLT that you want to download. <p> Note:</p> |

| Field | Description |
|-------|---|
| | <ul style="list-style-type: none"> • If the ONL download fails for some issues, the subsequent ONL download request resumes the ONL download from where it stopped. • Before you download the OLT software, you must specify the OLT software version using the Creating Model Version Configuration (on page 612) page. • Activate Software. Activates the OLT software. • Commit Software. Commits the OLT software. <p>Note: If the commit operation fails, you can roll back the failed software to the previously committed software using the Rollback On Commit Failed option.</p> <ul style="list-style-type: none"> • Rollback Software. Rollback to previous version of the OLT software. |

6. Click **Next**.

The Select Device page appears.

Figure 105. OLT Device

| Name | Admin State | Operational State | Software version | Software version to be Upgraded | Software Upgrade Status |
|--------|-------------|-------------------|------------------|---------------------------------|-------------------------|
| OLT55 | ACTIVE | UP | BIN5_1.17.69 | RLT-1600G-ver-1.17.75 | DOWNLOAD-SUCCESSFUL |
| OLT147 | ACTIVE | UP | BIN5_1.17.69 | | COMMIT-SUCCESSFUL |

The page displays the list of OLT devices that are active along with the following details.

Table 311. Managed Element Device Details

| Field | Description |
|------------|---|
| Site Group | Select the site from the left-hand side of the pane. You must create a site and associate the site in the Inventory > OLT page. |

| Field | Description |
|---------------------------------|---|
| Name | Specifies the device name. |
| Admin State | Specifies the admin state of the device. |
| Operational State | Specifies the operational status of the device. |
| Software Version | Specifies the software version of the device. |
| Software Version to be Upgraded | Specifies the new software version to which the OLT needs to be upgraded. |
| Software Upgrade Status | Specifies the status of the software upgrade operation. |



Note: You can upgrade the OLT in the following ways.

- **Template Upload (CSV file).** This method is used for the bulk upgrade of the OLT.
- **Selecting OLT on GUI.** This method is used for the single or bulk upgrade of the OLT.

7. Perform the following steps to upgrade the OLT through template (CSV file).



Note: Skip this step and see step [8 \(on page 653\)](#) to upgrade the OLT through OLT selection.

a. Click on **template.xlsx** to download the template.



Note: Ensure that the CSV file contain OLTs with same make and model.

b. Enter the OLT name and save the downloaded template.

Figure 106. Template

| | | |
|---|--|--|
| 1 | name | |
| 2 | Description: Specifies the name for the managed element. | |
| 3 | Presence*: Mandatory | |
| 4 | OLT55 | |
| 5 | OLT147 | |
| 6 | | |

- c. Click on **Upload Resource File** and select the updated template. Continue with step 9 *(on page 654)* to upgrade the OLT software.

A confirmation message indicates that the upload is successful.

Figure 107. Upload CSV File

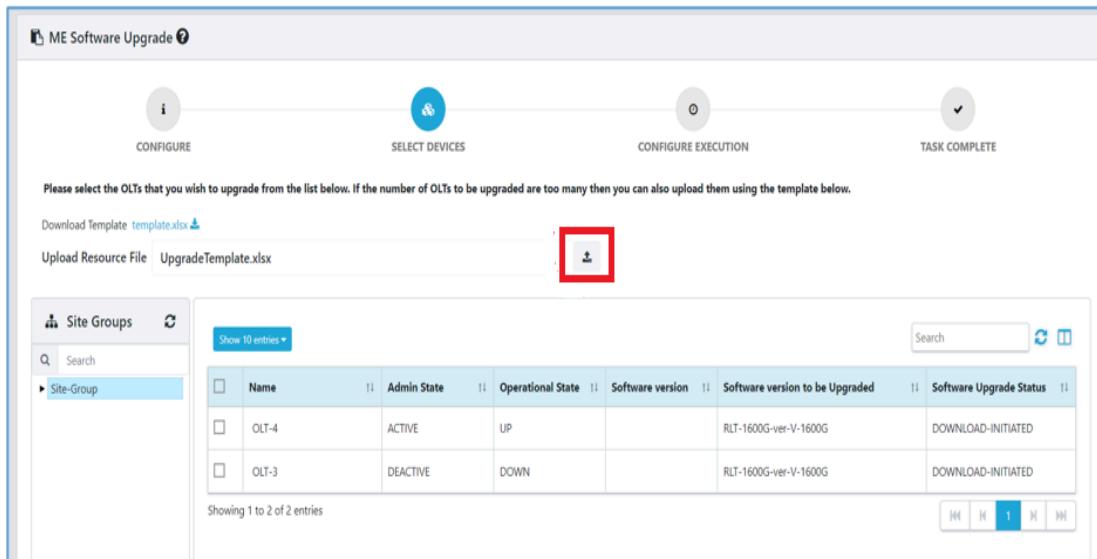
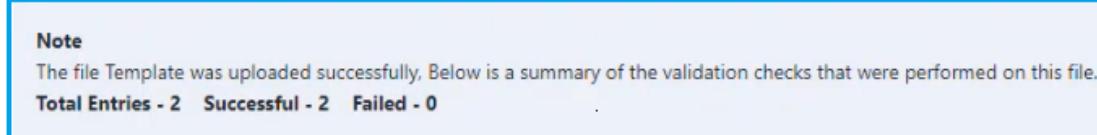


Figure 108. Upload Success



8. Perform the following steps to upgrade the OLT through OLT selection.



Note: Skip this step and see step 7 *(on page 652)* to upgrade the OLT through template (CSV file).

- a. Select the checkbox for the applicable OLT/OLTs. Continue with step 9 *(on page 654)* to upgrade the OLT software.

Figure 109. OLT Selection

| Name | Admin State | Operational State | Software version | Software version to be Upgraded |
|-------|-------------|-------------------|-----------------------|---------------------------------|
| OLT-4 | ACTIVE | UP | RLT-1600G-ver-V-1600G | |
| OLT-3 | DEACTIVE | DOWN | RLT-1600G-ver-V-1600G | |

9. Click **Next**.

The CONFIGURE EXECUTION page appears.

Figure 110. ME Configure Execution

10. Complete the configuration according to the guidelines provided in the following table.

Table 312. Managed Element Execution

| Field | Description |
|-----------------------------|--|
| Software Download Execution | Specifies whether you want to download the software immediately or schedule the software download for a later date and time. |

| Field | Description |
|-----------------------------|---|
| | <ul style="list-style-type: none"> • Immediate. Select this option if you want to upgrade the OLT software immediately. • Timing. Select this option if you want to schedule the OLT software upgrade for a later date and time. You can select daily, weekly, monthly, or one day. |
| Software Activate Execution | <p>Specifies whether you want to activate the software immediately or schedule the software activate for a later date and time.</p> <ul style="list-style-type: none"> • Immediate. Select this option if you want to upgrade the OLT software immediately. • Timing. Select this option if you want to schedule the OLT software upgrade for a later date and time. You can select daily, weekly, monthly, or one day. |
| Software Commit Execution | <p>Specifies whether you want to commit the software immediately or schedule the software commit for a later date and time.</p> <ul style="list-style-type: none"> • Immediate. Select this option if you want to upgrade the OLT software immediately. • Timing. Select this option if you want to schedule the OLT software upgrade for a later date and time. You can select daily, weekly, monthly, or one day. |

11. Click **Submit**.

A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

Click three dots on the corresponding task and then click **Monitor** or Navigate to **Monitor > Task** page to view the status of the task. For more information, see [OLT Software Upgrade \(on page 253\)](#).



Note: The OLT software upgrade task will be stuck and terminated automatically if the timeout value exceeds the below values for each operation. However, the upgrade continues for other working OLTs.

- Download – 60 minutes
- Activate – 60 minutes
- Commit – 15 minutes
- Rollback – 30 minutes

From the **Monitor > Task** page, the **Task Execution Status** is shown as **TERMINATED** and the **Status** is shown as DOWNLOAD-FAILED/ACTIVATE-FAILED/COMMIT-FAILED based on the operation on which it got stuck.

From the **Configuration > Inventory > OLT** page, the **Software Upgrade Status** is shown as DOWNLOAD-FAILED/ACTIVATE-FAILED/COMMIT-FAILED.

Creating Task for Report Generation

You must create a task to generate the following types of reports.

- Fault Summary
- Performance Summary

The report is generated based on the report type and the execution time that you have configured while creating the task.

You can generate reports on daily, weekly, and monthly or the specified duration. You can generate all types of reports at the same time.

Perform the following steps to create a task for generating reports.

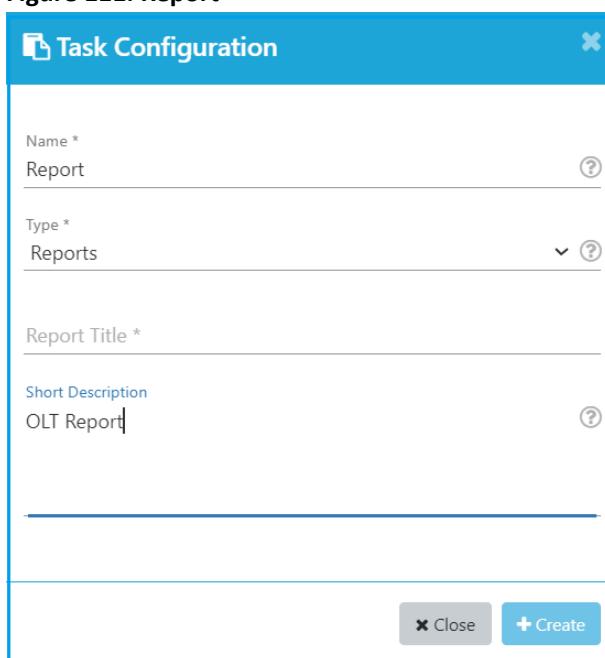
1. Select **Maintenance > Task**.

The Task List page appears.

2. Click **Create**.

The Task Configuration page appears.

Figure 111. Report



The screenshot shows the 'Task Configuration' dialog box. The 'Name' field is set to 'Report'. The 'Type' field is set to 'Reports'. The 'Report Title' field is empty. The 'Short Description' field contains 'OLT Report'. At the bottom, there are 'Close' and 'Create' buttons.

3. Complete the task configuration according to the guidelines provided in the following table.

Table 313. Report Task Configuration

| Field | Description |
|-------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. |

| Field | Description |
|-------------------|--|
| | <ul style="list-style-type: none"> Underscore (_) Hyphen (-) |
| Type | Select the task type as “Reports” under Reports . |
| Report Title | Enter the report title. |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.

The SELECT REPORT TYPE page appears.

Figure 112. Report Type

5. Complete the configuration according to the guidelines provided in the following table.

Table 314. Generate Report Task

| Field | Description |
|---|--|
| SELECT REPORT TYPE | You can select any of the following report type or all the report types at the same type. <ul style="list-style-type: none"> Fault Summary Performance Summary |
| If the report type is selected as “Fault Summary”, specify the following. | |
| Select Date Range | Select the date range to generate the fault summary report. You can also specify the duration (today, yesterday, last 7 days, last 30 days, this month, last month, and custom range) for which the report is generated. When you select the custom range, you must specify the From and To date (in MM/DD/YYYY and HH:MM:SS formats). |
| If the report type is selected as “Performance Summary”, specify the following. | |

| Field | Description |
|-----------------------|--|
| Select Date Range | Select the date range to generate the fault summary report. You can also specify the duration (today, yesterday, last 7 days, last 30 days, this month, last month, and custom range) for which the report is generated. When you select the custom range, you must specify the From and To date (in MM/DD/YYYY and HH:MM:SS formats). |
| Management Domain | Select the management domain from the list. |
| Devices | Select one or more OLT device(s) from the list. Example: olt-1 |
| Aggregation Type | Select the report aggregation type from the list. The supported values are. <ul style="list-style-type: none"> • Daily • Hourly • Weekly • Monthly The report is aggregated based on the aggregation type that you have selected. |
| CPU Threshold | Specifies the CPU threshold value configured for the OLT. The maximum threshold value for the CPU utilization is 90. |
| Disk Threshold | Specifies the disk threshold value configured for the OLT. The maximum threshold value for the disk utilization is 90. |
| Memory Threshold | Specifies the memory threshold value configured for the OLT. The maximum threshold value for the memory utilization is 90. |
| Temperature Threshold | Specifies the temperature threshold value configured for the OLT. The maximum threshold value for the temperature is 90° Celsius. |

6. Click **Next**.

The SET EXECUTION TIME page appears.

7. Select the option to generate the report immediately or schedule it for a later date and time.

- **Immediate Report.** Select this option if you want to generate the report immediately. You must select the time.
- **Timing Report.** Select this option if you want to schedule the report generation for a later date and time. You can select daily, weekly, monthly, or one day.

- **Daily.** If you have selected the option as Daily, select the time when the report needs to be generated. This option generates the report for 24 hours and the 24 hours starts from the previous day.
 - **Weekly.** If you have selected the option as Weekly, you must select the day (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday) from the Select Day list and then select the time from the Select Time list.
 - **Monthly.** If you have selected the option as Monthly, you must select the date (From 1 to 31, or Last Day of the Month) from the Select Date list and then select the time from the Select Time list.
 - **Single.** If you have selected the option as Single, you must select the time on the same day.
8. Click **Submit** to apply the settings.
- A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.
- If the status of the report is SCHEDULED, then the report generation is in progress and the status changes to COMPLETED once the report is generated.
 - Click three dots on the corresponding task and then click **Monitor** or Go to **Monitor > Task** page to view the status of the task and download the report. For more information, see [Reports \(on page 254\)](#).

Creating Task for EMS Database Backup

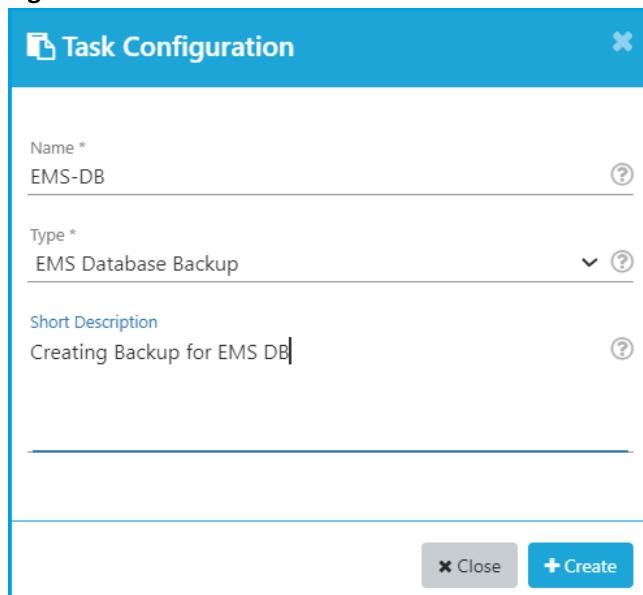
Database backup feature enables the user to take the snapshot of the EMS database and the snapshot can be used for database restoration.



Note: The backup and restore feature does not take the backup and restore of the device KPIs, service KPIs, historical events, and alarms.

Perform the following steps to create a task for EMS database backup.

1. Select **Maintenance > Task**.
The Task List page appears.
2. Click **Create**.
The Task Configuration page appears.

Figure 113. EMS DB Task

3. Complete the task configuration according to the guidelines provided in the following table.

Table 315. Database Backup Task Configuration

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-) |
| Type | Select the task type as “EMS Database Backup” under Others . |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.

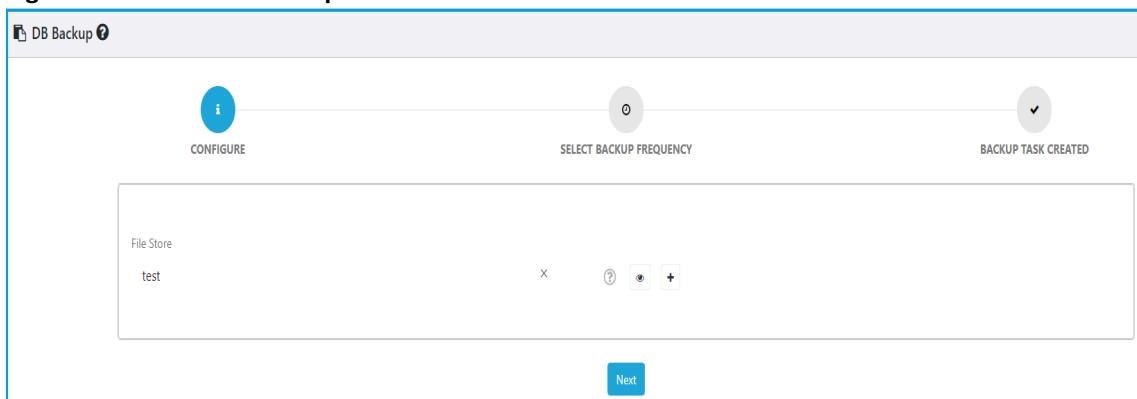
The DB Backup page appears.

5. Select the file storage from the list.



Note: The file storage must exist before the backup process is initiated.

- Click the plus icon (+) to create file store configuration. See [Creating File Store Configuration \(on page 618\)](#).
- Click the eye icon to view the file store configuration.

Figure 114. Database Backup

6. Click **Next**.

The SELECT BACKUP FREQUENCY page appears.

7. Select one of the options to take the EMS database backup.

- **Immediate.** Select this option to perform the EMS database backup immediately.
- **Timing.** Select this option to specify the date and time when you want to backup the EMS database.

8. Click **Submit**.

A confirmation message appears, indicating that the DB backup task is created successfully. The MongoDB backup file is created in the SFTP server path that you have provided while creating the file store configuration.

An event EMS-BACKUP-SUCCESSFUL is generated after successful EMS database backup.

If the backup operation is successful, a backup job is created on the **Monitor > Logs > Backup Jobs** page, and the event is generated on the **Monitor > Events** page. You can click the **Monitor** option from the task, and you are taken to the Monitor page to view the backup jobs. For more information, see [Backup Jobs \(on page 231\)](#).

You can monitor the task details using the **Monitor** page. For more information, see [Table 116: EMS Database Backup Task Details \(on page 255\)](#).

For more information on how to restore the EMS database, refer to the following guides based on the RMS deployment type.

- *Single Node RMS Installation and Upgrade Guide*
- *Multinode RMS Installation and Upgrade Guide*

Creating Task for Controller or OLT Backup

You must create a task to perform the scheduled OLT and controller backup operation. Before you create a task for the OLT backup, you must create a site group. See [Creating Site Group Configuration \(on page 290\)](#).

The following tasks are supported.

- [Creating Task for OLT Backup \(on page 662\)](#)
- [Creating Task for Controller Backup \(on page 664\)](#)

Creating Task for OLT Backup

You must create a task to perform the scheduled OLT backup operation. Before you create a task for the OLT backup, you must create a site group. See [Creating Site Group Configuration \(on page 290\)](#).

Perform the following steps to create a task for OLT backup.

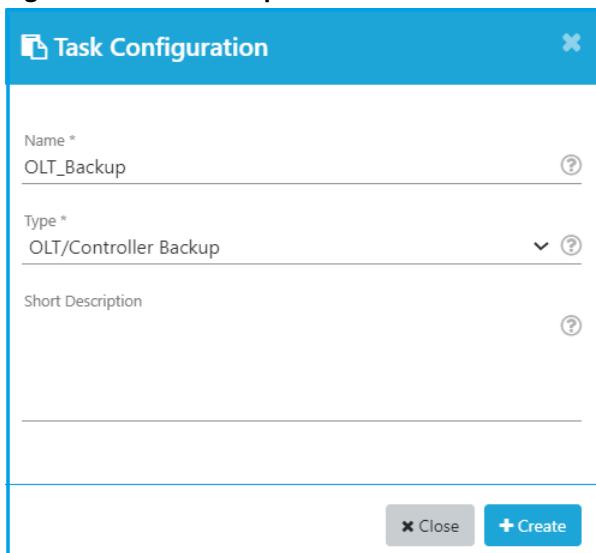
1. Select **Maintenance > Task**.

The Task List page appears.

2. Click **Create**.

The Task Configuration page appears.

Figure 115. OLT Backup Task



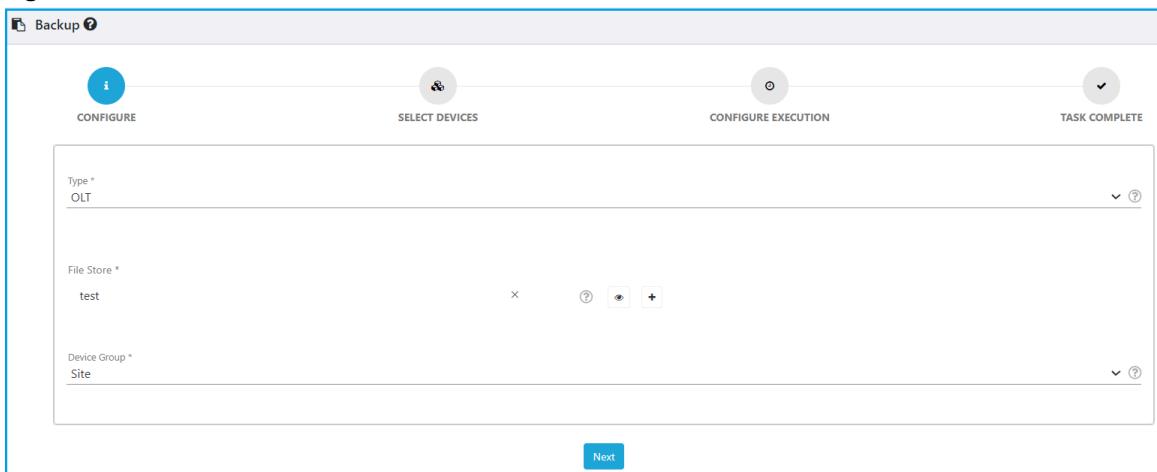
The screenshot shows the 'Task Configuration' dialog box. It has a blue header bar with the title 'Task Configuration' and a close button. The main area contains three input fields: 'Name' (containing 'OLT_Backup'), 'Type' (containing 'OLT/Controller Backup'), and 'Short Description' (empty). At the bottom are 'Close' and 'Create' buttons.

3. Complete the task configuration according to the guidelines provided in the following table.

Table 316. OLT Backup Task Configuration

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-) |
| Type | Select the task type as “Backup” under OLT . |
| Short Description | Enter a meaningful short description for the task. |

| Field | Description |
|------------------|--|
| CONFIGURE | |
| Type | Select the type as OLT. |
| File Store | <p>Select the file storage from the list.</p> <p> Note: The file storage must exist before the backup process is initiated.</p> <ul style="list-style-type: none"> Click the plus icon (+) to create file store configuration. See Creating File Store Configuration (on page 618). Click the eye icon to view the file store configuration. |
| Device Group | <p>The following fields are displayed in the device group list.</p> <ul style="list-style-type: none"> Site Management Domain Me Group |

Figure 116. OLT CONFIGURE


4. Click **Next**.

The SELECT DEVICES page appears with the following information provided in the following table.

Table 317. Select Devices

| Field | Description |
|-------|-----------------------------------|
| Name | Specifies name of the OLT. |
| Type | Specifies device type. |
| Make | Specifies vendor name of the OLT. |

| Field | Description |
|--------------------|---|
| Model | Specifies model name of the OLT. |
| Admin State | Specifies admin state of the OLT. The supported values are. <ul style="list-style-type: none">• ACTIVE• INACTIVE |
| Operational State | Specifies operational state of the OLT. The supported values are. <ul style="list-style-type: none">• UP• Down |
| Last Backup Status | Specifies last backup status of the OLT. |

5. Select the OLT on which you want to back up the configuration.
6. Click **Next**.
7. Select one of the options to take the OLT backup.
 - **Immediate**. Select this option to perform the OLT backup immediately.
 - **Timing**. Select this option to specify the date and time when you want to backup the OLT.
8. Click **Submit**.

A confirmation message appears, indicating that the backup task is initiated successfully.

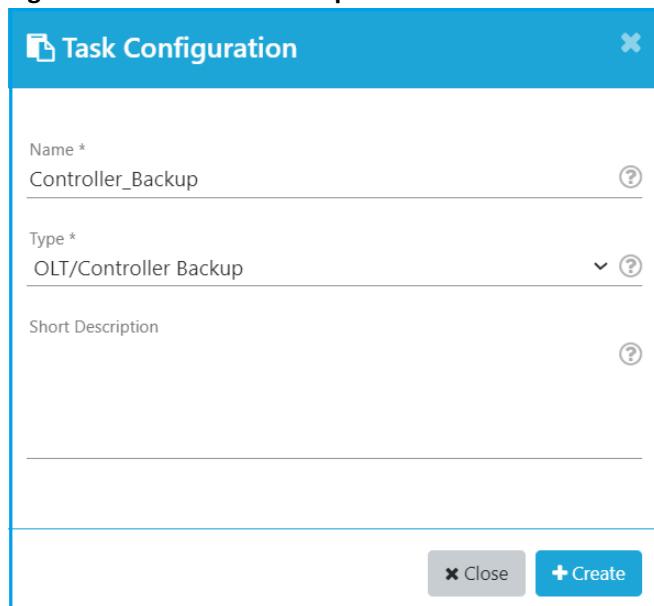
You can monitor the task details using the **Monitor** page. For more information, see [Table 117: OLT or Controller Backup Task Information \(on page 256\)](#).

Creating Task for Controller Backup

You must create a task to perform the scheduled controller backup operation. Before you create a task for the controller backup, you must create a site group. See [Creating Site Group Configuration \(on page 290\)](#).

Perform the following steps to create a task for controller backup.

1. Select **Maintenance > Task**.
The Task List page appears.
2. Click **Create**.
The Task Configuration page appears.

Figure 117. Controller Backup Task

3. Complete the task configuration according to the guidelines provided in the following table.

Table 318. Controller Backup Task Configuration

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-) |
| Type | Select the task type as “Backup” under Controller . |
| Short Description | Enter a meaningful short description for the task. |
| CONFIGURE | |
| Type | Select the type as controller. |
| File Store | <p>Select the file storage from the list.</p> <p> Note: The file storage must exist before the backup process is initiated.</p> <ul style="list-style-type: none">• Click the plus icon (+) to create file store configuration. See Creating File Store Configuration (on page 618).• Click the eye icon to view the file store configuration. |

| Field | Description |
|--------------|---|
| Device Group | When the Type is selected as “CONTROLLER”, the following fields are displayed in the device group list. <ul style="list-style-type: none"> • All Controller • Management Domain |

Figure 118. CONTROLLER CONFIGURE

The screenshot shows a four-step configuration wizard. Step 1 (CONFIGURE) shows 'Type *' set to 'CONTROLLER'. Step 2 (SELECT CONTROLLERS) shows a 'File Store *' field with 'backup' selected, accompanied by a delete (X) and three additional icons. Step 3 (CONFIGURE EXECUTION) and Step 4 (TASK COMPLETE) are shown as grayed-out steps. At the bottom is a 'Next' button.

4. Click **Next**.

The SELECT CONTROLLERS page appears with the following information provided in the following table.

Table 319. Select Controllers

| Field | Description |
|-------------------|---|
| Name | Specifies name of the controller. |
| Version | Specifies current version of the controller. |
| Admin State | Specifies admin state of the controller. The supported values are. <ul style="list-style-type: none"> • ACTIVE • INACTIVE |
| Operational State | Specifies operational state of the controller. The supported values are. |

| Field | Description |
|--------------------|--|
| | <ul style="list-style-type: none"> • UP • Down |
| Last Backup Status | Specifies last backup status of the controller. |

5. Select the controller on which you want to back up the configuration.
6. Click **Next**.
7. Select one of the options to take the controller backup.
 - **Immediate**. Select this option to perform the controller backup immediately.
 - **Timing**. Select this option to specify the date and time when you want to backup the controller.
8. Click **Submit**.

A confirmation message appears, indicating that the backup task is initiated successfully.

You can monitor the task details using the **Monitor** page. For more information, see [Table 117: OLT or Controller Backup Task Information \(on page 256\)](#).

Creating Task for Controller or OLT Restore

You must create a task to perform the scheduled OLT or controller restore operation.

Perform the following steps to create a task for controller or OLT restore.

1. Select **Maintenance > Task**.
The Task List page appears.
2. Click **Create**.
3. Complete the task configuration according to the guidelines provided in the following table.

Table 320. Controller Task Configuration

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) • Space |
| Type | Select the task type as “Restore” under OLT or Controller . |
| Short Description | Enter a meaningful short description for the task. |
| CONFIGURE | |

| Field | Description |
|------------|---|
| Type | Select whether you want to restore the OLT or the controller configuration. <ul style="list-style-type: none"> Controller OLT |
| File Store | Select the file storage from the list. <p> Note: The file storage must exist before the restore process is initiated.</p> <ul style="list-style-type: none"> Click the plus icon (+) to create file store configuration. See Creating File Store Configuration (on page 618). Click the eye icon to view the file store configuration. |
| | If the type is selected as “Controller”, the following controller information is displayed on the Controller List page. <ul style="list-style-type: none"> Name. Name of the controller File Name. Specifies the file name of the controller. Type. Device Type Version. Current version of the controller Admin State. Admin state of the controller (ACTIVE or INACTIVE) Operational State. Operational state of the controller (UP or Down) Last Restore Status. Restore status of the controller. If the type is selected as “OLT”, the following OLT information is displayed on the Device List page. <ul style="list-style-type: none"> Name. Name of the OLT File Name. Specifies the file name of the OLT. Type. Device Type Make. Vendor name of the OLT. Model. Model name of the OLT. Admin State. Admin state of the OLT (ACTIVE or INACTIVE) Operational State. Operational state of the OLT (UP or Down) Last Restore Status. Restore status of the OLT. |
| | Select the controller or OLT on which you want to restore the configuration. The selected controller or OLT appears on the Selected Device List page. If you want to delete the device (Controller or OLT), click the Delete icon from Action column. |
| | Enter the File Name for the controller or OLT. |
| | Click Next . |

| Field | Description |
|----------------------------|---|
| CONFIGURE EXECUTION | Select the option that you want to restore the controller or the OLT configuration immediately or schedule the restore for a later date and time. <ul style="list-style-type: none">• Immediate. Select this option to perform the restore operation immediately.• Timing. Select this option to specify the date and time to perform the restore operation. |

4. Click **Submit**.

The **TASK COMPLETE** tab is enabled and changed to green color.

A confirmation message appears, indicating that the restore task is initiated successfully.

You can monitor the task details using the **Monitor** page. For more information, see [Table 118: Task Information–OLT or Controller Restore \(on page 258\)](#).



Note: The controller upgrade task will be stuck and terminated automatically if the timeout value exceeds the below values for each operation. However, the upgrade continues for other working OLTs.

- Download – 60 minutes
- Upgrade – 45 minutes

From the **Monitor > Task** page, the **Task Execution Status** is shown as **TERMINATED** and the Status is shown as DOWNLOAD-FAILED/ACTIVATE-FAILED/COMMIT-FAILED based on the operation on which it got stuck.

From the **Configuration > Controller** page, the **Upgrade Status** is shown as DOWNLOADFAILED or UPGRADE-FAILED.

Creating Task for Single or Bulk Controller Software Upgrade

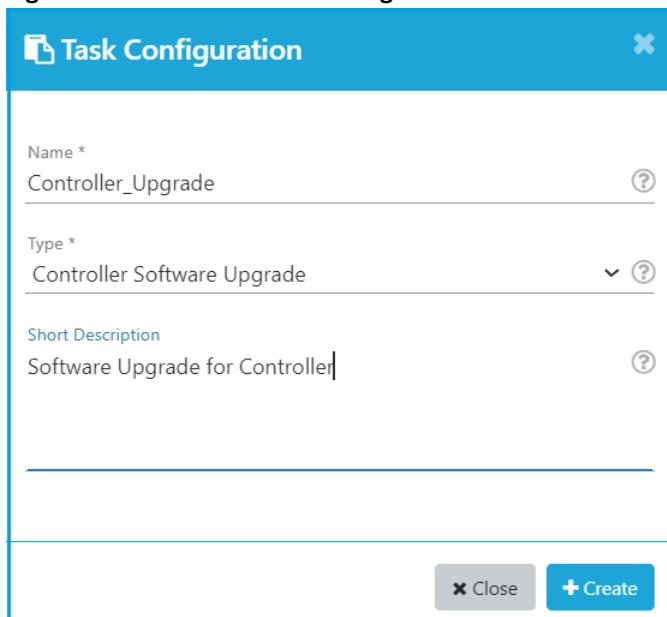
Perform the following steps to create a task for controller software upgrade.

1. Select **Maintenance > Task**.

The Task List page appears.

2. Click **Create**.

The Task Configuration page appears.

Figure 119. Controller Task Configuration

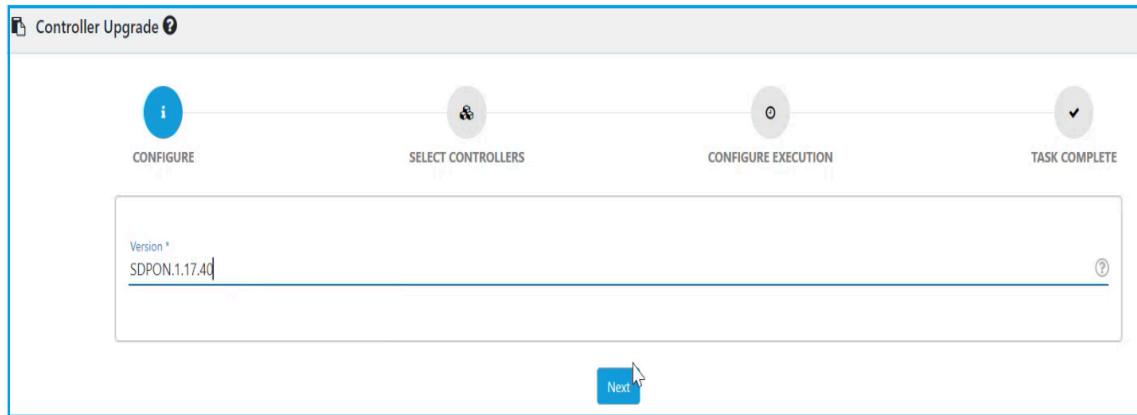
3. Complete the task configuration according to the guidelines provided in the following table.

Table 321. Controller Software Upgrade Task Configuration

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">Underscore (_)Hyphen (-) |
| Type | Select the task type as “Controller Software Upgrade” under Controller . |
| Short Description | Enter a meaningful short description for the task. |

4. Enter the controller version to be upgraded.

Figure 120. Controller Version

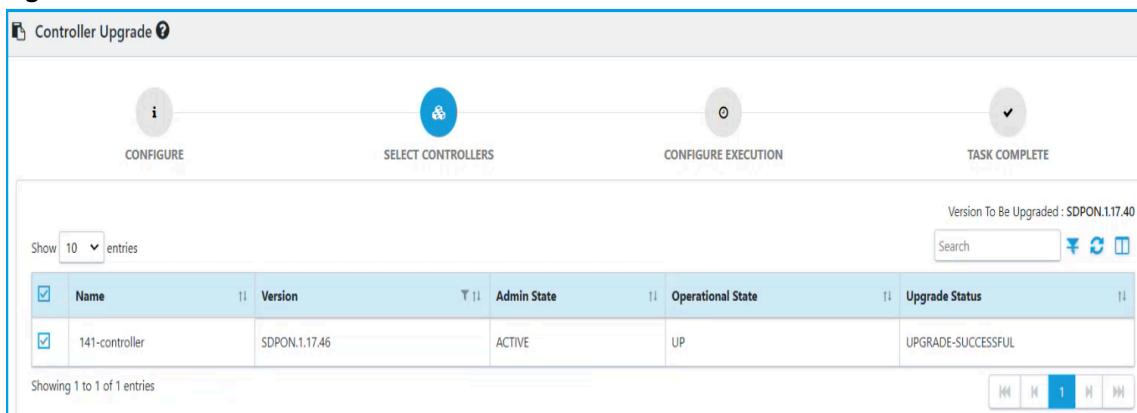


The screenshot shows the 'Controller Upgrade' interface. The 'CONFIGURE' step is active, indicated by a blue icon. The 'Version' field contains the value 'SDPON.1.17.40'. A 'Next' button is visible at the bottom right.

5. Click **Next**.

The controller information is displayed on the page.

Figure 121. Controller Selection



The screenshot shows the 'Controller Selection' page. The 'SELECT CONTROLLERS' step is active, indicated by a blue icon. A table lists one controller: '141-controller' with version 'SDPON.1.17.46', 'ACTIVE' Admin State, 'UP' Operational State, and 'UPGRADE-SUCCESSFUL' Upgrade Status. The table includes a search bar and navigation buttons.

The page displays the list of controller that are active and up along with the following details.

Table 322. Controller Details

| Field | Description |
|-------------------|---|
| Name | Specifies the name of the controller. |
| Version | Specifies the new version of the CBAC controller. |
| Admin State | Specifies the admin state of the controller. The supported values are. <ul style="list-style-type: none"> ◦ ACTIVE ◦ INACTIVE |
| Operational State | Specifies the operational state of the CBAC controller. The supported values are. |

| Field | Description |
|---------------|--|
| | <ul style="list-style-type: none">◦ UP◦ Down |
| Upgrade State | Specifies the upgrade state of the CBAC controller. The supported statuses are. <ul style="list-style-type: none">◦ UPGRADE_IN_PROGRESS◦ UPGRADE_FAILED◦ UPGRADE_SUCCESS◦ ROLLBACK_IN_PROGRESS◦ ROLLBACK_SUCCESS◦ ROLLBACK_FAILED |



Note: You can upgrade the controller in the following ways.

- **Template Upload (CSV file).** This method is used for the bulk upgrade of the controller.
 - **Selecting controllers on GUI.** This method is used for the single or bulk upgrade of the controller.
6. Perform the following steps to upgrade the controller through template (CSV file).



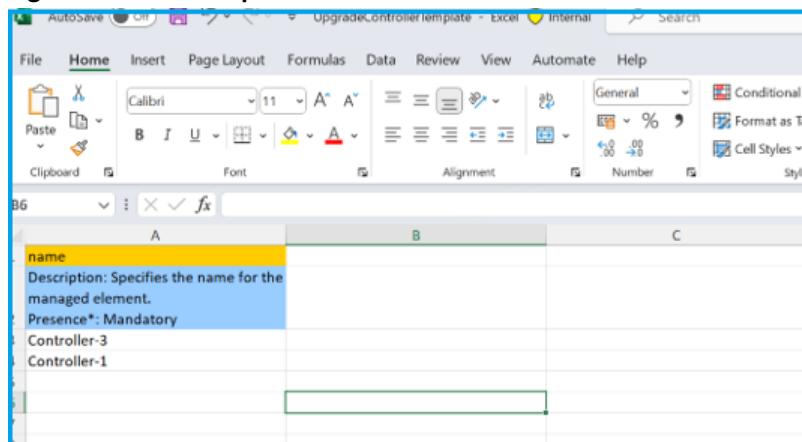
Note: Skip this step and see step [7 \(on page 673\)](#) to upgrade the controller through controller selection.

- Click on **template.xlsx** to download the template.
- Enter the controller name and save the downloaded template.



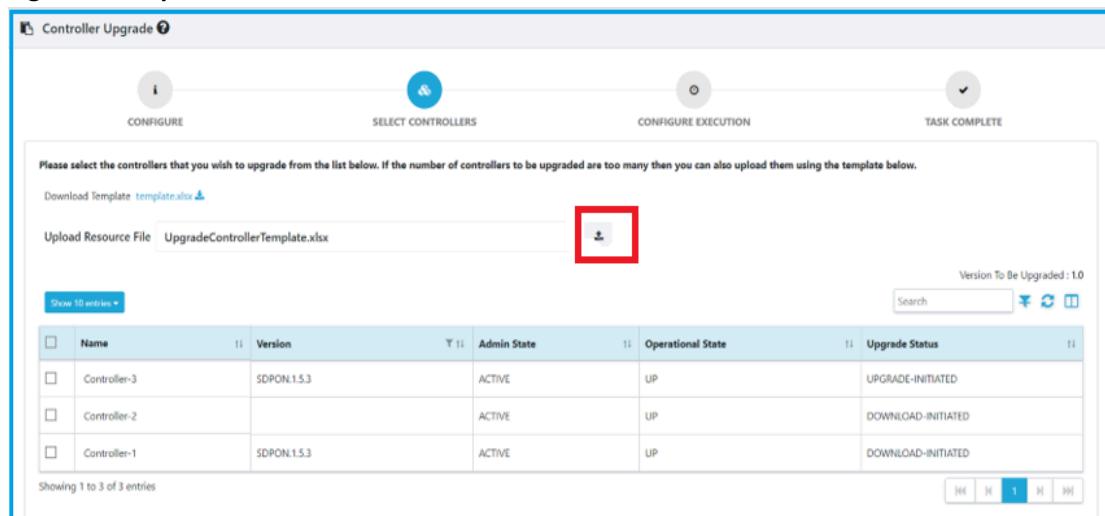
Note: The user can provide maximum 100 entries in the CSV file at single task.

Figure 122. CSV Template



- c. Click on **Upload Resource File** and select the updated template. Continue with step 8 [\(on page 673\)](#) to upgrade the controller software.
- A confirmation message indicates that the upload is successful.

Figure 123. Upload CSV File



7. Perform the following steps to upgrade the controller through controller selection.

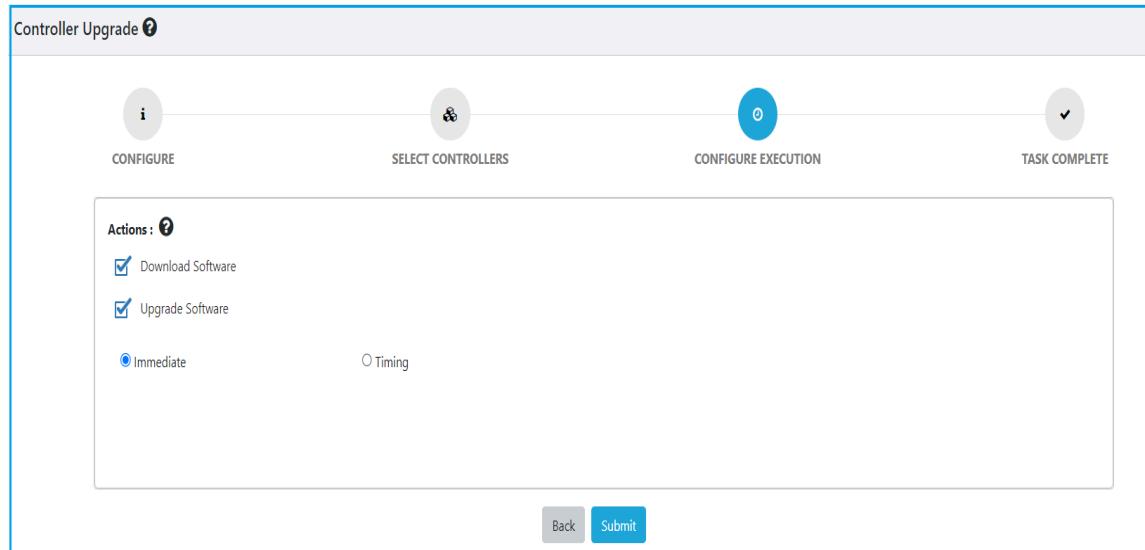


Note: Skip this step and see step 6 [\(on page 672\)](#) to upgrade the controller through template (CSV file).

- a. Select the checkbox for the applicable controllers for which the upgrade status is NEW-SDPON-SOFTWARE-AVAILABLE. Continue with step 8 [\(on page 673\)](#) to upgrade the controller software.
8. Click **Next**.

The Configure Execution page appears.

Figure 124. Controller Execution



9. Complete the task configuration according to the guidelines provided in the following table.

Table 323. Controller Software Upgrade Task Configuration

| Field | Description |
|----------------------------|--|
| CONFIGURE EXECUTION | <p>Select the option to download or upgrade the controller software immediately or schedule the upgrade for a later date and time.</p> <ul style="list-style-type: none">◦ Download Software. Select this option to perform the software download for the controller.◦ Upgrade Software. Select this option to perform the software upgrade for the controller. <p> Note: You can select both fields, download and upgrade the controller software.</p> <ul style="list-style-type: none">◦ Immediate. Select this option to perform the software upgrade or software download for the controller immediately.◦ Timing. Select this option to specify the date and time you want to download or upgrade the software for the controller. |

10. Click **Submit**.

The **TASK COMPLETE** tab is enabled and changed to green color.

A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

- If the status is **RUNNING**, then the controller software upgrade is in progress and the status changes to **COMPLETED** once the upgrade is successful.
- Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the controller software upgrade task. For more information, see [Controller Software Upgrade \(on page 259\)](#).

Creating Task for ONT Firmware Upgrade

Prerequisites

The following prerequisites must be fulfilled before creating task for ONT firmware upgrade.

- Ensure the ONT image is available on the `http://<webserverip>/onufw/ES6xx1vM_1.22.0.023.oneimage` server before initiating the ONT upgrade. If the ONT image is not available, the upgrade fails.
- Create a make and model configuration for the respective ONTs. See [Creating Make Configuration \(on page 606\)](#) and [Creating Model Configuration \(on page 610\)](#).
- Create a model version configuration for the respective ONT. See [Creating Model Version Configuration \(on page 612\)](#).

You can upgrade the firmware for a single ONT that belongs to the OLT.

The OMCI supports two types of message sets for upgrading the ONTs.

- **Baseline.** The payload of the OMCI message is 29 bytes.
- **Extended.** The payload of the OMCI message is 1900 bytes.

CBAC learns the capabilities of the ONT as part of the MIB upload and whether the ONT is capable of supporting the extended or baseline message type. When the operator performs the upgrade, the CBAC starts the upgrade process based on the capabilities learned.

The ONTs that support the Extended message type can complete the download in less time than the Baseline message type.



Note: The operator does not have an option to select the message type during the upgrade.

Perform the following steps to create a task for ONT firmware upgrade.

1. Select **Maintenance > Task**.
The Task List page appears.
2. Click **Create**.
The Task Configuration page appears.

Figure 125. ONT Firmware Upgrade

| Task Configuration | |
|--------------------------------------|---------------------------------------|
| Name * | Firmware_Upgrade |
| Type * | ONT Firmware Upgrade |
| Short Description | Firmware Upgrade for ONT |
| | |
| <input type="button" value="Close"/> | <input type="button" value="Create"/> |

3. Complete the task configuration according to the guidelines provided in the following table.

Table 324. ONT Firmware Upgrade Task Configuration

| Field | Description |
|-------------------|--|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Type | Select the task type as “ONT Firmware Upgrade” under ONT . |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.

The CONFIGURE page appears.

Figure 126. ONT Configuration

5. Complete the task configuration according to the guidelines provided in the following table.

Table 325. ONT Configuration

| Field | Description |
|------------------|--|
| CONFIGURE | |
| Type | Displays the type as ONT. This field cannot be modified. |
| Make | Select make for the ONT. If the make configuration does not exist, see Creating Make Configuration (on page 606) . |
| Model | Select model for the ONT. If the model configuration does not exist, see Creating Model Configuration (on page 610) . |
| Equipment ID | Select the equipment ID of the ONT. Example: BVM4K00BRA0915-0083  Note: You can select either Make and Model, or Equipment ID for upgrade configuration. |
| Version | Select the ONT firmware version that you want to download.  Note: You must specify the ONT software version in the Creating Model Version Configuration (on page 612) page. |
| OLT | Select an OLT to which you want to copy the ONT firmware. |
| Select Actions | <p>You can select the following options at the same time.</p> <ul style="list-style-type: none"> ◦ Download on OLT. Downloads the ONT firmware image on the OLT. You can skip this step if the ONT firmware image is already available at the OLT. ◦ Download on ONT. Downloads the ONT firmware image on the ONT. <ul style="list-style-type: none"> ▪ Enable Auto Commit. Enables and auto commits the ONT firmware on the ONT. ▪ Enable Activate Commit on ONT Reboot. Enables the auto-activation and commits the new ONT firmware after the ONT reboot.  Note: You can either select the Enable Auto Commit or Enable Activate Commit on ONT Reboot option. <ul style="list-style-type: none"> ◦ Activate and Commit on ONT. Activates and commits the ONT firmware on the ONT. |

6. Click **Next**.

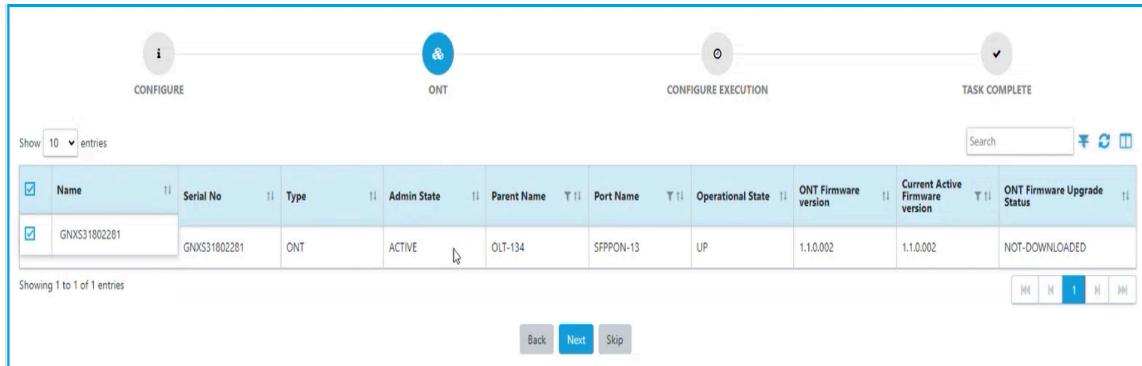
The ONT Information page is displayed.

The following table lists the information displayed on the ONT information page.

Table 326. ONT Information

| Field | Description |
|---------------------------------|---|
| Name | Specifies the name of the ONT. |
| Serial No | Specifies the serial number of the ONT. |
| Type | Specifies the element type. For example, ONT. |
| Admin State | Specifies the ONT admin state (ACTIVE or DEACTIVE). |
| Parent Name | Specifies the OLT details associate with the ONT. |
| Port Name | Specifies the port name attached to the ONT. |
| Operational State | Specifies the operational state of the ONT (UP or DOWN). |
| ONT Firmware Version | Specifies the latest ONT firmware version available on the ONT. |
| Current Active Firmware Version | Specifies the current active version of the ONT. You can apply filter based on the current active firmware version. |
| ONT Firmware Download Status | Specifies the ONT firmware download status (DOWNLOADED or NOT-DOWNLOADED). |

Figure 127. ONT Information



The screenshot shows a web-based interface for managing ONTs. At the top, there are four status indicators: 'CONFIGURE' (grey), 'ONT' (blue), 'CONFIGURE EXECUTION' (grey), and 'TASK COMPLETE' (grey). Below these are search and filter controls, including a 'Search' input field and a 'Show 10 entries' dropdown. The main content is a table with the following data:

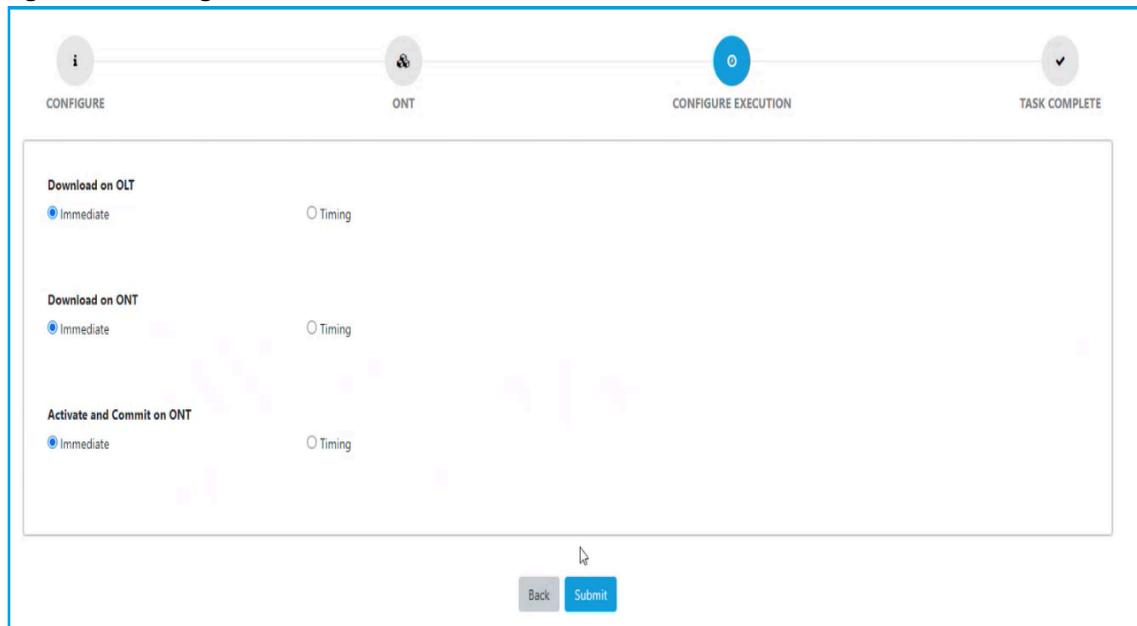
| Name | Serial No | Type | Admin State | Parent Name | Port Name | Operational State | ONT Firmware version | Current Active Firmware version | ONT Firmware Upgrade Status |
|--------------|--------------|------|-------------|-------------|-----------|-------------------|----------------------|---------------------------------|-----------------------------|
| GNX531802281 | GNX531802281 | ONT | ACTIVE | OLT-134 | SFPON-13 | UP | 1.1.0.002 | 1.1.0.002 | NOT-DOWNLOADED |

At the bottom of the table, it says 'Showing 1 to 1 of 1 entries' and has navigation buttons for 'Back', 'Next', and 'Skip'.

7. Select the ONT and click **Next**.

Note: A list of ONTs with the same make and model is displayed.

The CONFIGURE EXECUTION page is displayed.

Figure 128. Configure Execution

8. Select one of the options to upgrade the ONT firmware.
 - **Immediate.** Select this option to perform the ONT firmware upgrade immediately.
 - **Timing.** Select this option to specify the date and time when you want to upgrade the ONT firmware.

The above options are applicable for the following operations.

- Download on OLT
- Download on ONT
 - Enable Auto Commit
 - Enable Activate Commit on ONT Reboot
- Activate and Commit on ONT

9. Click **Submit**.

The **TASK COMPLETE** tab is enabled and changed to green color.

A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

- If the status is **RUNNING**, then the ONT bulk firmware upgrade is in progress and the status changes to **COMPLETED** once the upgrade is successful.
- Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the ONT firmware upgrade task. For more information, see [Table 120: ONT Firmware Upgrade Task Details \(on page 260\)](#).

Pausing, Resuming, and Stopping ONT Firmware Upgrade

The firmware upgrade on ONTs is a time-consuming procedure. The CBAC restricts a few operations on the OLT, PON, and ONT on which the upgrade is happening. There are certain cases when the operator needs to perform a few urgent configurations or get some information during the upgrade. The operator must wait for the download process to be completed on all ONTs to perform these operations.

You can pause, resume, and stop ONT firmware upgrade.

Perform the following steps to pause the ONT firmware upgrade.

1. Select **Maintenance > Task**.

The Task List page appears.

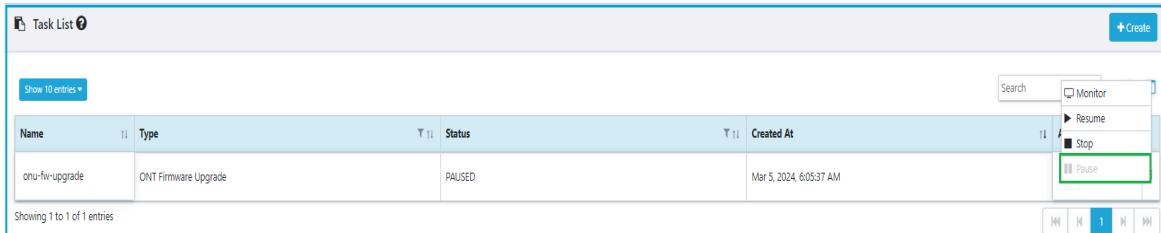
2. Click on the three dots (⋮) corresponding to the ONT firmware upgrade.
3. Click **Pause**.

A success message appears indicating the ONT firmware upgrade is paused successfully and the task status is changed to **PAUSED**.



Note: The pause operation is supported for ONTs for which the firmware download is **In-Progress** or **Pending-Download** state.

Figure 129. Pause ONT Firmware Upgrade



Perform the following steps to resume a paused ONT firmware upgrade.

1. Select **Maintenance > Task**.

The Task List page appears.

2. Click on the three dots (⋮) corresponding to the ONT firmware upgrade.
3. Click **Resume**.

A success message appears indicating the ONT firmware upgrade is resumed successfully and the task status is changed to **RUNNING**.



Note: You can resume the ONT firmware download if it is paused.

Figure 130. Resume ONT Firmware Upgrade

| Name | Type | Status | Created At |
|----------------|----------------------|--------|-------------------------|
| onu-fw-upgrade | ONT Firmware Upgrade | PAUSED | Mar 5, 2024, 6:05:37 AM |

Perform the following steps to stop the ONT firmware upgrade.

1. Select **Maintenance > Task**.

The Task List page appears.

2. Click on the three dots (⋮) corresponding to the ONT firmware upgrade.
3. Click **Stop**.

A success message appears indicating the ONT firmware upgrade is stopped successfully and the task status is changed to **TERMINATED**.



Note: You can stop the ONT firmware upgrade process for ONTs for which the firmware download is **In-Progress** or **Pending-Download** state.

Figure 131. Stop ONT Firmware Upgrade

| Name | Type | Status | Created At |
|----------------|----------------------|------------|-------------------------|
| onu-fw-upgrade | ONT Firmware Upgrade | TERMINATED | Mar 5, 2024, 6:05:37 AM |

You can monitor the task details using the **Monitor** page. For more information, see [Table 120: ONT Firmware Upgrade Task Details \(on page 260\)](#).

Creating Task for ONT Bulk Firmware Upgrade

Prerequisites

The following prerequisites must be fulfilled before creating task for ONT bulk firmware upgrade.

- Ensure the ONT image is available on the `http://<webserverip>/onufw/ES6xx1vM_1.22.0.023.oneimage` server before initiating the ONT upgrade. If the ONT image is not available, the upgrade fails.
- Create a make and model configuration for the respective ONTs. See [Creating Make Configuration \(on page 606\)](#) and [Creating Model Configuration \(on page 610\)](#).
- Create a model version configuration for the respective ONT. See [Creating Model Version Configuration \(on page 612\)](#).

You can upgrade the firmware for a bulk of ONTs that belongs to the OLT. However, for a bulk ONT upgrade, the time taken to finish the upgrade may vary based on the number of ONTs.

The OMCI supports two types of message sets for upgrading the ONTs.

- **Baseline.** The payload of the OMCI message is 29 bytes.
- **Extended.** The payload of the OMCI message is 1900 bytes.

CBAC learns the capabilities of the ONT as part of the MIB upload and whether the ONT is capable of supporting the extended or baseline message type. When the operator performs the upgrade, the CBAC starts the upgrade process based on the capabilities learned.

The ONTs that support the Extended message type can complete the download in less time than the Baseline message type.

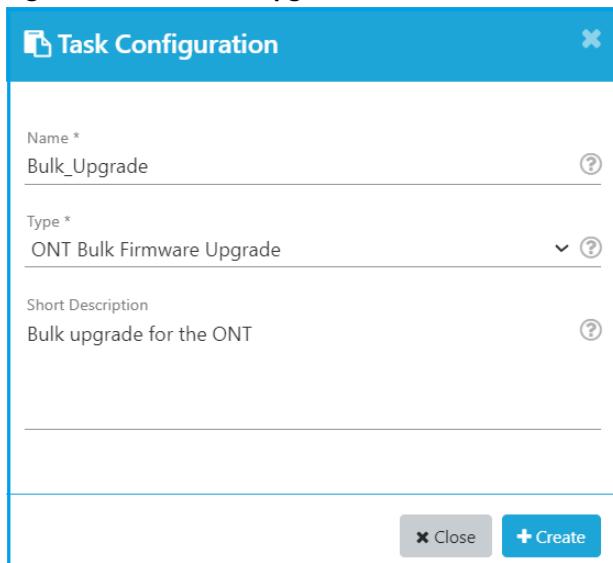


Note: The operator does not have an option to select the message type during the upgrade.

Perform the following steps to create a task for the ONT bulk firmware upgrade.

1. Select **Maintenance > Task**.
The Task List page appears.
2. Click **Create**.
The Task Configuration page appears.

Figure 132. ONT Bulk Upgrade



3. Complete the task configuration according to the guidelines provided in the following table.

Table 327. ONT Bulk Firmware Upgrade Task Configuration

| Field | Description |
|-------------------|--|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Type | Select the task type as “ONT Bulk Firmware Upgrade” under ONT . |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.

The CONFIGURE page appears.

Figure 133. Bulk ONT Configuration

5. Complete the task configuration according to the guidelines provided in the following table.

Table 328. Bulk ONT Configuration

| Field | Description |
|------------------|-------------|
| CONFIGURE | |

| Field | Description |
|----------------|---|
| Type | Displays the type as ONT. This field cannot be modified. |
| Make | Select make for the ONT. If the make configuration does not exist, see Creating Make Configuration (on page 606) . |
| Model | Select model for the ONT. If the model configuration does not exist, see Creating Model Configuration (on page 610) . |
| Equipment ID | Select the equipment ID of the ONT. Example: BVM4K00BRA0915-0083 |
| Version | Select the ONT firmware version that you want to download.  Note: You must specify the ONT software version in the Creating Model Version Configuration (on page 612) page. |
| OLT | Select a single or multiple OLTs to which you want to copy the ONT firmware. |
| Ports | Select the ports on which you want to upgrade the OLT.  Note: This field is disabled if you select multiple OLTs in the OLT field. |
| Select Actions | <p>You can select the following options at the same time.</p> <ul style="list-style-type: none"> ◦ Download on OLT. Downloads the ONT firmware image on the OLT. You can skip this step if the ONT firmware image is already available at the OLT. ◦ Download on ONT. Downloads the ONT firmware image on the ONT. <ul style="list-style-type: none"> ▪ Enable Auto Commit. Enables and auto commits the ONT firmware on the ONT. ▪ Enable Activate Commit on ONT Reboot. Enables the auto-activation of ONT and commits the new ONT firmware after the ONT reboot.  Note: You can either select the Enable Auto Commit or Enable Activate Commit on ONT Reboot option. <ul style="list-style-type: none"> ◦ Activate and Commit on ONT. Activates and commits the ONT firmware on the ONT. |

6. Click **Next**.

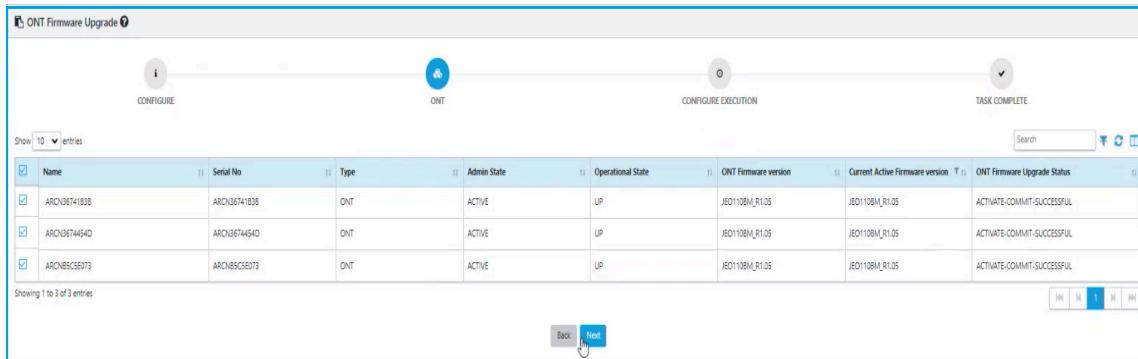
The ONT Information page is displayed.

The following table lists the information displayed on the ONT information page.

Table 329. ONT Information

| Field | Description |
|---------------------------------|--|
| Name | Specifies the name of the ONT. |
| Serial No | Specifies the serial number of the ONT. You can select ONTs based on serial number for firmware upgrade. |
| Type | Specifies the element type. For example, ONT. |
| Admin State | Specifies the ONT admin state (ACTIVE or DEACTIVE). |
| Parent Name | Specifies the OLT details associate with the ONT. |
| Port Name | Specifies the port name attached to the ONT. |
| Operational State | Specifies the operational state of the ONT (UP or DOWN). |
| ONT Firmware Version | Specifies the latest ONT firmware version available on the ONT. |
| Current Active Firmware Version | Specifies the current version of the ONT firmware. You can select ONTs based on the current active firmware version. |
| ONT Firmware Download Status | Specifies the ONT firmware download status (DOWNLOADED or NOT-DOWNLOADED). |

Figure 134. ONT Information



The screenshot shows a table with the following data:

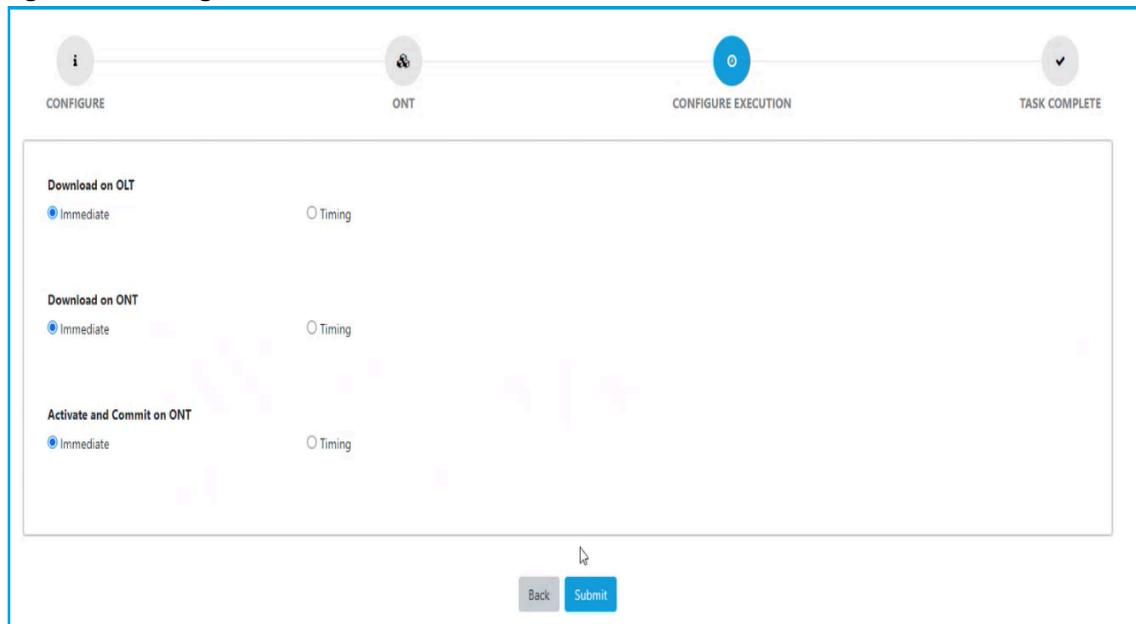
| Name | Serial No | Type | Admin State | Operational State | ONT Firmware version | Current Active Firmware version | ONT Firmware Upgrade Status |
|--------------|--------------|------|-------------|-------------------|----------------------|---------------------------------|-----------------------------|
| ARON06741338 | ARON06741338 | ONT | ACTIVE | UP | JBO108M_R1.05 | JBO1108M_R1.05 | ACTIVATE-COMMIT-SUCCESSFUL |
| ARON06744540 | ARON06744540 | ONT | ACTIVE | UP | JBO108M_R1.05 | JBO1108M_R1.05 | ACTIVATE-COMMIT-SUCCESSFUL |
| ARO185C56073 | ARO185C56073 | ONT | ACTIVE | UP | JBO108M_R1.05 | JBO1108M_R1.05 | ACTIVATE-COMMIT-SUCCESSFUL |

Showing 1 to 3 of 3 entries

- Select all the ONTs.
- A list of ONTs with the same make and model is displayed.
- Click **Next**.

The CONFIGURE EXECUTION page appears.

Figure 135. Configure Execution



9. Select one of the options to upgrade the ONT firmware.
 - **Immediate.** Select this option to perform the ONT firmware upgrade immediately.
 - **Timing.** Select this option to specify the date and time when you want to upgrade the ONT firmware.

The above options are applicable for the following operations.

- Download on OLT
- Download on ONT
 - Enable Auto Commit
 - Enable Activate Commit on ONT Reboot
- Activate and Commit on ONT

10. Click **Submit**.

The **TASK COMPLETE** tab is enabled and changed to green color.

A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

- If the status is **RUNNING**, then the ONT bulk firmware upgrade is in progress and the status changes to **COMPLETED** once the upgrade is successful.
- Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the ONT bulk firmware upgrade task. For more information, see [Table 121: ONT Bulk Firmware Upgrade Task Details \(on page 262\)](#).

Stopping ONT Bulk Firmware Upgrade

The firmware download on ONTs is a time-consuming procedure. CBAC restricts a few operations on the OLT, PON, and ONT on which the upgrade is happening.



Note: The **Pause** and **Resume** features are not supported for ONT bulk firmware upgrades.

Perform the following steps to stop the ONT bulk firmware upgrade.

1. Select **Maintenance > Task**.

The Task List page appears.

2. Click on the three dots (⋮) corresponding to the ONT bulk firmware upgrade.

3. Click **Stop**.

A success message appears indicating the ONT bulk firmware upgrade is stopped successfully and the task status is changed to **TERMINATED**.



Note: You can stop the bulk firmware upgrade of the ONTs for which the firmware download is **In-Progress** or **Pending-Download** state.

Figure 136. Stopping ONT Bulk Upgrade

| Name | Type | Status | Created At | Monitor |
|------|---------------------------|---------|--------------------------|-------------------|
| Test | ONT Bulk Firmware Upgrade | RUNNING | Aug 29, 2023, 4:06:44 PM | Stop |

You can monitor the task details using the **Monitor** page. For more information, see [Table 121: ONT Bulk Firmware Upgrade Task Details \(on page 262\)](#).

Creating Task for OLT Firmware Upgrade

You can upgrade the firmware for the OLT components (BIOS, CPLD, and FPGA).



Note: Before performing the OLT firmware upgrade, you must create a make and model configuration for the respective OLTs. For more information, see [Creating Make Configuration \(on page 606\)](#) and [Creating Model Configuration \(on page 610\)](#).

Perform the following steps to create a task for OLT firmware upgrade.

1. Select **Maintenance > Task**.

The Task List page appears.

2. Click **Create**.

3. Complete the task configuration according to the guidelines provided in the following table.

Table 330. OLT Firmware Upgrade Task Configuration

| Field | Description |
|---|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) ◦ Space |
| Type | Select the task type as “OLT Firmware Upgrade” under OLT . |
| Short Description | Enter a meaningful short description for the task. |
| <p>Click Create.</p> <p>The CONFIGURE page appears.</p> | |
| CONFIGURE | |
| Type | Displays the type as OLT. This field cannot be modified. |
| Make | Select make for the OLT. If the make configuration does not exist, see Creating Make Configuration (on page 606) . |
| Model | Select model for the OLT. If the model configuration does not exist, see Creating Model Configuration (on page 610) . |
| Select Actions | <p>You can select the following options at the same time.</p> <ul style="list-style-type: none"> ◦ Download Software. You must select the software version of the OLT that you want to download. <p> Note: Before you download the OLT software, you must specify the OLT software version using the Creating Model Version Configuration (on page 612) page.</p> <ul style="list-style-type: none"> ◦ Version. Select the OLT software version that you want to update. ◦ Activate Firmware. Select the checkbox to activate the firmware. |
| <p>Click Create.</p> <p>The Configure Execution page appears.</p> <p> Note: Before you are configuring the OLT firmware upgrade, you must create a site group and enable the OLT. For more information, see Creating Site Group Configuration (on page 290).</p> | |

| Field | Description |
|----------------------------|--|
| CONFIGURE EXECUTION | <p>Select the option to download and activate the software execution immediately or schedule the upgrade for a later date and time.</p> <ul style="list-style-type: none">◦ Download Software. Select this option to perform the software download for OLT.◦ Activate Software. Select this option to activate the software upgrade for OLT. <p> Note: You can select both fields, download and activate the software execution.</p> <ul style="list-style-type: none">◦ Immediate. Select this option to perform the OLT firmware upgrade operations immediately.◦ Timing. Select this option to specify the date and time when you want to upgrade the OLT firmware. |

4. Click **Submit**.

The **TASK COMPLETE** tab is enabled and changed to green color.

A confirmation message appears, indicating that the task is initiated successfully.



Note: RMS compares the software version of BIOS, CPLD, and FPGA with the OLT package. If the package and the OLT software versions are same, it skips the upgrade, or the firmware schedules the component to update.

Creating Task for Inventory Collection

This task allows the user to collect hardware inventory reports from the network. This can be used to provide automatic continuous snapshots of the state of the hardware in a network, allow the user to monitor device usage trends as well as to spot any anomalies that may occur.



Note: Before you create the task for inventory collection, you must create the file storage. For more information, see [Creating File Store Configuration \(on page 618\)](#).

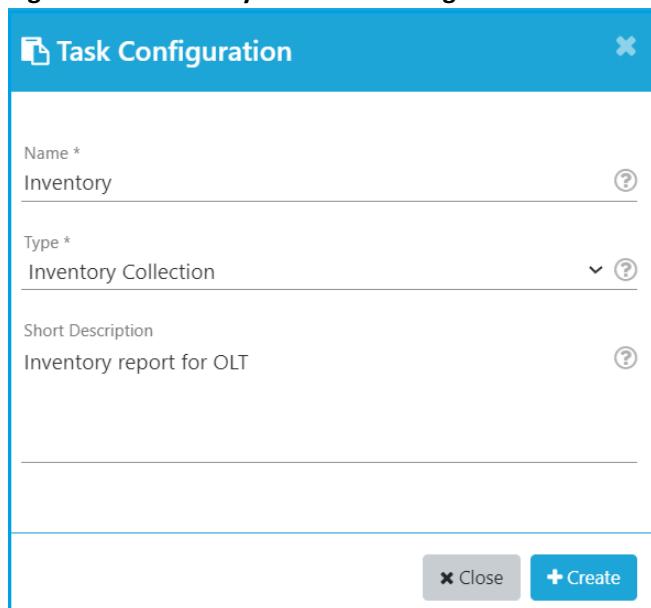
Perform the following steps to create a task for inventory collection.

1. Select **Maintenance > Task**.

The Task List page appears.

2. Click **Create**.

The Task Configuration page appears.

Figure 137. Inventory Collection Configuration

The image shows a 'Task Configuration' dialog box. At the top, it says 'Task Configuration' with a close button 'x'. The form contains three fields: 'Name *' with the value 'Inventory', 'Type *' with the value 'Inventory Collection' and a dropdown arrow, and 'Short Description' with the value 'Inventory report for OLT'. Each field has a question mark icon to its right. At the bottom are two buttons: 'Close' and 'Create'.

3. Complete the task configuration according to the guidelines provided in the following table.

Table 331. Inventory Task Configuration

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Type | Select the task type as “Inventory” under Collections . |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.

The Inventory Collection page appears.

Figure 138. Inventory Collection

The screenshot shows the 'Inventory Collection' configuration screen. At the top, there are three buttons: 'COLLECTION' (highlighted in blue), 'SET EXECUTION TIME', and 'REPORT COMPLETE'. Below these are several input fields: 'TYPE' (set to 'ONT'), 'Admin State' (set to 'ACTIVE'), 'Operational State' (set to 'UP'), and 'OUT' (set to 'olt-136'). To the right, there is a 'File Store' field set to 'oltbackup' and an 'Inventory Collection Fields' section containing 'Name' and 'Admin State'. A 'Next' button is located at the bottom right of the form.

5. Complete the task configuration according to the guidelines provided in the following table.

Table 332. Inventory Collection

| Field | Description |
|-------------------|--|
| TYPE | Select the managed element for which you want to generate the inventory report. You can generate the inventory report for the following managed elements. <ul style="list-style-type: none"> ◦ OLT ◦ ONT ◦ SFP ◦ CPE ◦ Splitter ◦ BNG ◦ Card ◦ Rack ◦ Cable |
| ADMIN_STATE | This field is displayed when you select ONT, or OLT from the TYPE field. Select the admin state of the managed element. The supported values are. <ul style="list-style-type: none"> ◦ ACTIVE ◦ DEACTIVE |
| OPERATIONAL_STATE | This field is displayed when you select ONT, or OLT from the TYPE field. Select the operational state of the managed element. The supported values are <ul style="list-style-type: none"> ◦ UP ◦ DOWN |

| Field | Description |
|-----------------------------|---|
| OLT | <p>This field is displayed when you select ONT, CARD, or SFP from the TYPE field.</p> <p> Note: Select the OLT from the list to filter the inventory report based on the selected OLT. This field is optional.</p> |
| File Storage | Select the file storage location where you want to store the inventory collection report. |
| Inventory Collection Fields | Select one or more parameters of the managed element that you want to include in the inventory report. |

6. Click **Next**.

The SET EXECUTION TIME page appears.

7. Complete the task configuration according to the guidelines provided in the following table.

Table 333. Inventory Execution Time

| Field | Description |
|-----------|---|
| Immediate | Select this option if you want to generate the inventory collection report immediately. |
| Timing | <p>Select this option if you want to schedule the inventory collection report for a later date and time.</p> <ul style="list-style-type: none"> ◦ Select daily, weekly, or monthly. <ul style="list-style-type: none"> ▪ Daily. If you have selected the option as Daily, select the time when the backup needs to be taken from the Select Time list. ▪ Weekly. If you have selected the option as Weekly, you must select the day (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday) from the Select Day list and then select the time from the Select Time list. ▪ Monthly. If you have selected the option as Monthly, you must select the date (From 1 to 31, or Last Day of the Month) from the Select Date list and then select the time from the Select Time list. |

8. Click **Submit**.

A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

- If the status is **RUNNING**, then the inventory collection task is in progress and the status changes to **COMPLETED** once the inventory collection is successful.
- Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the inventory collection task. For more information, see [Table 123: Inventory Collection Task \(on page 265\)](#).

Creating Task for Service Collection

This task allows the user to collect the service information configured in the network. This reports gives the extensive information about the services.



Note: Before you create the task for service collection, you must create the file storage. For more information, see [Creating File Store Configuration \(on page 618\)](#).

Perform the following steps to create a task for service collection.

1. Select **Maintenance > Task**.

The Task List page appears.

2. Click **Create**.

The Task Configuration page appears.

Figure 139. Service Collection

The screenshot shows the 'Task Configuration' dialog box. It has a blue header bar with the title 'Task Configuration' and a close button. The main area contains three input fields: 'Name *' with the value 'Service_Collection', 'Type *' with the value 'Service Collection', and 'Short Description' with the value 'Service Collection for OLT'. Each field has a question mark icon to its right. At the bottom of the dialog are two buttons: a grey 'Close' button and a blue 'Create' button with a plus sign.

3. Complete the task configuration according to the guidelines provided in the following table.

Table 334. Service Collection Task Configuration

| Field | Description |
|-------------------|--|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Type | Select the task type as “Service Collection” under Collections . |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.

The Service Collection page appears.

Figure 140. Service Collection

5. Complete the task configuration according to the guidelines provided in the following table.

Table 335. Service Collection Configuration

| Field | Description |
|---------------------------|---|
| File Configuration | |
| File Store | Select the file storage location where you want to store the service collection report. |
| Filter | |
| ADMIN STATE | Select the admin state of the service. The supported values are. |

| Field | Description |
|---------------------------|---|
| | <ul style="list-style-type: none"> ◦ ACTIVE ◦ DEACTIVE |
| SITE GROUP | Select the site group of the service. |
| Service Name | Enter the service name for which you want to generate the report. |
| Service Collection Fields | Select one or more parameters of the service that you want to include in the inventory report. |
| OPERATIONAL_STATE | Select the operational state of the service. The supported values are. <ul style="list-style-type: none"> ◦ UP ◦ DOWN |
| OLT | Enter the OLT name. |

6. Complete the task configuration according to the guidelines provided in the following table.

Table 336. Set Execution Time

| Field | Description |
|-----------|--|
| Immediate | Select this option if you want to generate the service collection report immediately. |
| Timing | Select this option if you want to schedule the service collection report for a later date and time. <ul style="list-style-type: none"> ◦ Select daily, weekly, or monthly. <ul style="list-style-type: none"> ▪ Daily. If you have selected the option as Daily, select the time when the backup needs to be taken from the Select Time list. ▪ Weekly. If you have selected the option as Weekly, you must select the day (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday) from the Select Day list and then select the time from the Select Time list. ▪ Monthly. If you have selected the option as Monthly, you must select the date (From 1 to 31, or Last Day of the Month) from the Select Date list and then select the time from the Select Time list. |

7. Click **Submit**.

A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

- If the status is **RUNNING**, then the service collection task is in progress and the status changes to **COMPLETED** once the service collection is successful.
- Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the service collection task. For more information, see [Table 124: Service Collection Task \(on page 267\)](#).

Creating Task for Fault Collection



Note: In case the fault collection task fails, an alarm is raised with entity as Filename and the same is displayed under **Monitor > Fault** page.

This task allows the user to create fault collection.

Perform the following steps to create a task for the fault collection.

1. Select **Maintenance > Task**.

The Task List page appears.

2. Click **Create**.

The Task Configuration page appears.

Figure 141. Fault Collection

The screenshot shows the 'Task Configuration' dialog box. The 'Name' field is set to 'Fault_Collect'. The 'Type' field is set to 'Fault Collection'. The 'Short Description' field contains the text 'Fault Collection for OLT and ONT'. At the bottom, there are 'Close' and 'Create' buttons.

3. Complete the task configuration according to the guidelines provided in the following table.

Table 337. Fault Collection Configuration

| Field | Description |
|-------------------|--|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Type | Select the task type as “Fault” under Collections . |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.

The Fault Collection page appears.

Figure 142. Fault Collection

5. Complete the configuration according to the guidelines provided in the following table.

Table 338. Fault Task

| Field | Description |
|-------------------|---|
| COLLECTION | |
| ENTITY TYPE | Select the entity type from the list. You can select more than one entity at a time. The supported values are. <ul style="list-style-type: none"> ◦ OLT ◦ ONT ◦ BACKUP ◦ CARD ◦ CONTROLLER |

| Field | Description |
|--|---|
| | <ul style="list-style-type: none"> ◦ SPLITTER ◦ LAG ◦ CPE ◦ ME_PORT ◦ SERVICE ◦ STORM_CONTROL_PROFILE ◦ TYPE_B_PROTECTION ◦ ACL_PROFILE |
|  Note: The following fields are displayed only if you select the entity type as OLT . | |
| ENTITY GROUP | Select the entity group from the list. |
| SITE/MANAGEMENT DOMAIN/ME GROUP | Select the site, management domain, or ME group from the list. |
| DEVICE IDs | Select one or more device IDs from the list.  Note: The users are allowed to select upto 10 device IDs. |
| Include all Entities that are children of the Device Id | If you select this parameter, the OLT entity and its children are included. |
| SEVERITY | Select the severity level from the list. The supported levels are. <ul style="list-style-type: none"> ◦ CRITICAL ◦ MAJOR ◦ MINOR ◦ WARNING ◦ INDETERMINATE |
| TIME RANGE | Select the date range to generate the fault collection report. You can also specify the duration (yesterday, last 7 days, last 30 days, this month, last month, and custom range) for which the report is generated. When you select the custom range, you must specify the From and To date in calendar (HH:MM:SS formats). |
| STATUS | Select the status from the list. The supported statuses are. |

| Field | Description |
|------------------------------|--|
| | <ul style="list-style-type: none">◦ ACTIVE◦ CLEARED |
| Fault Collection Fields | Select the fault collection field. The supported values are. <ul style="list-style-type: none">◦ Severity◦ Id◦ Fault◦ Controller Alarm Code◦ Entity◦ Entity Id◦ Type◦ Parent Entity◦ Parent Site◦ Error Code◦ Event Type◦ Site◦ Description◦ First Occurrence Time◦ Last Occurrence Time◦ Device Reported Time◦ Controller Reported Time◦ Data◦ Service Affecting◦ Probable Cause◦ Proposed Repair Action◦ OLT◦ Controller |
| File Store | Select the file storage location where you want to store the fault collection report. |
| EXECUTION TIME POLICY | |
| Immediate | Select this option if you want to generate the report immediately. |
| Timing | Select this option if you want to schedule the report generation for a later date and time. You can select daily, weekly, or monthly. |

| Field | Description |
|-------|--|
| | <ul style="list-style-type: none">◦ Daily. If you have selected the option as Daily, select the time when the report needs to be generated.◦ Weekly. If you have selected the option as Weekly, you must select the day (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday) from the Select Day list and then select the time from the Select Time list.◦ Monthly. If you have selected the option as Monthly, you must select the date (From 1 to 31, or Last Day of the Month) from the Select Date list and then select the time from the Select Time list. |

6. Click **Submit**.

A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

- If the status is **RUNNING**, then the fault collection task is in progress and the status changes to **COMPLETED** once the fault collection is successful.
- Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the fault collection task. For more information, see [Table 125: Fault Collection Task \(on page 269\)](#).

Creating Task for Event Collection

This task allows the user to create event collection.

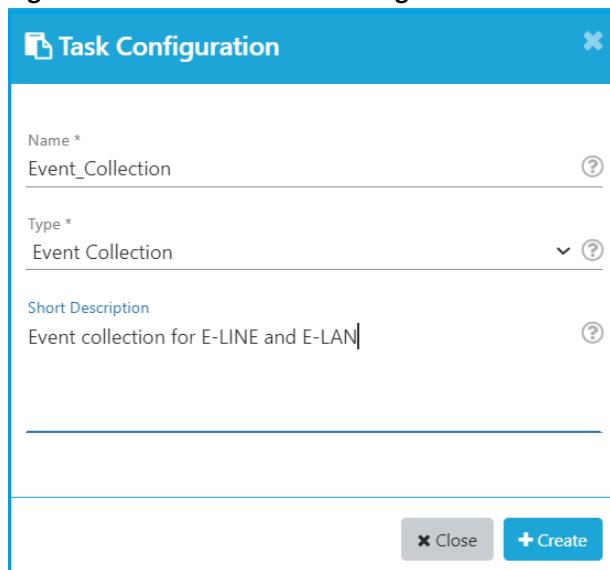
Perform the following steps to create a task for the event collection.

1. Select **Maintenance > Task**.

The Task List page appears.

2. Click **Create**.

The Task Configuration page appears.

Figure 143. Event Collection Configuration

3. Complete the task configuration according to the guidelines provided in the following table.

Table 339. Event Collection Configuration

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Type | Select the task type as “Event” under Collections . |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.

The Event Collection page appears.

Figure 144. Event Collection

5. Complete the configuration according to the guidelines provided in the following table.

Table 340. Event Collection Task

| Field | Description |
|--|---|
| COLLECTION | |
| ENTITY TYPE | <p>Select the entity type from the list. You can either select all or multiple entities at a time.</p> <p>The supported values are.</p> <ul style="list-style-type: none"> <input type="radio"/> ONT <input type="radio"/> BACKUP <input type="radio"/> CARD <input type="radio"/> CONTROLLER <input type="radio"/> SPILTTER <input type="radio"/> LAG <input type="radio"/> CPE <input type="radio"/> ME_PORT <input type="radio"/> UNKNOWN <input type="radio"/> STORM_CONTROL_PROFILE <input type="radio"/> TYPE_B_PROTECTION <input type="radio"/> ACL_PROFILE <input type="radio"/> OLT |
| <p> Note: The following fields are displayed only if you select the entity type as OLT.</p> | |
| ENTITY GROUP | Select the entity group from the list. |

| Field | Description |
|---------------------------------|--|
| SITE/MANAGEMENT DOMAIN/ME GROUP | Select the site, management domain, or ME group from the list. |
| DEVICE IDs | <p>Select one or more device IDs from the list.</p> <p> Note:</p> <ul style="list-style-type: none"> ◦ The users are allowed to select upto 10 device IDs. ◦ If you select include all entities that are children of the device ID, the OLT entity and its children are included. |
| EVENT CODE | <p>Select the event code from the list. You can either select all or multiple event codes at a time.</p> <p>The supported values are.</p> <ul style="list-style-type: none"> ◦ CONTROLLER-ACTIVATED ◦ CONTROLLER-AUTHENTICATION-FAILED ◦ CONTROLLER-AUTHENTICATION-SUCCESSFUL ◦ CONTROLLER-DEACTIVATED ◦ ENABLE-E-LINE-SUCCESSFUL ◦ INTERFACE-DOWN ◦ INTERFACE-UP ◦ ME-CONFIG ◦ ME-LOGIN-SUCCESS ◦ ME-UP ◦ PORT-DISCOVERED ◦ PORT-SFP-INVENTORY ◦ SDPON-NEW-SOFTWARE-VERSION-AVAILABLE ◦ SDPON-SOFTWARE-DOWNLOAD-SUCCESSFUL ◦ SDPON-SOFTWARE-UPGRADE-SUCCESSFUL ◦ SUBSCRIBER-SERVICE-IP-ADDRESS ◦ SUBSCRIBER-SERVICE-UP |
| TIME RANGE | <p>Select the date range to generate the event collection report.</p> <p>You can also specify the duration (yesterday, last 7 days, last 30 days, this month, last month, and custom range) for which the report is generated. When you select the custom range, you must specify the From and To date in calendar (HH:MM:SS formats).</p> |
| Event Collection Fields | Select the event collection field. You can either select all or multiple event collection fields at a time. |

| Field | Description |
|------------------------------|---|
| | <p>The supported values are.</p> <ul style="list-style-type: none"> ◦ Event Code ◦ Entity ◦ Entity Id ◦ Entity Type ◦ Parent Name ◦ Error Code ◦ Reported Time ◦ Device Reported Time ◦ Controller Reported Time ◦ Description ◦ Data |
| File Store | <p>Enter the file storage location where you want to store the event collection report.</p> <ul style="list-style-type: none"> ◦ RMS Backup File Store ◦ NE Backup File Store ◦ Performance Monitoring File Store <p> Note:</p> <ul style="list-style-type: none"> ◦ Before creating an Event Collection task you must create a file storage to store a CSV file. See Creating File Store Configuration (on page 618). ◦ Once the task is executed, a CSV file is uploaded to the SFTP server. |
| EXECUTION TIME POLICY | |
| Immediate | Select this option if you want to generate the report immediately. |
| Timing | <p>Select this option if you want to schedule the report generation for a later date and time. You can select daily, weekly, or monthly.</p> <ul style="list-style-type: none"> ◦ Daily. If you have selected the option as Daily, select the time when the report needs to be generated. ◦ Weekly. If you have selected the option as Weekly, you must select the day (Sunday, Monday, Tuesday, Wednesday, Thursday, |

| Field | Description |
|-------|--|
| | <p>Friday, or Saturday) from the Select Day list and then select the time from the Select Time list.</p> <ul style="list-style-type: none">◦ Monthly. If you have selected the option as Monthly, you must select the date (From 1 to 31, or Last Day of the Month) from the Select Date list and then select the time from the Select Time list. |

6. Click **Submit**.

A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

- If the status is **RUNNING**, then the event collection task is in progress and the status changes to **COMPLETED** once the event collection is successful.
- Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the event collection task. For more information, see [Table 126: Event Collection Task \(on page 270\)](#).

Creating Task for Audit Log Collection

This task allows the user to create audit log collection.



Note: Only admin can perform audit log collection.

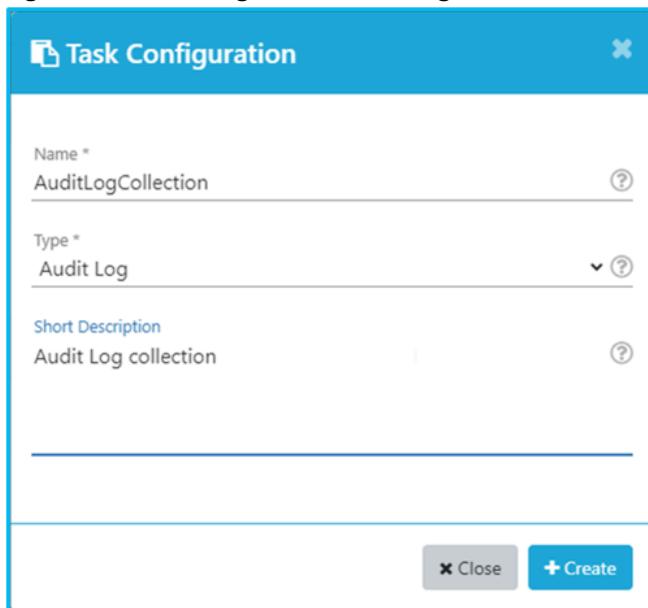
Perform the following steps to create a task for the audit log collection.

1. Select **Maintenance > Task**.

The Task List page appears.

2. Click **Create**.

The Task Configuration page appears.

Figure 145. Audit Log Collection Configuration

3. Complete the task configuration according to the guidelines provided in the following table.

Table 341. Audit Log Collection Configuration

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Type | Select the task type as “AuditLog” under Collections . |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.

The Audit Log Collection page appears.

Figure 146. Audit Logs Collection

The screenshot shows the 'Audit Log Collection' configuration interface. It includes the following fields and sections:

- USER ID:** admin x
- RESOURCE TYPE:** bandwidth_profile x
- RESOURCE NAME:** Activate ONT x
- RESOURCE ACTION:** ACTIVATE x
- STATUS:** Select
- TIME RANGE:** 03/04/2024 00:00:00 - 03/04/2024 18:06:45
- Audit Log Collection Fields:** User Name x, User Id x
- File Store:** Select File Store...
- Execution Time Policy:** Immediate, Timing

A 'Submit' button is located at the bottom right of the form.

5. Complete the configuration according to the guidelines provided in the following table.

Table 342. Audit Log Collection

| Field | Description |
|-------------------|---|
| COLLECTION | |
| USER ID | Specifies the user ID. |
| RESOURCE TYPE | Specifies the resource type. |
| RESOURCE NAME | Specifies the resource name. |
| RESOURCE ACTION | Specifies the type of action performed on the resource. The supported actions are: <ul style="list-style-type: none">◦ ACTIVATE◦ ACTIVATE_SOFTWARE◦ ADD◦ CHANGE_PASSWORD◦ COMMIT_SOFTWARE◦ CREATE◦ DEACTIVATE◦ DELETE◦ DISABLE |

| Field | Description |
|------------------------------|---|
| | <ul style="list-style-type: none"> ◦ ENABLE ◦ DOWNLOAD_SOFTWARE ◦ LOGIN ◦ LOGOUT ◦ MANUAL-SWITCHOVER ◦ MODIFY ◦ ONT_REBOOT ◦ ONT_INITIATED ◦ RECONCILE ◦ REPLACE ◦ SCHEDULE ◦ SDPON-UPGRADE ◦ SOFTWARE_ACTIVATE ◦ SOFTWARE_COMMIT ◦ SOFTWARE_DOWNLOAD ◦ SUBSCRIBE_KPI ◦ UPDATE-RMS-VERSION-TO-CBAC |
| STATUS | <p>Specifies the status of the task that triggered the audit log.</p> <ul style="list-style-type: none"> ◦ SUCCESS. Indicates that the job has completed successfully. ◦ FAILED. Indicates that the job has failed and is terminated. |
| TIME RANGE | <p>Select the date range to generate the audit log collection report. You can also specify the duration (yesterday, last 7 days, last 30 days, this month, last month, and custom range) for which the report is generated. When you select the custom range, you must specify the From and To date in calendar (HH:MM:SS formats).</p> |
| Audit Logs Collection Fields | <p>Select the audit log collection field. You can either select all or multiple audit log collection fields at a time.</p> <p>The supported values are.</p> <ul style="list-style-type: none"> ◦ User Name ◦ User ID ◦ Time ◦ Resource ID ◦ Resource Name ◦ Resource Type ◦ Resource Action ◦ IP Address |

| Field | Description |
|------------------------------|---|
| | <ul style="list-style-type: none"> ◦ Parent Name ◦ Status ◦ Request Data |
| File Store | <p>Enter the file storage location where you want to store the audit log collection report.</p> <ul style="list-style-type: none"> ◦ RMS Backup File Store ◦ NE Backup File Store ◦ Performance Monitoring File Store <p> Note:</p> <ul style="list-style-type: none"> ◦ Before creating an Audit Log Collection task you must create a file storage to store a CSV file. See Creating File Store Configuration (on page 618). ◦ Once the task is executed, a CSV file is uploaded to the SFTP server. |
| EXECUTION TIME POLICY | |
| Immediate | Select this option if you want to generate the report immediately. |
| Timing | <p>Select this option if you want to schedule the report generation for a later date and time. You can select daily, weekly, or monthly.</p> <ul style="list-style-type: none"> ◦ Daily. If you have selected the option as Daily, select the time when the report needs to be generated. ◦ Weekly. If you have selected the option as Weekly, you must select the day (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday) from the Select Day list and then select the time from the Select Time list. ◦ Monthly. If you have selected the option as Monthly, you must select the date (From 1 to 31, or Last Day of the Month) from the Select Date list and then select the time from the Select Time list. |

6. Click **Submit**.

A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

- If the status is **RUNNING**, then the audit log collection task is in progress and the status changes to **COMPLETED** once the audit log collection is successful.
- Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the audit log collection task. For more information, see [Audit Log Collection \(on page 272\)](#).

Creating Task for Bulk Port Modification

This task allows the user to update the configuration of more than one PON port at the same time.

The bulk port modification includes the following updates.

- Activation of PON ports
- Deactivation of PON ports
- Configuration updates for PON ports

Perform the following steps to create a task for the bulk port modification.

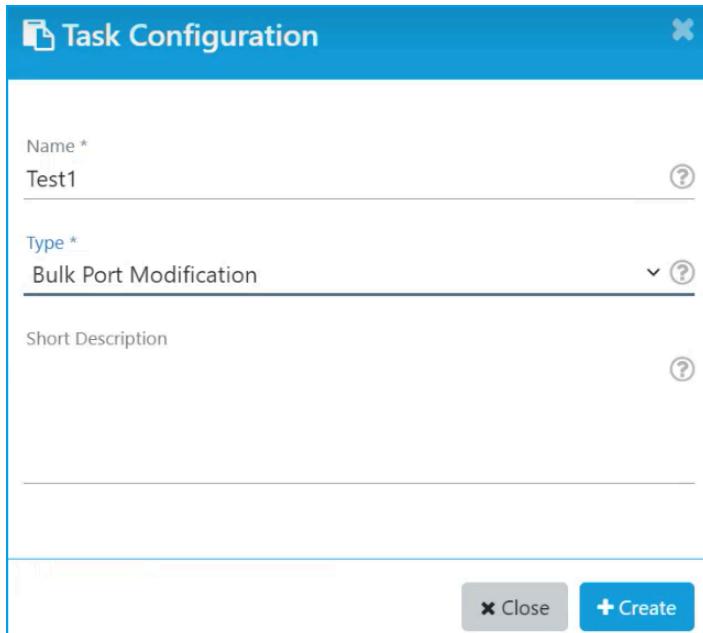
1. Select **Maintenance > Task**.

The Task List page appears.

2. Click **Create**.

The Task Configuration page appears.

Figure 147. Bulk Port Modification



3. Complete the task configuration according to the guidelines provided in the following table.

Table 343. Bulk Port Modification Configuration

| Field | Description |
|-------------------|--|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| Type | Select the task type as Bulk Port Modification under OLT . |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.

The CONFIGURE page appears.

Figure 148. Bulk Port Modification

5. Complete the configuration according to the guidelines provided in the following table.

Table 344. Bulk Port Modification Task

| Field | Description |
|-----------|--|
| OLT | Select the OLT from the list. |
| Port Type | Select the port type as PON from the list. |

| Field | Description |
|-------------|---|
| Port Action | Select the port action from the list. The supported values are. <ul style="list-style-type: none"> ◦ Activate. See step 6 (on page 712). ◦ Deactivate. See step 7 (on page 713). ◦ Configuration Update. See step 8 (on page 713). |
| Port Mode | Specifies the port mode. This field is displayed only when the Port Action field is selected as Configuration Update . The supported values are. <ul style="list-style-type: none"> ◦ GPON ◦ XGSPON ◦ ANYPON |

6. Perform the following steps to activate the PON ports.

- Select the **Port Action** as **Activate**.

A list of deactivated PON ports are displayed.

- Select the checkbox for the PON ports that you want to activate.
- Click **Submit**.

A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

- If the status is **RUNNING**, then the bulk port modification is in progress and the status changes to **COMPLETED** once the modification is successful.
- Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the bulk port modification task. For more information, see [Bulk Port Modification \(on page 275\)](#).

Figure 149. Activate PON Ports

The screenshot shows the 'Bulk Port Modification' configuration interface. At the top, there are three buttons: 'CONFIGURE' (with an info icon), 'SELECT CONFIGURATIONS' (with a gear icon), and 'TASK COMPLETE' (with a checkmark icon). Below these are several configuration fields:

- OLT**: olt:185
- Port Type ***: PON
- Port Action ***: Activate
- Port Mode ***: Select the option

 A section titled 'Choose the ports to Activate' follows, with a table showing port details:

| Name | Port Mode | Admin State | Operational State |
|---------|-----------|-------------|-------------------|
| SFPON-2 | gp0n | REACTIVE | DOWN |
| SFPON-1 | gp0n | REACTIVE | DOWN |

 The table includes a 'Show 10 entries' dropdown, a search bar, and a navigation bar at the bottom. A note at the bottom left says 'Showing 31 to 32 of 32 entries' and '2 selected out of 32'.

7. Perform the following steps to deactivate the PON ports.

- a. Select the **Port Action** as **Deactivate**.

A list of activate PON ports are displayed.

Figure 150. Deactivate PON Ports

| <input type="checkbox"/> | Name | Port Mode | Admin State | Operational State |
|--------------------------|-----------|-----------|-------------|-------------------|
| <input type="checkbox"/> | SFPPON-32 | gpon | ACTIVE | UP |
| <input type="checkbox"/> | SFPPON-31 | auto | ACTIVE | UP |
| <input type="checkbox"/> | SFPPON-30 | gpon | ACTIVE | UP |

Showing 1 to 3 of 3 entries

0 selected out of 3

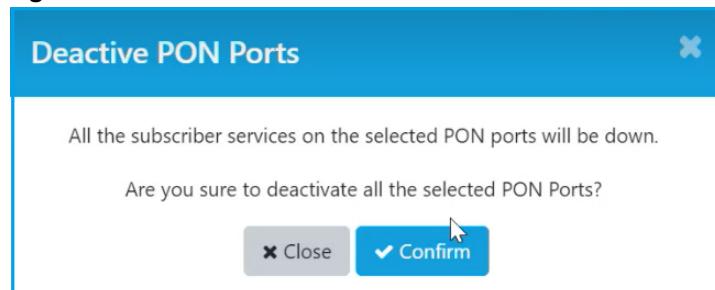
Submit

- b. Select the checkbox for the PON ports that you want to deactivate.

- c. Click **Submit**.

The Deactive PON Ports page appears with a warning message.

Figure 151. Deactive PON Ports



- d. Click **Confirm**.

Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the bulk port modification task. For more information, see [Bulk Port Modification \(on page 275\)](#).

8. Perform the following steps to update the PON ports configuration.

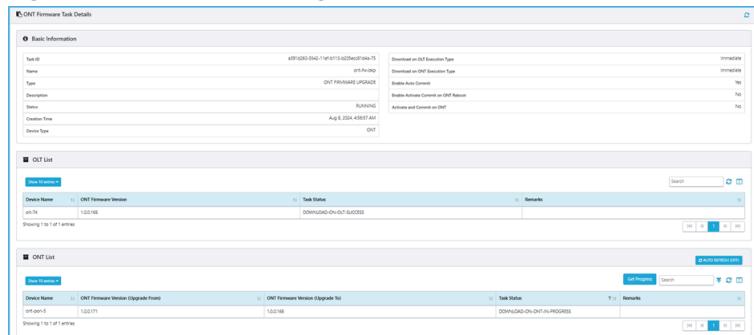
- a. Select the **Port Action** as **Configuration Update**.
- b. Select the **Port Mode** from the list.

A list of PON ports are displayed.

- c. Select the checkbox for the PON ports that you want to update.
- d. Click **Submit**.

The SELECT CONFIGURATIONS page appears.

Figure 152. Bulk Port Configuration



- e. Complete the configuration according to the guidelines provided in the following table.

Table 345. Bulk Port Configuration

| Field | Description |
|---------------------------------|--|
| Port Mode | Specifies the port mode. |
| GPON | |
| GPON Alarm Profile | Select the OLT port alarm profile from the list. This field is applicable for GPON and CPON port mode. |
| GPON Multicast Shaper Profile | Select the GPON multicast shaper profile. This field is applicable only for the PON port. This field is applicable for GPON and CPON port mode. |
| GPON Downstream FEC | Specifies whether the Forward Error Correction (FEC) is enabled in the downstream traffic for GPON port. This field is applicable for GPON and CPON port mode. The supported values are: <ul style="list-style-type: none"> ▪ ENABLED ▪ DISABLED |
| XGSPON | |
| XGSPON Alarm Profile | Select the OLT port alarm profile from the list. This field is applicable for Auto, XGSPON, and CPON port mode. |
| XGSPON Multicast Shaper Profile | Select the XGSPON multicast shaper profile. This field is applicable only for the PON port. |

| Field | Description |
|--|--|
| | This field is applicable for Auto, XGSPON, and CPON port mode. |
| XGSPON Downstream FEC | Specifies whether the Forward Error Correction (FEC) is enabled in the downstream traffic for XGSPON port. This field is applicable for XGSPON and CPON port mode. The supported values are: <ul style="list-style-type: none"> ▪ ENABLED ▪ DISABLED |
| PON Encryption | |
| Enable PON Encryption | Specifies PON encryption. |
| Multicast Queue Priority | Specifies the priority to be applied on the downstream multicast queue. This field is applicable only for the PON. |
| SFP Alarm Profile | Specifies the SFP alarm profile. |
| PON Encryption Key Interval (milliseconds) | This field is displayed only when the “PON Encryption Enabled” field is selected. Enter the PON encryption key exchange interval in milliseconds. |
| Active IGMP Channels | Specifies the active IGMP channels for the PON port. The supported value ranges from 0 to 11,648. |
| Rogue ONT | |
| Periodic Rogue ONT Detection Control | Select whether the periodic rogue ONT detection needs to be enabled. The supported values are: <ul style="list-style-type: none"> ▪ ENABLED ▪ DISABLED |
| Periodic Rogue ONT Detection Measurement Type | Select the RSSI measurement window type. The supported values are: <ul style="list-style-type: none"> ▪ SILENT-WINDOW ▪ CUTOFF-WINDOW |
| Periodic Rogue ONT Detection Interval (milliseconds) | Enter the periodic rogue ONU detection procedure initiation interval in milliseconds. The value ranges from 1000 to 10000000 milliseconds. |
| Alloc Type to Scan | Select the alloc ID type to scan. The supported values are: <ul style="list-style-type: none"> ▪ UNUSED ▪ PREVIOUSLY-USED ▪ ALL |

| Field | Description |
|----------------------------|---|
| Others | |
| Maximum Logical Distance | Specifies the maximal logical distance in kilometers between the ONU and the OLT on the PON port. The supported value ranges from 0 to 60. |
| Maximum Differential Reach | Specifies the maximum distance in kilometers between the closest ONU to the farthest ONU from the OLT. The value ranges from 0 to 40. |

- f. If you want to activate the deactivated ports, select the **Activate all the deactivated ports selected in the previous screen** check box.

The following notes are displayed.

- Configuration changes made in this screen will override existing configuration for the chosen ports.
- Certain configuration are disabled as they are not applicable if any of the ports are in activated state.

- g. Click **Update Configuration**.

A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

- If the status is **RUNNING**, then the bulk port modification is in progress and the status changes to **COMPLETED** once the modification is successful.
- Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the bulk port modification task. For more information, see [Bulk Port Modification \(on page 275\)](#).

Creating Task for Configuration Update

This task allows the user to update the configuration of single or more than one OLT. The OLT configuration includes NTP profile, log profile, authentication profile, TACACS profile, alarm soak profile, alarm profile, and bandwidth validation.

Creating Single or Bulk OLT Configuration Update



Note: Before you perform the OLT configuration update, you must create the following profile configuration.

- [Creating NTP Profile \(on page 553\)](#)
- [Creating Log Profile \(on page 503\)](#)
- [Creating Authentication Profile \(on page 537\)](#)

- [Creating TACACS Profile \(on page 559\)](#)
- [Alarm Profile \(on page 473\)](#)

Perform the following steps to create a task for OLT configuration update.

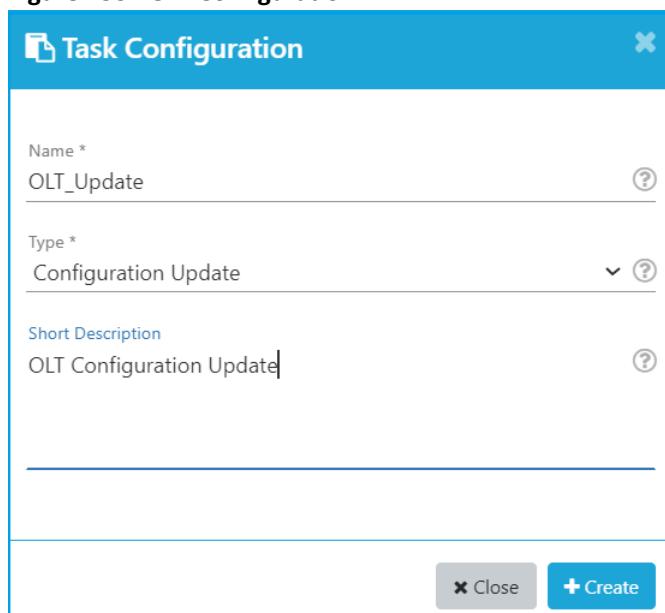
1. Select **Maintenance > Task**.

The Task List page appears.

2. Click **Create**.

The Task Configuration page appears.

Figure 153. OLT Configuration



The screenshot shows the 'Task Configuration' dialog box. It has a blue header bar with the title 'Task Configuration'. The main area contains three input fields: 'Name *' with value 'OLT_Update', 'Type *' with value 'Configuration Update', and 'Short Description' with value 'OLT Configuration Update'. Each field has a question mark icon to its right. At the bottom are two buttons: a grey 'Close' button and a blue 'Create' button with a plus sign.

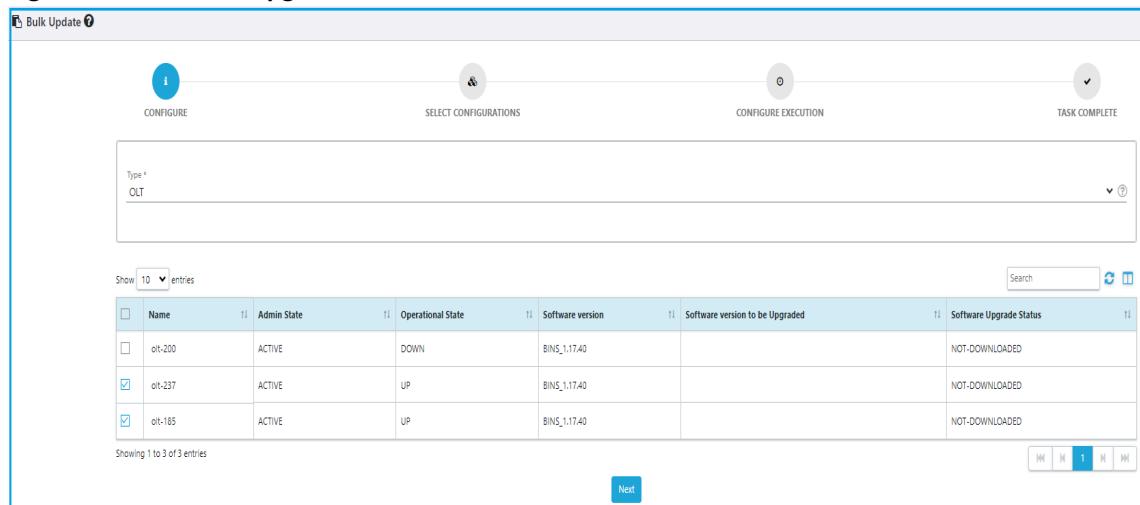
3. Complete the task configuration according to the guidelines provided in the following table.

Table 346. OLT Configuration Update

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Type | Select the task type as “Configuration Update” under OLT . |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.

The Bulk Update page appears.

Figure 154. Bulk OLT Upgrade

5. Select the device type as OLT.

The page displays the number of OLTs configured in the system with the following information.

Table 347. OLT Information

| Field | Description |
|---------------------------------|---|
| Name | Specifies the name of the OLT. |
| Admin State | Specifies the admin state of the OLT (ACTIVE or INACTIVE). |
| Operational State | Specifies the operational state of the OLT (UP or Down). |
| Software Version | Specifies the software version of the OLT. |
| Software Version to be Upgraded | Specifies the new software version to which the OLT needs to be upgraded. |
| Software Upgrade Status | Specifies the status of the software upgrade operation. The supported status are: <ul style="list-style-type: none"> ◦ DOWNLOAD_IN_PROGRESS ◦ DOWNLOAD_FAILED ◦ ACTIVATION_IN_PROGRESS ◦ ACTIVATION_FAILED ◦ COMMIT_IN_PROGRESS ◦ COMMIT_FAILED/ ◦ ROLLBACK_IN_PROGRESS ◦ ROLLBACK_FAILED ◦ NOT-DOWNLOADED |

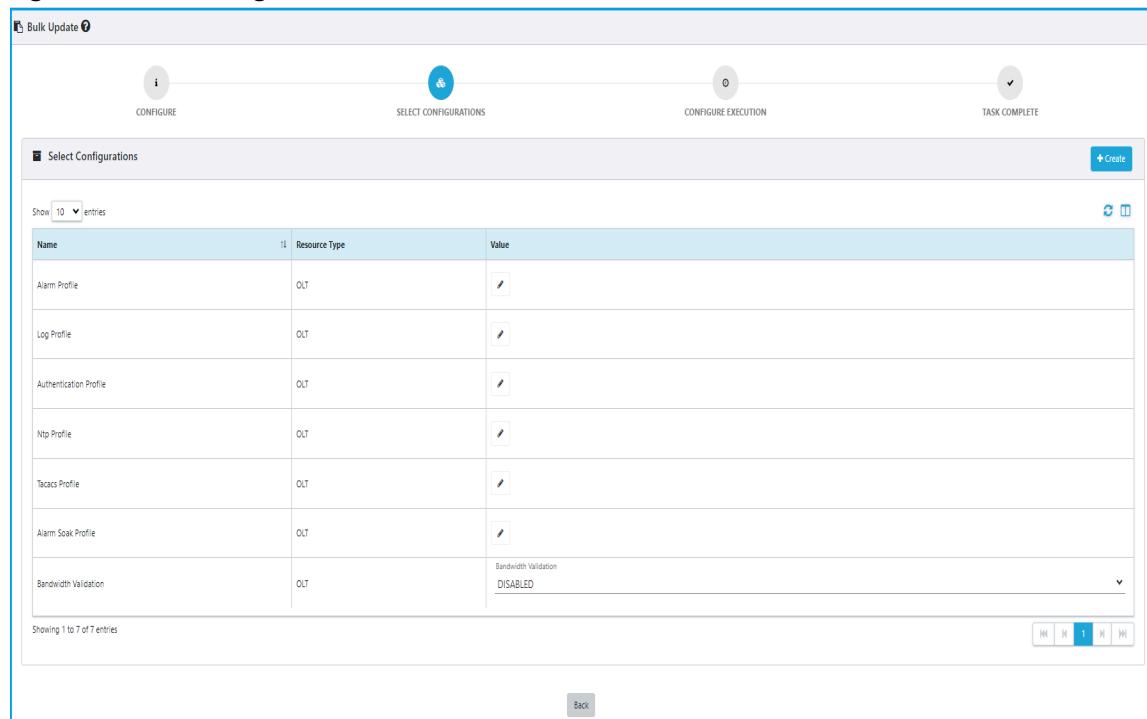
6. Select one (single) or more OLT (bulk) for the configuration update.

7. Click **Next**.

The Select Configuration page appears with the following profile configuration information.

- Alarm Profile
- Log Profile
- Authentication Profile
- NTP Profile
- TACACS Profile
- Alarm Soak Profile
- Bandwidth Validation

Figure 155. OLT Configuration



| Name | Resource Type | Value |
|------------------------|---------------|----------------------------------|
| Alarm Profile | OLT | / |
| Log Profile | OLT | / |
| Authentication Profile | OLT | / |
| Ntp Profile | OLT | / |
| Tacacs Profile | OLT | / |
| Alarm Soak Profile | OLT | / |
| Bandwidth Validation | OLT | Bandwidth Validation DISABLED |

8. Update the required profile configuration of the OLT by clicking the **Edit** option from the **Value** column corresponding to the profile.

9. Click **Save** to save the updated configuration.

10. Click **Create**.

The CONFIGURE EXECUTION page appears.

11. Select one of the option for OLT configuration update.

- **Immediate**. Select this option to perform the OLT configuration immediately.
- **Timing**. Select this option to specify the date and time when you want to perform the OLT configuration.

12. Click **Submit**.

A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

- If the status is **RUNNING**, then the configuration update is in progress and the status changes to **COMPLETED** once the update is successful.
- Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the OLT configuration task. For more information, see [Table 128: OLT Configuration Update Task \(on page 273\)](#).

Creating Task for OLT Reboot

You can reboot the OLT when the OLT goes into an irrecoverable state of function. You can perform bulk OLT reboot using this page. You can also perform on-demand reboot of the OLT from RMS. For more information, see [Reboot the OLT \(on page 388\)](#).



Note: Before you create a task to perform the OLT reboot, you must create a site group and the OLT must be part of the site group. For more information, see [Creating Site Group Configuration \(on page 290\)](#).

Perform the following steps to create a task for the OLT reboot.

1. Select **Maintenance > Task**.
The Task List page appears.
2. Click **Create**.
The Task page appears.
3. Complete the task configuration according to the guidelines provided in the following table.

Table 348. OLT Reboot Task Configuration

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space |
| Type | Select the task type as “Reboot” under OLT . |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.
5. Complete the configuration according to the guidelines provided in the following table.

Table 349. OLT Reboot Task

| Field | Description |
|---|---|
| Configure | |
| Type | Select the device type. Example: OLT |
| Reason | Enter the reason for rebooting the OLT. |
| Site Group | Select the site from the left-hand side of the pane. You must create a site and associate the site in the Inventory > OLT page. |
| <p>The page displays the list of OLT devices that are active along with the following details. Select one or more devices that you want to reboot.</p> <ul style="list-style-type: none"> ◦ Name. Specifies the name of the OLT. ◦ Type. Specifies the device type. ◦ Make. Specifies the make of the device. ◦ Model. Specifies the model of the device. ◦ Admin State. Specifies the admin state of the device. ◦ Operational State. Specifies the operational state of the device. ◦ Software Version. Specifies the software version of the device. ◦ Last Reboot Status. Specifies last reboot status of the device. | |
| Click Next. | |
| CONFIGURE EXECUTION | <p>Specifies whether you want to reboot the OLT immediately or schedule the OLT reboot for a later date and time.</p> <ul style="list-style-type: none"> ◦ Immediate. Select this option if you want to reboot the OLT immediately. ◦ Timing. Select this option if you want to schedule the OLT reboot for a later date and time. You can select daily, weekly, monthly, or one day. |

6. Click **Submit**.

The **TASK COMPLETE** tab is enabled and changed to green color.

A confirmation message appears, indicating that the task is initiated successfully.

Creating Task for PON Port Migration

Prerequisites

The following prerequisites must be fulfilled before creating task for PON port migration.

- The source PON port must be in a **Deactive** state and the destination PON port can be in **Activate** or **Deactive** state.
- The source and destination PON ports must be in the same mode. For example, GPON, XGSPON, and so on.

A user can create a task to move the subscriber services from one PON port to another PON port under the same OLT. This is required when the PON port becomes non-functional due to SFP failure, PON hardware fault, or other reasons. The user connects the fiber to another PON port and moves all the subscriber services to the new PON port.

The PON port movement is supported only within the same OLT. The failed port and the new port must belong to the same OLT.

Perform the following steps to create a task for the PON port migration.

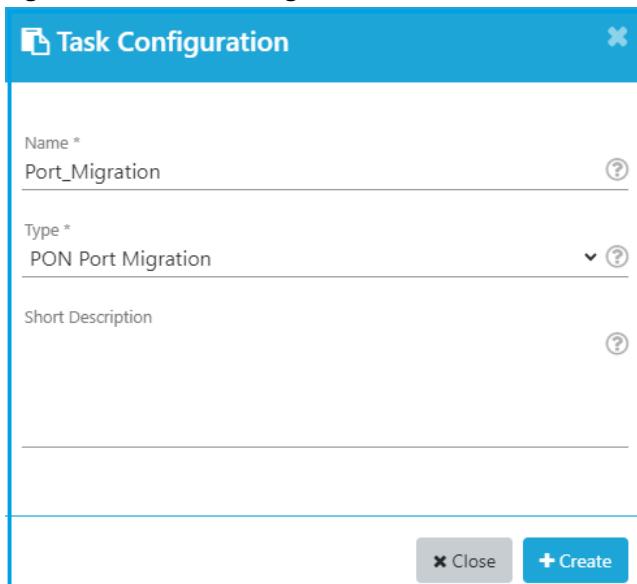
1. Select **Maintenance > Task**.

The Task List page appears.

2. Click **Create**.

The Task Configuration page appears.

Figure 156. PON Port Migration



The screenshot shows the 'Task Configuration' dialog box. The 'Name' field is filled with 'Port_Migration'. The 'Type' field is set to 'PON Port Migration'. The 'Short Description' field is empty. At the bottom, there are 'Close' and 'Create' buttons.

3. Complete the task configuration according to the guidelines provided in the following table.

Table 350. PON Port Migration Configuration

| Field | Description |
|-------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. |

| Field | Description |
|-------------------|--|
| | <ul style="list-style-type: none"> Underscore (_) Hyphen (-) |
| Type | Select the task type as “PON port migration” under Service . |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.

The PON Port Migration page appears.

Figure 157. PON Port Migration

5. Complete the configuration according to the guidelines provided in the following table.

Table 351. PON Port Migration Task

| Field | Description |
|------------------|--|
| Source OLT | Select the source OLT. These OLTs have service associated with them. |
| Source Port | Select the source port of the OLT. These ports have service associated with them and are in deactivated state. |
| Movement Type | Select the movement type. The supported type is. <ul style="list-style-type: none"> Move on same ME |
| Destination Port | Select the destination port of the OLT. These ports are in deactivated and free state. |

6. Click **Next**.

The CONFIGURE EXECUTION page appears.

7. Select one of the option for PON port migration.
 - **Immediate.** Select this option to perform the PON port migration immediately.
 - **Timing.** Select this option to specify the date and time when you want to perform the PON port migration.
8. Click **Submit.**

A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

 - If the status is **RUNNING**, then the PON port migration is in progress and the status changes to **COMPLETED** once the movement is successful.
 - Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the PON port migration task. For more information, see [Table 132: PON Port Migration Task Details \(on page 277\)](#).
9. Disconnect the PON cable from the source port of the OLT and connect it to the destination port.



Note: You must perform this step where the OLT is located.

Creating Task for Banner Update

Prerequisites

The following prerequisites must be fulfilled before creating task for banner update.

- Update the OLT banner text in the `/var/www/html/config_files/<banner-name>` path.

Figure 158. Banner Path

```
radisys@ubuntu:/var/www/html$ tree config-files/
config-files/
├── certs
│   └── domain.crt
│   └── domain.key
├── mgmtvlan
└── oltbanner
```

- Navigate to **Configuration > Controller > Edit > Settings > SDPON Settings** and update the following fields.
 - **Artifact Repo IP.** Specifies the IPv4/IPv6 address of the repository server. Artifact repository server is used for storing and downloading the ONL/ONT firmware image to the ME.
 - **Artifact SFTP Username.** Enter a valid username for the artifact SFTP server.

- **Artifact SFTP Password.** Enter a valid password for the artifact SFTP server.

Figure 159. Controller Configuration

Controller Configuration

Settings

Security Settings

SDPON Settings

Log server *:

Log level: ERROR

Alarm Retention policy (in Days) *: 7

Audit Logs Retention Policy (in Days) *: 2

KPI Retention policy (in Days) *: 2

KPI Reporting Intervals (in minutes)*: 15 x 60 x 1440 x

SFTP User name (#):

SFTP Password (#):

Artifact Repo IP:

Artifact SFTP Username:

Artifact SFTP Password:

Inter SDPON Endpoint (IP):

Inter SDPON Endpoint (Port):

Would be deprecated in future release.

Close **Create**

- The Admin State of the controller must be **ACTIVE**.

A banner shows legal notice and warning to provide adequate protection and awareness of legal issues. By default, the OLT has a security banner as shown in the below figure. A user can create a task to update the OLT banner.

Figure 160. OLT Banner

```
root@vijay-VirtualBox:/home/vijay/opennetworklinux/polt/scripts/edgcore_1.0.0/etc/ssh (SDPON) $ cat sshd-banner
#####
## DO NOT LOGON WITHOUT AUTHORIZATION ##
You are attempting to log in to a system owned and operated by Radisys
If you are not authorized to access this system, please cancel your login attempt immediately
All activities on this system may be monitored
All data residing on this system is a property of Radisys
Any unauthorized use, duplication, or disclosure of this device or its contents
and/or the attempt to gain unauthorized access is strictly prohibited and unlawful
and may lead to legal prosecution
#####

```



Note:

- Only users with admin roles can update the task for banner update.
- Users with other than admin roles can only monitor the task. However, they cannot create, update, and delete the task for banner update.

Perform the following steps to create a task for the OLT banner update.

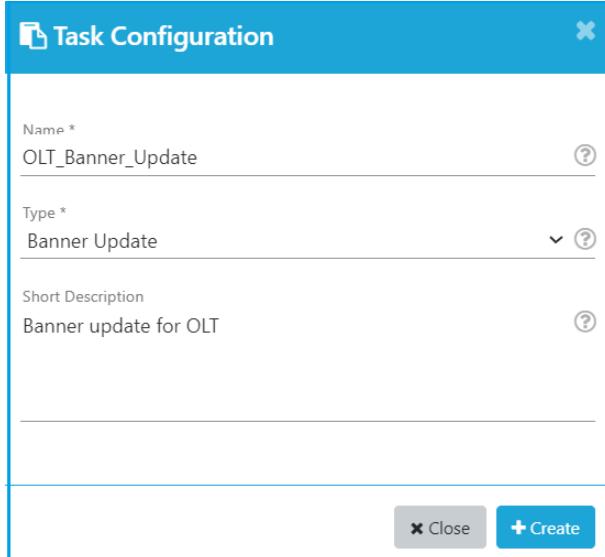
1. Select **Maintenance > Task**.

The Task List page appears.

2. Click **Create**.

The Task Configuration page appears.

Figure 161. Task Configuration



The screenshot shows a 'Task Configuration' dialog box. At the top, there is a blue header bar with the title 'Task Configuration' and a close button. Below the header, there are three input fields: 'Name *' with the value 'OLT_Banner_Update', 'Type *' with the value 'Banner Update', and 'Short Description' with the value 'Banner update for OLT'. Each field has a question mark icon to its right. At the bottom of the dialog box are two buttons: a grey 'Close' button and a blue 'Create' button with a plus sign.

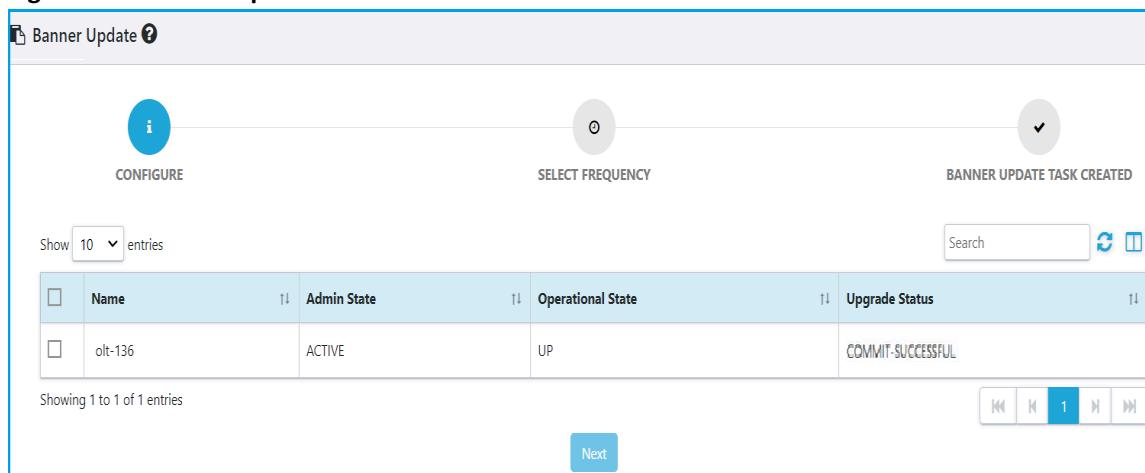
3. Complete the task configuration according to the guidelines provided in the following table.

Table 352. Banner Update

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-) |
| Type | Select the task type as "Banner Update" under Others . |
| Short Description | Enter a meaningful short description for the task. |

4. Click **Create**.

The Banner Update page appears.

Figure 162. Banner Update


The screenshot shows the 'Banner Update' page. At the top, there are three circular icons: 'CONFIGURE' (blue), 'SELECT FREQUENCY' (grey), and 'BANNER UPDATE TASK CREATED' (grey). Below these are buttons for 'Show 10 entries' and a 'Search' field. A table lists one OLT entry:

| | Name | Admin State | Operational State | Upgrade Status |
|--------------------------|---------|-------------|-------------------|-------------------|
| <input type="checkbox"/> | olt-136 | ACTIVE | UP | COMMIT-SUCCESSFUL |

At the bottom, it says 'Showing 1 to 1 of 1 entries' and has navigation buttons. A 'Next' button is highlighted in blue.

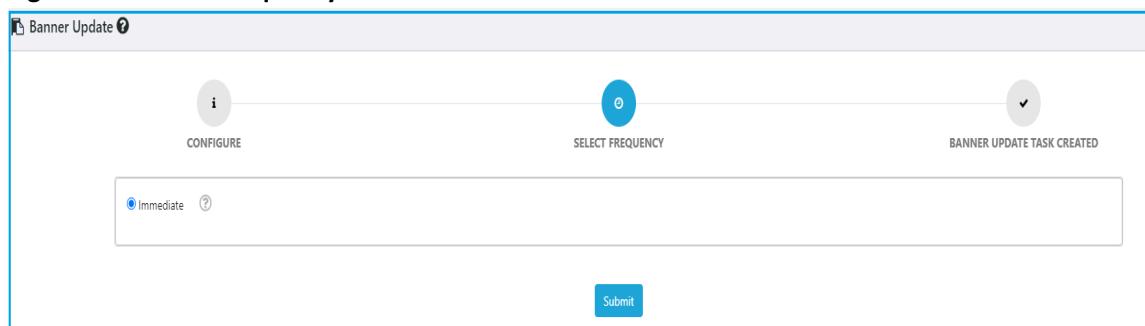
5. Select one or more OLTs for which the banner needs to be updated.



Note: OLTs that are ACTIVE and UP are displayed.

6. Click **Next**.

The SELECT FREQUENCY page appears.

Figure 163. Select Frequency


The screenshot shows the 'SELECT FREQUENCY' page. At the top, there are three circular icons: 'CONFIGURE' (grey), 'SELECT FREQUENCY' (blue), and 'BANNER UPDATE TASK CREATED' (grey). Below these is a radio button group for 'Immediate' (selected) and a 'Submit' button.

7. Select **Immediate** option to update the banner immediately.

8. Click **Submit**.

A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

- If the status is **RUNNING**, then the banner update is in progress and the status changes to **COMPLETED** once the banner update is successful.
- Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the banner update task. For more information, see [Banner Update \(on page 279\)](#).

9. Login to the applicable OLT and verify the updated banner.

Editing and Deleting Task Configuration

You can modify or delete the existing task configuration of the following tasks.

- OLT Software Upgrade
- Reports
- EMS Database Backup (Mongo DB)
- OLT or Controller Backup
- Restore OLT and Controller
- Controller Software Upgrade
- ONT Firmware Upgrade
- ONT Bulk Firmware Upgrade
- OLT Firmware Upgrade
- Inventory Collection
- Service Collection
- Fault Collection
- Event Collection
- Configuration Update (Single and Bulk OLT)
- Port Configuration Update
- Reboot
- PON Port Migration
- Banner Update



Note: You can modify the existing tasks if the task state is “CREATED” or “SCHEDULED”. However, you cannot modify the existing tasks if the task state is “COMPLETED”.

Perform the following steps to modify the task configuration.

1. Select **Maintenance > Task**.

The Task List page appears.

2. Select the Task Update icon corresponding to the task from the **Action** column.

The corresponding task configuration page appears.

3. Modify the parameters as needed.
4. Click **Save** to save the changes.

A confirmation message appears, indicating the status of the edit operation.

Perform the following steps to delete the task configuration.

1. Select **Maintenance > Task**.

The Task List page appears.

2. Select the delete task icon from the **Action** column.

A confirmation window appears, asking you to confirm the delete operation.

3. Click **Confirm** to delete the task.

A confirmation message appears, indicating the status of the delete operation.

Automation

You can create and manage bulk operation and single click provisioning.

Bulk Operation

To access this page, click **Configuration** from the top right corner and select **Automation > Bulk Operation** from the left-hand side of the menu.

Bulk operation allow the users to perform similar operations on multiple resources based on filtering criteria.

- Activate, deactivate, and reboot multiple ONTs. See [Activate, Deactivate, and Reboot ONT \(on page 730\)](#).
- Activate, and deactivate multiple UNI Ports. See [Activate and Deactivate UNI Port \(on page 735\)](#).
- Activate, deactivate, and delete multiple services. See [Activate, Deactivate, and Delete Service \(on page 741\)](#).
- Provision New Service. See [Provision New Service \(on page 746\)](#).
- Update Configuration (For example, upgrading subscribers service bandwidth from 50 Mbps to 100 Mbps). See [Update Service Configuration \(on page 755\)](#).

Activate, Deactivate, and Reboot ONT

Perform the following steps to activate, deactivate, or reboot more than one ONT.



Note: When VEIP ports are deactivated and reactivated, an ONU reboot is required to trigger the DHCP cycle for ONU types, which does not trigger the DHCP cycle.

1. Select **Configuration > Automation > Bulk Operations**.
A Bulk Operation page appears.
2. Complete the configuration according to the guidelines provided in the following table.

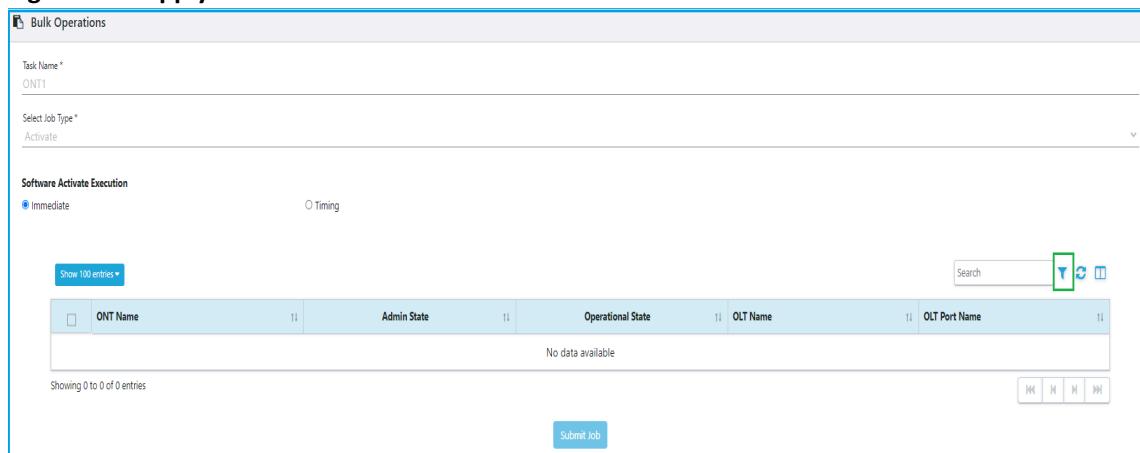
Table 353. Bulk ONT Task

| Field | Description |
|-----------|---|
| Task Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space |

| Field | Description |
|------------------------------------|--|
| Select Job Type | <p>Select the job type from the list. The supported values are.</p> <ul style="list-style-type: none">◦ ONT<ul style="list-style-type: none">▪ Activate▪ Deactivate▪ Reboot◦ UNI Port<ul style="list-style-type: none">▪ Activate▪ Deactivate◦ Service<ul style="list-style-type: none">▪ Activate▪ Deactivate▪ Delete▪ Provision New Service▪ Update Configuration <p> Note: You must select the respective job type based on the task that you are creating. For example, if you are creating a task for ONT, you must select the job type that belongs to the ONT.</p> |
| Software Activate Execution | |
| Immediate | Select this option if you want to perform the action immediately. |
| Timing | Select this option if you want to activate the software for a later date and time. |

3. Click **Apply Filter**.

An Apply Filters page appear.

Figure 164. Apply Filter

Bulk Operations

Task Name *
ONT1

Select Job Type *
Activate

Software Activate Execution
 Immediate Timing

Show 100 entries

| ONT Name | Admin State | Operational State | OLT Name | OLT Port Name |
|-------------------|-------------|-------------------|----------|---------------|
| No data available | | | | |

Showing 0 to 0 of 0 entries

Submit Job

4. Complete the configuration according to the guidelines provided in the following table.

Table 354. Apply Filters

| Field | Description |
|-----------------------|--|
| Device Group | |
| Site | Specifies the site on which the OLT is installed.  Note: <ul style="list-style-type: none">◦ You can select a maximum of 10,000 ONTs in the site and management domain.◦ You can either select the site, management domain, or managed element group to filter the OLTs. |
| Management Domain | Specifies the name of the management domain.  Note: You can select a maximum of 10,000 ONTs in the site and management domain. |
| Managed Element Group | Specifies the managed element group to which the OLT belongs to.  Note: |

| Field | Description |
|---------------------|---|
| |  <ul style="list-style-type: none"> ◦ You can select a maximum of 2000 ONTs in the ME Group. ◦ If you select managed element group all other fields are disabled. |
| OLT Details | |
| OLT Release Version | <p>Specifies the release version of the OLT.</p> <p> Note: You can filter the OLTs based on OLT release version.</p> |
| OLTs | <p>Select a single or multiple OLTs from the list.</p> <p> Note:</p> <ul style="list-style-type: none"> ◦ You can select a maximum of 10 OLTs from the list. ◦ You can select multiple PON ports if a single OLT is selected. |
| PON Technology Type | <p>Specifies the PON technology. The supported values are.</p> <ul style="list-style-type: none"> ◦ GPON ◦ XGSPON |
| Port Details | |
| Port Type | <p>Specifies the port type.</p> <p> Note: Only PON port is supported for R4.0 release.</p> |
| PON Port | <p>Specifies the type of the PON port.</p> <p> Note: This field is disabled if you select multiple OLTs in the OLT field.</p> |
| ONT Details | |
| ONT Make | Specifies vendor name of the ONT. |
| ONT Model | Specifies model name of the ONT. |

| Field | Description |
|----------------------|---|
| ONT Equipment ID | Specifies the equipment ID of the ONT. |
| ONT Type | Specifies the ONT type. The supported values are. <ul style="list-style-type: none"> • Bridged. This ONT only reports to PPTP Ethernet UNIs. Devices connected to PPTP Ethernet UNIs get their IP addresses from the network or static IP addresses. • Routed. This ONT provides home gateway functionality and reports to the VEIP interface. The PPTP interfaces might be reported, but CBAC ignores them. • Hybrid. This ONT reports to both the PPTP Ethernet UNIs and VEIP ports. Services can be provisioned on both PPTP Ethernet UNIs and VEIP ports. |
| ONT Firmware Version | Specifies the firmware version of the ONT. |

Figure 165. Apply Filter

5. Click **Apply**.

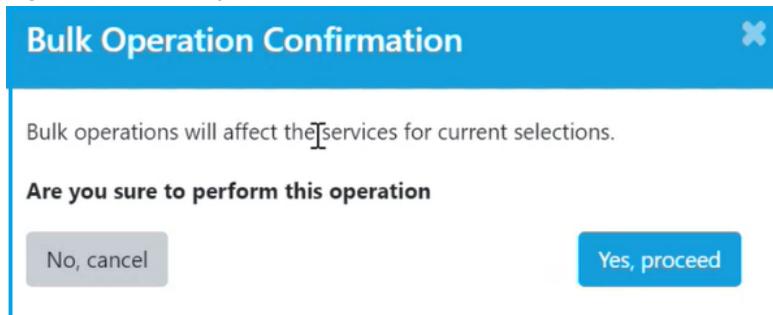
The page displays the list of ONT devices along with the following details.

Table 355. Managed Element Device Details

| Field | Description |
|-------------------|--|
| ONT Name | Specifies the ONT name. |
| Admin State | Specifies admin state of the ONT. The supported values are. <ul style="list-style-type: none"> ◦ ACTIVE ◦ DEACTIVE |
| Operational State | Specifies operational state of the ONT. The supported values are. <ul style="list-style-type: none"> ◦ Up. Shows that the ONT is operationally up. ◦ Down. Shows that the ONT is operationally down. |
| OLT Name | Specifies the OLT name. |
| OLT Port Name | Specifies the OLT port. |

6. Click **Submit Job**.

A Bulk Operation Confirmation page appears.

Figure 166. Bulk Operation Confirmation

7. Click **Yes, proceed**.

A confirmation message is displayed indicating successful operation.

Activate and Deactivate UNI Port

Perform the following steps to activate and deactivate UNI port.

1. Select **Configuration > Automation > Bulk Operations**.

A Bulk Operation page appears.

2. Complete the configuration according to the guidelines provided in the following table.

Table 356. Bulk UNI Port Task

| Field | Description |
|------------------------------------|---|
| Task Name | <p>Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) ◦ Space |
| Select Job Type | <p>Select the job type from the list. The supported values are.</p> <ul style="list-style-type: none"> ◦ ONT <ul style="list-style-type: none"> ▪ Activate ▪ Deactivate ▪ Reboot ◦ UNI Port <ul style="list-style-type: none"> ▪ Activate ▪ Deactivate ◦ Service <ul style="list-style-type: none"> ▪ Activate ▪ Deactivate ▪ Delete ▪ Provision New Service ▪ Update Configuration <p> Note: You must select the respective job type based on the task that you are creating. For example, if you are creating a task for ONT, you must select the job type that belongs to the ONT.</p> |
| Software Activate Execution | |
| Immediate | Select this option if you want to perform the action immediately. |
| Timing | Select this option if you want to activate the software for a later date and time. |

3. Click **Apply Filter**.

An Apply Filters page appear.

Figure 167. Bulk UNI Port Details

4. Complete the configuration according to the guidelines provided in the following table.

Table 357. Apply Filters

| Field | Description |
|-----------------------|--|
| Device Group | |
| Site | <p>Specifies the site on which the OLT is installed.</p> <p> Note:</p> <ul style="list-style-type: none"> ◦ You can select a maximum of 10,000 ONTs in the site and management domain. ◦ You can either select the site, management domain, or managed element group to filter the OLTs. |
| Management Domain | <p>Specifies the name of the management domain.</p> <p> Note: You can select a maximum of 10,000 ONTs in the site and management domain.</p> |
| Managed Element Group | <p>Specifies the managed element group to which the OLT belongs to.</p> <p> Note:</p> <ul style="list-style-type: none"> ◦ You can select a maximum of 2000 ONTs in the ME Group. ◦ If you select managed element group all other fields are disabled. |

| Field | Description |
|---------------------|---|
| OLT Details | |
| OLT Release Version | <p>Specifies the release version of the OLT.</p> <p> Note: You can filter the OLTs based on OLT release version.</p> |
| OLTs | <p>Select a single or multiple OLTs from the list.</p> <p> Note:</p> <ul style="list-style-type: none"> ◦ You can select a maximum of 10 OLTs from the list. ◦ You can select multiple PON ports if a single OLT is selected. |
| PON Technology Type | <p>Specifies the PON technology. The supported values are.</p> <ul style="list-style-type: none"> ◦ GPON ◦ XGSPON |
| Port Details | |
| Port Type | <p>Specifies the port type.</p> <p> Note: Only PON port is supported for R4.0 release.</p> |
| PON Port | <p>Specifies the type of the PON port.</p> <p> Note: This field is disabled if you select multiple OLTs in the OLT field.</p> |
| ONT Details | |
| ONT Make | Specifies vendor name of the ONT. |
| ONT Model | Specifies model name of the ONT. |
| ONT Equipment ID | Specifies the equipment ID of the ONT. |
| ONT Type | Specifies the ONT type. The supported values are. |

| Field | Description |
|----------------------|---|
| | <ul style="list-style-type: none"> ◦ Bridged. This ONT only reports to PPTP Ethernet UNIs. Devices connected to PPTP Ethernet UNIs get their IP addresses from the network or static IP addresses. ◦ Routed. This ONT provides home gateway functionality and reports to the VEIP interface. The PPTP interfaces might be reported, but CBAC ignores them. ◦ Hybrid. This ONT reports to both the PPTP Ethernet UNIs and VEIP ports. Services can be provisioned on both PPTP Ethernet UNIs and VEIP ports. |
| ONT Firmware Version | Specifies the firmware version of the ONT. |
| UNI Port Type | Specifies the UNI port type. The supported UNI port types are. <ul style="list-style-type: none"> ◦ PPTP ◦ VEIP ◦ IP ◦ POTS |
| UNI Port Number | Specifies the port number associated with the ONT. |

Figure 168. Apply Filter

5. Click **Apply**.

The page displays the list of UNI ports along with the following details.

Table 358. Managed Element Device Details

| Field | Description |
|-------------------|--|
| UNI Port Type | Specifies the UNI port type, for example, PPTP. |
| UNI Port Number | Specifies the port number associated with the ONT. |
| Admin State | Specifies admin state of the ONT. The supported values are. <ul style="list-style-type: none"> ◦ ACTIVE ◦ DEACTIVE |
| Operational State | Specifies operational state of the ONT. The supported values are. <ul style="list-style-type: none"> ◦ Up. Shows that the ONT is operationally up. ◦ Down. Shows that the ONT is operationally down. |
| ONT Name | Specifies the ONT name. |
| OLT Name | Specifies the OLT name. |

Figure 169. UNI Port Details

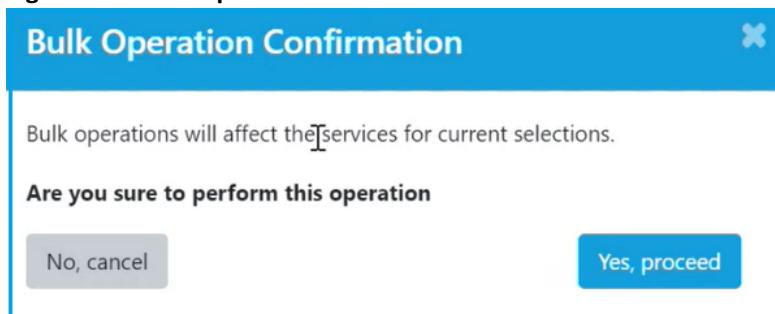
| UNI Port Type | UNI Port Number | Admin State | Operational State | ONT Name | OLT Name |
|---------------|-----------------|-------------|-------------------|----------------|----------|
| PPTP-ETHERNET | 4 | DEACTIVE | UNKNOWN | ont-237-gpon-7 | olt-237 |
| PPTP-ETHERNET | 3 | DEACTIVE | UNKNOWN | ont-237-gpon-7 | olt-237 |
| PPTP-ETHERNET | 2 | DEACTIVE | UNKNOWN | ont-237-gpon-7 | olt-237 |



Note: If the UNI ports are 100 or more the user cannot deselect the UNI ports.

6. Click **Submit Job**.

A Bulk Operation Confirmation page appears.

Figure 170. Bulk Operation Confirmation

7. Click **Yes, proceed**.

A confirmation message is displayed indicating successful operation.

Activate, Deactivate, and Delete Service

Perform the following steps to activate, deactivate, or delete more than one service.

1. Select **Configuration > Automation > Bulk Operations**.

A Bulk Operation page appears.

2. Complete the configuration according to the guidelines provided in the following table.

Table 359. Bulk Service Task

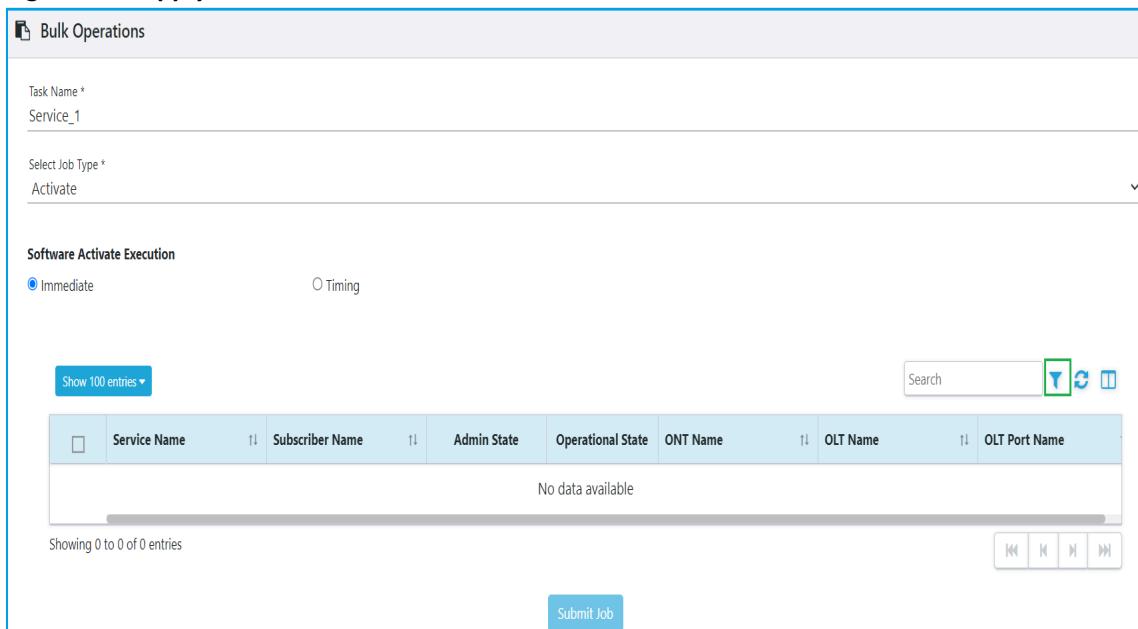
| Field | Description |
|-----------------|---|
| Task Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space |
| Select Job Type | Select the job type from the list. The supported values are. <ul style="list-style-type: none">◦ ONT<ul style="list-style-type: none">▪ Activate▪ Deactivate▪ Reboot◦ UNI Port<ul style="list-style-type: none">▪ Activate▪ Deactivate◦ Service<ul style="list-style-type: none">▪ Activate▪ Deactivate |

| Field | Description |
|------------------------------------|---|
| | <ul style="list-style-type: none"> ▪ Delete ▪ Provision New Service ▪ Update Configuration <p> Note: You must select the respective job type based on the task that you are creating. For example, if you are creating a task for ONT, you must select the job type that belongs to the ONT.</p> |
| Software Activate Execution | |
| Immediate | Select this option if you want to perform the action immediately. |
| Timing | Select this option if you want to activate the software for a later date and time. |

3. Click **Apply Filter**.

An Apply Filters page appear.

Figure 171. Apply Filter



The screenshot shows the 'Bulk Operations' page with the following details:

- Task Name:** Service_1
- Select Job Type:** Activate
- Software Activate Execution:**
 - Immediate
 - Timing
- Table Headers:** Service Name, Subscriber Name, Admin State, Operational State, ONT Name, OLT Name, OLT Port Name
- Table Message:** No data available
- Table Statistics:** Showing 0 to 0 of 0 entries
- Buttons:** Submit Job

4. Complete the configuration according to the guidelines provided in the following table.

Table 360. Apply Filters

| Field | Description |
|-----------------------|--|
| Device Group | |
| Site | <p>Specifies the site on which the OLT is installed.</p> <p> Note:</p> <ul style="list-style-type: none"> ◦ You can select a maximum of 10,000 ONTs in the site and management domain. ◦ You can either select the site, management domain, or managed element group to filter the OLTs. |
| Management Domain | <p>Specifies the name of the management domain.</p> <p> Note: You can select a maximum of 10,000 ONTs in the site and management domain.</p> |
| Managed Element Group | <p>Specifies the managed element group to which the OLT belongs to.</p> <p> Note:</p> <ul style="list-style-type: none"> ◦ You can select a maximum of 2000 ONTs in the ME Group. ◦ If you select managed element group all other fields are disabled. |
| OLT Details | |
| OLT Release Version | <p>Specifies the release version of the OLT.</p> <p> Note: You can filter the OLTs based on OLT release version.</p> |
| OLTs | Select a single or multiple OLTs from the list. |
| |  Note: |

| Field | Description |
|------------------------|---|
| |  <ul style="list-style-type: none">◦ You can select a maximum of 10 OLTs from the list.◦ You can select multiple PON ports if a single OLT is selected. |
| PON Technology Type | Specifies the PON technology. The supported values are. <ul style="list-style-type: none">◦ CPON◦ GPON◦ XGSPON◦ Any PON |
| Port Details | |
| Port Type | Specifies the port type.  Note: Only PON port is supported for R4.0 release. |
| PON Port | Specifies the type of the PON port.  Note: This field is disabled if you select multiple OLTs in the OLT field. |
| Service Details | |
| Service Name | Specifies the service name. |

Figure 172. Apply Filter

5. Click **Apply**.

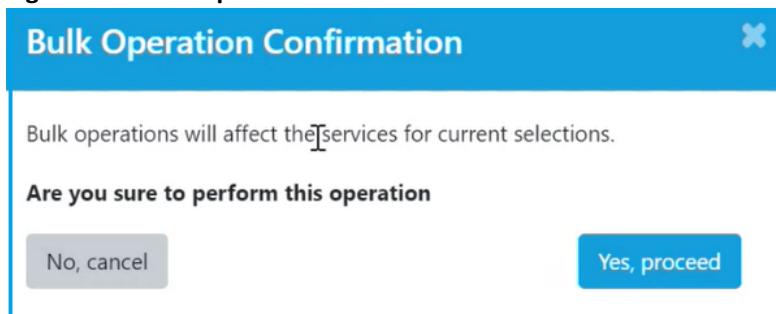
The page displays the list of services along with the following details.

Table 361. Service Details

| Field | Description |
|-------------------|--|
| Service Name | Specifies the name of the service. |
| Subscriber Name | Specifies the name of the subscriber. |
| Admin State | Specifies admin state of the service. The supported values are. <ul style="list-style-type: none"> ◦ ACTIVE ◦ DEACTIVE |
| Operational State | Specifies operational state of the ONT. The supported values are. <ul style="list-style-type: none"> ◦ Up. Shows that the ONT is operationally up. ◦ Down. Shows that the ONT is operationally down. |
| ONT Name | Specifies the ONT name. |
| OLT Name | Specifies the OLT name. |

6. Click **Submit Job**.

A Bulk Operation Confirmation page appears.

Figure 173. Bulk Operation Confirmation

7. Click **Yes, proceed**.

A confirmation message is displayed indicating successful operation.

Provision New Service

Prerequisite. You must create a subscriber before you provision a new service.

Perform the following steps to provision new service.

1. Select **Configuration > Automation > Bulk Operations**.
A Bulk Operation page appears.
2. Complete the configuration according to the guidelines provided in the following table.

Table 362. Provision New Service Task

| Field | Description |
|------------------------------------|---|
| Task Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">◦ Underscore (_)◦ Hyphen (-)◦ Space |
| Select Job Type (Service) | Select the job type as Provision New Service from the list. |
| Software Activate Execution | |
| Immediate | Select this option if you want to perform the action immediately. |
| Timing | Select this option if you want to activate the software for a later date and time. |

3. Click **Apply Filter**.

An Apply Filters page appear.

Figure 174. Apply Filter

The screenshot shows the Radisys Bulk Operations interface. At the top, there is a 'Task Name' field set to 'Service Provisioning' and a 'Select Job Type' dropdown set to 'Provision New Service'. Below this, under 'Software Activate Execution', the 'Immediate' radio button is selected. A table below lists 'Subscriber Name', 'ONT Name', and 'OLT Port Name' with a note 'No data available'. At the bottom, there is a 'Next' button.

4. Complete the configuration according to the guidelines provided in the following table.

Table 363. Apply Filters

| Field | Description |
|-----------------------|--|
| Device Group | |
| Site | Specifies the site on which the OLT is installed.  Note: <ul style="list-style-type: none">◦ You can select a maximum of 10,000 ONTs in the site and management domain.◦ You can either select the site, management domain, or managed element group to filter the OLTs. |
| Management Domain | Specifies the name of the management domain.  Note: You can select a maximum of 10,000 ONTs in the site and management domain. |
| Managed Element Group | Specifies the managed element group to which the OLT belongs to.  Note: |

| Field | Description |
|---------------------|---|
| |  <ul style="list-style-type: none">◦ You can select a maximum of 2000 ONTs in the ME Group.◦ If you select managed element group all other fields are disabled. |
| OLT Details | |
| OLT Release Version | Specifies the release version of the OLT.  Note: You can filter the OLTs based on OLT release version. |
| OLTs | Select a single or multiple OLTs from the list.  Note: <ul style="list-style-type: none">◦ You can select a maximum of 10 OLTs from the list.◦ You can select multiple PON ports if a single OLT is selected. |
| PON Technology Type | Specifies the PON technology. The supported values are. <ul style="list-style-type: none">◦ GPON◦ XGSPON |
| Port Details | |
| Port Type | Specifies the port type.  Note: Only PON port is supported for R4.0 release. |
| PON Port | Specifies the type of the PON port. |

Figure 175. Apply Filters

5. Click **Apply**.

The page displays the list of new services along with the following details.

Table 364. Service Details

| Field | Description |
|-----------------|---------------------------------------|
| Subscriber Name | Specifies the name of the subscriber. |
| ONT Name | Specifies the ONT name. |
| OLT Port Name | Specifies the OLT port name. |

6. Click **Next**.

A Bulk Operation page appears.

7. Complete the configuration according to the guidelines provided in the following table.

Table 365. Bulk Operation

| Field | Description |
|--------------------------------------|--|
| Service Information | |
| Enter Service Name | Specifies the service name. |
| Aggregate Upstream Bandwidth Profile | Specifies the bandwidth profile ID for the aggregate upstream bandwidth control. This field is required only when multiple GEM to 1 T-CONT is in upstream direction. All sub-services are configured on different GEM, and they share the same T-CONT. |

| Field | Description |
|-------------------------------------|---|
| | The aggregate upstream bandwidth profile maps to the T-CONT configurations for the upstream QoS. |
| Aggregate Downstream Shaper Profile | Specifies the shaper profile ID for the aggregate downstream bandwidth control. |
| Service Queue Stats | Specifies the location where the GEM KPI must be enabled. The supported values are. <ul style="list-style-type: none"> ◦ ENABLE_ON_OLT ◦ ENABLE_ON_ONT ◦ ENABLE_OLT_ONT ◦ DISABLE The default value is DISABLE. |
| Service | |
| Service Name | Enter a unique name for the sub-service. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| UNI Port | Specifies the physical UNI port number of the ONT device to which the service needs to be associated. The same UNI port can have two service configurations. |
| UNI Port Type | Specifies the UNI port type. This field is mandatory if the <i>UNI Port</i> field is configured. The supported values are. <ul style="list-style-type: none"> ◦ VEIP ◦ PPTP-ETHERNET ◦ IP-HOST ◦ PPTP-POTS |
| AES Encryption | Select whether the AES encryption is supported for the service. <ul style="list-style-type: none"> ◦ True. Supports AES encryption. ◦ False. Does not support AES encryption. Example: True |
| Remote ID Type | Specifies the type of remote ID. The supported values are. <ul style="list-style-type: none"> ◦ MAC_Address ◦ Custom |

| Field | Description |
|---------------------------|---|
| | This field is applicable only when the MAC Learning Type is set to DHCP, PPPoE, or PPPoEIA. Otherwise, this field is ignored. |
| Data Rate Attribute | <p>Specifies the data rate attribute. The supported values are.</p> <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED <p>This field is enabled only when the 'encapsulation' field is set to PPPoE-IA in the VNET profile or in the <i>vnet_config</i> file. If this field is ENABLED, the intermediate agent adds the minimum bandwidth upstream, minimum bandwidth downstream, maximum bandwidth upstream, and maximum bandwidth downstream in the upstream PPPoE control packets.</p> <p>The default value is DISABLED.</p> |
| CPE IP Type | <p>Specifies the Customer Premises Equipment (CPE) IP type. The supported values are.</p> <ul style="list-style-type: none"> ◦ IPv4 ◦ IPv6 ◦ NONE <p>The default value is NONE.</p> |
| CPE IP Address | <p>Specifies the IP address of the CPE/CE router device connected to the particular UNI port for the enterprise (Bridged Mode) solution. The length is 4 bytes. The length is 4 bytes. A standard valid IP range is supported. This field can take IPv4 or IPv6 addresses based on the value provided in the CPE IP Type field.</p> <p>The CPE IP Address is mandatory when the CPE IP Type is IPv4 or IPv6. When the CPE IP Type is NONE, CPE IP Address is not required.</p> <p>Example: 1.1.1.1 or 2001:db8:3333:4444:5555:6666:7777:8888</p> |
| CPE IP Subnet Mask | <p>Specifies the subnet mask for the CPE IP Address.</p> <p>The CPE IP Subnet Mask is mandatory when the CPE IP Type is IPv4 or IPv6. When the CPE IP Type is NONE, CPE IP Subnet Mask is not required.</p> <p>Example:</p> <p>The value is 255.255.255.255 if CPE IP Type is IPv4.</p> <p>The value is ffff.ffff.ffff.ffff.ffff.ffff.ffff.ffff if CPE IP Type is IPv6.</p> |
| Profiles | |
| MVLAN Profile | Select the MVLAN profile from the list. |
| VNet Profile | Select the VNet profile from the list. |
| VNET Configuration | |

| Field | Description |
|------------------------|---|
| SVLAN | Specifies the subscriber S-Tag value of the subscriber. The supported value ranges from 2 to 4094. |
| CVLAN | Specifies the subscriber C-Tag value of the subscriber. The supported value ranges from 2 to 4094. |
| VLAN CONTROL | <p>Specifies the VLAN tagging supported at the ONU and OLT. The supported values are:</p> <ul style="list-style-type: none"> ◦ ONU_CVLAN_OLT_SVLAN ◦ OLT_CVLAN_OLT_SVLAN ◦ ONU_CVLAN ◦ OLT_SVLAN ◦ ONU_CVLAN_ONU_SVLAN ◦ NONE <p>The default value is ONU_CVLAN_OLT_SVLAN. For more information, see Table 270: VLAN Tagging (on page 582).</p> |
| UNI VLAN | Specifies the VLAN or UNI port. The value UNI VLAN zero indicates an un-tagged packet classification. |
| UNI VLAN Range End | Specifies the end uni vlan for L2VPN subscriber vlans range. The UNI VLAN field is mandatory when this field is configured. |
| Allow Transparent VLAN | <p>Specifies the configuration to allow the transparent VLAN from RG. This indicates that the upstream traffic needs to be classified based on the Ether type. The supported values are:</p> <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED <p>When the field is set to ENABLED, the traffic from RG is passed transparently.</p> |
| Encapsulation | <p>Specifies the type of access protocol used to establish the access link.</p> <p>The supported values are:</p> <ul style="list-style-type: none"> ◦ IPoE ◦ PPPoE ◦ PPPoE-IA <p> Note: When this field value is selected as PPPoE-IA, the Remote-ID Type field value in the service configuration can be selected as Custom or left blank.</p> |

| Field | Description |
|------------------------------|---|
| ONT Ethertype Classification | Specifies if the upstream traffic needs to be classified based on the Ether type. The supported values are. <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED |
| MAC Learning Type | Specifies the type of method used to learn device MAC address. The supported values are. <ul style="list-style-type: none"> ◦ DHCP ◦ ARP ◦ DHCP ALLOW RELEARN ◦ ARP ALLOW RELEARN ◦ DHCP IP ANTI SPOOFING NO MAC ◦ DHCP IP ANTI SPOOFING MAC ◦ None ◦ DHCP NO MAC ◦ ARP NO MAC |
| CoSQ Profile | Select the CoSQ profile ID. When this field is configured in the Vnet Config , the allowed pbits in the CoSQ profile are used for downstream control IPv6 solicit message and downstream ARP request message to remark the pbits. |
| SVLAN TPID | Specifies the Tag Protocol Identifier (TPID) that must be used with s-tag. The supported values are. <ul style="list-style-type: none"> ◦ 0x88A8 ◦ 0x8100 The default value is 0x8100. |
| PON Hair Pinning | Specifies whether the PON hair pinning is enabled for the VLAN model. The supported values are. <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED The default value is DISABLED. |
| Circuit ID | Select the circuit ID format from the list. |
| Upstream Profile | |
| Bandwidth Profile | Select the bandwidth profile for the upstream traffic from the list. The bandwidth profile maps to T-CONT configuration for US QoS for 1-GEM per T-CONT model. |

| Field | Description |
|---|---|
| Shaper Profile | Select the shaper profile for the upstream traffic from the list. The field maps to GEM level traffic shaping for upstream QoS for the multiple-GEM to 1 TCONT model. |
| COSQ Profile | Select the COSQ profile for the upstream traffic from the list. |
| Downstream Profile | |
| Bandwidth Profile | Select the bandwidth profile for the downstream traffic from the list. |
| Shaper Profile | Select the shaper profile for the downstream traffic from the list. Specifies the traffic shaping parameters for downstream QoS. |
| COSQ Profile | Select the COSQ profile for the downstream traffic from the list. |
| The following additional fields are displayed if the UNI Port Type is selected as IP-HOST . | |
| Voice Service Config | |
| Pots UNI Port ID | Specifies the POTS port ID. The supported values are. <ul style="list-style-type: none"> ◦ ont-185-PPTP-POTS-1 ◦ ont-185-PPTP-POTS-2 |
| Pots UNI Port | Specifies the POTS port number. |
| Phone Number | Specifies the phone number. This field do not have restriction on the number of digits as it is a string. |
| User Name | Specifies the username for the voice service profile. |
| Password | Specifies the password for the voice service profile. |
| Display Name | Specifies the display name. |
| VOIP Config Method | Specifies the VoIP configuration method. The default value is OMCI. |
| Pots Signaling Code | Specifies the POTS signaling code when the port type is IP-HOST. The supported values and signaling methods are. <ul style="list-style-type: none"> ◦ 1-LoopStart ◦ 2-GroundStart ◦ 3-LoopReverseBattery ◦ 4-CoinFirst |

| Field | Description |
|----------------|---|
| | <ul style="list-style-type: none"> ◦ 5-DialToneFirst ◦ 6-MultiParty |
| Voice Protocol | Specifies the voice protocol. The default value is SIP. |

8. Click **Submit Job**.

A confirmation message is displayed indicating successful operation.

Update Service Configuration

Perform the following steps to update the configuration.

1. Select **Configuration > Automation > Bulk Operations**.

A Bulk Operation page appears.

2. Complete the configuration according to the guidelines provided in the following table.

Table 366. Update Configuration Task

| Field | Description |
|------------------------------------|---|
| Task Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) ◦ Space |
| Select Job Type (Service) | Select the job type as Update Configuration from the list. |
| Software Activate Execution | |
| Immediate | Select this option if you want to perform the action immediately. |
| Timing | Select this option if you want to activate the software for a later date and time. |

3. Click **Apply Filter**.

An Apply Filters page appear.

Figure 176. Apply Filter

The screenshot shows the 'Bulk Operations' configuration page. At the top, 'Task Name' is set to 'Service_Update' and 'Select Job Type' is set to 'Update Configuration'. Under 'Software Activate Execution', 'Immediate' is selected. Below this is a table with the following columns: Service Name, Subscriber Name, Admin State, Operational State, ONT Name, OLT Name, and OLT Port Name. The table displays 'No data available' and shows 'Showing 0 to 0 of 0 entries'. Navigation buttons for 'Next' and 'Previous' are at the bottom.

4. Complete the configuration according to the guidelines provided in the following table.

Table 367. Apply Filters

| Field | Description |
|-----------------------|--|
| Device Group | |
| Site | <p>Specifies the site on which the OLT is installed.</p> <p>Note:</p> <ul style="list-style-type: none"> ◦ You can select a maximum of 10,000 ONTs in the site and management domain. ◦ You can either select the site, management domain, or managed element group to filter the OLTs. |
| Management Domain | <p>Specifies the name of the management domain.</p> <p>Note: You can select a maximum of 10,000 ONTs in the site and management domain.</p> |
| Managed Element Group | <p>Specifies the managed element group to which the OLT belongs to.</p> <p>Note:</p> |

| Field | Description |
|-------------------------|---|
| |  <ul style="list-style-type: none"> ◦ You can select a maximum of 2000 ONTs in the ME Group. ◦ If you select managed element group all other fields are disabled. |
| OLT Details | |
| OLT Release Version | <p>Specifies the release version of the OLT.</p> <p> Note: You can filter the OLTs based on OLT release version.</p> |
| OLTs | <p>Select a single or multiple OLTs from the list.</p> <p> Note:</p> <ul style="list-style-type: none"> ◦ You can select a maximum of 10 OLTs from the list. ◦ You can select multiple PON ports if a single OLT is selected. |
| PON Technology Type | <p>Specifies the PON technology. The supported values are.</p> <ul style="list-style-type: none"> ◦ CPON ◦ GPON ◦ XGSPON ◦ Any PON |
| Port Details | |
| Port Type | <p>Specifies the port type.</p> <p> Note: Only PON port is supported for R4.0 release.</p> |
| PON Port | Specifies the type of the PON port. |
| Service Details | |
| Service Name | Specifies the service name. |
| Upstream Profile | |

| Field | Description |
|---------------------------|---|
| Bandwidth Profile | Select the bandwidth profile for the upstream traffic from the list. The bandwidth profile maps to T-CONT configuration for US QoS for 1-GEM per T-CONT model. |
| Shaper Profile | Select the shaper profile for the upstream traffic from the list. The field maps to GEM level traffic shaping for upstream QoS for the multiple-GEM to 1 TCONT model. |
| COSQ Profile | Select the COSQ profile for the upstream traffic from the list. |
| Downstream Profile | |
| Bandwidth Profile | Select the bandwidth profile for the downstream traffic from the list. |
| Shaper Profile | Select the shaper profile for the downstream traffic from the list. Specifies the traffic shaping parameters for downstream QoS. |
| COSQ Profile | Select the COSQ profile for the downstream traffic from the list. |

Figure 177. Apply Filter

Apply Filters

Device Group

Site Management Domain Managed Element Group

Select the option DEFAULT_MANAGEMENT_DOMAIN Select the option

OLT Details

OLT Release Version 2

OLTs * PON Technology Type * CPON GPON XGSPON Any PON

Port Details

Port Type Alarm NNI PON

PON Port

Service Details

Service Name Service

Upstream Profile

Bandwidth Profile Shaper Profile COSQ Profile

Downstream Profile

Bandwidth Profile Shaper Profile COSQ Profile

5. Click **Apply**.

The page displays the list of services along with the following details.

Table 368. Service Details

| Field | Description |
|-------------------|--|
| Service Name | Specifies the name of the service. |
| Subscriber Name | Specifies the name of the subscriber. |
| ONT Name | Specifies the ONT name. |
| Admin State | Specifies admin state of the ONT. The supported values are. <ul style="list-style-type: none"> ◦ ACTIVE ◦ DEACTIVE |
| Operational State | Specifies operational state of the ONT. The supported values are. <ul style="list-style-type: none"> ◦ Up. Shows that the ONT is operationally up. ◦ Down. Shows that the ONT is operationally down. |
| OLT Name | Specifies the OLT name. |
| OLT Port Name | Specifies the OLT port. |

6. Click **Next**.

A Bulk Operation page appears.

7. Complete the configuration according to the guidelines provided in the following table.

Table 369. Bulk Operation

| Field | Description |
|--------------------------------------|---|
| Service Information | |
| Aggregate Upstream Bandwidth Profile | Specifies the bandwidth profile ID for the aggregate upstream bandwidth control. This field is required only when multiple GEM to 1 T-CONT is in upstream direction. All sub-services are configured on different GEM, and they share the same T-CONT. The aggregate upstream bandwidth profile maps to the T-CONT configurations for the upstream QoS. |
| Aggregate Downstream Shaper Profile | Specifies the shaper profile ID for the aggregate downstream bandwidth control. |
| Service Queue Stats | Specifies the location where the GEM KPI must be enabled. The supported values are. |

| Field | Description |
|---------------------------|---|
| | <ul style="list-style-type: none"> ◦ ENABLE_ON_OLT ◦ ENABLE_ON_ONT ◦ ENABLE_OLT_ONT ◦ DISABLE <p>The default value is DISABLE.</p> |
| Sub Service | |
| Service Name | <p>Enter a unique name for the sub-service. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> ◦ Underscore (_) ◦ Hyphen (-) |
| AES Encryption | <p>Select whether the AES encryption is supported for the service.</p> <ul style="list-style-type: none"> ◦ True. Supports AES encryption. ◦ False. Does not support AES encryption. <p>Example: True</p> |
| Data Rate Attribute | <p>Specifies the data rate attribute. The supported values are.</p> <ul style="list-style-type: none"> ◦ ENABLED ◦ DISABLED <p>This field is enabled only when the 'encapsulation' field is set to PPPoE-IA in the V-Net profile or in the <i>vnet_config</i> file. If this field is ENABLED, the intermediate agent adds the minimum bandwidth upstream, minimum bandwidth downstream, maximum bandwidth upstream, and maximum bandwidth downstream in the upstream PPPoE control packets.</p> <p>The default value is DISABLED.</p> |
| Vnet Profile | Select the VNet profile from the list. |
| Upstream Profile | |
| Bandwidth Profile | Select the bandwidth profile for the upstream traffic from the list. The bandwidth profile maps to T-CONT configuration for US QoS for 1-GEM per T-CONT model. |
| COSQ Profile | Select the COSQ profile for the upstream traffic from the list. |
| Downstream Profile | |
| Shaper Profile | Select the shaper profile for the downstream traffic from the list. Specifies the traffic shaping parameters for downstream QoS. |

| Field | Description |
|--------------|---|
| COSQ Profile | Select the COSQ profile for the downstream traffic from the list. |

8. Click **Submit Job**.

A confirmation message is displayed indicating successful operation.

Single Click Provisioning

To access this page, click **Configuration** from the top right corner and select **Automation > Single Click Provisioning** from the left-hand side of the menu.

Single-click provisioning allows the creation of ONT, subscriber, and service automatically with minimum input selection using a template. The auto-generated names for ONT, subscriber, and service are derived from the ONT serial number.

User can connect the ONT to OLT. When the ONT is listed under **Monitor > Blacklisted ONT** page, the user can whitelist this ONT, provision subscribers services, and activate them in a single click. To achieve this, as a prerequisite, the user must configure the pre-configuration template and that must be reviewed by the Radisys TAC team before using this feature.



Note: To perform single click provisioning, you can give all permissions of normal subscriber provisioning along with the single click provisioning.

Field Descriptions

The following table describes the fields on the single click provisioning page.

Table 370. Single Click Provisioning List

| Field | Description |
|------------------|---|
| ONT Serial No. | Specifies the serial number of the ONT. |
| ONT Vendor ID | Specifies the vendor ID of the ONT. |
| ONT Equipment ID | Specifies the equipment ID of the ONT. |
| OLT Name | Specifies the name of the OLT. |
| OLT Serial No. | Specifies the serial number of the OLT. |
| OLT Port | Specifies the OLT port number. |
| UNI Port Count | Specifies the number of UNI ports connected to the ONT. |
| Technology | Specifies the technology supported by the ONT. For example, GPON or XGSPON. |

Table 370. Single Click Provisioning List (continued)

| Field | Description |
|-------------------------------|--|
| Supported Connectivity Models | <p>Specifies the supported connectivity model that must be used for the services on the ONU. The supported values are.</p> <ul style="list-style-type: none"> • N:1 bridging • 1:M mapping • 1:P filtering • N:M bridge-mapping • 1:MP map-filtering • N:P bridge-filtering • N:MP bridge-map-filtering <p>The default value for the residential service is 1:MP map-filtering.</p> |
| Current Connectivity Models | <p>Specifies the current connectivity model that must be used for the services on the ONT.</p> <p>The default value for the residential service is 1:MP map-filtering.</p> |
| UNI Ports | Specifies the list of UNI ports connected to the ONT. |
| Registration ID | <p>Specifies the registration ID of ONT.</p> <p>The reregistration ID must contain only alphanumeric characters and length must be 72 alphanumeric characters.</p> |
| Date | Specifies the date and time when the ONT was created. |
| Action | <p>Specifies the action that you can perform on single click provisioning. The supported actions are.</p> <ul style="list-style-type: none"> • Edit • Delete • Clone |

Creating Single Click Provisioning

Perform the following steps to provision the ONT using single click.

1. Select **Configuration > Automation > Single Click Provisioning**.
A list of blacklisted ONTs are displayed.
2. Navigate to the applicable ONT.
3. Click on the three dots icon () and select **Single Click Provisioning**.

Figure 178. Single Click Provisioning

| Serial No. | OLT Name | OLT Serial No. | Technology | Supported Connectivity Models | Current Connectivity Models | OLT Port | Registration Id | Vendo |
|--------------|----------|----------------|------------|--|-----------------------------|----------|--------------------------|---|
| ISKT4285D740 | vs4 | RSYSD9E47D89 | gpon | N:1 bridging, 1:M mapping, 1:P filtering Read more | 1:MP map-filtering | SFPON-1 | 0xONU747876003806214405 |  Single Click Provisioning |
| ISKT4285D730 | vs4 | RSYSD9E47D89 | gpon | N:1 bridging, 1:M mapping, 1:P filtering Read more | 1:MP map-filtering | SFPON-1 | 0xONU4539589599778027461 | ISKT  |
| ISKT4285D720 | vs4 | RSYSD9E47D89 | gpon | N:1 bridging, 1:M mapping, 1:P filtering Read more | 1:MP map-filtering | SFPON-1 | 0xONU546185760471285372 | ISKT  |

4. Click **Activate** under Action Column.

Figure 179. Activate ONT

| Single Click Provisioning | | | | | | | | |
|---|---------------|------------------|----------|----------------|----------|--------------------------|--|--|
| You can select any blacklisted ONT from the list below to quickly create subscribers and activate them. | | | | | | | | |
| ONT Serial No. | ONT Vendor Id | ONT Equipment Id | OLT Name | OLT Serial No. | OLT Port | Action | | |
| ISKT4285D740 | ISKT | G64_10 | vs4 | RSYSD9E47D89 | SFPON-1 | Activate | | |

Showing 1 to 1 of 1 entries

5. Select the **Service Template** from the list to active services for the ONT and verify the other details.

Figure 180. ONT Service Template

The screenshot shows a 'Single Click Provisioning' interface. It includes fields for 'Blacklisted ME's Serial Number' (ISKT4285D740) and 'Blacklisted ME's Equipment ID' (G64_10). Below these are sections for 'Connected OLT's Configuration' with 'OLT Name' (vs4) and 'OLT Serial Number' (RSYSD9E47D89), and 'OLT PON Port' (SFPPON-1). A note says 'Select a template from below to activate services for the ONT'. A dropdown for 'Service Template *' is set to 'Select'. A note below says 'Configure the prefix that will be used for configuring the ONT, subscribers and their services. By default the blacklisted ONT's serial number will be used. This is introduced to shorten the time required to create an ONT, subscribers and activate the services.' A 'Prefix word to be used' field contains 'RSYSD9E47D89'. At the bottom are 'Cancel' and 'Activate' buttons.

6. Click **Activate.**

A success message is displayed with ONT, subscriber, and service detail.



Note: While creating single click provision, the following resources must have the attributes as a variable in the subscriber template and the other attributes must be constant.

- **ONT. parent_id, parent_port_id, serial_no, and name**
- **Subscriber. display_id and name**
- **Subscriber_Service. name**

Figure 181. Success Message

The screenshot shows a 'Single Click Provisioning' success message. It states 'Successfully activated services for the blacklisted ME with serial number ISKT4285D730, below are the details.' It lists the activated resources: 'ONT' (RSYSD9E47D89 ISKT4285D730), 'Subscriber' (RSYSD9E47D89_ISKT4285D730_Subscriber), and 'Services' (RSYSD9E47D89_ISKT4285D730_Service_1). At the bottom is a 'Close' button.

Administration

You can create and manage the management domain, user, user role, user role permissions, and security policy.

Management Domain

To access this page, click **Administration** from the top right corner and select **Management Domain** from the left-hand side of the menu.

The management domain is a logical grouping of the managed elements (OLTs) managed by the EMS/RMS. Users can create multiple domains and assign them to ME.



Note: If the user wants to create multiple controllers, they need not create multiple management domains. RMS does not verify and validate the management domain anywhere. Hence, creating a single management domain is sufficient for creating multiple controllers.

Creating Management Domain

The management domain is a logical grouping of the managed elements (OLTs) managed by the EMS/RMS. Users can create multiple domains and assign them to ME.

Perform the following steps to create a management domain.

1. Select **Administration > Management Domain > Create**.
The Management Domain Configuration page appears.
2. Complete the configuration according to the guidelines provided in the following table.

Table 371. Management Domain Configuration

| Field | Description |
|-------|--|
| Name | Enter a unique name for the management domain. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-)• Space |

3. Click **Create**.
A new management domain is created on the Management Domain List page.

To edit, clone, and delete the management domain configuration, see [Common Operations \(on page 27\)](#).

Activating and Deactivating the Management Domain

When you activate the management domain, the master RMS starts managing the domain RMS.



Note: In a single mode, where only the master RMS is running, it is mandatory to create one domain RMS.

Perform the following steps to activate the management domain.

1. Select **Administration > Management Domain**.

The Management Domain List page appears.

2. Click on the three dots (⋮) corresponding to the management domain that you want to activate and click the **Activate** option.

A confirmation message appears, indicating the status of the activate operation.

Perform the following steps to deactivate the management domain.

1. Select **Administration > Management Domain**.

The Management Domain List page appears.

2. Click on the three dots (⋮) corresponding to the management domain that you want to deactivate and click the **Deactivate** option.

Monitoring Management Domain

Perform the following steps to monitor the management domain details.

1. Select **Administration > Management Domain**.

The Management Domain List page appears.

2. Click on the three dots (⋮) corresponding to the management domain that you created and click the **Monitor** option.

You are taken to the **Monitor > Management Domain** page.

User

To access this page, click **Administration** from the top right corner and select **User** from the left-hand side of the menu.

RMS is shipped with an administrator account (admin) and that provides full access to the RMS resources. When you first log in to the RMS application as a default administrator user account, you can perform all tasks and access all RMS resources. Administrator can create new users and assign roles and workspaces to those users to specify which tasks that the users can perform.

Through authentication, RMS validates users based on passwords. RMS supports both local and remote user authentication. When a user tries to access RMS, the user can be authenticated locally by confirming that the password entered by the user at login matches the password stored in the RMS database or remotely through a RADIUS server. For information about configuring RADIUS servers for remote authentication and authorization, see [Authentication Profile \(on page 537\)](#).

Use this page to create the following type of users.

- **System User.** A user who configures the access for the master RMS.

User types enable you to classify users based on the privileges and allows you to perform the tasks on RMS resources. A user type assigned to a user determines the tasks and actions that the user can perform.

- **Deployment User.** A user who can view only non HOTO OLTs and its associated resources.

Tasks

You can perform the following operations from this page.

- Create a user configuration. See [Creating User Configuration \(on page 770\)](#).
- Lock and Unlock User Configuration. See [Locking and Unlocking the User \(on page 774\)](#).
- You can view active sessions for the user. See [Viewing Active Sessions for the User \(on page 773\)](#).
- Activate and deactivate the user account. See [Activating and Deactivating the Custom User Account \(on page 774\)](#).
- RMS supports changing the user password for all the users.

Field Descriptions

The following table describes the fields on the Users List page.

Table 372. Users List

| Field | Description |
|---------------|--|
| Name | Specifies the name of the user. |
| Type | Specifies the type of the user. The supported types are. <ul style="list-style-type: none">• System User• Deployment User |
| Username | Specifies the username of the user. Example: admin |
| Email | Specifies the e-mail address of the user. |
| Account State | Specifies the state of the user account. The supported types are. |

Table 372. Users List (continued)

| Field | Description |
|--------------------------|---|
| | <ul style="list-style-type: none"> ACTIVE. When the user account is created, or the deactivated user account is activated. DEACTIVE. When the admin user explicitly deactivates the user account. DORMANT. When the user account is inactive for a number of days as specified in the inactive user account time period. The dormant user cannot login to the RMS application. An admin user needs to activate the dormant user account. EXPIRED. When the user account expires after a number of days as specified in the user account expiry time period. An admin user needs to activate the expired user account. |
| Third Party | <p>Specifies whether the user is the third-party user.</p> <ul style="list-style-type: none"> Tick mark (✓). Specifies that the user is a third-party user. Cross mark (x). Specifies that the user is not a third-party user. |
| Disallow Password Expiry | <p>Enable the check box to remove the password expiry feature for the user account. If this option is enabled, the user's password never expires. It overrides the Password Expiry Days value configured in the security policy and controller configuration (security settings). See Creating Security Policy Configuration (on page 785) and Creating Controller Configuration (on page 297).</p> |
| Disallow User Inactivity | <p>Enable the check box to remove the user inactivity feature for the user account. If this option is enabled, the user's account never goes dormant due to inactivity. It overrides the Deactivate Account (days) on account settings and the Inactive Account (Days) value configured in controller configuration (security settings). See Settings (on page 603) and Creating Controller Configuration (on page 297).</p> |
| Disallow Account Expiry | <p>Enable the check box to remove the account expiry feature for the user account. If this option is enabled, the user's account never expires. It overrides the Third Party Account Expiry Days on account settings and the Account Expiry (Days) value configured in controller configuration (security settings). See Settings (on page 603) and Creating Controller Configuration (on page 297).</p> |
| Disallow Account Lock | <p>Specifies whether the user account is allowed for account lock.</p> <ul style="list-style-type: none"> Tick mark (✓). Specifies that the user account is not allowed for the account lock feature. Cross mark (x). Specifies that the user account is allowed for the account lock feature. |

Table 372. Users List (continued)

| Field | Description |
|-------------------------------|--|
| Authentication Type | Specifies the authentication type configured for the user. The supported type is LOCAL. |
| Max Concurrent Sessions | Specifies the support for multiple concurrent sessions for a user from different IPs. |
| Login With Temporary Password | <p>When an administrator creates a default user account, an e-mail is sent to the e-mail address containing login credentials (username and default password). If the e-mail address is not provided during the user configuration, a user with the admin privilege can navigate to Administration > User and view the temporary password. The temporary password is valid only for one time and must be changed after the first login.</p> <ul style="list-style-type: none"> Tick mark (✓). Specifies that the user has to login with the temporary password. Cross mark (✗). Specifies that the user cannot login with a temporary password as the temporary password is updated after the first login. |
| Temporary Password | <p>Specifies the temporary password of the user.</p> <p> Note: The SMTP INTEGRATION ENABLED flag must be selected as false while upgrading the RMS to see the temporary password on the user interface for the admin user role.</p> |
| User Locked | <p>Specifies whether the user account is locked.</p> <ul style="list-style-type: none"> Tick mark (✓). Specifies that the user account is locked. Cross mark (✗). Specifies that the user account unlocked. |
| Mobile | Specifies the mobile number of the user. |
| Role | Specifies the role name assigned to the user. |
| Account Expire Time | Specifies the user account expiration time. |
| Last Login Time | Specifies the date and time when the user last logged into RMS. Example: Jul 21, 2020, 3:32:49 PM Date and time are not displayed when the user has not logged in RMS. |
| Action | Specifies the action that you can perform on the user configuration. The supported actions are. |

Table 372. Users List (continued)

| Field | Description |
|-------|--|
| | <ul style="list-style-type: none">• Edit• Delete• Clone• Lock and unlock the user. See Locking and Unlocking the User (on page 774).• View the active sessions for the user. See Viewing Active Sessions for the User (on page 773). |

Creating User Configuration

Use this page to create one or more users and assign roles to them. When you create a new user account, you must assign a user role, and a security policy to the user. User roles define what actions the user has permission to perform.

After the administrator adds the user, the user account is created in RMS and the user can access the RMS resources based on the privileges assigned to the role.



Note: Before you create a user account, you must ensure that the user role and security policy are created. For more information, see the following topics.

- Security Policy. See [Security Policy \(on page 785\)](#).
- User Role. See [User Role \(on page 775\)](#).

Perform the following steps to create a new user.

1. Select **Administration > Users > Create**.
The User Configuration page appears.
2. Complete the configuration according to the guidelines provided in the following table.

Table 373. Creating User Configuration

| Field | Description |
|-------|---|
| Type | Select the type of user from the list. The user types are. <ul style="list-style-type: none">• System User. A user who can access the resources for the master RMS. A system user can view both HOTO and Non HOTO OLTs and its associated resources.• Deployment User. A deployment user can view only Non HOTO OLTs and its associated resources. |

| Field | Description |
|--------------------------|--|
| Security Policy | Select the security policy that you want to configure for the user. If the security policy does not exist, click the plus icon (+) to create a security policy. See Creating Security Policy Configuration (on page 785) . |
| Third Party | Enable the check box to specify whether the user is from third party. |
| Disallow Account Lock | Enable the check box to remove the account lock feature for the user account. If this option is enabled, the user account never gets locked even if you provide the wrong password. If this option is disabled, the user account is locked as per the settings configured in RMS. See Settings (on page 603) . |
| Disallow Password Expiry | Enable the check box to remove the password expiry feature for the user account. If this option is enabled, the user's password never expires. It overrides the Password Expiry Days value configured in the security policy and controller configuration (security settings). See Creating Security Policy Configuration (on page 785) and Creating Controller Configuration (on page 297) . |
| Disallow User Inactivity | Enable the check box to remove the user inactivity feature for the user account. If this option is enabled, the user's account never goes dormant due to inactivity. It overrides the Deactivate Account (days) on account settings and the Inactive Account (Days) value configured in controller configuration (security settings). See Settings (on page 603) and Creating Controller Configuration (on page 297) . |
| Disallow Account Expiry | Enable the check box to remove the account expiry feature for the user account. If this option is enabled, the user's account never expires. It overrides the Third Party Account Expiry Days on account settings and the Account Expiry (Days) value configured in controller configuration (security settings). See Settings (on page 603) and Creating Controller Configuration (on page 297) . |
| Name | <p>Enter a unique name for the user. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) • Space |
| User Name | <p>Enter a unique name that identifies the user. The following special characters are supported.</p> <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) • Dot (.) |

| Field | Description |
|-----------------------------|---|
| | <ul style="list-style-type: none">• Comma (,)• At the rate (@) <p>The minimum character length for this field is 5 and the maximum is 20. Special characters are not allowed in the beginning and end of the username. Example: admin@12_34</p> |
| Email | Enter a valid e-mail address for the user to receive the notifications. The user receives an email notification for the following. <ul style="list-style-type: none">• When a new user account is created• When the password is about to expire• When the password is changed• When the user account is deactivated• When the user account is deleted |
| Mobile | Enter mobile number for the user. |
| Authentication Type | Select the authentication type as LOCAL to configure the user. <ul style="list-style-type: none">• LOCAL. User accounts are maintained locally in the RMS database, and users are authenticated and authorized by RMS. |
| User Role | Select the user role to be assigned to the user. If the user role does not exist, click the plus icon (+) to create a user role for the user. See Creating Custom User Role Configuration (on page 778) . |
| Maximum Concurrent Sessions | Specifies the support for multiple concurrent sessions for a user from different IPs. The value ranges from 1 to 512 sessions per user and the default value is 25. |

3. Click **Create**.

A new user account is created on the Users List page.

To enhance the security related to your login credentials, an automatically generated default password is sent to the e-mail address that you have specified for the user. You are prompted to change the password after you log in with the automatically generated default password. For more information about changing the password on first login, see [Changing the Password on First Login \(on page 26\)](#).



Note: You cannot modify the **Username** and **Type** of the user.

To edit, clone, and delete the user configuration, see [Common Operations \(on page 27\)](#).

Configuring or Updating Administrator E-Mail ID

A user with administrator or pajmapuser privilege can configure the email ID of the admin/pajmapuser user account so that the password can be recovered or reset in case of any issue.

Perform the following steps to configure the e-mail address.

1. Select **Administration > Users**.
The User List page appears.
2. Select the Edit User icon from the **Action** column.
The User Configuration page appears.
3. Enter the valid email ID in the **Email** field.
4. Click **Save** to save the user configuration.

Viewing Active Sessions for the User

In RMS, you can view and delete active sessions of the user.

You can view the list of users who are logged in along with details of their user id, username, including the date, and time when they logged in to the RMS application.

Perform the following steps to view active sessions for the user.

1. Select **Administration > Users**.
The Users List page appears.
2. Select the Session icon from the **Action** column.
The Active Session page appears.

Table 374. Active Sessions

| Field | Description |
|---------------|--|
| ID | Specifies the ID of the user. |
| IP Address | Specifies the IP address of the user. |
| User Name | Specifies the name of the user. |
| Creation Time | Specifies the date and time when the user had accessed the RMS application. |
| Action | Specifies the action that you can perform on the active session. The supported action is. <ul style="list-style-type: none">• Delete |

Locking and Unlocking the User

RMS locks out users who enter more than the permitted number of incorrect passwords. If your user account is locked out, then an error message is displayed when you try to log in to RMS. You can request the administrator to unlock your account.

Perform the following steps to lock or unlock the user.

1. Select **Administration > Users**.

The Users List page appears.

2. Click the lock or unlock icon from the **Action** column.

A confirmation window appears, asking you to confirm the operation.

3. Click **Yes** to lock or unlock the user.

A confirmation message appears, indicating the status of the operation.

Activating and Deactivating the Custom User Account



Note: The user account state is in ACTIVE state when it was created. You need to activate the account only if the account was deactivated.



Note: You cannot activate or deactivate the default user accounts (admin, viewer, and operator).

Perform the following steps to activate the custom user account.

1. Select **Administration > Users**.

The Users List page appears.

2. Click on the three dots (⋮) corresponding to the custom user that you want to activate and click the **Activate** option.

A success message appears indicating the status of the operation, and the **Account State** of the custom user is changed to ACTIVE.

Perform the following steps to deactivate the custom user account.

1. Select **Administration > Users**.

The Users List page appears.

2. Click on the three dots (⋮) corresponding to the custom user that you want to deactivate and click the **Deactivate** option.

A success message appears indicating the status of the operation, and the **Account State** of the custom user is changed to DEACTIVE.

Exporting User Accounts

You can export the user account as a CSV file from RMS to your local computer. The CSV file can be opened or edited using an application such as Microsoft Excel. You can view and analyze the exported user information, as needed.

Perform the following steps to export user accounts.

1. Select **Administration > Users**.

The Users List page appears.

2. Click **Export**.

The file is downloaded and appears at the bottom of the page. Click on it to open the .csv file using an application such as Microsoft Excel. You can optionally save this file on your PC for later use and rename it if necessary.

User Role

To access this page, click **Administration** from the top right corner and select **User Role** from the left-hand side of the menu.

A user role is assigned to a user that defines the tasks the user can perform within RMS. Each user can be assigned a role depending on the tasks that the user is expected to perform.



Note: You must assign at least one role to the user. Multiple users can be assigned the same role.

Based on the role assigned to the user, the RMS GUI menu and options appear when the user logs in to the RMS application.

Users receive permission to perform tasks only through the roles that they are assigned. A role defines the tasks (for example, create, modify, and delete) that can be performed on the objects (for example, make, model, subscribers, service, template, and so on). In most cases, a single role assignment enables a user to view and to perform tasks on the objects within a workspace. A user with the “admin” role can create, modify, and delete other users in RMS.

Field Descriptions

The following table describes the fields on the User Role page.

Table 375. User Role List

| Field | Description |
|--------|--|
| Name | Specifies the name of the user role. |
| Action | Specifies the action that you can perform on the user role. The supported actions are. |

Table 375. User Role List (continued)

| Field | Description |
|-------|--|
| | <ul style="list-style-type: none"> • Edit • Delete • Clone • Assign permissions for the user role • Synchronize the user between CBAC and RMS |

Role Based Access Control

RMS supports the authentication and authorization of users. Administrator, Operator, viewers, and custom users access the resources within the RMS application based on their role and access permissions.

With role-based access control (RBAC) enforcement, a RMS administrator creates users and then assigns them roles so that they are able to access and manage tasks and objects within workspaces in RMS. The roles determine which workspace or workspaces a user can access, and which tasks the user can perform within the workspace or workspaces.

A user can access only those resources of the RMS that are explicitly granted through access privileges. RMS defines the policies for user roles according to the guidelines defined in the security policy.

- Users can login to PIM using their accounts and PIM maps the user accounts with RMS.
- RMS maps the user accounts to the CBAC CLI and the OLT.

Table 376. User Roles and Access Privileges

| Role | Access Privileges |
|-------------|---|
| Admin | Users with the Admin role have full access to the RMS application. They can use the UI or APIs to add one or more users with operator and viewer user roles and update password for all the users. The default username and password for the admin user is admin/ADmin@123 . |
| Operator | Users with the Operator role have read and write access to the RMS application. The default username and password for the operator user is operator/OPerator@123 . |
| Viewer | Users with the Viewer role have read-only access to the RMS application. The default username and password for the viewer user is viewer/Viewer@123 . |
| Custom User | User with customized role and permission to the RMS application. |

User Role Exception

The following table lists the permission exceptions for admin, operator, and viewer roles.



Note: The asterisk (*) symbol indicates permissions are only given to the default admin role. These permissions are denied for any user with a custom role.

Table 377. User Roles and Permission Exception

| Operation | Admin | Operator | Viewer |
|--|-------|----------|--------|
| Reboot OLT | ✓ | x | x |
| Create User | ✓ | x | x |
| Update User | ✓ | x | x |
| Delete User | ✓ | x | x |
| Activate User | ✓ | x | x |
| Deactivate User | ✓ | x | x |
| Create Role | ✓ | x | x |
| Delete Role | ✓ | x | x |
| Retrieve User own | ✓ | x | x |
| Retrieve User Role/Roles | ✓ | x | x |
| Retrieve Users | ✓ | x | x |
| Retrieve Audit Logs | ✓ | x | x |
| Subscribe to Live KPIs | ✓ | ✓ | ✓ |
| Unsubscribe to Live KPIs | ✓ | ✓ | ✓ |
| Clear Counters on a Live KPIs Subscription | ✓ | ✓ | ✓ |
| CLI Cut-thru | ✓ | ✓ | ✓ |
| Reboot ONT | ✓ | ✓ | x |
| Retrieve Permissions | ✓ | x | x |
| Change Permissions | ✓ | x | x |
| Retrieve RMS Settings | ✓ | x | x |
| Modify RMS Settings | ✓ | x | x |
| Retrieve RMS Security Policy | ✓ | x | x |

Table 377. User Roles and Permission Exception (continued)

| Operation | Admin | Operator | Viewer |
|-----------------------------------|-------|----------|--------|
| Modify RMS Security Policy | ✓ | x | x |
| OLT Force Delete* | ✓ | x | x |
| Show Session of Users | ✓ | x | x |
| Show Session of User Own | ✓ | ✓ | ✓ |
| Show temporary password for user* | ✓ | x | x |

Field Descriptions

The following table describes the fields on the User Role page.

Table 378. User Role List

| Field | Description |
|--------|--|
| Name | Specifies the name of the user role. |
| Action | Specifies the action that you can perform on the user role. The supported actions are. <ul style="list-style-type: none"> • Edit • Delete • Clone • Assign permissions for the user role • Synchronize the user between CBAC and RMS. |

Creating Custom User Role Configuration

Use this page to create a custom user role and assign required permissions to the user role. You must have administrator privilege or a user with user management privilege to create a custom user role.

The following predefined user roles are available in RMS. For more information about user roles, see [Role Based Access Control \(on page 776\)](#).

- Admin
- Operator
- Viewer

Perform the following steps to create a custom user role.

1. Select **Administration > User Role > Create**.
The User Role Configuration page appears.
2. Complete the configuration according to the guidelines provided in the following table.

Table 379. Creating User Role List

| Field | Description |
|-------|--|
| Name | Enter a unique role name. You can use any number of alphanumeric characters. Only the following special character is supported. <ul style="list-style-type: none">• Hyphen (-) |

3. Click **Create**.
A new user role is created on the Users Role List page.
4. Click the **User Permissions** icon under the **Action** column and provide the required role permission.
For more information, see [Assigning Access Permissions for User Roles \(on page 779\)](#).
5. Click the **Sync** icon under the **Action** column to synchronize the user role between CBAC and RMS.



Note:

- You can edit a user role configuration to modify the permission configured for a user role. If you modify a role name to a user, the change becomes effective only when the user initiates another session.
- Only administrator or a user with customized role and relevant permission can perform the clone operation.
- The clone functionality copies all the associated permissions from the existing role to the newly created role.

To edit, clone, and delete the user role configuration, see [Common Operations \(on page 27\)](#).

Assigning Access Permissions for User Roles

You can assign the following permissions to a user role to access resources (Alarm Profile, Device Audit Log, Controller, and so on) in RMS.

- Create
- Modify
- Delete
- Get
- Activate
- Deactivate
- Reboot
- Acknowledge
- Clear

- Upgrade
- Enable
- Disable and so on

When the user is assigned a role, the user can view only those workspaces that contain the tasks that the user has permissions to execute.

For example, a user who is assigned the device manager role, which grants access privileges to all tasks in the Inventory workspace, can access only the Inventory workspace. No other workspaces are visible to this user unless other roles or permissions are assigned to this user.

Perform the following steps to assign permissions to the user role.

1. Select **Administration > User Role**.

The Users List page appears.

2. Click on the **User Permissions** icon under the **Action** column.

The Role Permission List [User Role - < *Role Name* >] page appears.

3. You must select the check box against each **Resource Name** and then select the type of privileges (create, modify, delete, get, activate, deactivate, and reboot) that you want to assign the user role for the selected resources. You can select one or more access privileges to assign to the user role.

Resource Name. Displays the resources of RMS. You must select the check box against each resource and then select the type of permissions (create, get, modify, delete, activate, deactivate, and reboot) that you want to assign to the user role for the selected resource. You can select one or more access privileges to assign to the user role.

You can select the check box from the column level to assign certain permission to all the resources. For example, if you want to assign create permission for all the resources, then select the column level check box, which is adjacent to the **Create** operation.



Note: You must assign at least one permission to the user role.

Table 380. Access Permissions

| Permission | Description |
|------------|---|
| Create | Enables the user to create new resources. |
| Modify | Enables the user to modify the existing resources. |
| Delete | Enables the user to delete existing resources. |
| Get | Enables the user to retrieve the resources. |
| Activate | Enables the user to activate the following resources. |

Table 380. Access Permissions (continued)

| Permission | Description |
|-------------|--|
| | <ul style="list-style-type: none"> Managed element Management domain Subscriber service Controller. |
| Deactivate | <p>Enables the user to deactivate the following resources.</p> <ul style="list-style-type: none"> Managed element Management domain Subscriber service Controller. |
| ONT Reboot | Enables the users to reboot the ONT. |
| Reboot | Enables the user to reboot the managed element. |
| Acknowledge | <p>Enables the user to acknowledge the following.</p> <ul style="list-style-type: none"> Faults OSS faults Suppressed faults. |
| Clear | <p>Enables the user to clear the following.</p> <ul style="list-style-type: none"> ERPS Instances Faults OSS faults Suppressed faults |
| Upgrade | <p>Enables the user to perform the software upgrade operation on the following.</p> <ul style="list-style-type: none"> OLT Controller. |
| Enable | <p>Allows the user to enable the following configuration for the OLT.</p> <ul style="list-style-type: none"> E-LAN E-Line LAG |
| Disable | <p>Allows the user to disable the following configuration for the OLT.</p> <ul style="list-style-type: none"> E-LAN E-Line LAG |

Table 380. Access Permissions (continued)

| Permission | Description |
|-------------------|--|
| Associate. | Enables the user to associate the following resources with the OLT. <ul style="list-style-type: none"> • ACL profile • LAG |
| Disassociate | Enables the user to disassociate the following resources from the OLT. <ul style="list-style-type: none"> • ACL profile • LAG |
| Reset | Enables the user to perform the reset operation on the OLT. |
| Reconcile | Enables the user to perform the reconcile operation on the controller. |
| Backup | Enables the user to perform the backup operation on the following resources. <ul style="list-style-type: none"> • OLT • Controller |
| Restore | Enables the user to perform the restore operation on the following resources. <ul style="list-style-type: none"> • OLT • Controller |
| Upload ZTP | Enables the user to upload ZTP variables to OLT. |
| Software Download | Enables the user to perform the software download operation on the OLT. |
| Software Activate | Enables the user to perform the software activate operation on the OLT. |
| Software Commit | Enables the user to perform the software commit operation on the OLT. |
| Software Rollback | Enables the user to perform the software rollback operation on the OLT. |
| Lock | Enables the user to perform the lock operations on the user accounts. |
| Unlock | Enables the user to perform the unlock operations on the user accounts. |
| Enable KPI | Enables the Live KPI ON button for the following resources. <ul style="list-style-type: none"> • Managed Element • Eline • ELan • Service • Lag Port |
| Disable KPI | Enables the Live KPI OFF button for the following resources. |

Table 380. Access Permissions (continued)

| Permission | Description |
|-----------------------------------|---|
| | <ul style="list-style-type: none"> Managed Element Eline ELan Service Lag Port |
| Clear KPI | Enables the user to clear the reported KPIs. |
| CLI Access | Enables the user to login to the following from RMS. <ul style="list-style-type: none"> SDPON CLI OLT Console |
| Manual Switchover | Enables the user to perform the manual switchover operation for the type-B protection pair. |
| Manual Switch | Enables the user to perform the manual switch operation on the ERPS instance. |
| Force Switch | Enables the user to perform the force switch operation on the ERPS instance. |
| Replace | Enables the user to perform the replace operation. |
| Subscribe KPI | Enables the user to subscribe the KPI. |
| Unsubscribe KPI | Enables the user to unsubscribe the KPI. |
| Download ONT Firmware on OLT | Enables the user to download the ONT firmware on OLT. |
| Download ONT Firmware on ONT | Enables the user to download the ONT firmware on ONT. |
| Activate Standby Partition on ONT | Enables the user to activate the standby partition on ONT. |
| Cleanup Firmware Partition on OLT | Enables the user to clean up the firmware partition on OLT. |
| Activate Commit ONT Firmware | Enables the user to activate and commit the ONT firmware. |
| Clear ERPS protocol statistics | Enables the user to clear the ERPS protocol statistics. |
| Enable Serial Number | Allows the user to enable OLT serial number. |

Table 380. Access Permissions (continued)

| Permission | Description |
|----------------------|--|
| Initiate Mac Dump | Enables the user to initiate the MAC dump. |
| Cancel Mac Dump | Enables the user to cancel the MAC dump. |
| Export Mac Dump | Enables the user to export the MAC dump. |
| Sdpon Upgrade | Enables the user to upgrade the SDPON. |
| Sdpon Download | Enables the user to download the SDPON. |
| Firmware Activate | Enables the user to activate the firmware. |
| Enable Theft Config | Allows the user to enable OLT theft configuration. |
| Disable Theft Config | Allows the user to disable OLT theft configuration. |
| Banner Update | Enables the user to perform the banner update on the OLT. |
| Ping | Enables the user to perform the ping operation from RMS to check the reachability of controller. |
| Traceroute | Enable the user to perform the traceroute. |



Note: Some of the above operations are not applicable to some of the resources and those are marked as Not Applicable (icon) in the column against those resources.

Figure 182. User Permissions

For example,

- If you disable the “Get” operation of the alarm profile for the user role, the user cannot see the alarm profile object when the user log into the RMS.
- If you enable only the “Get” operations for all the resources for the user role, the user can only view the resources and they cannot perform any operations.

Security Policy

To access this page, click **Administration** from the top right corner and then select **Security Policy** from the left-hand side of the menu.

RMS provides security policy that enables the system administrator to configure the default policy related to login attempts, session inactivity, password history count, and password expiry.

You can either use a default security policy as is if the policy suits your specific requirements or customize the policy to meet your specific requirements. You can also create your own security policy.

Creating Security Policy Configuration

Perform the following steps to create a security policy.

1. Select **Administration > Security Policy**.

The Security Policy List page appears.

2. Complete the configuration according to the guidelines provided in the following table.

Table 381. Security Policy Configuration

| Field | Description |
|--------------------------------------|--|
| Name | Enter a unique name for the security policy. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-)• Space Example: default security policy |
| Failed Login Attempts | Enter the number of times the user can attempt failed login before account is disabled. Example: 3 |
| Session Inactivity Timeout (Minutes) | Enter the timeout value (in minutes) for the RMS to automatically logout the user after an inactivity timeout. Unattended terminals are automatically “blank the screen” and “suspend the session” after the amount of time specified in the security policy. Re-establishment of the session must take place only after the user has provided a valid password. The value ranges from 15 to 20 minutes. |
| Session Expiry Timeout (hours) | Enter the session expiry timeout value in hours. The value ranges from 1 hour to 90 hours. The default value is 24 hours. |

| Field | Description |
|---------------------------------|--|
| Password Expiry Days | Enter the duration (in days) after which the password expires and must be changed. An administrator can configure the password expiry time (in days) at the global level and this applies to all users. Example: 180 days The value ranges from 180 to 365 days. |
| Password Expiry Warning Days | Enter the duration (in days) in advance that the users are warned that their passwords will expire. The default value is 7 days. For example, if you enter 7, users receive a notification 7 days before their current passwords expire. |
| Password History Count | Enter the password history count to restrict the password reuse. The password history is enforced to ensure that users are forced to select unique new passwords upon password expiry. The value ranges from 7 to 32. The default value is 7. |
| Password Minimum Length | Specifies the minimum number of characters required for the user password. This prevents the users from using short passwords, which is easier to decode and discover. The default value is 8 characters. The value ranges from 8 to 32 characters. |
| Reject User Credentials Strings | Specifies the list of strings provided by the operator that must not be used as part of the user credentials. If this field not configured, all the strings are allowed by default. |

3. Click **Create**.

A new security policy is created and appears on the Security List page.

To edit, clone, and delete the security policy configuration, see [Common Operations \(on page 27\)](#).

Template Builder

To access this page, click **Template Builder** from the top right corner of the page.

Template builder expedite integration and maintenance time, offering significant reduction of the underlying technology complexity.

The RMS Northbound Interface (NBI) uses templates to provision services. The template expedites configuration or updates of attributes that are visible for the OSS client application, only the essential attributes are visible.

Template builder is a way to create a framework required for the resource configuration. This feature enables the operators to quickly create a framework in the form of a template that you can apply to multiple resources in your network.

For example, you can create a framework template for the OLT and the template can be applied while creating the OLT configuration. The same template can be applied to one or more OLT devices.

Using the template builder, you can automate the resource configuration and define the resource parameters either as variables or constants.

While creating the template, you can define the resource attribute as a variable or constant.

- If the attribute is defined as a variable,
 - You must assign the variable name.
 - Assign default value for the variable at the time of template creation or during the configuration of the resource.
- If the attribute is not defined as variable, you can assign the attribute value.

You can create a template for the following RMS resources.

- OLT
- ONT
- CARD
- RACK
- SHELF
- SUBSCRIBER
- SUBSCRIBER SERVICE
- CONTROLLER
- Zero Touch Provisioning (ZTP)

Tasks

You can perform the following tasks using this page.

- Create OLT Template. See [Creating OLT Template \(on page 788\)](#).
- Create ONT Template. See [Creating ONT Template \(on page 791\)](#).
- Create Card Template. See [Creating Card Template \(on page 792\)](#).
- Create Rack Template. See [Creating Rack Template \(on page 794\)](#).
- Create Shelf Template. See [Creating Shelf Template \(on page 795\)](#).
- Create Subscriber Template. See [Creating Subscriber Template \(on page 796\)](#).
- Create Subscriber Service Template. See [Creating Subscriber Service Template \(on page 798\)](#).
- Create Controller Template. See [Creating Controller Template \(on page 799\)](#).
- Create ZTP Template. See [Creating ZTP Template \(on page 801\)](#).
- Export a Template. See [Exporting Template \(on page 803\)](#).
- Import a Template. See [Importing Template \(on page 803\)](#).

Creating OLT Template

Perform the following steps to create an OLT template.

1. Select **Template Builder** from the top right corner of the page.
The Template Builder page appears.
2. Click **Plus** icon from the left-hand side of the menu.
3. Complete the configuration according to the guidelines provided in the following table.

Table 382. Creating OLT Template

| Field | Description |
|--|---|
| TEMPLATE | |
| Name | Enter the name for the OLT template. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-) Example: OLT_1 |
| Template Type | Select the template type from the list. You must select the template type as OLT. |
| Version | Enter the version for the OLT template. |
| Click Next . A OLT template is created in the left-hand of the hierarchy tree and the Add New page appears with the following fields. | |
| RESOURCES | |

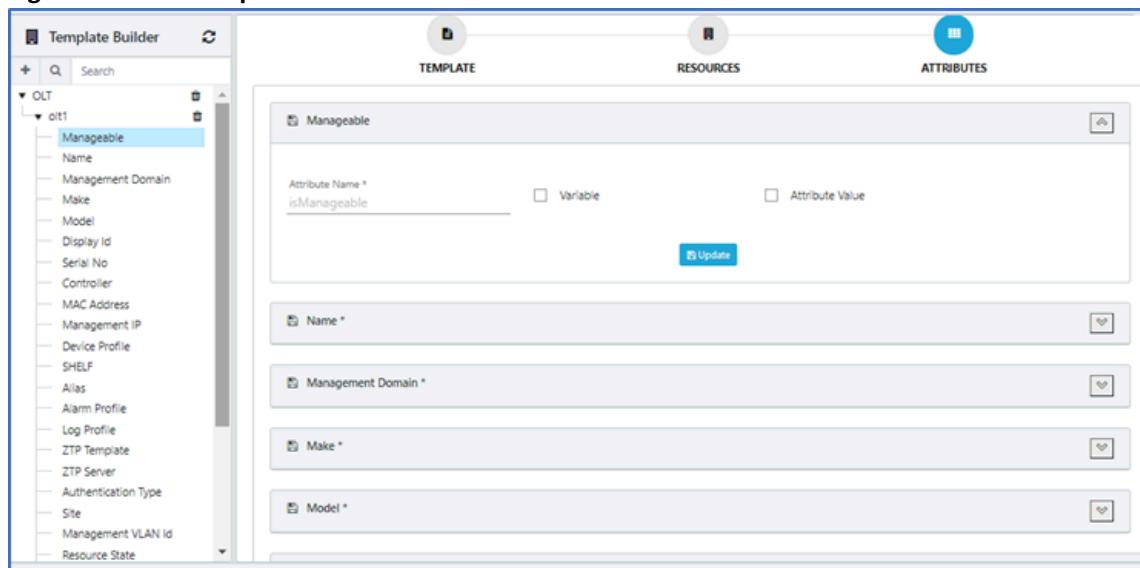
| Field | Description |
|---|---|
| Name | <p>Enter the name for the configuration. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> Underscore (_) Hyphen (-) <p>Example: OLT_Config</p> |
| Template Name | <p>Displays the OLT template name that was created. You cannot edit this field.</p> <p>Example: OLT_1</p> |
| Attachment Type | <p>Select the attachment type from the list. The supported values are.</p> <ul style="list-style-type: none"> RESOURCE. Select this value if you want to create a resource configuration. TEMPLATE. Select this value if you want to refer the template. |
| When the attachment type is selected as RESOURCE , the following fields are displayed. | |
| Resource Type | <p>Select the resource type for which you are creating the OLT template.</p> <ul style="list-style-type: none"> CONTROLLER RACK SHELF OLT CARD |
| When the attachment type is selected as TEMPLATE , the following fields are displayed. | |
| Attachment ID | <p>Select the attachment ID for which you are creating the OLT template. The supported values are.</p> <ul style="list-style-type: none"> OLT-Template-Radisys-RLT-3200G OLT-Template-Radisys-RLT-1600G OLT-Template-Radisys-RLT-1600C OLT-Template-Radisys-RLT-1600X OLT-Template-Radisys-RLT-3200C |

4. Click **Create**.

The OLT configuration is created as a sub option of the OLT template in the left-hand of the hierarchy tree.

Click on the name to display the attributes of the OLT. All attributes of the OLT are displayed in the left pane as well on the right-hand side of the page shown in [Figure 183: OLT Template Creation \(on page 790\)](#).

Figure 183. OLT Template Creation



5. A list of attributes associated with the resource are displayed. Update each attribute according to the guidelines provided in the following table.

Table 383. Updating Attributes

| Attribute Name | Specifies the attribute name. You cannot edit this field. |
|-----------------------------------|---|
| Variable | <p>You can define the resource attribute as a variable or constant.</p> <ul style="list-style-type: none"> • If the attribute is defined as a variable, <ul style="list-style-type: none"> ◦ You must assign the variable name. ◦ Assign default value for the variable at the time of template creation or while applying the template to other resource. • If the attribute is not defined as variable, you can assign the attribute value. <p>Note: The attribute set as a Variable gives the flexibility to user to assign or unassign the value at the time of execution of template.</p> |
| <input type="checkbox"/> Variable | The Variable field checkbox is disabled and not selected, indicating that the selected Attribute Value is used as default when applying this template to other resource. |
| <input type="checkbox"/> Variable | The Variable field checkbox is enabled and not selected. |

Table 383. Updating Attributes (continued)

| | |
|--|---|
| | <ul style="list-style-type: none"> • If you select the checkbox, this attribute acts as a variable and the Variable Default field must be updated when applying the template to other resource. • If you do not select the checkbox, the selected Attribute Value is used as default when applying this template to other resource. |
|  Variable | The Variable field checkbox is disabled and selected which indicates that the Variable Default field must be updated when applying this template to other resource. |
| Variable Name | Enter the variable name. This field is displayed if the Variable checkbox is selected. |
| Variable Default | Specifies the default value for the variable name. This field is displayed if the Variable checkbox is selected. |
| Attribute Value | Specifies the attribute supported value. For example, if the attribute name is mode then the attribute values are CENTRALIZED or DISTRIBUTED. |
| Update | Click Update to apply the changes. |

Creating ONT Template

Perform the following steps to create an ONT template.

1. Select **Template Builder** from the top right corner of the page.
The Template Builder page appears.
2. Click **Plus** icon from the left-hand side of the menu.
3. Complete the configuration according to the guidelines provided in the following table.

Table 384. Creating ONT Template Configuration

| Field | Description |
|-------|--|
| Name | <p>Enter the name for the ONT template. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) <p>Example: ONT_1</p> |

| Field | Description |
|---|---|
| Template Type | Select the template type from the list. You must select the template type as ONT. |
| Version | Enter the version for the ONT template. |
| Click Next. A ONT template is created in the left-hand of the hierarchy tree and the Add New page appears with the following fields. | |
| Name | Enter the name for the configuration. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> Underscore (_) Hyphen (-) |
| Template Name | Displays the ONT template name that was created. You cannot edit this field. Example: ONT_1 |
| Attachment Type | Select the attachment type from the list. The supported values are. <ul style="list-style-type: none"> RESOURCE. Select this value if you want create a resource configuration. TEMPLATE. Select this value if you want to refer to the template. |
| When the attachment type is selected as RESOURCE , the following fields are displayed. | |
| Resource Type | Select the resource type for which you are creating the ONT template. Example: ONT |
| When the attachment type is selected as TEMPLATE , the following fields are displayed. | |
| Attachment ID | Select the attachment ID for which you are creating the ONT template. |

4. **Click Create.**

The ONT configuration is created as a sub option of the ONT template in the left-hand of the hierarchy tree and displays all parameters of the ONT.

Creating Card Template

Perform the following steps to create a card template.

1. Select **Template Builder** from the top right corner of the page.
 The Template Builder page appears.
2. Click **Plus** icon from the left-hand side of the menu.
3. Complete the configuration according to the guidelines provided in the following table.

Table 385. Creating Card Template Configuration

| Field | Description |
|---|---|
| Name | <p>Enter the name for the card template. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) <p>Example: Card_Template</p> |
| Template Type | Select the template type from the list. You must select the template type as CARD. |
| Version | Enter the version for the CARD template. |
| <p>Click Next.</p> <p>A card template is created in the left-hand of the hierarchy tree and the Add New page appears with the following fields.</p> | |
| Name | <p>Enter the name for the configuration. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) |
| Template Name | <p>Displays the card template name that was created. You cannot edit this field.</p> <p>Example: Card_Template</p> |
| Attachment Type | <p>Select the attachment type from the list. The supported values are.</p> <ul style="list-style-type: none"> • RESOURCE. Select this value if you want to create a resource configuration. • TEMPLATE. Select this value if you want to refer to the template. |
| <p>When the attachment type is selected as RESOURCE, the following fields are displayed.</p> | |
| Resource Type | <p>Select the resource type for which you are creating the card template.</p> <ul style="list-style-type: none"> • RACK • SHELF • CARD |
| <p>When the attachment type is selected as TEMPLATE, the following fields are displayed.</p> | |
| Attachment ID | Select the attachment ID for which you are creating the card template. |

4. Click **Create**.

A confirmation message appears indicating the status of the activate operation and the admin state of the controller changes to ACTIVATION IN PROGRESS and then changes to ACTIVE.

The card configuration is created as a sub option of the card template in the left-hand of the hierarchy tree and displays all the parameters of the card.

Creating Rack Template

Perform the following steps to create a rack template.

1. Select **Template Builder** from the top right corner of the page.

The Template Builder page appears.

2. Click **Plus** icon from the left-hand side of the menu.

3. Complete the configuration according to the guidelines provided in the following table.

Table 386. Creating RACK Template Configuration

| Field | Description |
|--|--|
| Name | Enter the name for the rack template. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">Underscore (_)Hyphen (-) Example: Rack_Template |
| Template Type | Select the template type from the list. You must select the template type as RACK. |
| Version | Enter the version for the rack template. |
| Click Next. A rack template is created in the left-hand of the hierarchy tree and the Add New page appears with the following fields. | |
| Name | Enter the name for the configuration. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">Underscore (_)Hyphen (-) |
| Template Name | Displays the rack template name that was created. You cannot edit this field. Example: Rack_Template |
| Attachment Type | Select the attachment type from the list. The supported values are. |

| Field | Description |
|---|--|
| | <ul style="list-style-type: none"> RESOURCE. Select this value if you want to create a resource configuration. TEMPLATE. Select this value if you want to refer to the template. |
| When the attachment type is selected as RESOURCE , the following fields are displayed. | |
| Resource Type | Select the resource type for which you are creating the rack template. <ul style="list-style-type: none"> RACK SHELF |
| When the attachment type is selected as TEMPLATE , the following fields are displayed. | |
| Attachment ID | Select the attachment ID for which you are creating the rack template. |

4. Click **Create**.

A confirmation message appears indicating the status of the activate operation and the admin state of the rack changes to ACTIVATION IN PROGRESS and then changes to ACTIVE.

The rack configuration is created as a sub option of the rack template in the left-hand of the hierarchy tree and displays all the parameters of the rack.

Creating Shelf Template

Perform the following steps to create a shelf template.

- Select **Template Builder** from the top right corner of the page.
The Template Builder page appears.
- Click **Plus** icon from the left-hand side of the menu.
- Complete the configuration according to the guidelines provided in the following table.

Table 387. Creating Shelf Template Configuration

| Field | Description |
|---------------|---|
| Name | Enter the name for the shelf template. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> Underscore (_) Hyphen (-) Example: Shelf_Template |
| Template Type | Select the template type from the list. You must select the template type as SHELF. |
| Version | Enter the version for the shelf template. |

| Field | Description |
|--|---|
| <p>Click Next.</p> <p>A shelf template is created in the left-hand of the hierarchy tree and the Add New page appears with the following fields.</p> | |
| Name | <p>Enter the name for the configuration. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> Underscore (_) Hyphen (-) |
| Template Name | Displays the shelf template name that was created. You cannot edit this field. Example: Shelf_Template |
| Attachment Type | <p>Select the attachment type from the list. The supported values are.</p> <ul style="list-style-type: none"> RESOURCE. Select this value if you want to create a resource configuration. TEMPLATE. Select this value if you want to refer to the template. |
| When the attachment type is selected as RESOURCE , the following fields are displayed. | |
| Resource Type | Select the resource type for which you are creating the rack template. |
| When the attachment type is selected as TEMPLATE , the following fields are displayed. | |
| Attachment ID | Select the attachment ID for which you are creating the shelf template. |

4. Click **Create**.

A confirmation message appears indicating the status of the activate operation and the admin state of the shelf changes to ACTIVATION IN PROGRESS and then changes to ACTIVE.

The shelf configuration is created as a sub option of the shelf template in the left-hand of the hierarchy tree and displays all the parameters of the shelf.

Creating Subscriber Template

Perform the following steps to create a subscriber template.

- Select **Template Builder** from the top right corner of the page.
The Template Builder page appears.
- Click **Plus** icon from the left-hand side of the menu.
- Complete the configuration according to the guidelines provided in the following table.

Table 388. Creating Subscriber Template Configuration

| | |
|---|--|
| Name | Enter the name for the subscriber template. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) Example: subscriber_template |
| Template Type | Select the template type from the list. You must select the template type as SUBSCRIBER. |
| Version | Enter the version for the subscriber template. |
| <p>Click Next.</p> <p>A subscriber template is created in the left-hand of the hierarchy tree and the Add New page appears with the following fields.</p> | |
| Name | Enter the name for the configuration. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) |
| Template Name | Displays the subscriber template name that was created. You cannot edit this field. Example: subscriber_template |
| Attachment Type | Select the attachment type from the list. The supported values are. <ul style="list-style-type: none"> • RESOURCE. Select this value if you want to create a resource configuration. • TEMPLATE. Select this value if you want to refer to the template. |
| When the attachment type is selected as RESOURCE , the following fields are displayed. | |
| Resource Type | Select the resource type for which you are creating the template. <ul style="list-style-type: none"> • SUBSCRIBER • SUBSCRIBER_SERVICE • SERVICE • ONT |
| Resource to Resource Mapping | Specifies the resource mapped to existing resource present within the template. Example: Service resource is mapped to subscriber service. |
| When the attachment type is selected as TEMPLATE , the following fields are displayed. | |

| | |
|-------------------------------|--|
| Attachment ID | Select the attachment ID for which you are creating the subscriber template. |
| Associate From Template | Select the checkbox to associate the attribute with the existing resource configured in a template. Clear the checkbox to associate the default values from the database. |
| Attribute to Resource Mapping | Specifies the attribute mapped to existing resource present within the template. Example: ONT attribute is mapped to subscriber resource. |

4. Click **Create**.

A confirmation message appears indicating the status of the activate operation and the admin state of the subscriber changes to ACTIVATION IN PROGRESS and then changes to ACTIVE.

The subscriber configuration is created as a sub option of the subscriber template in the left-hand of the hierarchy tree and displays all the parameters of the subscriber.

Creating Subscriber Service Template

Perform the following steps to create a subscriber service template.

1. Select **Template Builder** from the top right corner of the page.
The Template Builder page appears.
2. Click **Plus** icon from the left-hand side of the menu.
3. Complete the configuration according to the guidelines provided in the following table.

Table 389. Creating Subscriber Service Template Configuration

| Field | Description |
|---------------------|---|
| Name | Enter the name for the service template. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) Example: sub_service_template |
| Template Type | Select the template type from the list. You must select the template type as SUBSCRIBER_SERVICE. |
| Version | Enter the version for the subscriber service template. |
| Click Next . | |

| Field | Description |
|--|---|
| A subscriber service template is created in the left-hand of the hierarchy tree and the Add New page appears with the following fields. | |
| Name | <p>Enter the name for the configuration. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> Underscore (_) Hyphen (-) |
| Template Name | <p>Displays the subscriber service template name that was created. You cannot edit this field.</p> <p>Example: sub_service_template</p> |
| Attachment Type | <p>Select the attachment type from the list. The supported values are.</p> <ul style="list-style-type: none"> RESOURCE. Select this value if you want to create a resource configuration. TEMPLATE. Select this value if you want to refer to the template. |
| When the attachment type is selected as RESOURCE , the following fields are displayed. | |
| Resource Type | <p>Select the resource type for which you are creating the template.</p> <ul style="list-style-type: none"> SUBSCRIBER_SERVICE SERVICE |
| When the attachment type is selected as TEMPLATE , the following fields are displayed. | |
| Attachment ID | Select the attachment ID for which you are creating the subscriber service template. |

4. Click **Create**.

The subscriber service configuration is created as a sub option of the subscriber service template in the left-hand of the hierarchy tree and displays all the parameters of the subscriber service.

Creating Controller Template

Perform the following steps to create a controller template.

- Select **Template Builder** from the top right corner of the page.
The Template Builder page appears.
- Click **Plus** icon from the left-hand side of the menu.
- Complete the configuration according to the guidelines provided in the following table.

Table 390. Creating Controller Template Configuration

| Field | Description |
|---|---|
| Name | <p>Enter the name for the controller template. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) <p>Example: Controller_Template</p> |
| Template Type | Select the template type from the list. You must select the template type as CONTROLLER . |
| Version | Enter the version for the controller template. |
| <p>Click Next.</p> <p>A controller template is created in the left-hand of the hierarchy tree and the Add New page appears with the following fields.</p> | |
| Name | <p>Enter the name for the configuration. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) |
| Template Name | <p>Displays the controller template name that was created. You cannot edit this field.</p> <p>Example: Controller_Template</p> |
| Attachment Type | <p>Select the attachment type from the list. The supported values are.</p> <ul style="list-style-type: none"> • RESOURCE. Select this value if you want to create a resource configuration. • TEMPLATE. Select this value if you want to refer to the template. |
| <p>When the attachment type is selected as RESOURCE, the following fields are displayed.</p> | |
| Resource Type | <p>Select the resource type for which you are creating the template.</p> <ul style="list-style-type: none"> • Controller |
| <p>When the attachment type is selected as TEMPLATE, the following fields are displayed.</p> | |
| Attachment ID | Select the attachment ID for which you are creating the controller template. |

4. Click **Create**.

The controller configuration is created as a sub option of the controller template in the left-hand of the hierarchy tree and displays all the parameters of the controller.

Creating ZTP Template

Zero Touch Provisioning (ZTP) removes the need for an IT personnel to manually provision and configure the hardware devices and thus reduces the risk of human error. ZTP allows you to provision new OLT devices in your network automatically, with minimal manual intervention.

- The automated push of network service configuration and golden configuration from RMS after a successful reconciliation of CBAC-D.
- The network service configuration includes network provisioning. For example, the configuration and management of network towards the BNG. Features such as VLAN (E- LAN), Access Control List (ACL), Link Aggregation Group (LAG), Ethernet Ring Protection Switching (ERPS), and Connectivity Fault Management (CFM) are configured over the NNI towards BNG.
- The golden configuration includes all profiles such as device-specific profiles (managed element and port alarm profiles), subscriber and service profiles (bandwidth, shaper, and CoSQ profiles), along with other profiles such as log server, ACL, LAG profile, and so on.

Prerequisites- User must create an OLT with port and both OLT and port should be ACTIVE and UP.

Perform the following steps to create a ZTP template.

1. Select **Template Builder** from the top right corner of the page.
The Template Builder page appears.
2. Click **Plus** icon from the left-hand side of the menu.
3. Complete the configuration according to the guidelines provided in the following table.

Table 391. Creating ZTP Template Configuration

| Field | Description |
|---------------|--|
| Name | Enter the name for the ZTP template. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">• Underscore (_)• Hyphen (-) Example: ZTP_Template |
| Template Type | Select the template type from the list. You must select the template type as ZTP. |
| Version | Enter the version for the ZTP template. |

Click **Next**.
A ZTP template is created in the left-hand of the hierarchy tree and the **Add New** page appears with the following fields.

| Field | Description |
|-----------------|---|
| Name | <p>Enter the name for the configuration. You can use any number of alphanumeric characters. Only the following special characters are supported.</p> <ul style="list-style-type: none"> • Underscore (_) • Hyphen (-) <p>Example: LAG</p> |
| Template Name | <p>Displays the controller template name that was created. You cannot edit this field.</p> <p>Example: ZTP_Template</p> |
| Attachment Type | <p>Select the attachment type from the list. The supported values are.</p> <ul style="list-style-type: none"> • RESOURCE. Select this value if you want to create a resource configuration. |
| Resource Type | <p>Select the resource type for which you are creating the template.</p> <ul style="list-style-type: none"> • LAG • ELAN • ERPS Profile • ERPS Instance • MEP Profile • MEP Instance • ERPS Ring • ME_ACL_Profile |

4. Click **Create**.

The ZTP configuration is created as a sub option of the ZTP template in the left-hand of the hierarchy tree and displays all parameters of the controller.

Perform the following steps after the successful creation of the ZTP template.

1. Navigate to the **Configuration > Inventory** page.
2. Click on the **OLT** tab.
3. Click on the three dots icon (⋮) and select the **ZTP Provisioning** option.

The Variables page appears and all the attributes that are marked as variable while creating the ZTP template.



Note: If the OLT is activated, the **ZTP Provisioning** option of the OLT is enabled.

4. Select ZTP template that you have created from the **ZTP Template** list.
5. Assign values to the variables.



Note: If the attribute is selected as constant, the attribute does not appear on the **Variables** page.

6. Click the **Provision** option.

A success message appears indicating that the request for ZTP is submitted successfully and the **ZTP Status** of the OLT is changed to INITIATED. Once the ZTP operation is successful, the **ZTP Status** of the OLT changes to SUCCESS.

You can click on the ZTP Status to view the sequence of operations performed as part of the OLT ZTP provisioning and the status of each operation.

Exporting Template

You can export the template as a JSON file from RMS to your local computer or a remote server. The JSON file can be opened or edited using a JSON editor. You can view and analyze the exported template information as needed.



Note: Bulk export of the templates is not supported.

Perform the following steps to export a template.

1. Select **Template Builder** from the top right corner of the page.

The Template Builder page appears.

2. Select the template from the left-hand side of the menu.

3. Click **Export** to export the details.

The file is downloaded and appears at the bottom of the page. Click on it to open the JSON file using an application such as JSON editor. Optionally, you can save this file on your computer for later use.

Importing Template

You can import the template configuration from your local computer to RMS by uploading the JSON file.



Note:

- You cannot import a JSON template file if the same template version is available in the RMS.
- Bulk import of the templates is not supported.

Perform the following steps to import a template.

1. Select **Template Builder** from the top right corner of the page.

The Template Builder page appears.

2. Click **Import** from the left-hand side of the menu.

3. Select one of the locations from the following list.
 - Home
 - Desktop
 - RMS
 - SDPON
 - Other Location
4. Select the folder and click **Open**.
5. Select the JSON template file and click **Open** to import the template.
A success message appears and indicates that the file is uploaded successfully.

Configuration Examples

This section covers configuration examples with step-by-step instructions and guidelines for setting up the managed elements and other resources. It makes it easier for users to find the necessary information, understand, and implement the configurations.

Example: Configuring and Activating HSIA Services for the Subscriber

This example shows how to configure and activate the High Speed Internet Applications (HSIA) services for the subscriber.

- [Overview \(on page 805\)](#)
- [HSIA Service Activation Workflow \(on page 805\)](#)
- [Verification \(on page 829\)](#)

Overview

The High Speed Internet Applications (HSIA) are software programs that leverage fast and reliable internet connections to enhance user experiences. These applications are designed to take advantage of high bandwidth and low latency connections, enabling seamless video streaming, online gaming, real-time video conferencing, and rapid data transfer.

HSIA Service Activation Workflow

Perform the following steps to create and activate the HSIA service.

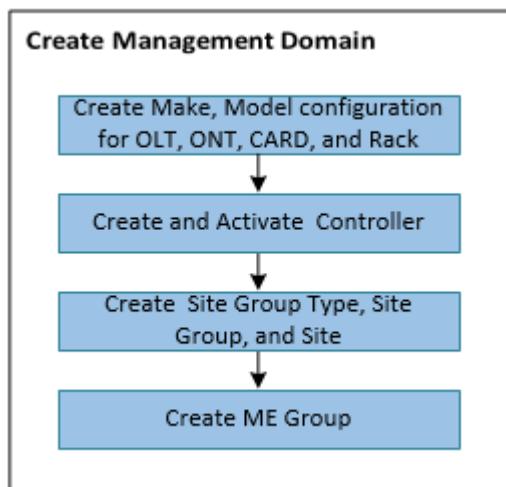
1. Create Management Domain. See [Creating Management Domain \(on page 806\)](#).
2. Create OLT Profiles. See [Creating OLT Profiles \(on page 810\)](#).
3. Create and activate OLT. See [OLT Activation Workflow \(on page 815\)](#).
4. Create PON Profiles. See [PON Profiles Workflow \(on page 821\)](#).
5. Create and activate ONT. See [ONT Activation Workflow \(on page 825\)](#).
6. Create, activate, subscriber and service. See [Service Activation Workflow \(on page 827\)](#).

Figure 184. HSIA Activation Workflow



Creating Management Domain

The following diagram illustrates the workflow for creating a management domain.

Figure 185. Management Domain Workflow

Perform the following steps to create a management domain.

1. Create a make configuration for OLT, ONT, CARD, and Rack. See [Creating Make Configuration \(on page 606\)](#).



Note: If the default OLT device profile does not exist in RMS, you must create a make for the OLT.

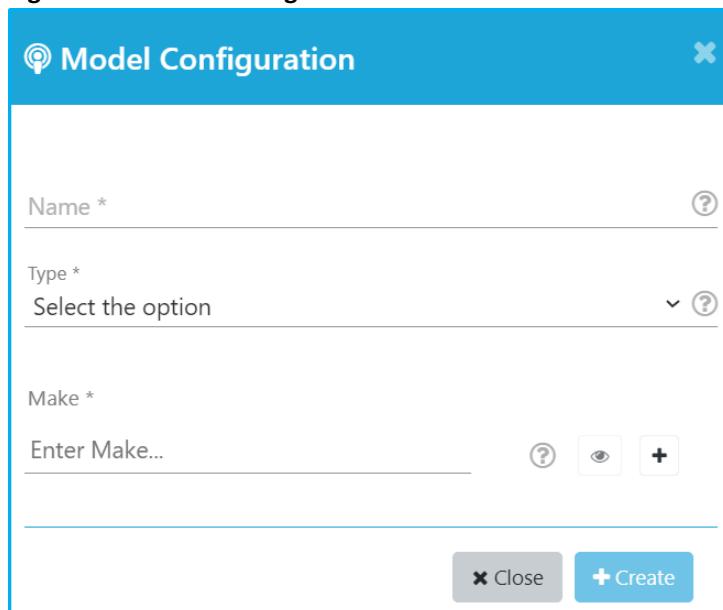
Figure 186. Make Configuration

The form is titled 'Make Configuration'. It contains fields for Name, OLT, ONT, CPE, SPLITTER, RACK, CARD, BNG, SFP, and CABLE. Each field is marked with a required indicator (*). The 'Name' field has a question mark icon. The 'OLT', 'ONT', 'CPE', 'SPLITTER', 'RACK', 'CARD', 'BNG', 'SFP', and 'CABLE' fields have dropdown menus. The 'CPE' field is set to 'No'. The 'SPLITTER' field is set to 'No'. The 'RACK' field is set to 'No'. The 'CARD' field is set to 'No'. The 'BNG' field is set to 'No'. The 'SFP' field is set to 'No'. The 'CABLE' field is set to 'No'. At the bottom right are 'Close' and 'Create' buttons.

2. Create a model configuration for OLT, ONT, CARD, and Rack. See [Creating Model Configuration \(on page 610\)](#).

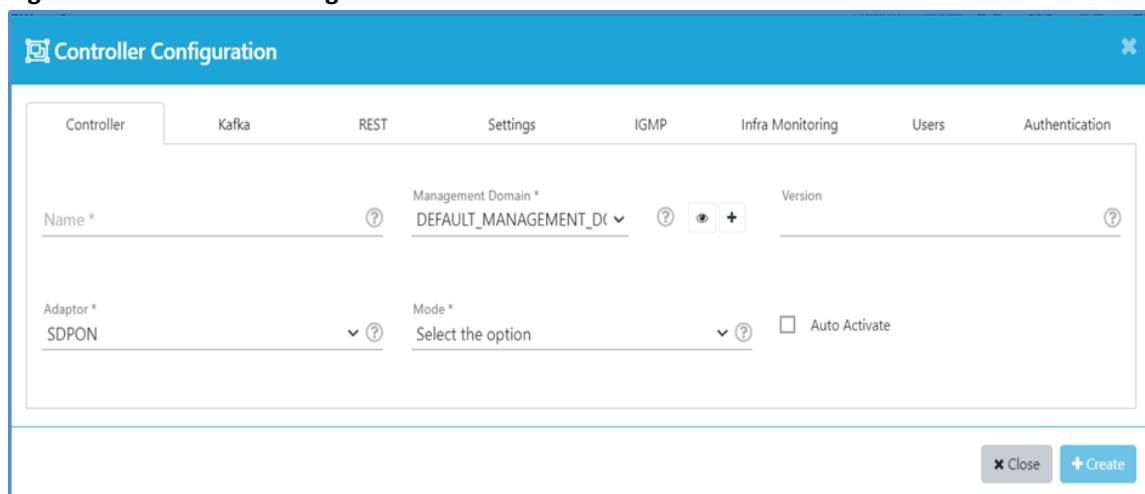


Note: If the default OLT device profile does not exist in RMS, you must create a model for the OLT.

Figure 187. Model Configuration

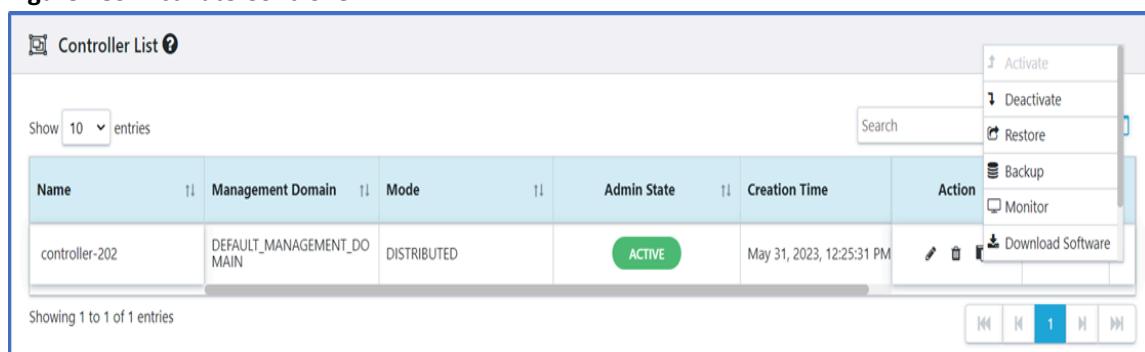
The dialog box is titled "Model Configuration". It contains fields for "Name" (with a required asterisk), "Type" (a dropdown menu with "Select the option" placeholder), and "Make" (a text input field with "Enter Make..." placeholder). Below these are three small buttons: a question mark, an eye icon, and a plus icon. At the bottom are "Close" and "Create" buttons.

3. Create a controller. See [Creating Controller Configuration \(on page 297\)](#).

Figure 188. Controller Configuration

The dialog box is titled "Controller Configuration". It has tabs for "Controller" (selected), "Kafka", "REST", "Settings", "IGMP", "Infra Monitoring", "Users", and "Authentication". The "Controller" tab contains fields for "Name" (with a required asterisk), "Management Domain" (a dropdown menu with "DEFAULT_MANAGEMENT_DOMAIN" placeholder), "Version" (a text input field with a question mark icon), "Adaptor" (a dropdown menu with "SDPON" placeholder), "Mode" (a dropdown menu with "Select the option" placeholder), and "Auto Activate" (a checkbox). At the bottom are "Close" and "Create" buttons.

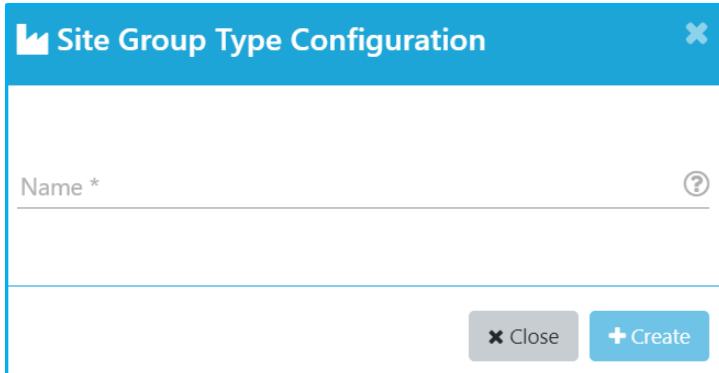
4. Activate a controller. See [Activating the Controller \(on page 305\)](#).

Figure 189. Activate Controller

The table is titled "Controller List". It has columns for "Name", "Management Domain", "Mode", "Admin State", "Creation Time", and "Action". A single row is shown with "controller-202" in the Name column, "DEFAULT_MANAGEMENT_DOMAIN" in Management Domain, "DISTRIBUTED" in Mode, "ACTIVE" in Admin State, and "May 31, 2023, 12:25:31 PM" in Creation Time. The "Action" column contains a context menu with options: "Activate", "Deactivate", "Restore", "Backup", "Monitor", "Download Software", and "Edit", "Delete", "Download Software". At the bottom are navigation buttons and a message "Showing 1 to 1 of 1 entries".

5. Create a site group type, site group, and site.
 - a. Create a site group type. See [Creating Site Group Type Configuration \(on page 292\)](#).

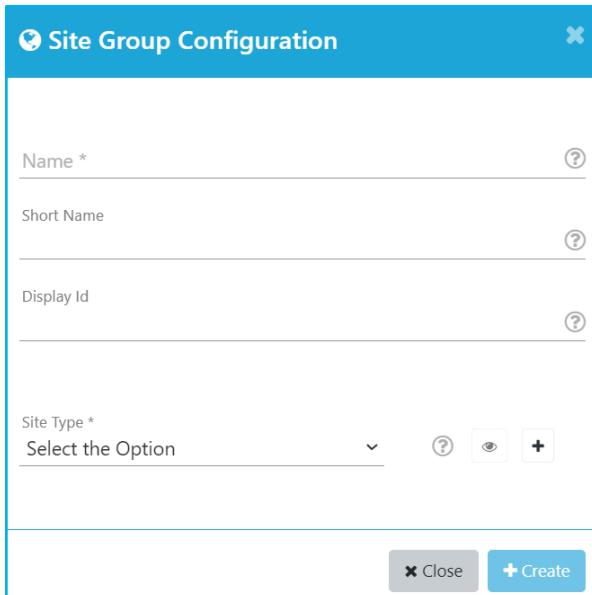
Figure 190. Site Group Type



The dialog box is titled "Site Group Type Configuration". It contains a single input field labeled "Name *". Below the input field are two buttons: "Close" and "Create".

- b. Create a site group. See [Creating Site Group Configuration \(on page 290\)](#).

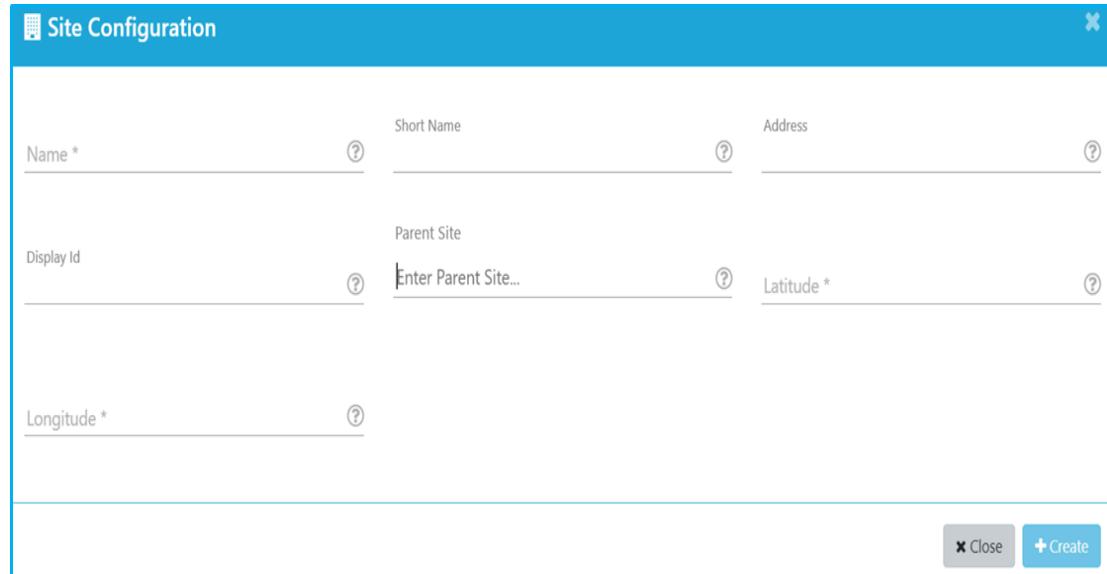
Figure 191. Site Group



The dialog box is titled "Site Group Configuration". It contains four input fields: "Name *", "Short Name", "Display Id", and a dropdown menu labeled "Site Type *". The dropdown menu has an option "Select the Option" and three icons: a question mark, a magnifying glass, and a plus sign. Below the input fields are two buttons: "Close" and "Create".

- c. Create a site. See [Creating Site Configuration \(on page 289\)](#).

Figure 192. Site Configuration



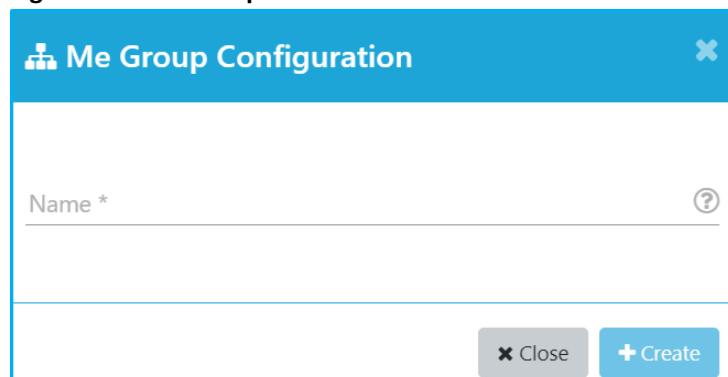
The Site Configuration dialog box contains the following fields:

- Name * (input field)
- Short Name (input field)
- Address (input field)
- Display Id (input field)
- Parent Site (input field)
- Latitude * (input field)
- Longitude * (input field)

Buttons at the bottom right: Close (grey) and Create (blue)

6. Create a ME group. See [Creating ME Group Configuration \(on page 293\)](#).

Figure 193. ME Group



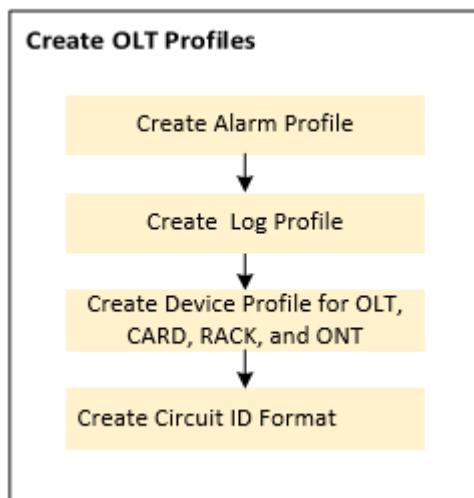
The Me Group Configuration dialog box contains the following field:

- Name * (input field)

Buttons at the bottom right: Close (grey) and Create (blue)

Creating OLT Profiles

The following diagram illustrates the workflow for creating a profile.

Figure 194. OLT Profile Workflow

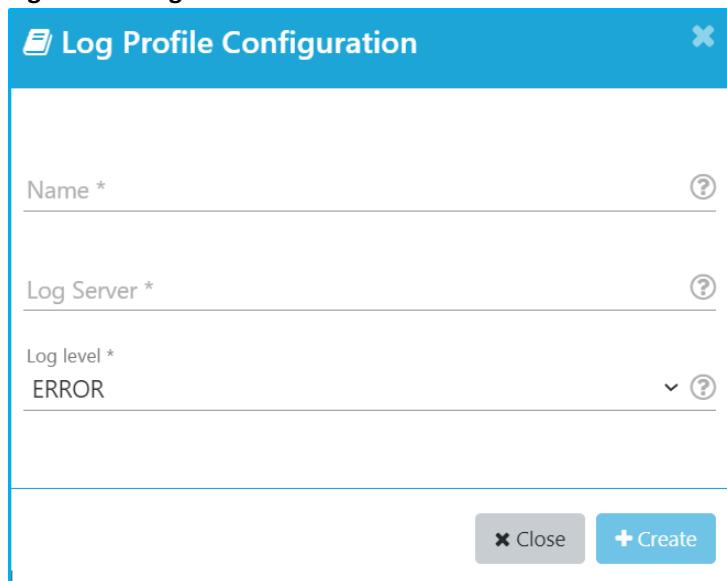
Perform the following steps to create a profile.

1. Create an alarm profile. The following are the different alarm profile that can be created based on the requirement. See [Alarm Profile \(on page 473\)](#).
 - OLT Alarm Profile
 - OLT Port Alarm Profile
 - ONT Alarm Profile
 - LAG Alarm Profile
 - ACE Alarm Profile
 - SFP (NNI) Alarm Profile
 - SFP (PON) Alarm Profile
 - ANI-G Alarm Profile

Figure 195. Alarm Profile

The screenshot shows a software interface for creating an alarm profile. The title bar is 'Alarm Profile Configuration'. The 'Name' field is marked with a red asterisk and has a note 'Name is required.' The 'Type' field is a dropdown menu with 'Select the Option' at the top. A list of options is shown below, with 'ACE' currently selected and highlighted in blue. Other options include OLT, OLT PORT, ONT, LAG, SFP, and ANI-G.

2. Create a log profile. See [Creating Log Profile \(on page 503\)](#).

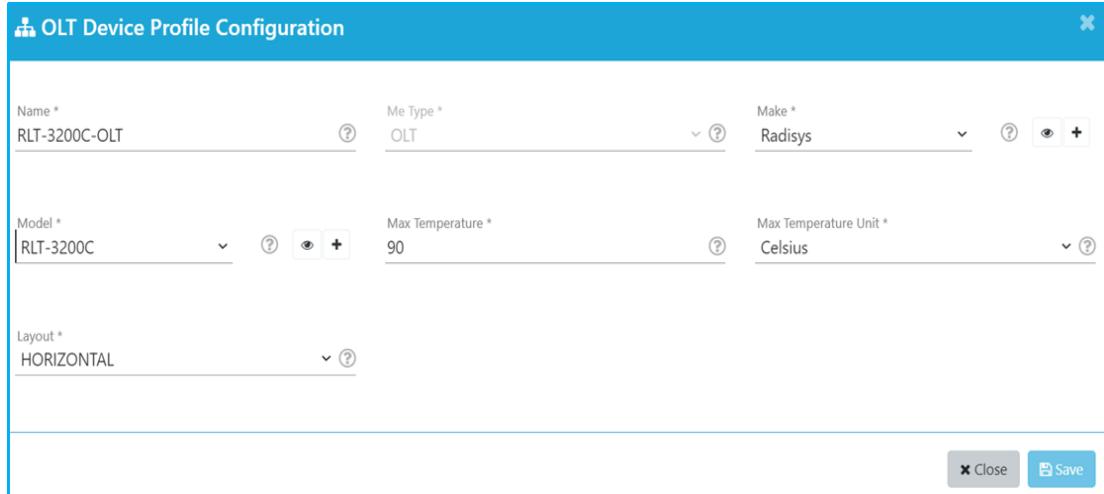
Figure 196. Log Profile

The dialog box is titled "Log Profile Configuration". It contains three input fields: "Name *", "Log Server *", and "Log level *". The "Name" field is set to "ERROR". The "Log Server" field is empty. The "Log level" field is set to "ERROR". At the bottom are "Close" and "Create" buttons.

3. Create a device profile for OLT, CARD, RACK, and ONT.
 - a. Create an OLT device profile. See [Creating OLT Device Profile \(on page 509\)](#).



Note: The OLT device profile contains the OLT, rack, shelf, and slot configuration.

Figure 197. OLT Device Profile

The dialog box is titled "OLT Device Profile Configuration". It contains several input fields: "Name *", "Me Type *", "Make *", "Model *", "Max Temperature *", "Max Temperature Unit *", and "Layout *". The "Name" field is "RLT-3200C-OLT", "Me Type" is "OLT", "Make" is "Radisys", "Model" is "RLT-3200C", "Max Temperature" is "90", "Max Temperature Unit" is "Celsius", and "Layout" is "HORIZONTAL". At the bottom are "Close" and "Save" buttons.

3. Create a device profile for OLT, CARD, RACK, and ONT.
 - b. Create a card device profile. See [Creating Card Device Profile \(on page 522\)](#).

Figure 198. CARD Device

CARD Device Profile Configuration

Basic Details

Advanced Details

Name *

Me Type * **CARD**

Make * **Select the option**

Model * **Select the option**

Layout - Total Rows *

Layout - Total Columns *

Technology Capabilities * **gpox**

Close **Create**

- c. Create a PON or NNI port configuration for the card device profile. See [Creating PON and NNI Port Configuration \(on page 528\)](#).

Figure 199. PON and NNI Port

Port Detail Configuration

Name *

Description

Port Number *

Port Media * **Select the option**

Port Direction * **Select the option**

Capacity *

Capacity Type * **Select the option**

X Axis *

Y Axis *

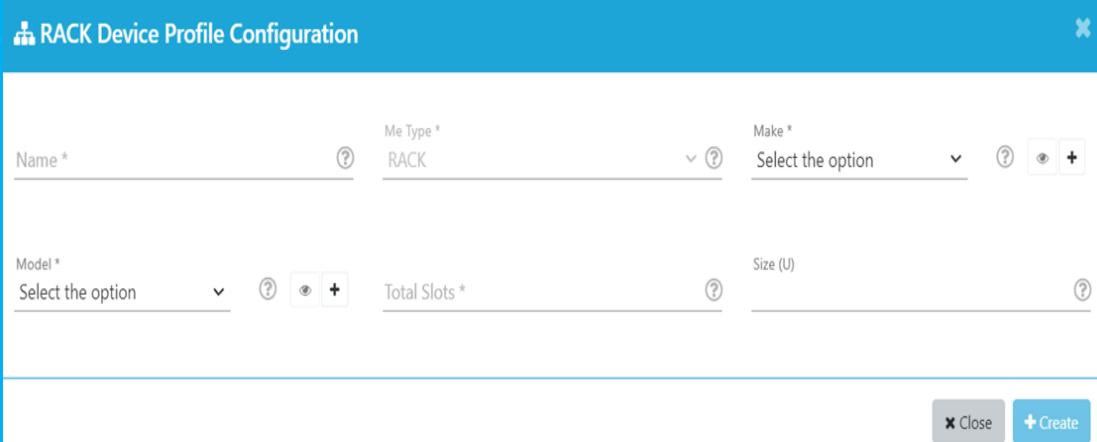
Row Number

Column Number

Alarm Profile

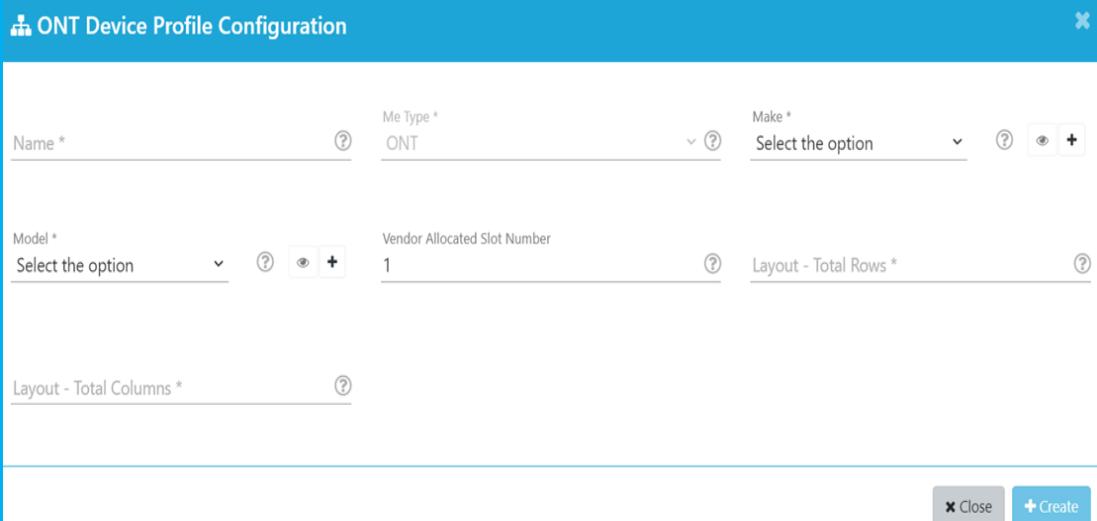
Close **Create**

- d. Create a rack device profile. See [Creating Rack Device Profile \(on page 524\)](#).

Figure 200. Rack Device Profile

The dialog box is titled "RACK Device Profile Configuration". It contains fields for "Name" (with a required asterisk), "Me Type" (set to "RACK"), "Make" (set to "Select the option"), "Model" (set to "Select the option"), "Total Slots" (with a required asterisk), and "Size (U)". At the bottom are "Close" and "Create" buttons.

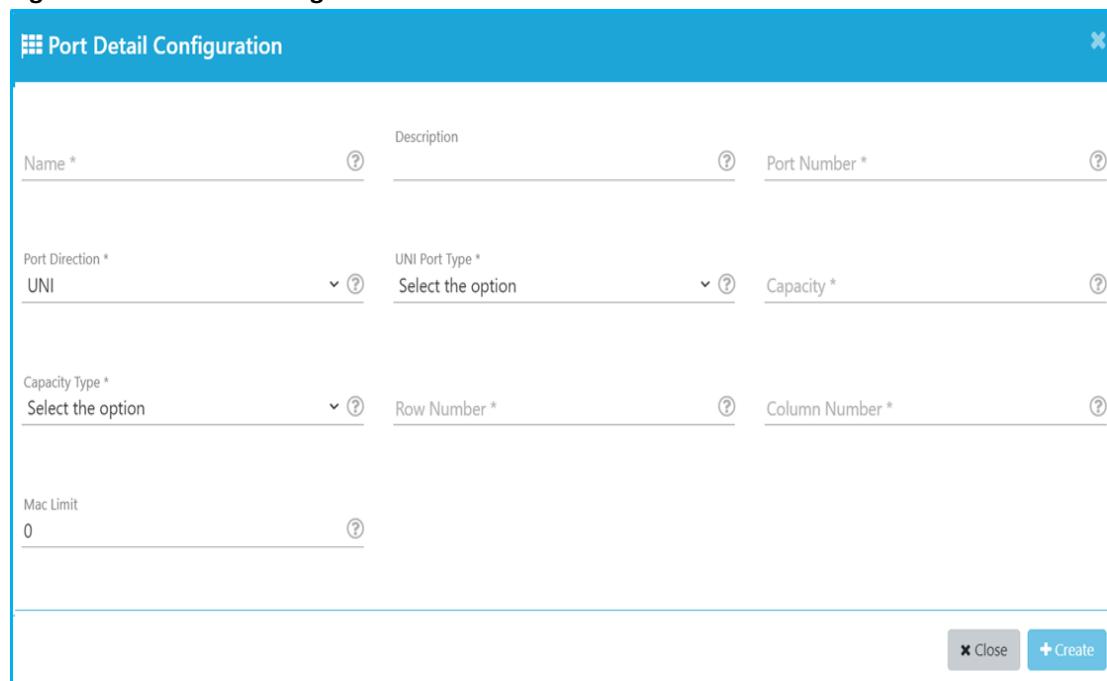
- e. Create an ONT device profile. See [Creating ONT Device Profile \(on page 515\)](#).

Figure 201. ONT Device Profile

The dialog box is titled "ONT Device Profile Configuration". It contains fields for "Name" (with a required asterisk), "Me Type" (set to "ONT"), "Make" (set to "Select the option"), "Model" (set to "Select the option"), "Vendor Allocated Slot Number" (set to "1"), "Layout - Total Rows" (with a required asterisk), and "Layout - Total Columns" (with a required asterisk). At the bottom are "Close" and "Create" buttons.

- f. Create a UNI port configuration for the ONT device profile. See [Creating UNI Port Configuration \(on page 534\)](#).

Figure 202. UNI Port Configuration



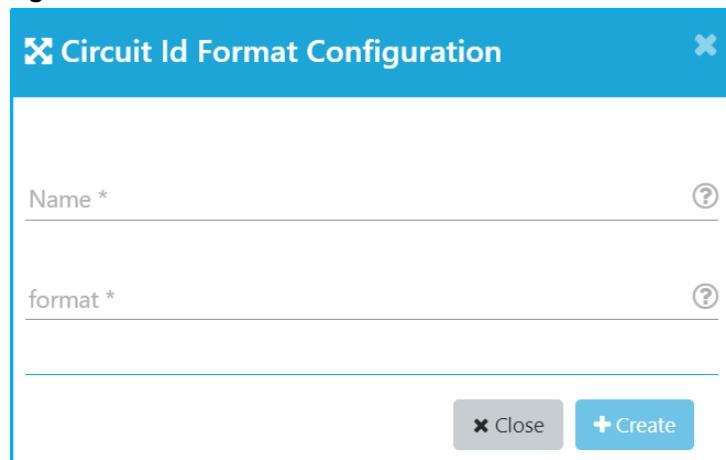
The dialog box is titled "Port Detail Configuration". It contains the following fields:

- Name *: Text input field
- Description: Text input field
- Port Number *: Text input field
- Port Direction *: Select box with "UNI" selected
- UNI Port Type *: Select box with "Select the option" selected
- Capacity *: Text input field
- Capacity Type *: Select box with "Select the option" selected
- Row Number *: Text input field
- Column Number *: Text input field
- Mac Limit: Text input field with "0" entered

At the bottom right are "Close" and "Create" buttons.

4. Create a circuit id format. See [Creating Circuit ID Format \(on page 554\)](#).

Figure 203. Circuit ID Format



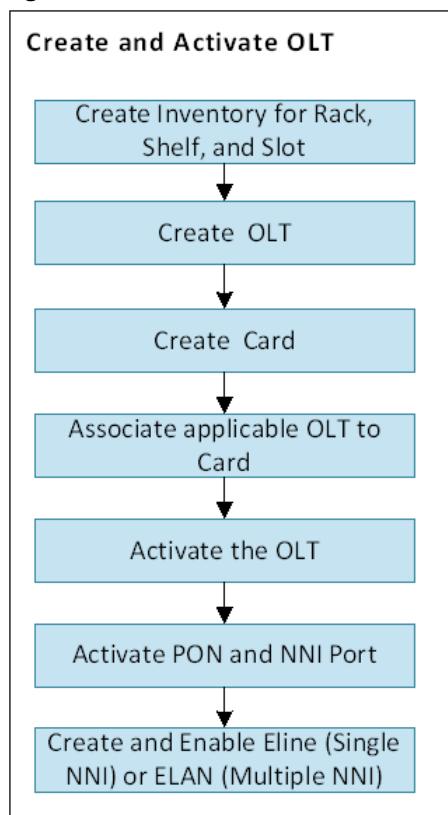
The dialog box is titled "Circuit Id Format Configuration". It contains the following fields:

- Name *: Text input field
- format *: Text input field

At the bottom right are "Close" and "Create" buttons.

OLT Activation Workflow

The following diagram illustrates the workflow for creating and activating the OLT.

Figure 204. OLT Activation Workflow

Perform the following steps to create and activate the OLT.

1. Create an inventory for Rack, Shelf, and Slot. See [Creating Rack Configuration \(on page 446\)](#).

Figure 205. Rack Configuration

The screenshot shows the 'RACK Configuration' dialog box. It has a blue header bar with the title. The main area contains several input fields and dropdown menus. Top row: 'Name *' (text input), 'Make *' (dropdown), 'Model *' (dropdown). Second row: 'Device Profile *' (dropdown), 'Display Id *' (text input), 'Serial No. *' (text input). Third row: 'Site' (dropdown), 'Enter Site...', 'Resource State' (dropdown), 'Holder State' (dropdown). Bottom row: 'Planned Type' (text input), 'Alias' (text input), 'RACK Number *' (text input). At the bottom right are 'Close' and 'Create' buttons.

2. Create an OLT. See [Creating OLT Configuration \(on page 318\)](#).

Figure 206. OLT Configuration

The OLT Configuration dialog box is divided into two main sections: Basic Details and Advanced Details.

Basic Details:

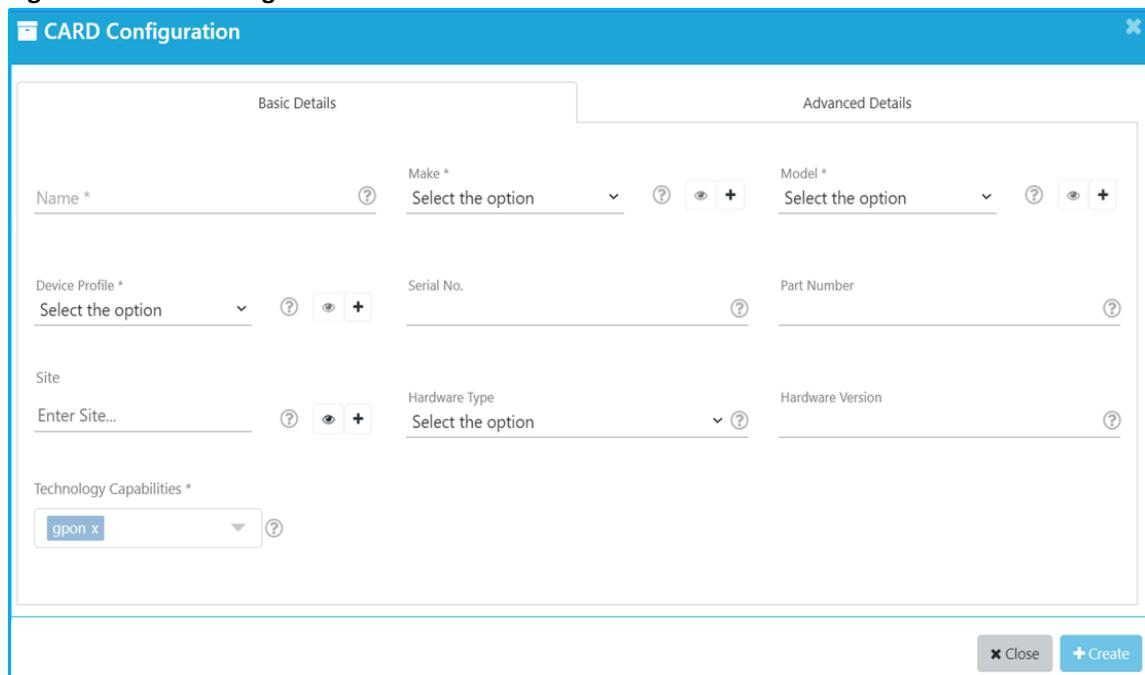
- Management Domain *: Select the option (dropdown with a question mark icon)
- Name *: Text input field (dropdown with a question mark icon)
- Model *: Select the option (dropdown with a question mark icon)
- Device Profile *: Select the option (dropdown with a question mark icon)
- Display Id *: Text input field (dropdown with a question mark icon)
- Serial No. *: Text input field (dropdown with a question mark icon)
- Controller *: Select (dropdown with a question mark icon)
- Management IP *: Text input field (dropdown with a question mark icon)
- HOTO Status *: Non HOTO (dropdown with a question mark icon)
- Site: Select (dropdown with a question mark icon)
- Management VLAN Id *: Text input field (dropdown with a question mark icon)
- Enable PM Collection Policy: (checkbox with a question mark icon)
- External Alarm VLAN Id: Text input field (dropdown with a question mark icon)
- Force Delete: FALSE (dropdown with a question mark icon)
- Service MAC Limit: Text input field (dropdown with a question mark icon)
- Enterprise Number: 4337 (text input field)
- Auto Activate: (checkbox with a question mark icon)

Advanced Details:

Buttons at the bottom right:

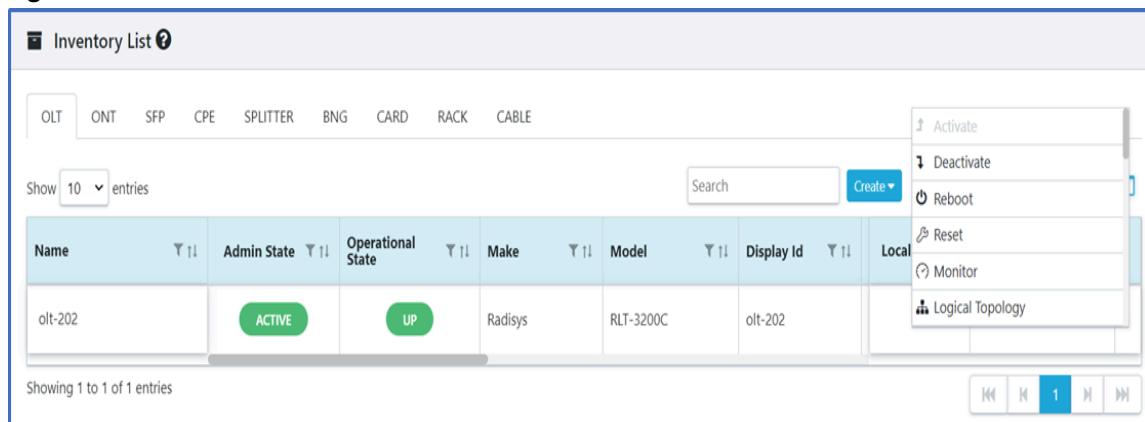
- (grey button)
- (blue button)

3. Create a card. See [Creating Card Configuration \(on page 444\)](#).

Figure 207. Card Configuration

| | | |
|---------------------------|-------------------|-------------------|
| Name * | Make * | Model * |
| Select the option | Select the option | Select the option |
| Device Profile * | Serial No. | Part Number |
| Select the option | | |
| Site | Hardware Type | Hardware Version |
| Enter Site... | Select the option | |
| Technology Capabilities * | | |
| gpon x | | |

4. Associate the applicable OLT to the CARD. See [Creating Card Configuration \(on page 444\)](#).
5. Activate the OLT. See [Activating and Deactivating the OLT \(on page 324\)](#).

Figure 208. Activate OLT

| OLT | ONT | SFP | CPE | SPLITTER | BNG | CARD | RACK | CABLE |
|---------|--------|-----|---------|-----------|---------|------|------|-------|
| olt-202 | ACTIVE | UP | Radisys | RLT-3200C | olt-202 | | | |

6. Activate the PON and NNI port. See [Activating the PON and NNI Port \(on page 380\)](#).

Figure 209. Activate PON and NNI Port

| Ports List [Inventory - olt-202] | | | | | | |
|--|-----------------------|----------------------|----------|--------------------------------------|---|---|
| Show 10 entries <input type="button" value="▼"/> <input type="button" value="▲"/> <input type="button" value="Search"/> <input type="button" value="Export"/> <input type="button" value="Print"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/> | | | | | | |
| Name | Admin State | Operational State | Media | Display Id | Action | |
| SFPON-3 | DEACTIVE | UNKNOWN | PON | /rack=1/shelf=1/slot=LT-1/port=SFP1 | <input type="button" value="Activate"/> <input type="button" value="Deactivate"/> <input type="button" value="Logical Topology"/> <input type="button" value="Physical Link"/> <input type="button" value="Enable ONT Serial Number"/> <input type="button" value="Monitor"/> | <input type="button" value="Edit"/> <input type="button" value="More"/> |
| SFPON-2 | ACTIVE | DOWN | PON | /rack=1/shelf=1/slot=LT-1/port=SFP2 | | <input type="button" value="Edit"/> <input type="button" value="More"/> |
| SFPON-1 | DEACTIVE | UNKNOWN | PON | /rack=1/shelf=1/slot=LT-1/port=SFP1 | | <input type="button" value="Edit"/> <input type="button" value="More"/> |
| NNI-8 | ACTIVE | DOWN | ETHERNET | /rack=1/shelf=1/slot=LT-1/port=NNI-8 | | <input type="button" value="Edit"/> <input type="button" value="More"/> |
| NNI-7 | ACTIVE | DOWN | ETHERNET | /rack=1/shelf=1/slot=LT-1/port=NNI-7 | | <input type="button" value="Edit"/> <input type="button" value="More"/> |
| NNI-6 | ACTIVE | DOWN | ETHERNET | /rack=1/shelf=1/slot=LT-1/port=NNI-6 | | <input type="button" value="Edit"/> <input type="button" value="More"/> |
| NNI-5 | ACTIVE | DOWN | ETHERNET | /rack=1/shelf=1/slot=LT-1/port=NNI-5 | | <input type="button" value="Edit"/> <input type="button" value="More"/> |

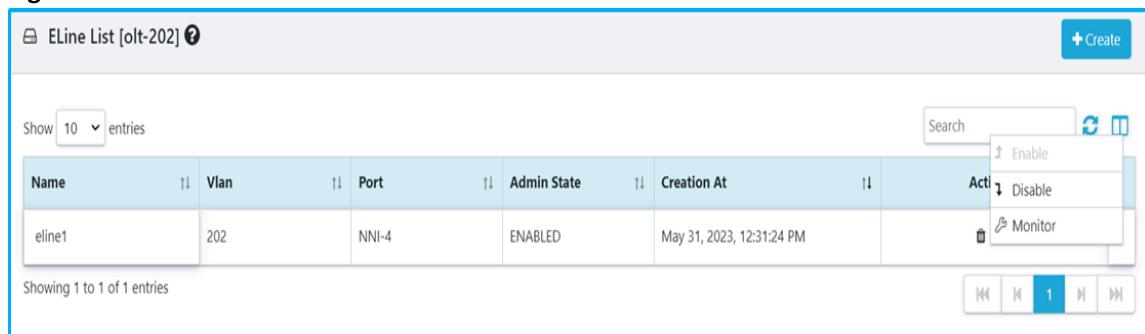
7. Create a ELine if a single NNI port needs to be a part of the VLAN. See [Creating ELine Configuration \(on page 332\)](#).

Figure 210. ELine Configuration

ELine Configuration

| | | |
|--|----------------------------------|----------------------------------|
| Name * | <input type="text"/> | <input type="button" value="?"/> |
| Vlan Id * | <input type="text"/> | <input type="button" value="?"/> |
| Port * | <input type="text"/> | <input type="button" value="?"/> |
| NNI-2 | <input type="button" value="X"/> | |
| <input type="button" value="Close"/> <input type="button" value="Create"/> | | |

8. Enable ELine. See [Enabling and Disabling ELine Configuration \(on page 333\)](#).

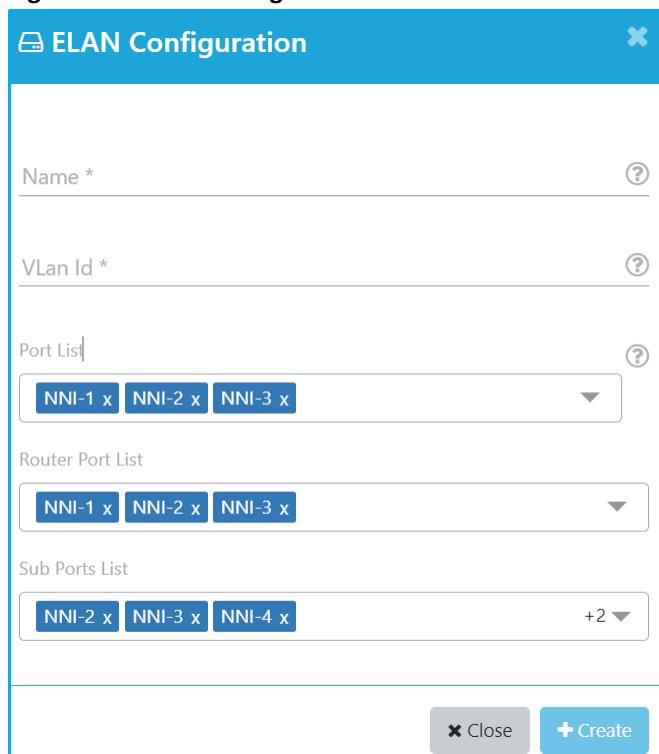
Figure 211. Enable ELine


The screenshot shows a table titled "ELine List [olt-202]". The table has columns: Name, Vlan, Port, Admin State, Creation At, and Action. There is one entry: Name is "eline1", Vlan is "202", Port is "NNI-4", Admin State is "ENABLED", Creation At is "May 31, 2023, 12:31:24 PM", and Action has options: Enable, Disable, and Monitor. The table shows 10 entries.

| Name | Vlan | Port | Admin State | Creation At | Action |
|--------|------|-------|-------------|---------------------------|--|
| eline1 | 202 | NNI-4 | ENABLED | May 31, 2023, 12:31:24 PM | Enable Disable Monitor |

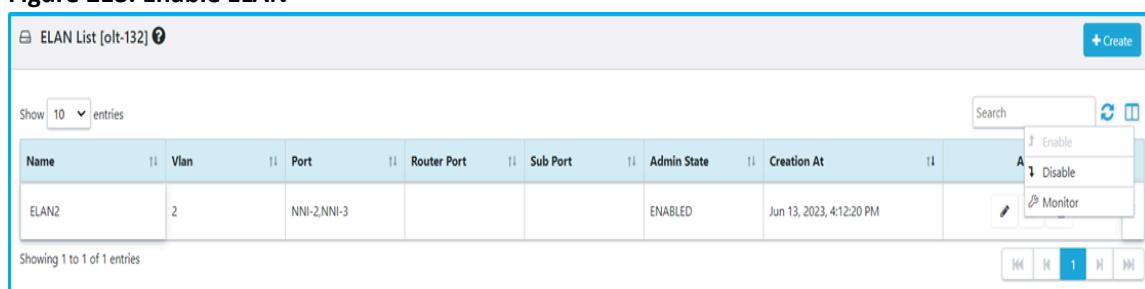
Showing 1 to 1 of 1 entries

9. Create a ELAN configuration if multiple NNI port need to be a part of the VLAN. See [Creating ELAN Configuration \(on page 335\)](#).

Figure 212. ELAN Configuration


The screenshot shows the "ELAN Configuration" dialog box. It has fields for "Name" (with a required asterisk), "VLAN Id" (with a required asterisk), "Port List" (with a dropdown containing "NNI-1 x", "NNI-2 x", "NNI-3 x"), "Router Port List" (with a dropdown containing "NNI-1 x", "NNI-2 x", "NNI-3 x"), and "Sub Ports List" (with a dropdown containing "NNI-2 x", "NNI-3 x", "NNI-4 x"). At the bottom are "Close" and "Create" buttons.

10. Enable ELAN. See [Enabling and Disabling ELAN Configuration \(on page 335\)](#).

Figure 213. Enable ELAN


The screenshot shows a table titled "ELAN List [olt-132]". The table has columns: Name, Vlan, Port, Router Port, Sub Port, Admin State, Creation At, and Action. There is one entry: Name is "ELAN2", Vlan is "2", Port is "NNI-2,NNI-3", Admin State is "ENABLED", Creation At is "Jun 13, 2023, 4:12:20 PM", and Action has options: Enable, Disable, and Monitor. The table shows 10 entries.

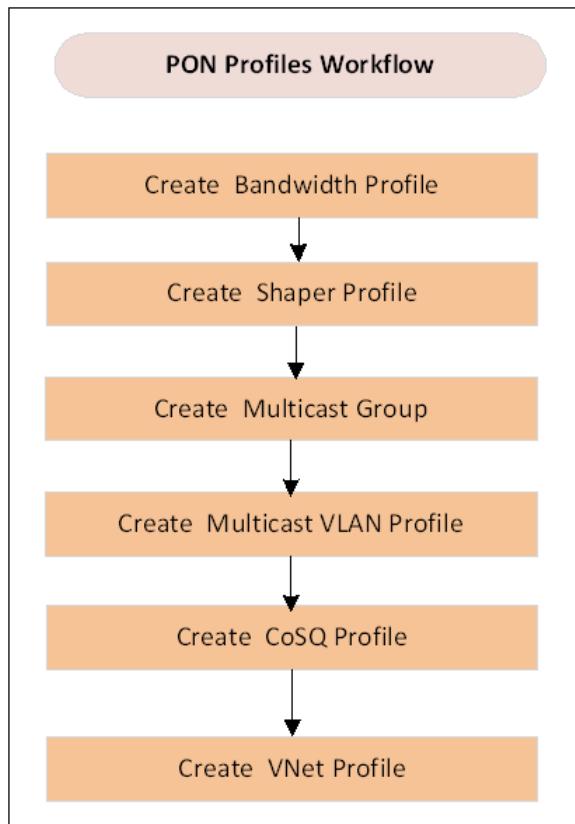
| Name | Vlan | Port | Router Port | Sub Port | Admin State | Creation At | Action |
|-------|------|-------------|-------------|----------|-------------|--------------------------|--|
| ELAN2 | 2 | NNI-2,NNI-3 | | | ENABLED | Jun 13, 2023, 4:12:20 PM | Enable Disable Monitor |

Showing 1 to 1 of 1 entries

PON Profiles Workflow

The following diagram illustrates the workflow for creating the PON profiles.

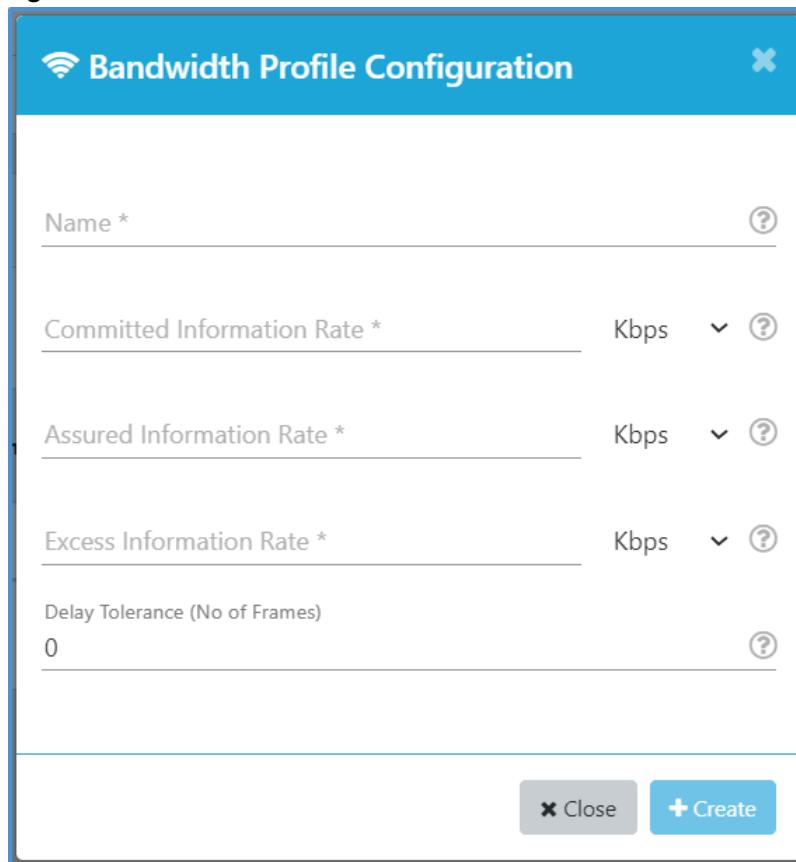
Figure 214. PON Profiles Workflow



Perform the following steps to create the PON profiles.

1. Create a bandwidth profile. See [Creating Bandwidth Profile \(on page 564\)](#).

Figure 215. Bandwidth Profile

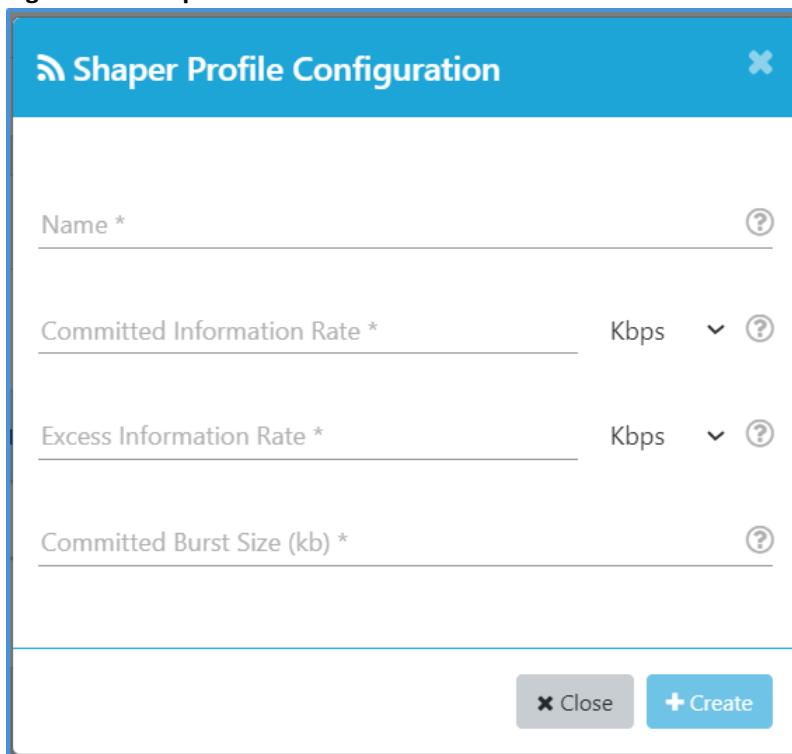


The dialog box is titled "Bandwidth Profile Configuration" and contains the following fields:

- Name ***: A text input field with a question mark icon.
- Committed Information Rate ***: A text input field with a dropdown menu set to "Kbps" and a question mark icon.
- Assured Information Rate ***: A text input field with a dropdown menu set to "Kbps" and a question mark icon.
- Excess Information Rate ***: A text input field with a dropdown menu set to "Kbps" and a question mark icon.
- Delay Tolerance (No of Frames)**: A text input field with a value of "0" and a question mark icon.

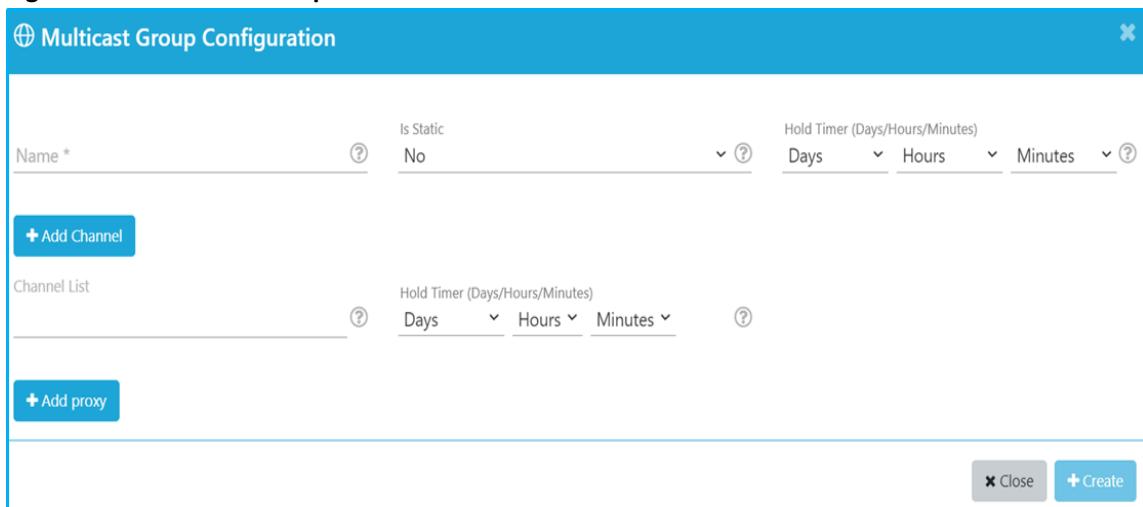
At the bottom right are two buttons: "Close" and "Create" (highlighted in blue).

2. Create a shaper profile. See [Creating Shaper Profile \(on page 567\)](#).

Figure 216. Shaper Profile

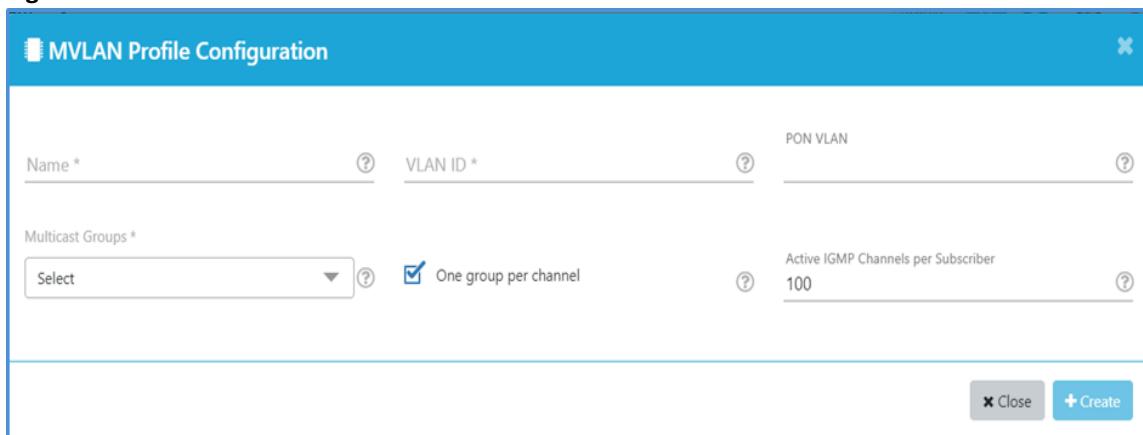
The dialog box is titled "Shaper Profile Configuration". It contains four input fields: "Name *", "Committed Information Rate *", "Excess Information Rate *", and "Committed Burst Size (kb) *". Each field has a unit of "Kbps" and a help icon. At the bottom are "Close" and "Create" buttons.

3. Create a multicast group. See [Creating Multicast Group \(on page 561\)](#).

Figure 217. Multicast Group

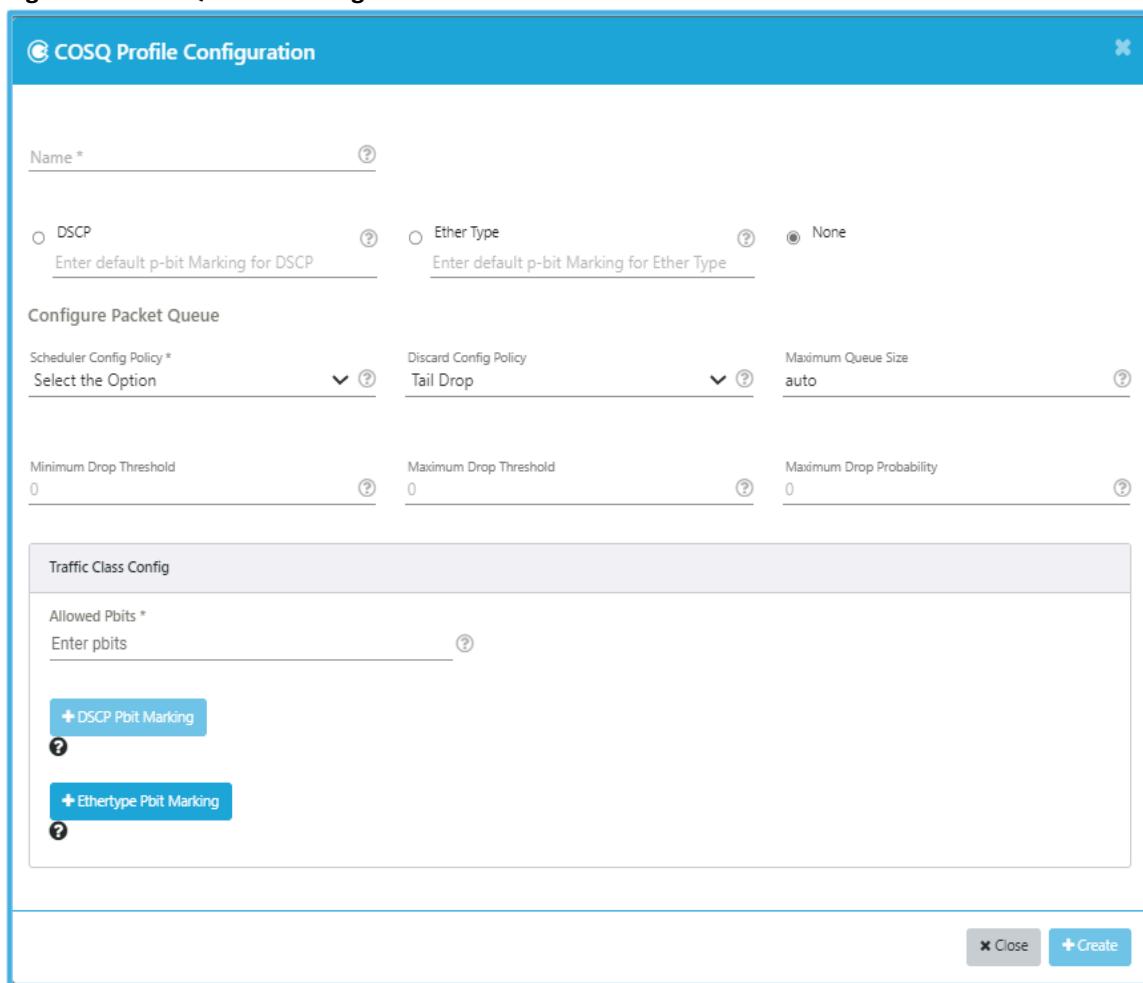
The dialog box is titled "Multicast Group Configuration". It contains fields for "Name *", "Is Static" (set to "No"), and "Hold Timer (Days/Hours/Minutes)". Below these are "Add Channel" and "Add proxy" buttons. A "Channel List" section includes a "Hold Timer (Days/Hours/Minutes)" field. At the bottom are "Close" and "Create" buttons.

4. Create a multicast VLAN (MVLAN) profile. See [Creating MVLAN Profile \(on page 568\)](#).

Figure 218. MVLAN Profile

The screenshot shows the 'MVLAN Profile Configuration' dialog box. It includes fields for 'Name *' (with a question mark icon), 'VLAN ID *' (with a question mark icon), and 'PON VLAN' (with a question mark icon). Below these are sections for 'Multicast Groups' (with a dropdown menu 'Select' and a checked checkbox 'One group per channel') and 'Active IGMP Channels per Subscriber' (set to 100). At the bottom are 'Close' and 'Create' buttons.

5. Create a Class of Service Queue (CoSQ) profile. See [Creating COSQ Profile \(on page 570\)](#).

Figure 219. CoSQ Profile Configuration

The screenshot shows the 'COSQ Profile Configuration' dialog box. It includes fields for 'Name *' (with a question mark icon), 'DSCP' (radio button), 'Ether Type' (radio button), and 'None' (radio button). Below these are sections for 'Configure Packet Queue' (Scheduler Config Policy dropdown 'Select the Option', Discard Config Policy dropdown 'Tail Drop', Maximum Queue Size dropdown 'auto'), 'Traffic Class Config' (Allowed Pbits dropdown 'Enter pbts'), and buttons for '+ DSCP Pbit Marking' and '+ Ethertype Pbit Marking'. At the bottom are 'Close' and 'Create' buttons.

6. Create a VNet profile. See [Creating VNet Profile \(on page 577\)](#).

Figure 220. VNet Profile Configuration

VNet Profile Configuration

Name *

SVLAN *

CVLAN *

Encapsulation *

ONT Ethertype Classification

MAC Learning Type *

UNI VLAN

UNI VLAN Range End

VLAN Control

Allow Transparent VLAN

CosQ Profile

SVLAN TPID

PON Hair Pinning

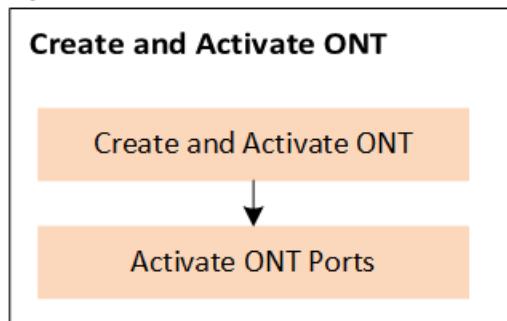
Remote Id Profile

CVLAN TPID

ONT Activation Workflow

The following diagram illustrates the workflow for creating and activating the ONT.

Figure 221. ONT Activation Workflow



Perform the following steps to create and activate the ONT.

1. Create an ONT. See [Creating ONT Configuration \(on page 427\)](#).

Figure 222. ONT Configuration

The screenshot shows the 'ONT Configuration' dialog box. It has two tabs: 'Basic Details' and 'Advanced Details'. The 'Basic Details' tab is active. It contains the following fields:

- Name ***: A text input field with a question mark icon.
- Make**: A dropdown menu with 'Select the option' and a question mark icon. To its right are three buttons: a minus sign, a plus sign, and a refresh icon.
- Model**: A dropdown menu with 'Select the option' and a question mark icon. To its right are three buttons: a minus sign, a plus sign, and a refresh icon.
- Device Profile**: A dropdown menu with 'Select the option' and a question mark icon. To its right are three buttons: a minus sign, a plus sign, and a refresh icon.
- OLT**: A dropdown menu with 'Select' and a question mark icon.
- Port**: A dropdown menu with 'Select' and a question mark icon.
- Active Firmware Version**: A text input field with a question mark icon.
- Serial No. ***: A text input field with a question mark icon.
- Registration Id ***: A text input field with a question mark icon.
- ONT Number**: A dropdown menu with 'Select' and a question mark icon.
- Enable Time of Day**: A dropdown menu with 'Select the option' and a question mark icon.
- Upstream FEC**: A dropdown menu with 'ENABLED' and a question mark icon.
- Connectivity Mode**: A dropdown menu with '1:MP map-filtering' and a question mark icon.
- Force Delete**: A dropdown menu with 'FALSE' and a question mark icon.
- MAC Limit**: A text input field with '0' and a question mark icon.
- MAC Ageing Time**: A text input field with '0' and a question mark icon.
- Auto Upgrade**: A dropdown menu with a question mark icon.
- Planned Firmware version**: A text input field with a question mark icon.
- DBA Type**: A dropdown menu with 'NSR' and a question mark icon.
- Auto Activate**: A checkbox.

At the bottom right are 'Close' and 'Create' buttons.

2. Activate the ONT. See [Activating the ONT \(on page 431\)](#).

Figure 223. Activate ONT

The screenshot shows the 'Inventory List' interface. The top navigation bar has tabs: OLT, ONT, SFP, CPE, SPLITTER, BNG, CARD, RACK, and CABLE. The 'ONT' tab is selected. Below the tabs, there is a search bar and a dropdown for 'Show 10 entries'. The main table has the following columns: Name, Admin State, Operational State, Make, Model, Technology, and a Actions column. The table shows one entry:

| Name | Admin State | Operational State | Make | Model | Technology | Actions |
|---------|-------------|-------------------|---------|-------|------------|---|
| ont-202 | ACTIVE | UP | Radisys | xgspn | | <ul style="list-style-type: none">ActivateDeactivateRebootUpload ZtpMonitorLogical Topology T-28/remote_unit=1 |

At the bottom, it says 'Showing 1 to 1 of 1 entries' and there are navigation buttons.

3. Activate ONT ports and ensure that the operational status of the port must be **UP**. See [Activating the UNI Port \(on page 436\)](#).

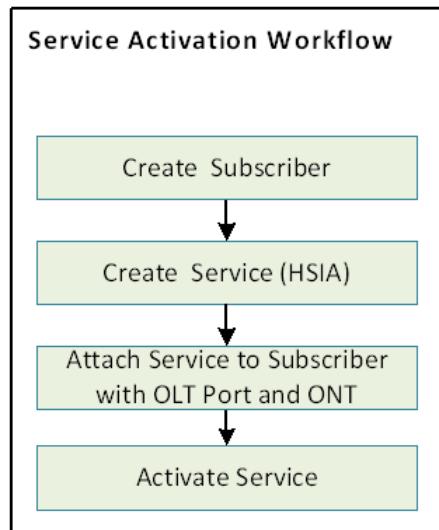
Figure 224. Activate ONT Ports

| Ports List [Inventory - ont-202] | | | | | | | |
|------------------------------------|-------------|-------------------|--|---------|---|---|--|
| Show 10 entries | | Search | | Export | | | |
| Name | Admin State | Operational State | Display Id | Port No | Action | | |
| ont-202-PPTP-ETHERNET-6 | DEACTIVE | UNKNOWN | /rack=1/shelf=1/slot=LT-1/port=SFPON-28/remote_unit=1/port=6 | 6 |   |  | |
| ont-202-PPTP-ETHERNET-5 | DEACTIVE | UNKNOWN | /rack=1/shelf=1/slot=LT-1/port=SFPON-28/remote_unit=1/port=5 | 5 |   |  | |
| ont-202-PPTP-ETHERNET-4 | DEACTIVE | UNKNOWN | /rack=1/shelf=1/slot=LT-1/port=SFPON-28/remote_unit=1/port=4 | 4 |   |  | |
| ont-202-PPTP-ETHERNET-3 | DEACTIVE | UNKNOWN | /rack=1/shelf=1/slot=LT-1/port=SFPON-28/remote_unit=1/port=3 | 3 |   |  | |
| ont-202-PPTP-ETHERNET-2 | ACTIVE | UP | /rack=1/shelf=1/slot=LT-1/port=SFPON-28/remote_unit=1/port=2 | 2 |   |  | |
| ont-202-PPTP-ETHERNET-1 | DEACTIVE | UNKNOWN | /rack=1/shelf=1/slot=LT-1/port=SFPON-28/remote_unit=1/port=1 | 1 |   |  | |

Service Activation Workflow

The following diagram illustrates the workflow for creating, activating, subscriber, and services.

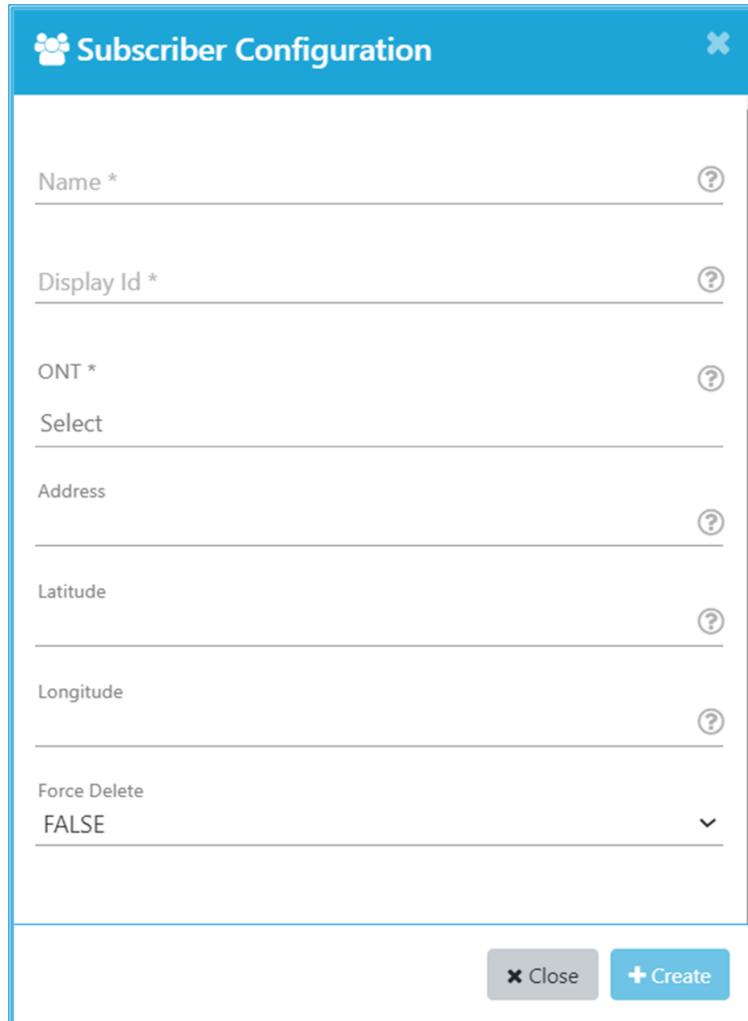
Figure 225. Service Activation Workflow



Perform the following steps to create, activate, subscriber and services.

1. Create a subscriber. See [Creating Subscriber \(on page 455\)](#).

Figure 226. Subscriber Configuration



The image shows a 'Subscriber Configuration' dialog box with a blue header and a white body. The header contains the title 'Subscriber Configuration' and a close button (X). The body contains the following fields:

- Name *: Text input field with a question mark icon.
- Display Id *: Text input field with a question mark icon.
- ONT *: Text input field with a question mark icon.
- Select: Text input field with a question mark icon.
- Address: Text input field with a question mark icon.
- Latitude: Text input field with a question mark icon.
- Longitude: Text input field with a question mark icon.
- Force Delete: A dropdown menu currently showing 'FALSE'.

At the bottom right are two buttons: 'Close' (gray) and 'Create' (blue).

2. Create a service. See [Creating Service \(on page 459\)](#).

Figure 227. Service Configuration

The screenshot shows the 'Service Configuration' dialog box. At the top, there are fields for 'ID' (5103be50-ff80-11ed-8033-1e5143e5279f-3-service), 'Name' (ser-202), and 'Aggregate Upstream Bandwidth Profile' (Select the option). Below these are fields for 'Aggregate Downstream Shaper Profile' (Select the option), 'Service Queue Stats' (DISABLE), and 'Force Delete' (FALSE). The main area contains a list of services: '1. service - ser-202'. Below the list are fields for 'Service Name' (ser-202), 'Uni Port Id' (ont-202-PPTP-ETHERNET-2), and 'Uni Port' (OR). There are also fields for 'Uni Port Type' (PPTP-ETHERNET), 'CPE MAC', and 'AES Encryption' (True). At the bottom right are 'Close' and 'Save' buttons.

3. Activate the service for the subscriber. See [Activating and Deactivating the Service for the Subscriber \(on page 467\)](#).

Verification

Verify that the service is activated for the subscriber.

1. Navigate to **Configuration > Subscriber > Service or Monitor > Services > Subscriber Service**.
 2. Verify the admin and operational state of the service.
- The **Operational State** for the service must be **UP**, indicating that the HSIA service is up and running for the subscriber, and the **Admin State** of the service must be **ACTIVE** indicating that the service is activated for the subscriber.

Figure 228. Subscriber Service Status

The screenshot shows the 'Service List [Subscriber - sub1]' table. The table has columns: Name, Admin State, Operational State, Creation Time, and Action. There is one entry: 'ser-202' with 'ACTIVE' Admin State, 'UP' Operational State, and 'May 31, 2023, 12:31:04 PM' Creation Time. The Action column contains icons for edit, delete, and more. At the bottom, it says 'Showing 1 to 1 of 1 entries'.

3. Navigate to **Monitor > Events**.
4. Verify the SERVICE-UP event is reported in RMS to confirm the service activation for the subscriber is successful, or the service status is UP.

Related information

[Workflow for Activating a Service for the Subscriber \(on page 36\)](#)

Example: Configuring Voice Service for Subscriber

This example shows how to configure and activate voice services for the subscriber.

- [Overview \(on page 830\)](#)
- [Voice Service Activation Workflow \(on page 830\)](#)
- [Verification \(on page 836\)](#)

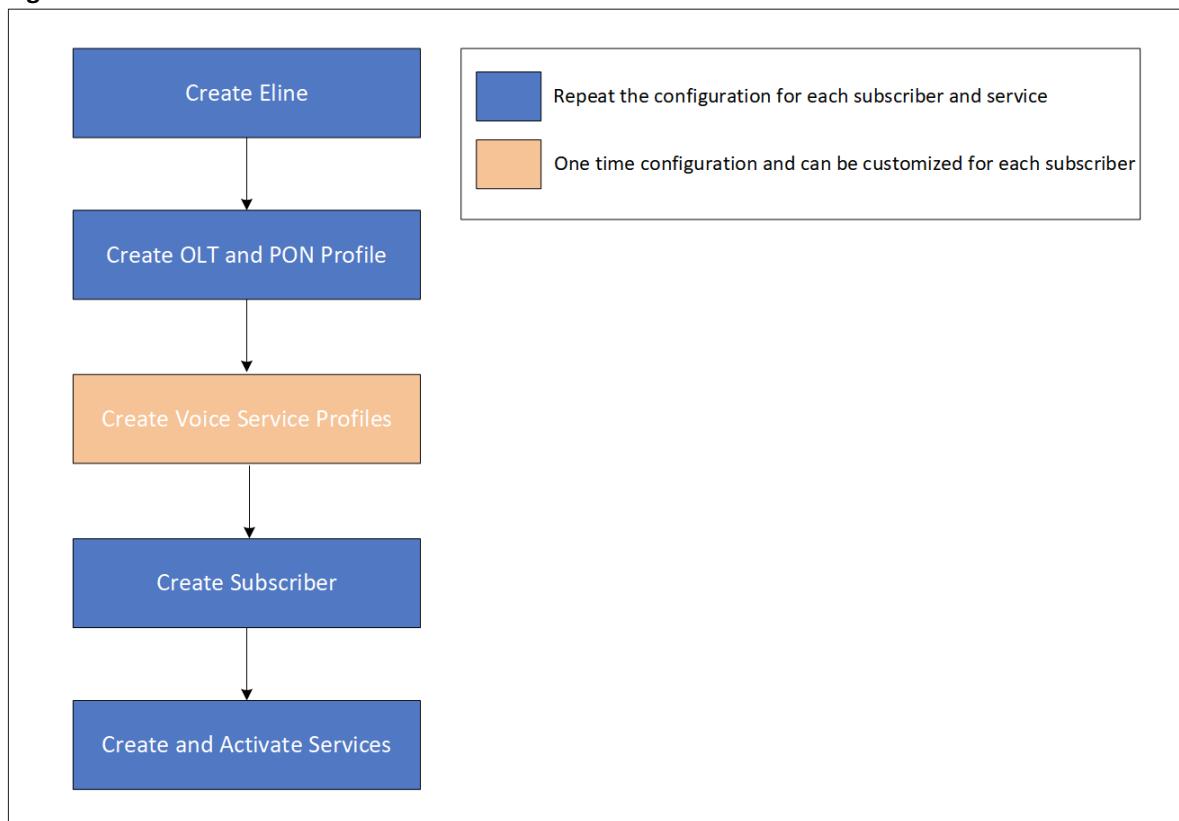
Overview

The voice service configuration refers to the process of setting up and customizing the parameters and settings for voice-based applications or services. This includes configuring dial plan support, dual tone multi-frequency, caller ID, call waiting and indication, call hold, three way call, call forwarding, call transfer, interactive voice response, and voice mail.

Voice Service Activation Workflow

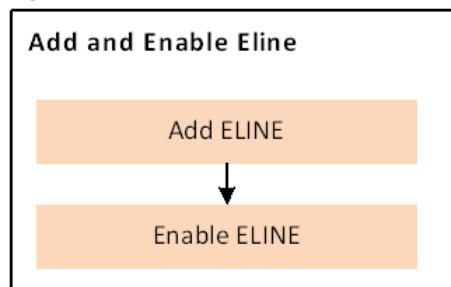
Perform the following steps to create and activate the voice service.

1. Create Eline. See [Creating Eline \(on page 831\)](#).
2. Create OLT and PON Profile. See [Creating OLT and PON Profile \(on page 832\)](#).
3. Create Voice Service Profile. See [Creating Voice Service Profile \(on page 833\)](#).

Figure 229. Voice Activation Workflow

Creating Eline

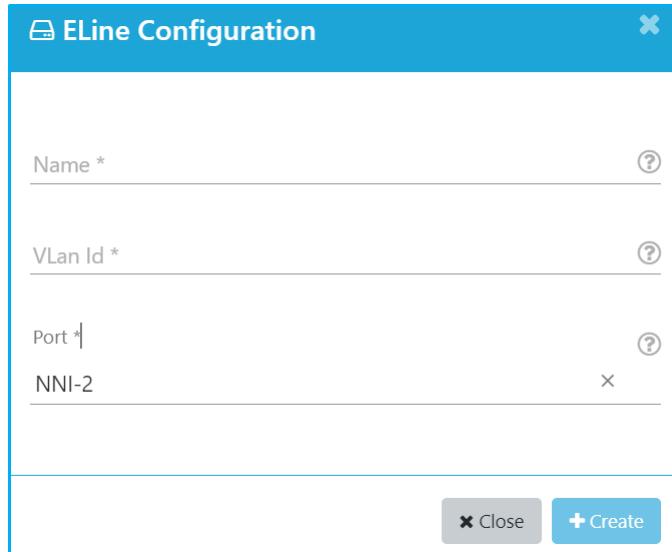
The following diagram illustrates the workflow for adding and enabling eline.

Figure 230. Eline Activation Workflow

Perform the following steps to add and enable the eline.

1. Create a ELine. See [Creating ELine Configuration \(on page 332\)](#).

Figure 231. ELine Configuration



ELine Configuration

Name *

VLAN Id *

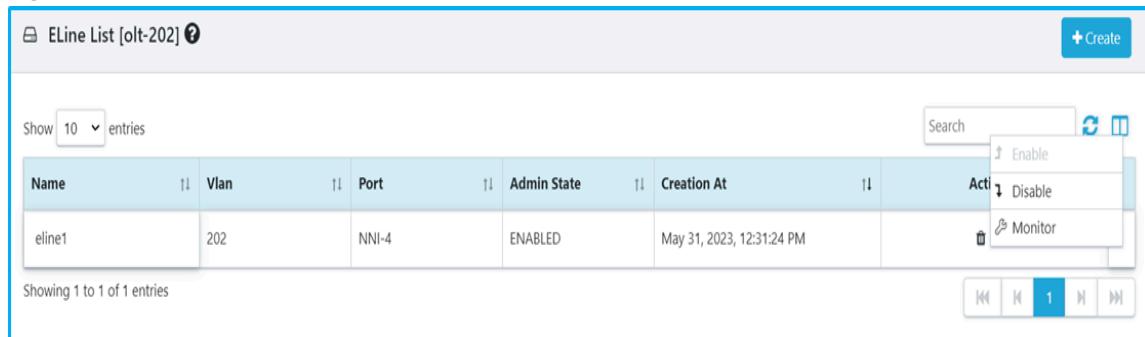
Port *

NNI-2

Close Create

2. Enable ELine. See [Enabling and Disabling ELine Configuration \(on page 333\)](#).

Figure 232. Enable ELine



ELine List [olt-202]

Show 10 entries

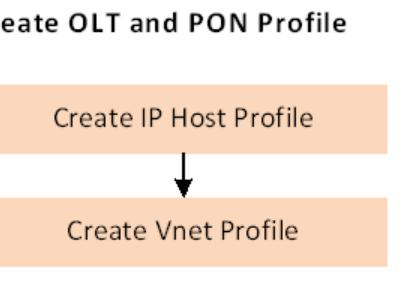
| Name | Vlan | Port | Admin State | Creation At | Actions |
|--------|------|-------|-------------|---------------------------|---|
| eline1 | 202 | NNI-4 | ENABLED | May 31, 2023, 12:31:24 PM | Enable Disable Monitor |

Showing 1 to 1 of 1 entries

Creating OLT and PON Profile

The following diagram illustrates the workflow for adding OLT and PON profile.

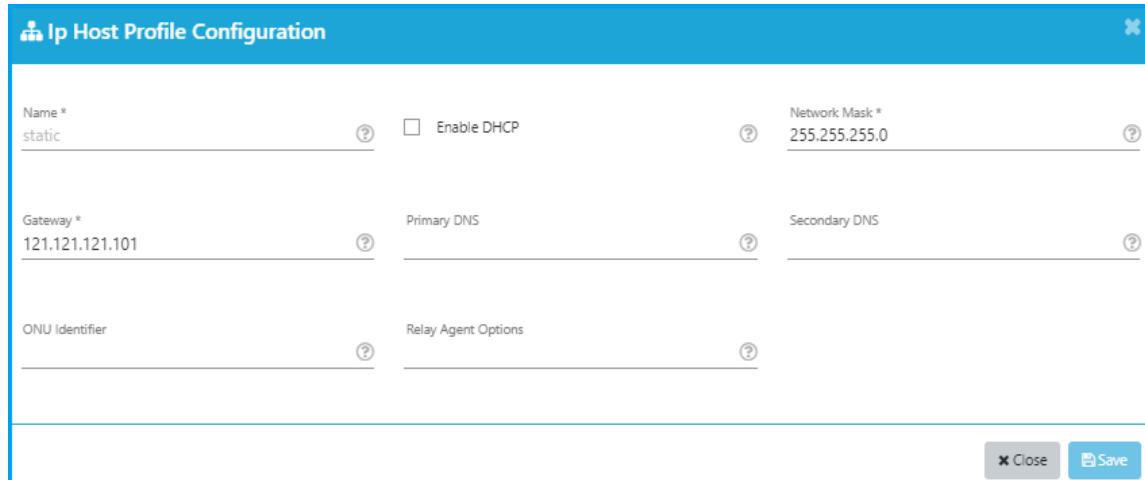
Figure 233. OLT and PON Profile



Perform the following steps to create OLT and PON profile.

1. Create an IP host profile. See [Creating IP Host Profile \(on page 549\)](#).

Figure 234. IP Host Profile



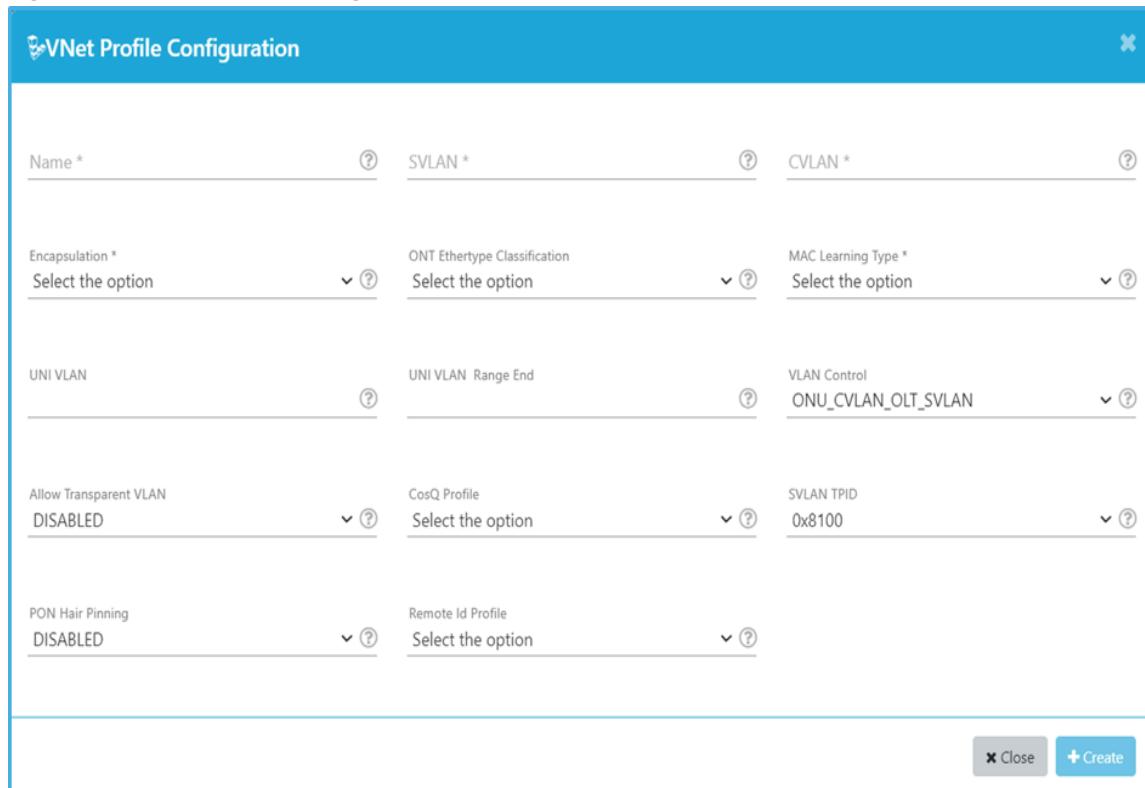
The dialog box is titled "Ip Host Profile Configuration". It contains the following fields:

- Name *: static
- Enable DHCP:
- Network Mask *: 255.255.255.0
- Gateway *: 121.121.121.101
- Primary DNS:
- Secondary DNS:
- ONU Identifier:
- Relay Agent Options:

At the bottom are "Close" and "Save" buttons.

2. Create a VNet profile. See [Creating VNet Profile \(on page 577\)](#).

Figure 235. VNet Profile Configuration



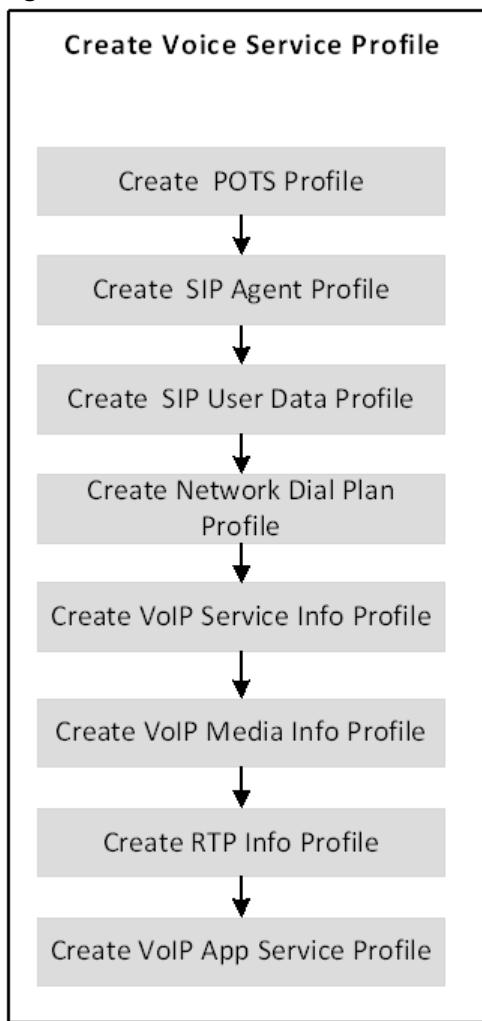
The dialog box is titled "VNet Profile Configuration". It contains the following fields:

- Name *:
- SVLAN *:
- CVLAN *:
- Encapsulation *: Select the option (dropdown)
- ONT Ethertype Classification: Select the option (dropdown)
- MAC Learning Type *: Select the option (dropdown)
- UNI VLAN:
- UNI VLAN Range End:
- VLAN Control: ONU_CVLAN_OLT_SVLAN (dropdown)
- Allow Transparent VLAN: DISABLED (dropdown)
- CosQ Profile: Select the option (dropdown)
- SVLAN TPID: 0x8100 (dropdown)
- PON Hair Pinning: DISABLED (dropdown)
- Remote Id Profile: Select the option (dropdown)

At the bottom are "Close" and "Create" buttons.

Creating Voice Service Profile

The following diagram illustrates the workflow for adding voice service profile.

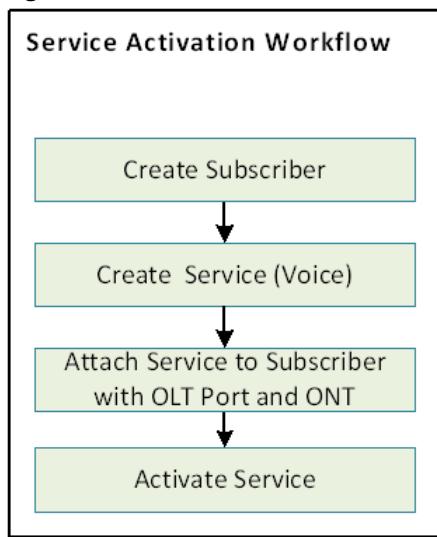
Figure 236. Voice Service Profile Workflow

Create a voice service profile. The following are the different voice service profile that can be created based on the requirement.

- Create POTS profile. See [Creating POTS Profile \(on page 589\)](#).
- Create SIP agent profile. See [Creating SIP Agent Profile \(on page 590\)](#).
- Create SIP user data profile. See [Creating SIP User Data Profile \(on page 592\)](#).
- Create network dial plan profile. See [Creating Network Dial Plan Profile \(on page 593\)](#).
- Create VoIP service info profile. See [Creating VoIP Service Info Profile \(on page 595\)](#).
- Create VoIP media info profile. See [Creating VoIP Media Info Profile \(on page 596\)](#).
- Create RTP info profile. See [Creating RTP Info Profile \(on page 598\)](#).
- Create VoIP App service profile. See [Creating VoIP Application Service Profile \(on page 600\)](#).

Creating, Activating, Subscriber and Services

The following diagram illustrates the workflow for creating, activating, subscriber, and services.

Figure 237. Service Activation Workflow

Perform the following steps to create, activate, subscriber and services.

1. Create a subscriber. See [Creating Subscriber \(on page 455\)](#).

Figure 238. Subscriber Configuration

Subscriber Configuration

| | |
|--------------------------------------|---------------------------------------|
| Name * | (?) |
| Display Id * | (?) |
| ONT * | (?) |
| Select | |
| Address | (?) |
| Latitude | (?) |
| Longitude | (?) |
| Force Delete | ▼ |
| Buttons: | |
| <input type="button" value="Close"/> | <input type="button" value="Create"/> |

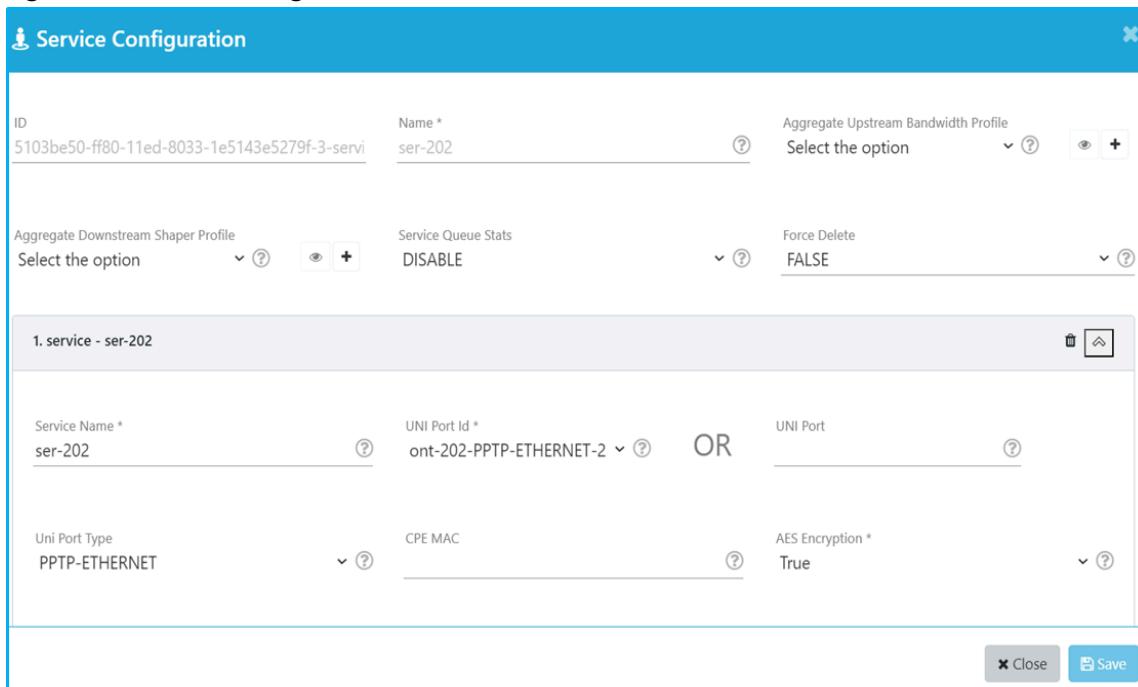
2. Create a service. See [Creating Service \(on page 459\)](#).

The following table describes the other mandatory fields and values for voice service configuration.

Table 392. Voice Service Configuration

| Field | Values |
|-------------------|---|
| AES Encryption | Select True from the list. |
| VLAN Control | Select ONU_CVLAN from the list.  Note: SVLAN and CVLAN ID must be same if you select VLAN control as ONU_CVLAN. |
| Encapsulation | Select IPoE from the list. |
| MAC Learning Type | Select ARP or Static as per the configuration in IP host profile. |

Figure 239. Service Configuration



3. Activate the service for the subscriber. See [Activating and Deactivating the Service for the Subscriber \(on page 467\)](#).

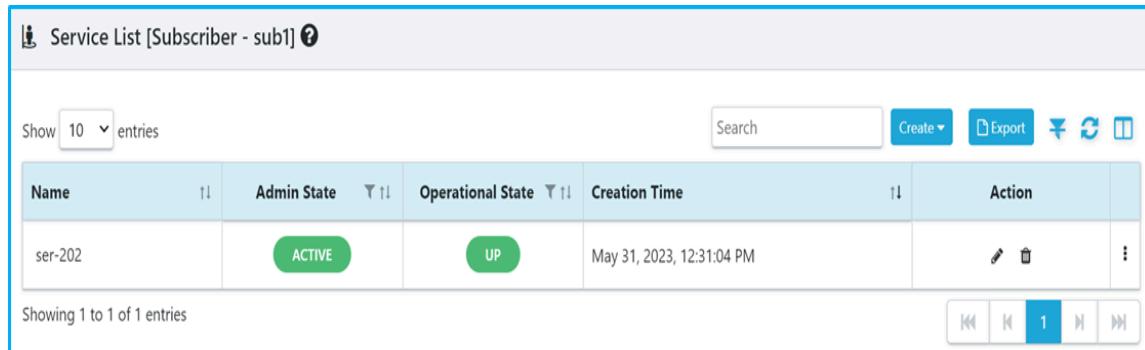
Verification

Verify that the service is activated for the subscriber.

1. Navigate to **Configuration > Subscriber > Service or Monitor > Services > Subscriber Service**.
2. Verify the admin and operational state of the service.

The **Operational State** for the service must be **UP**, indicating that the voice service is up and running for the subscriber, and the **Admin State** of the service must be **ACTIVE** indicating that the service is activated for the subscriber.

Figure 240. Subscriber Service Status



The screenshot shows a table titled "Service List [Subscriber - sub1]". The table has columns: Name, Admin State, Operational State, Creation Time, and Action. There is one entry: "ser-202" with Admin State "ACTIVE", Operational State "UP", Creation Time "May 31, 2023, 12:31:04 PM", and Action buttons. The table shows 10 entries and is on page 1 of 1.

| Name | Admin State | Operational State | Creation Time | Action |
|---------|-------------|-------------------|---------------------------|---|
| ser-202 | ACTIVE | UP | May 31, 2023, 12:31:04 PM |    |

3. Navigate to **Monitor > Events**.
4. Verify the SERVICE-UP event is reported in RMS to confirm the service activation for the subscriber is successful, or the service status is UP.

Related information

[Workflow for Activating a Service for the Subscriber \(on page 36\)](#)

Example: Voice Service Priority for SIP and RTP Packets

This example shows how to create SIP and RTP packets remarking.

Overview

The ONT generates SIP and RTP voice packets. The ONT generates SIP messages when the user dials and RTP packets when the user starts talking.

You can configure the voice priority in the following ways.

1. The user can prioritize VoIP service over HSIA and Multicast when the main service contains HSIA, Multicast, and VoIP services.

This can be achieved by configuring a higher scheduler config priority value in the COSQ profile of the VoIP service.

2. The user can prioritize the SIP packets over the RTP packets in a VoIP service. This can be achieved by using dscp-to-pbit remaking.

The Voice service primarily carries SIP and RTP/RTCP packets. SIP packets are used for session establishment and RTP packets are media packets.

Users can remark SIP and RTP packets based on the DSCP values.



Note: Only the ONT PM4254G (Firmware 1.2.0.006 and above versions) supports the SIP packet priority over the RTP packet.

The default DSCP values for SIP and RTP packets for PM4254G ONT are given below.

- SIP value - 24
- RTP value - 46



Note:

- The user can modify the DSCP values for the SIP and RTP packets through the ONT GUI.
- If the DSCP values for the SIP and RTP packets change in GUI, the user must create a COSQ profile with the modified DSCP values for SIP and RTP packets.
- The User can configure a COSQ profile with a higher pbit marking for a DSCP value of 24 and a lower pbit marking for a DSCP value of 46.

SIP and RTP Packets Remarking Methods

There are two ways to prioritize the SIP packets over and RTP packets.

- Single sub-service
- Multiple sub-service

Single Sub-Service Configuration

A single sub-service is used to prioritize the SIP packets over RTP packets.

Scenario 1

Perform the following steps to prioritize the signaling packets over SIP packets.

1. Configure SIP and RTP remarking with non-zero pbits and other packets remark to 0.

Table 393. PBITS Remarking

| DSCP | PBITS Remarking |
|--------|-----------------|
| SIP | 2 (Non zero) |
| RTP | 1 (Non zero) |
| Others | 0 (Zero) |

2. The user can configure the COSQ profile with a non-zero pbit for DSCP values 24 for SIP packets and 46 for RTP packets.
3. Create a sub-service with a COSQ and voice service profile. See [Creating COSQ Profile \(on page 570\)](#) and [Voice Service Profiles \(on page 589\)](#).

4. Configure the **Allowed Pbits** values to 0 for others, 1 for RTP, and 2 for SIP packets.
5. Configure the values for PBIT as 2 for DSCP value 24 and PBIT as 1 for DSCP value 46.
6. In the COSQ Profile Configuration page, configure the **Default DSCP Pbit Marking** to 0. See [Creating COSQ Profile \(on page 570\)](#).

Figure 241. CoSQ Profile

Scenario 2

Perform the following steps to prioritize the SIP packets over RTP packets.

1. Configure SIP with non-zero pbits remarking, and the RTP and other packets 0.

Table 394. PBITS Remark

| DSCP | PBITS Remark |
|--------|--------------|
| SIP | 2 (Non zero) |
| Others | 0 (Zero) |

2. The user can configure the COSQ profile with a non-zero pbit for DSCP values 24 for SIP packets.
3. Create a sub-service with a COSQ and voice service profile. See [Creating COSQ Profile \(on page 570\)](#) and [Voice Service Profiles \(on page 589\)](#).

4. Configure the **Allowed Pbits** values to 0 for others, and 2 for SIP packets.
5. Configure the values for PBIT as 2 for DSCP value 24 and PBIT as 0 for DSCP value 46.
6. In the COSQ Profile Configuration page, configure the **Default DSCP Pbit Marking** to 0. See [Creating COSQ Profile \(on page 570\)](#).

Multiple Sub-Service Configuration

If the user wants the SIP and RTP packets in different queues, then the user must configure an aggregate bandwidth profile with multiple sub-services (each sub-service for SIP and RTP).

When the allocated bandwidth is less for voice service, it is recommended to use multiple queues for SIP and RTP packets. The SIP packet queue is processed and the RTP queue drops during bandwidth congestion.

This can be achieved by creating two or three sub-services.

- If the user wants SIP packets to be a non-zero value and other packets remarking to 0. Create 2 sub-services (The first sub-service carries other packets, and the second sub-service will carry SIP packets)
- Create 3 sub-services (The first sub-service carries other packets, the second sub-service carries RTP packets, and the third sub-service carries SIP packets)

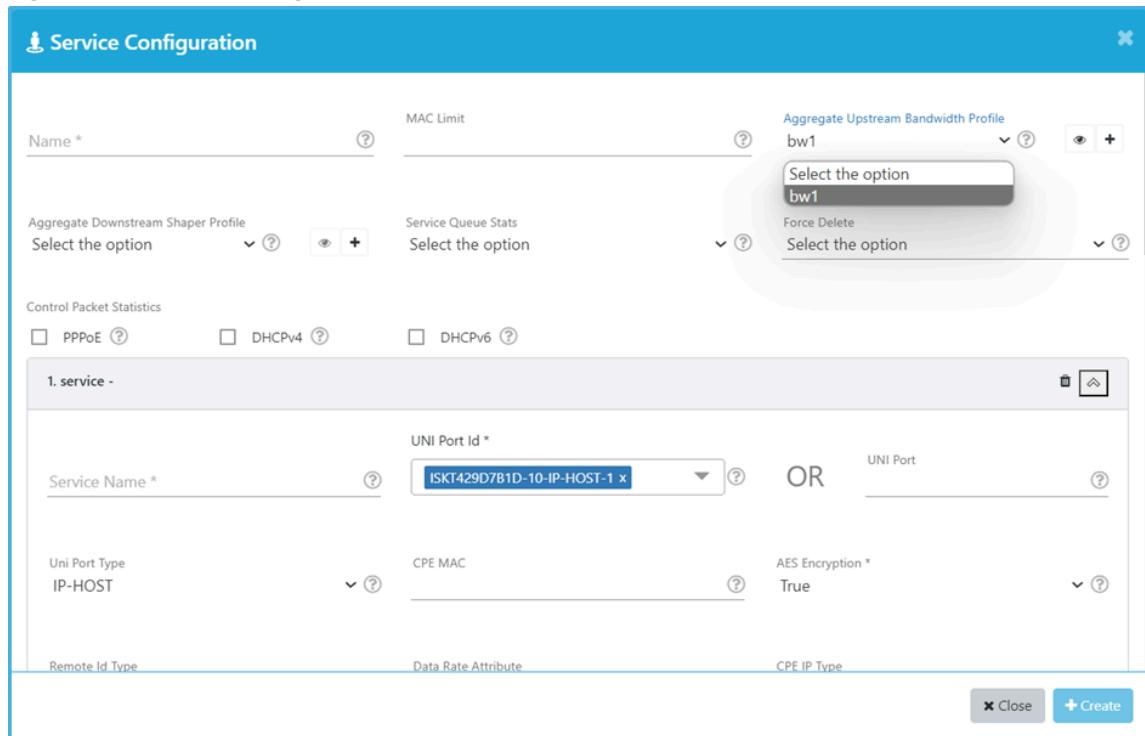


Note: Multiple sub-service model is useful when type-4 tcont is used for voice service.

Perform the following steps to configure the COSQ profile with an aggregate bandwidth, SIP profile, and RTP profile.

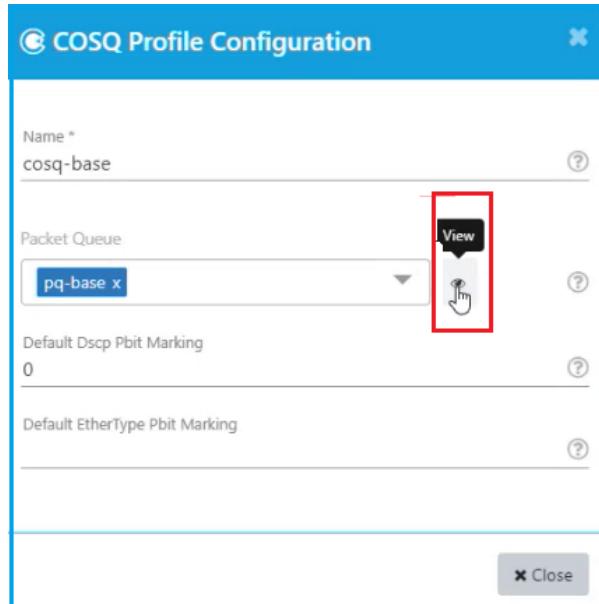
1. Select a default- COSQ profile with an aggregate bandwidth profile in the service configuration page. See [Creating COSQ Profile \(on page 570\)](#).

Figure 242. Service Configuration

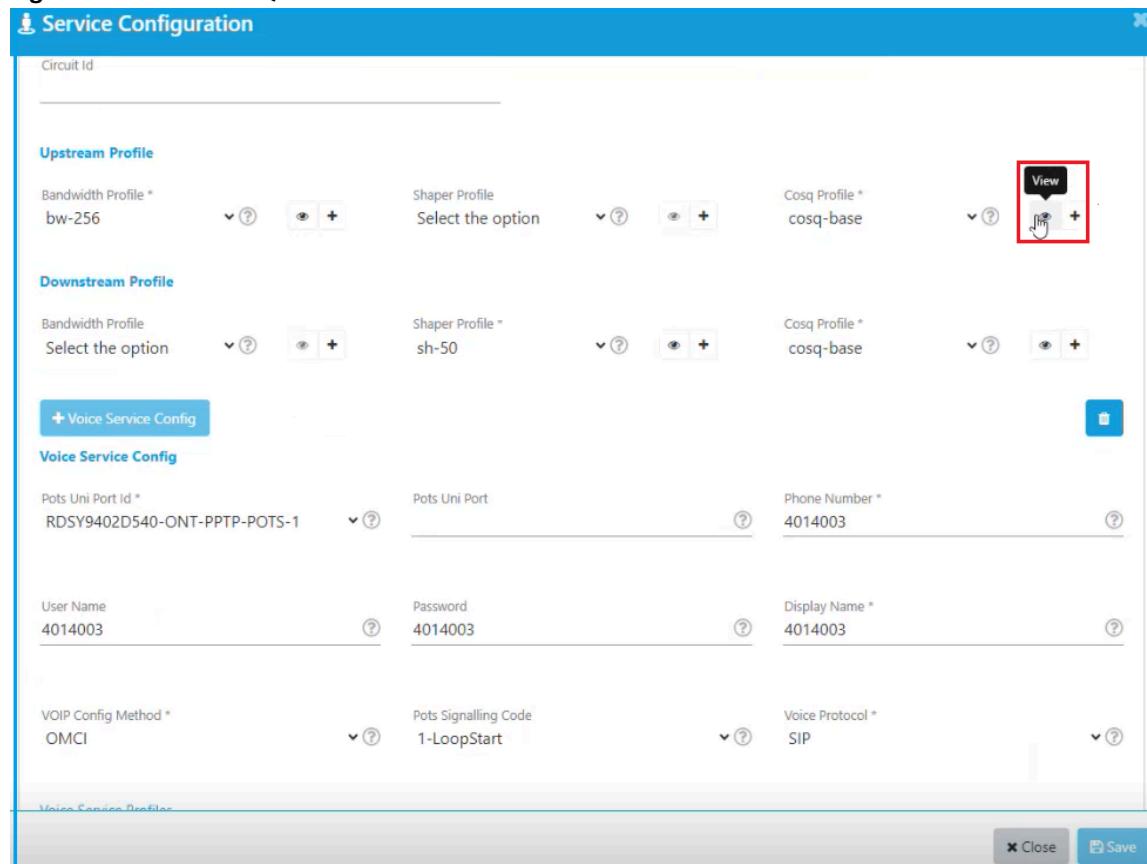


2. Click on the eye icon to view the packet queue and check the DSCP Pbit Marking. See [Creating COSQ Profile \(on page 570\)](#).

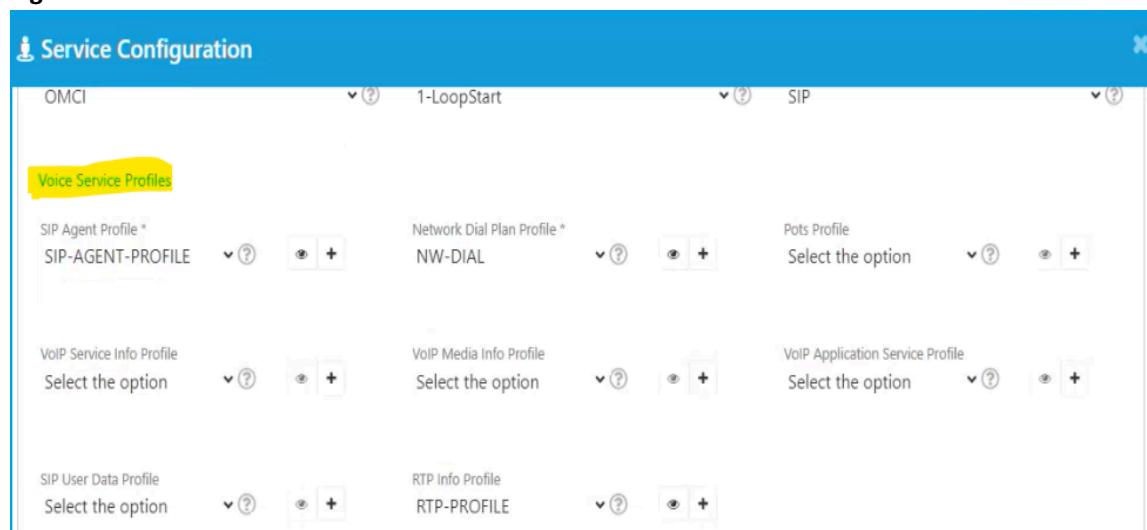
Figure 243. Viewing COSQ Profile



3. In the Service Configuration page, click the eye icon to view the COSQ profile.

Figure 244. View COSQ Profile

- Configure the Allowed Pbits to 0, DSCP value to 0-10, and PBIT to 0.
- Select Ethertype ARP as 0 from the list, configure the default PBIT to 0, and scheduler config priority to 0.
- Select the voice service profile in the service configuration page. See [Voice Service Profiles \(on page 589\)](#).

Figure 245. Voice Service Profile

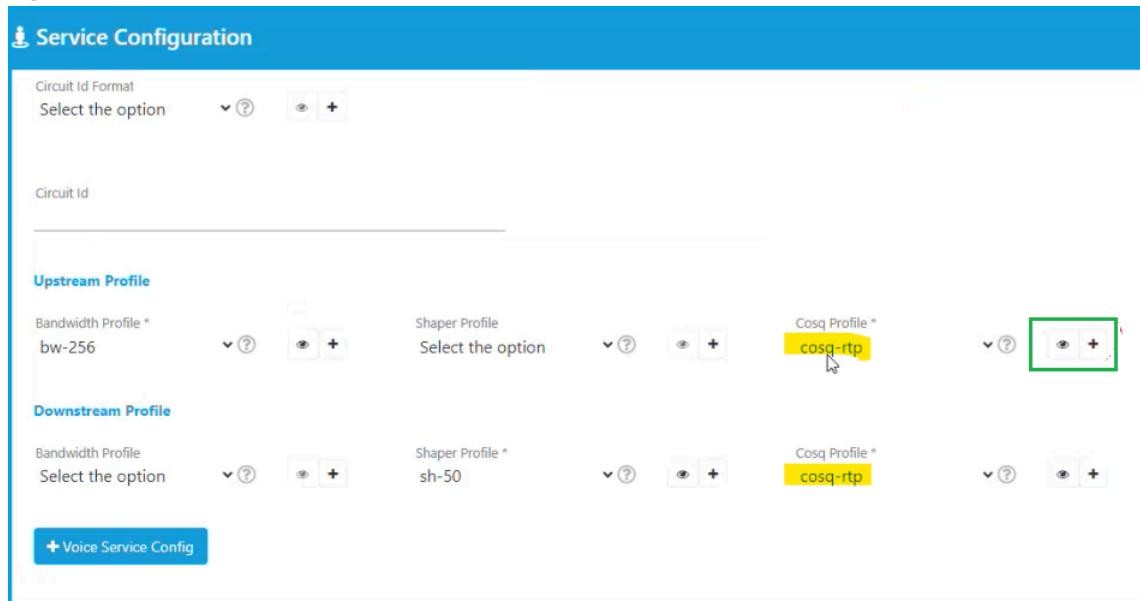
Configuring RTP COSQ Profile

Perform the following steps to configure an RTP COSQ Profile.

1. In the service configuration page, select the Cosq Profile as cosq-rtp from the list and click the eye icon.

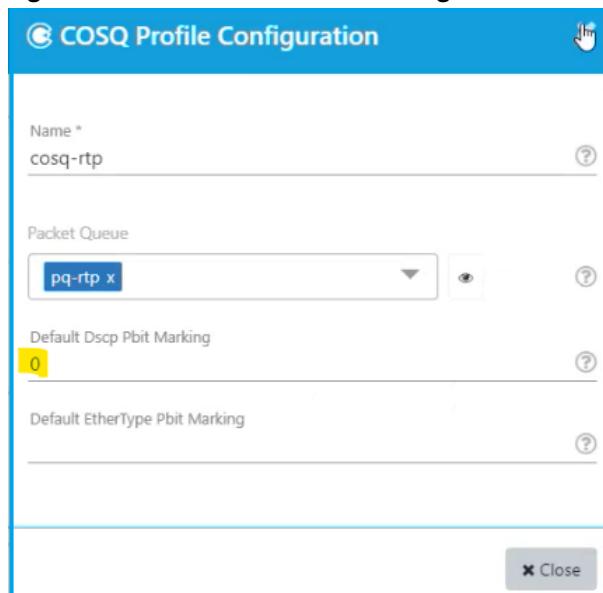
The COSQ Profile Configuration page appears.

Figure 246. RTP COSQ Profile



2. Configure the **Default DSCP Pbit Marking** to 0. See [Creating COSQ Profile \(on page 570\)](#).

Figure 247. Default DSCP Pbit Marking



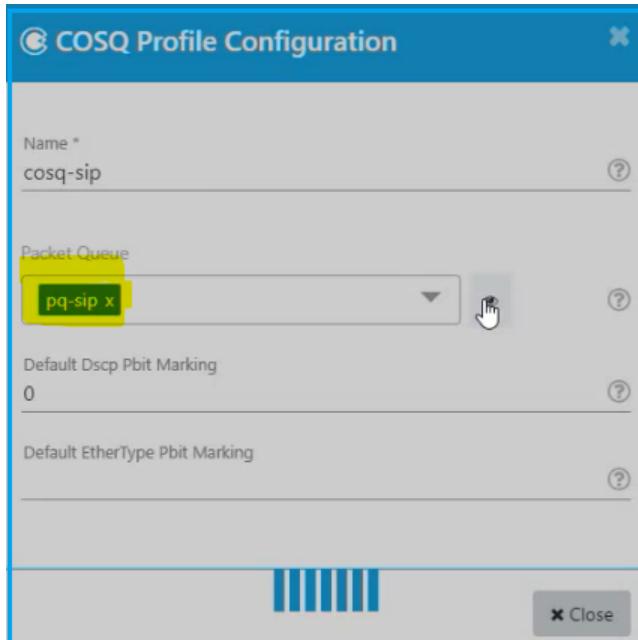
3. Select the Scheduler Config Priority to 1.

Configuring SIP COSQ Profile

Perform the following steps to create a SIP COSQ Profile.

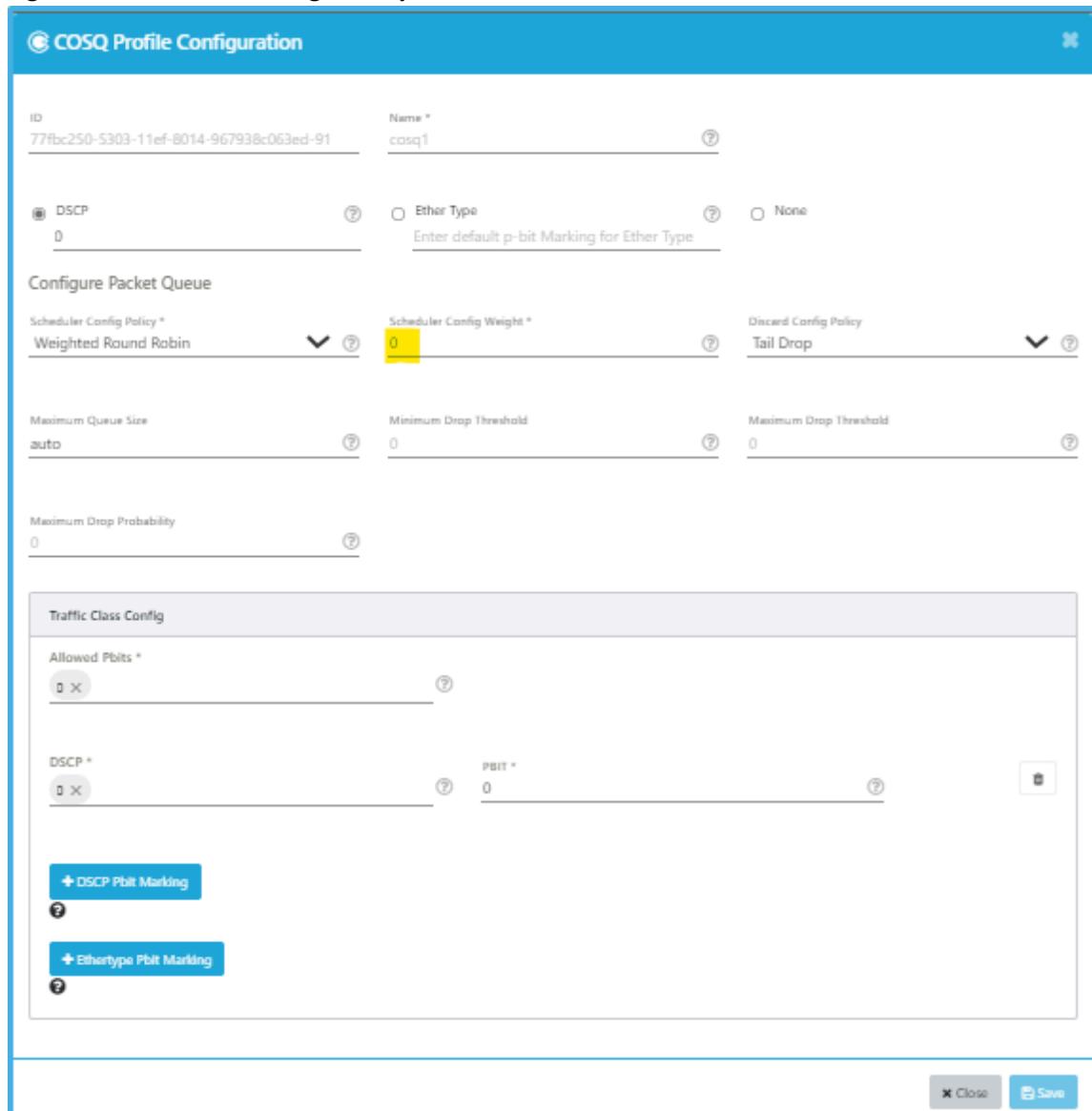
1. In the Service Configuration page, click the eye icon to view the COSQ profile.
2. Configure the Allowed Pbits to 0 and 2, DSCP value to 24, and PBIT to 2.
3. Configure the **Default DSCP Pbit Marking** to 0. See [Creating COSQ Profile \(on page 570\)](#).

Figure 248. Default DSCP Pbit Marking



4. In the Service Configuration page, select the COSQ Profile as cosq-sip from the list and click the eye icon.
5. Configure the Scheduler Config Priority to 2.

Figure 249. Scheduler Config Priority



The screenshot shows the 'COSQ Profile Configuration' dialog box. The 'Name' field is set to 'cosq1'. The 'Scheduler Config Policy' is 'Weighted Round Robin'. The 'Scheduler Config Weight' is set to 0.5. The 'Discard Config Policy' is 'Tail Drop'. The 'Maximum Queue Size' is 'auto'. The 'Minimum Drop Threshold' and 'Maximum Drop Threshold' are both 0. The 'Traffic Class Config' section shows 'Allowed Pbits' as an empty list, 'DSCP' as an empty list, and 'PBIT' as 0. There are buttons for 'DSCP Pbit Marking' and 'Ethertype Pbit Marking'. At the bottom, there are 'Close' and 'Save' buttons.

The default-cosq, rtp-cosq, and sip-cosq profiles are created.

Scenario 1

Perform the following steps to prioritize the signaling packets over SIP packets.



Note: If the user wants SIP to be a non-zero value and other packets remarking to 0. The user must create 2 sub-services (The first sub-service carries other packets and the second sub-service carries SIP packets).

Configure pbits remarking for the SIP, RTP, and other packets as per the following table.

Table 395. PBITS Remark

| DSCP | PBITS Remark |
|--------|--------------|
| SIP | 2 (Non zero) |
| RTP | 0 (Zero) |
| Others | 0 (Zero) |

Perform the following steps to create the first sub-service.

1. Create a sub-service that carries SIP and RTP packets and attach the voice profile. See [Voice Service Profiles \(on page 589\)](#).
2. Create a COSQ profile with an aggregate bandwidth. See [Creating COSQ Profile \(on page 570\)](#).
3. Configure the default COSQ profile with the voice profile. See [Voice Service Profiles \(on page 589\)](#).
4. Configure the Default DSCP Pbit Marking to 0. See [Creating COSQ Profile \(on page 570\)](#).

The first sub-service is created.

Perform the following steps to create a second sub-service and prioritize the signaling packets over RTP packets.

1. Create a SIP-COSQ profile. See [Configuring SIP COSQ Profile \(on page 844\)](#).
2. Configure the Allowed pbits values to 2 for SIP.

A second sub-service is created and the signaling packets are prioritized over RTP packets.

Scenario 2

Perform the following steps to prioritize the signaling packets over SIP and RTP packets.



Note: If the user wants SIP and RTP to be a non-zero value and other packets remarking to 0. The user must create 3 sub-services (The first sub-service will carry other packets, the second sub-service will carry RTP packets, and the third sub-service will carry SIP packets).

Configure pbits remarking for the SIP, RTP, and other packets as per the following table.

Table 396. PBITS Remark

| DSCP | PBITS Remark |
|--------|--------------|
| SIP | 2 (Non zero) |
| RTP | 1 (Non zero) |
| Others | 0 (Zero) |

Perform the following steps to create the first sub-service.

1. Create a sub-service that carries SIP and RTP profiles and attach the voice profile.
2. Create a COSQ profile with an aggregate bandwidth. See [Creating COSQ Profile \(on page 570\)](#).
3. Configure the default COSQ profile with the voice profile. See [Voice Service Profiles \(on page 589\)](#).
4. Configure the Default DSCP Pbit Marking to 0. See [Creating COSQ Profile \(on page 570\)](#).

The first sub-service is created.

Perform the following steps to create a second sub-service.

1. Create a RTP-COSQ profile. See [Configuring RTP COSQ Profile \(on page 843\)](#).
2. Configure the Allowed pbits values to 1 for RTP.

The second sub-service is created.

Perform the following steps to create a third sub-service and prioritize the signaling packets over SIP and RTP packets.

1. Create a SIP-COSQ profile. See [Configuring SIP COSQ Profile \(on page 844\)](#).
2. Configure the Allowed pbits values to 2 for SIP.

A third sub-service is created and the signaling packets are prioritized over SIP and RTP packets.

Related information

[Workflow for Activating a Service for the Subscriber \(on page 36\)](#)

Example: Configuring IPTV for Subscriber

This example shows how to configure and activate IPTV (multicast) for the subscriber.

- [Overview \(on page 847\)](#)
- [IPTV Activation Workflow \(on page 847\)](#)
- [Verification \(on page 856\)](#)

Overview

Internet Protocol Television (IPTV), is a technology that allows television services to be delivered over the Internet protocol, such as a local area network (LAN) or the Internet, instead of being delivered through traditional satellite signals or cable television formats.

An IPTV service, typically distributed by a service provider, delivers live TV programs or ondemand video content through the IP networks.

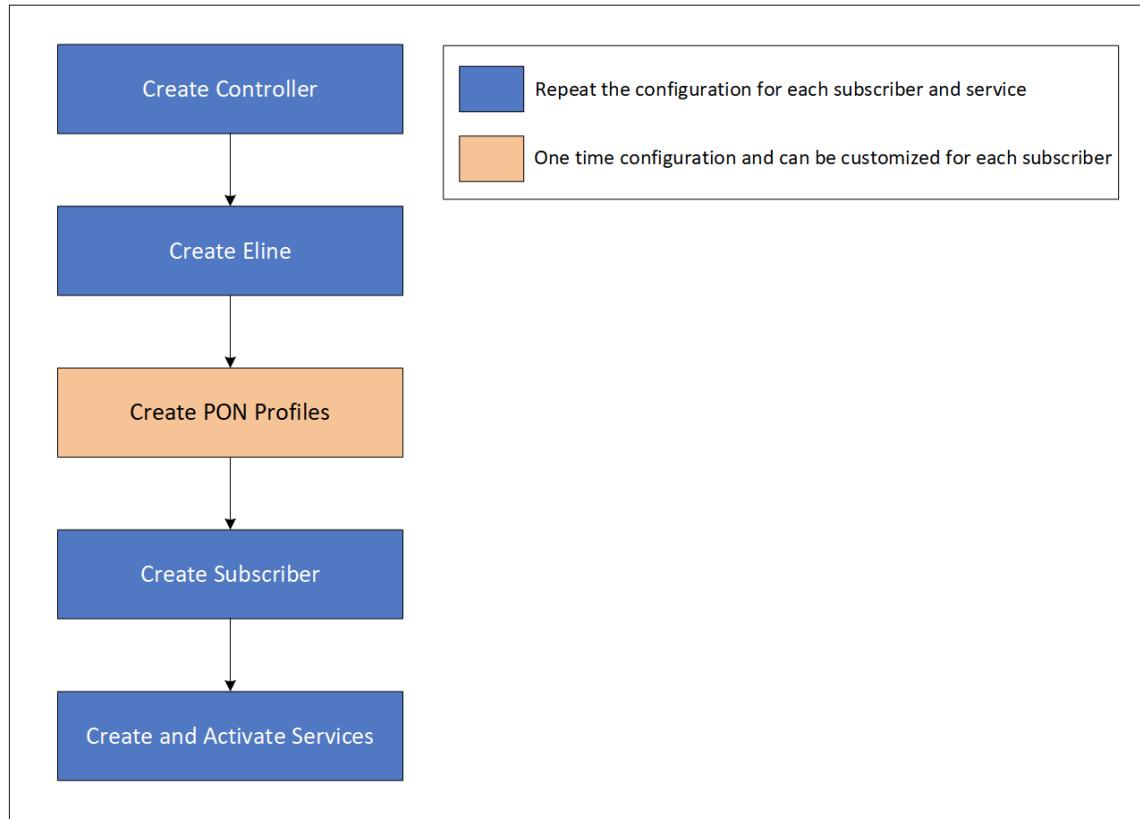
IPTV Activation Workflow

Perform the following steps to create and activate the voice service.

1. Create Controller. See [Creating Controller \(on page 848\)](#).
2. Create Eline. See [Creating Eline \(on page 849\)](#).

3. Create PON Profile. See [Creating PON Profile \(on page 850\)](#).

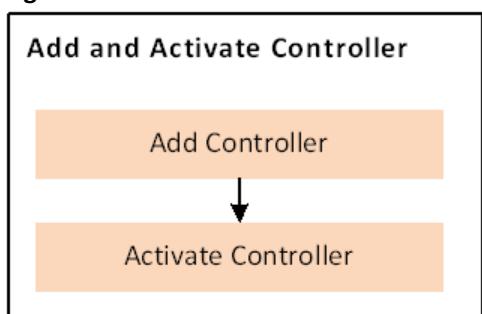
Figure 250. IPTV Activation Workflow



Creating Controller

The following diagram illustrates the workflow for adding and activating controller.

Figure 251. Controller Activation Workflow



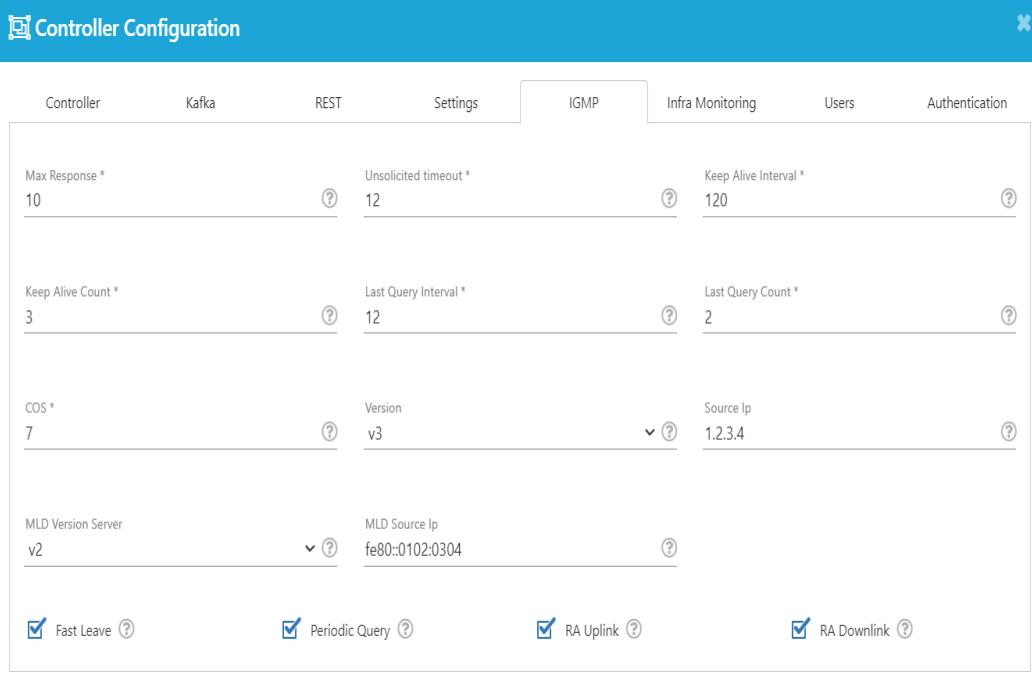
Perform the following steps to add and activate the controller.

1. Create a controller with IGMP configuration. See [Creating Controller Configuration \(on page 297\)](#).



Note: Select IGMP version as v3.

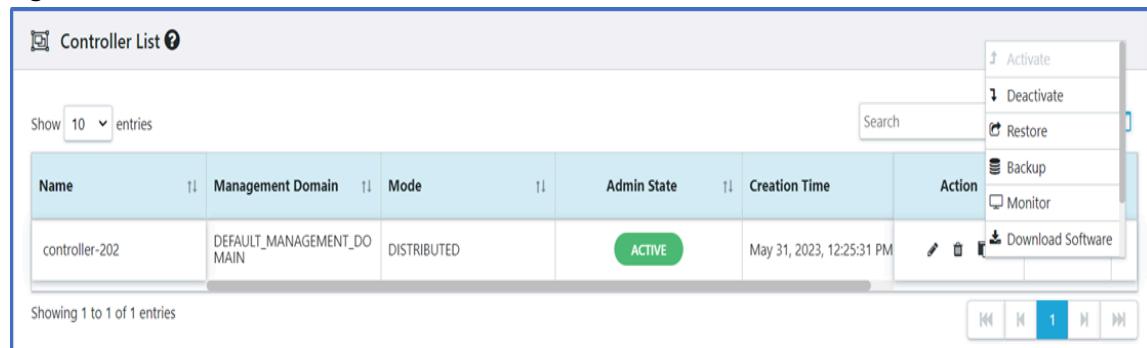
Figure 252. Controller Configuration



The screenshot shows the 'Controller Configuration' page with the 'IGMP' tab selected. The interface includes sections for Max Response (10), Unsolicited timeout (12), Keep Alive Interval (120), Keep Alive Count (3), Last Query Interval (12), Last Query Count (2), COS (7), Version (v3), Source Ip (1.2.3.4), MLD Version Server (v2), MLD Source Ip (fe80::0102:0304), and checkboxes for Fast Leave, Periodic Query, RA Uplink, and RA Downlink. Buttons for Close and Create are at the bottom right.

2. Activate a controller. See [Activating the Controller \(on page 305\)](#).

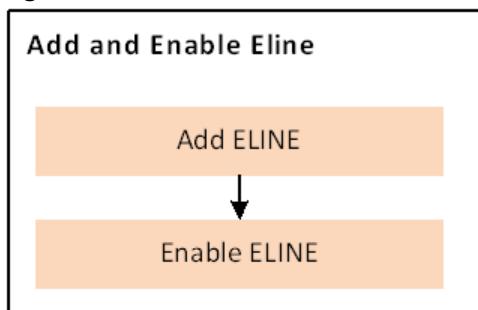
Figure 253. Activate Controller



The screenshot shows the 'Controller List' page with a single entry: 'controller-202' in 'DEFAULT_MANAGEMENT_DOMAIN' with 'DISTRIBUTED' mode, 'ACTIVE' Admin State, and 'May 31, 2023, 12:25:31 PM' Creation Time. A context menu is open over this entry, showing options: Activate, Deactivate, Restore, Backup, Monitor, and Download Software. The 'Activate' option is highlighted.

Creating Eline

The following diagram illustrates the workflow for adding and enabling eline.

Figure 254. Eline Activation Workflow

Perform the following steps to add and enable eline.

1. Create a ELine. See [Creating ELine Configuration \(on page 332\)](#).

Figure 255. ELine Configuration

ELine Configuration

| | | |
|--|----------------------------|---|
| Name * | <input type="text"/> | ? |
| Vlan Id * | <input type="text"/> | ? |
| Port * | <input type="text"/> NNI-2 | ? |
| | | |
| <input type="button" value="x Close"/> <input type="button" value="+ Create"/> | | |

2. Enable ELine. See [Enabling and Disabling ELine Configuration \(on page 333\)](#).

Figure 256. Enable ELine

ELine List [olt-202]

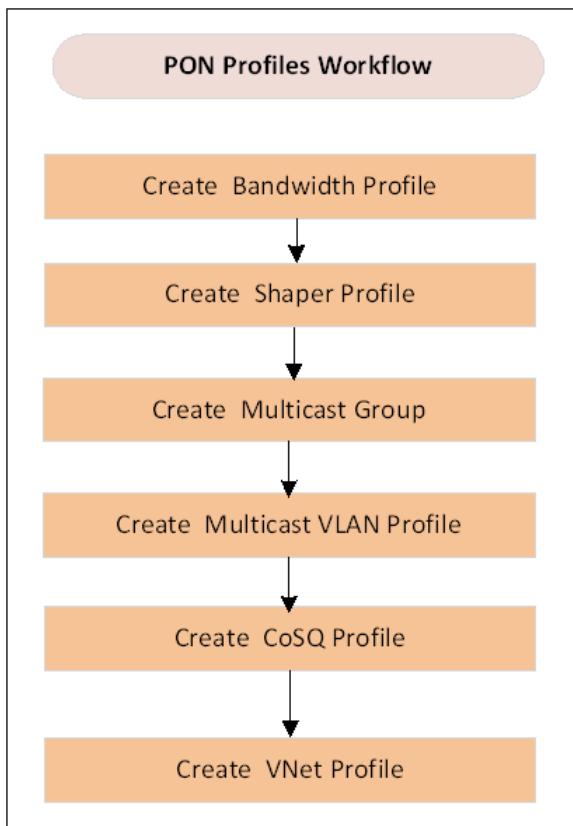
| Name | Vlan | Port | Admin State | Creation At | Action |
|--------|------|-------|-------------|---------------------------|----------------------------------|
| eline1 | 202 | NNI-4 | ENABLED | May 31, 2023, 12:31:24 PM | Enable Disable Monitor |

Showing 1 to 1 of 1 entries

Creating PON Profile

The following diagram illustrates the workflow for creating PON profile.

Figure 257. PON Profile Workflow



Perform the following steps to add the PON profiles.

1. Create a bandwidth profile. See [Creating Bandwidth Profile \(on page 564\)](#).

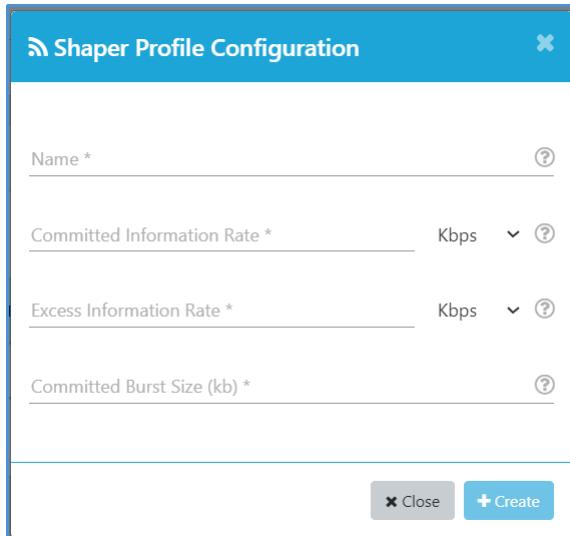
 **Note:** The AIR and EIR fields value must be same.

Figure 258. Bandwidth Profile

| Bandwidth Profile Configuration | |
|--------------------------------------|---------------------------------------|
| Name * | <input type="text"/> |
| Committed Information Rate * | <input type="text"/> Kbps |
| Assured Information Rate * | <input type="text"/> Kbps |
| Excess Information Rate * | <input type="text"/> Kbps |
| Delay Tolerance (No of Frames) | <input type="text"/> 0 |
| | |
| <input type="button" value="Close"/> | <input type="button" value="Create"/> |

2. Create a shaper profile. See [Creating Shaper Profile \(on page 567\)](#).

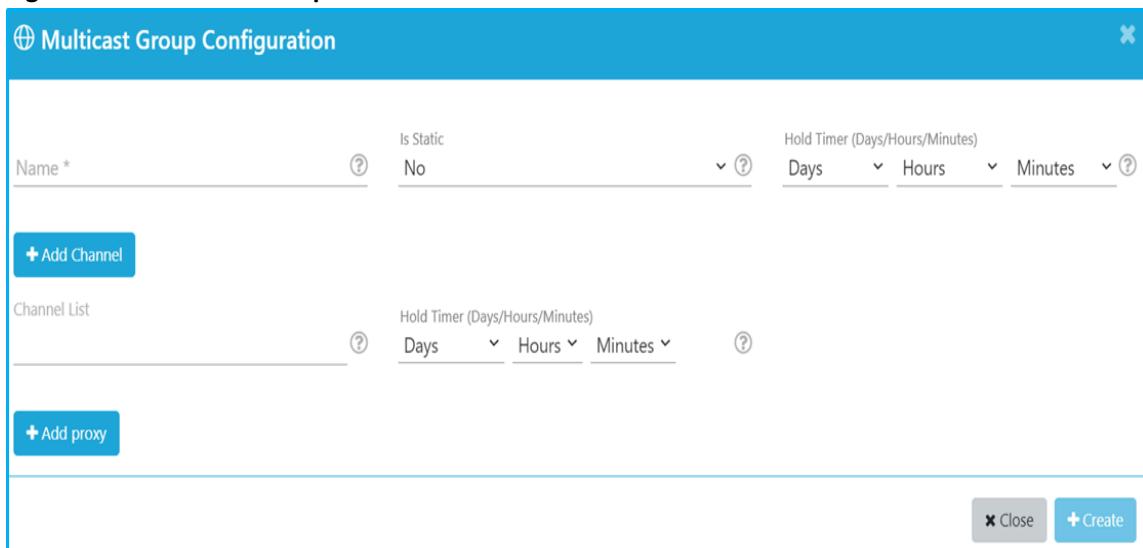
Figure 259. Shaper Profile



The dialog box is titled "Shaper Profile Configuration". It contains four input fields: "Name *", "Committed Information Rate *", "Excess Information Rate *", and "Committed Burst Size (kb) *". Each field has a unit of "Kbps" and a help icon. At the bottom are "Close" and "Create" buttons.

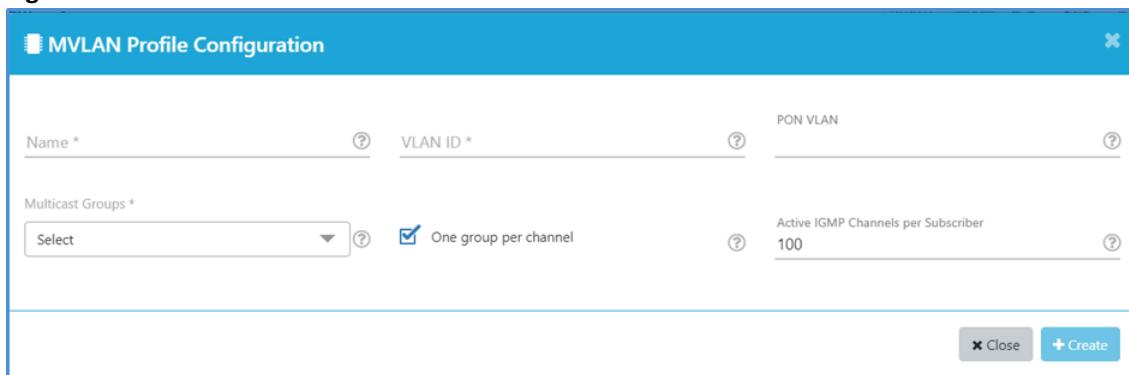
3. Create a multicast group. See [Creating Multicast Group \(on page 568\)](#).

Figure 260. Multicast Group



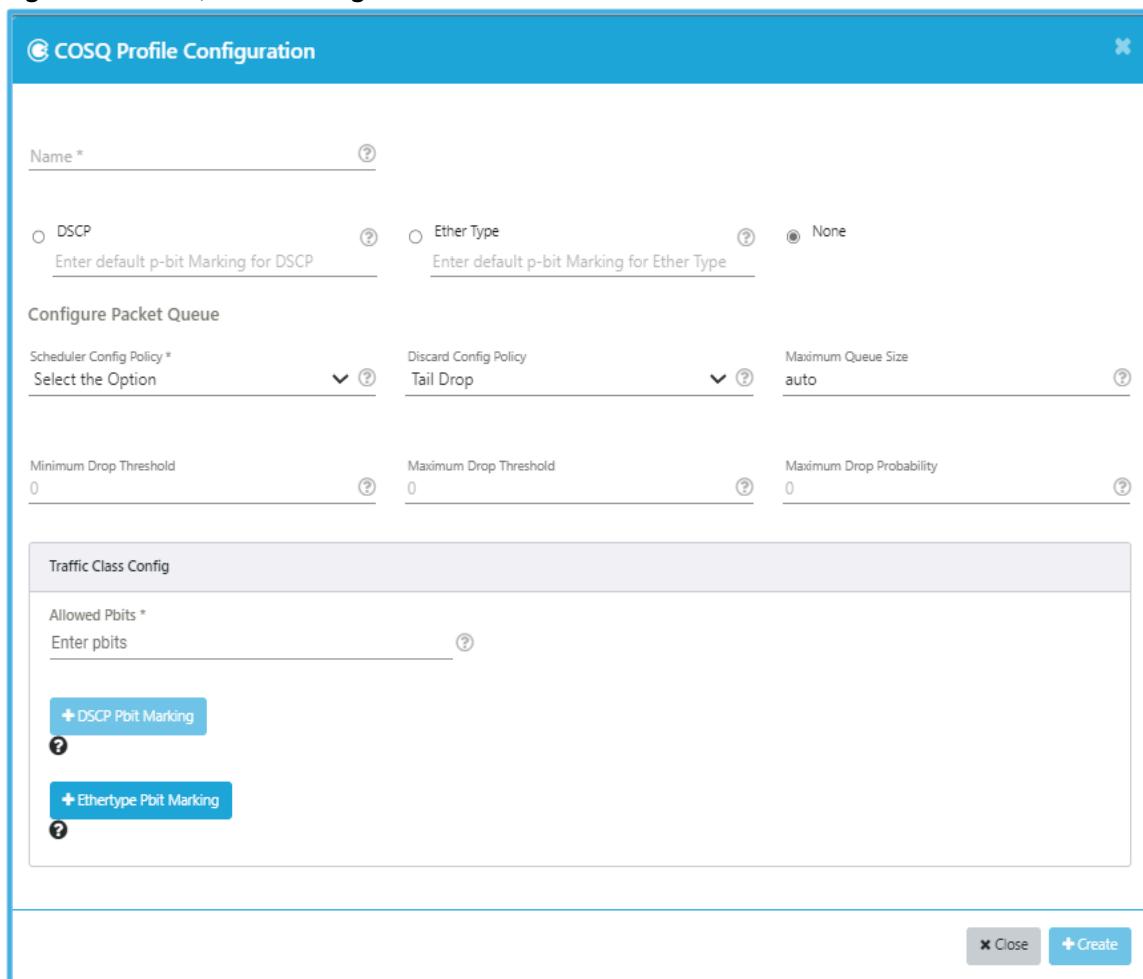
The dialog box is titled "Multicast Group Configuration". It contains fields for "Name *", "Is Static" (set to "No"), and "Hold Timer (Days/Hours/Minutes)" (set to "Days", "Hours", and "Minutes"). Below these are "Add Channel" and "Add proxy" buttons. At the bottom are "Close" and "Create" buttons.

4. Create a multicast VLAN (MVLAN) profile. See [Creating MVLAN Profile \(on page 568\)](#).

Figure 261. MVLAN Profile

The screenshot shows the 'MVLAN Profile Configuration' dialog box. It includes fields for 'Name *' (with a question mark icon), 'VLAN ID *' (with a question mark icon), and 'PON VLAN' (with a question mark icon). Below these are sections for 'Multicast Groups *' (with a dropdown menu labeled 'Select' and a question mark icon) and 'One group per channel' (with a checked checkbox and a question mark icon). To the right is a field for 'Active IGMP Channels per Subscriber' with the value '100' and a question mark icon. At the bottom right are buttons for 'Close' and '+ Create'.

5. Create a Class of Service Queue (CoSQ) profile. See [Creating COSQ Profile \(on page 570\)](#).

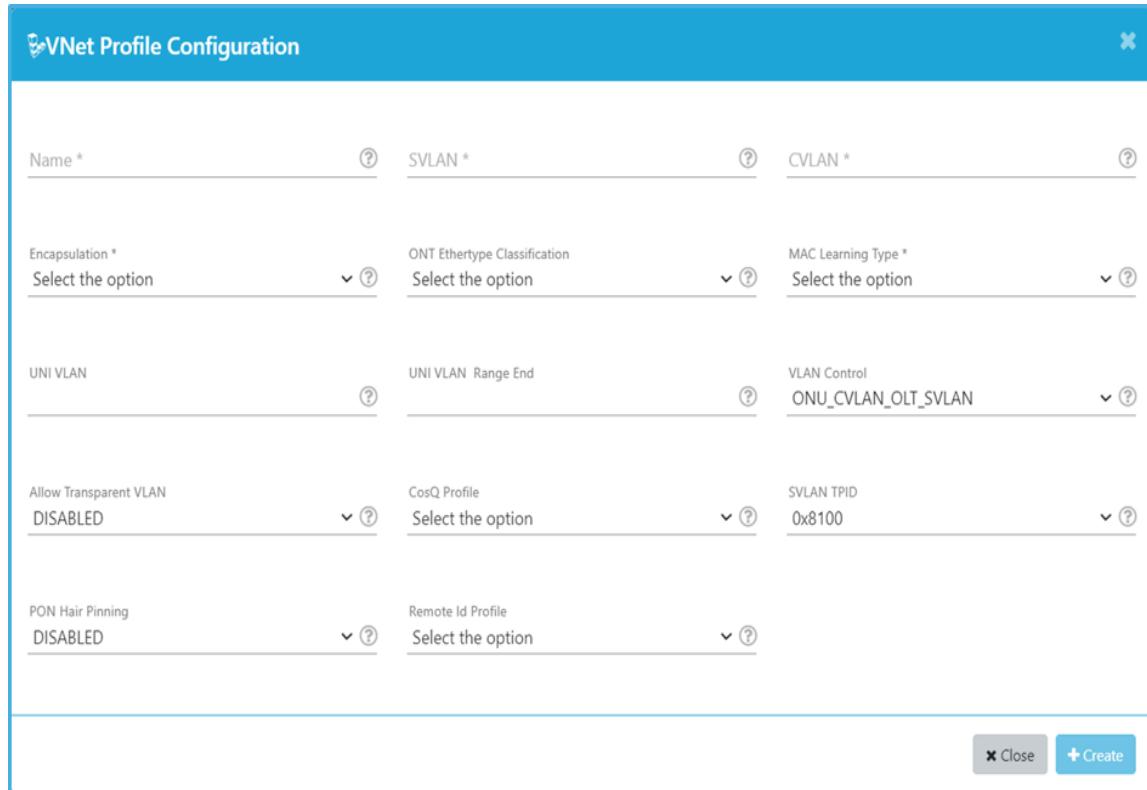
Figure 262. CoSQ Profile Configuration

The screenshot shows the 'COSQ Profile Configuration' dialog box. It starts with a 'Name *' field (with a question mark icon). Below it are three radio button options: 'DSCP' (selected), 'Ether Type' (unchecked), and 'None' (unchecked). Each option has a text input field for 'Enter default p-bit Marking' (with a question mark icon). The 'Configure Packet Queue' section includes 'Scheduler Config Policy *' (with a dropdown menu labeled 'Select the Option' and a question mark icon), 'Discard Config Policy' (with a dropdown menu labeled 'Tail Drop' and a question mark icon), and 'Maximum Queue Size' (with a dropdown menu labeled 'auto' and a question mark icon). Further down are 'Minimum Drop Threshold' (0), 'Maximum Drop Threshold' (0), and 'Maximum Drop Probability' (0). A 'Traffic Class Config' section contains an 'Allowed Pbits *' field (with a question mark icon) and two buttons: '+ DSCP Pbit Marking' and '+ Ethertype Pbit Marking', each with a question mark icon. At the bottom right are buttons for 'Close' and '+ Create'.

6. Create a VNet profile. See [Creating VNet Profile \(on page 577\)](#).

 **Note:** Ensure that SVLAN is equals to CVLAN.

Figure 263. VNet Profile Configuration



The dialog box is titled 'VNet Profile Configuration'. It contains the following fields:

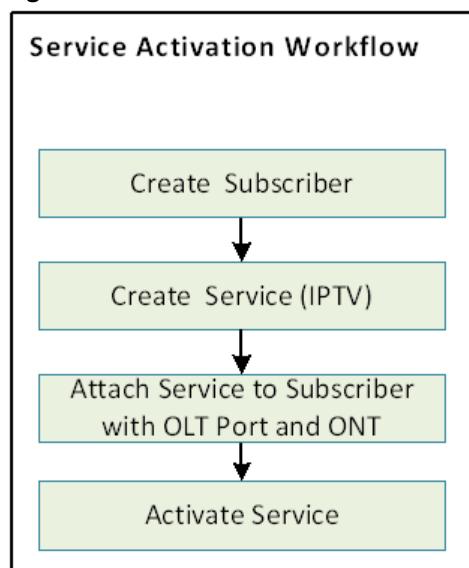
| Name * | SVLAN * | CVLAN * |
|------------------------|------------------------------|---------------------|
| Encapsulation * | ONT Ethertype Classification | MAC Learning Type * |
| Select the option | Select the option | Select the option |
| UNI VLAN | UNI VLAN Range End | VLAN Control |
| Allow Transparent VLAN | CosQ Profile | SVLAN TPID |
| DISABLED | Select the option | 0x8100 |
| PON Hair Pinning | Remote Id Profile | |
| DISABLED | Select the option | |

Buttons at the bottom right: 'Close' and 'Create'.

Creating, Activating, Subscriber and Services

The following diagram illustrates the workflow for creating, activating, subscriber, and services.

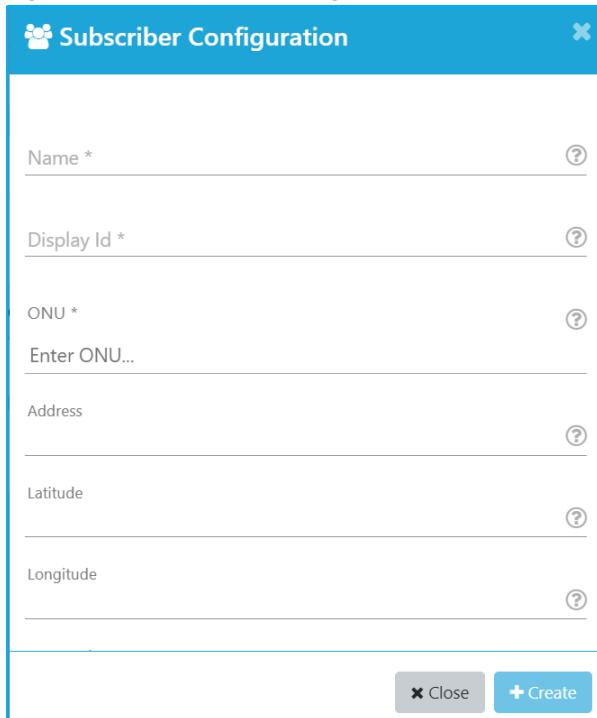
Figure 264. Service Activation Workflow



Perform the following steps to create, activate, subscriber and services.

1. Create a subscriber. See [Creating Subscriber \(on page 455\)](#).

Figure 265. Subscriber Configuration



The image shows a 'Subscriber Configuration' dialog box. It has a blue header bar with the title 'Subscriber Configuration' and a close button. The main area contains several input fields: 'Name *' (with a question mark icon), 'Display Id *' (with a question mark icon), 'ONU *' (with a question mark icon), 'Enter ONU...', 'Address' (with a question mark icon), 'Latitude' (with a question mark icon), and 'Longitude' (with a question mark icon). At the bottom are two buttons: a grey 'Close' button and a blue '+ Create' button.

2. Create a service. See [Creating Service \(on page 459\)](#).

The following table describes the mandatory fields and values for IPTV configuration.

Table 397. IPTV Service Configuration

| Field | Values |
|----------------|---|
| AES Encryption | Select True from the list. |
| VLAN Control | Select ONU_CVLAN from the list.  Note: SVLAN and CVLAN ID must be same if you select VLAN control as ONU_CVLAN. |

Figure 266. IPTV Configuration

Service Configuration

Name * ser-iptv

MAC Limit

Aggregate Upstream Bandwidth Profile Select the option

Aggregate Downstream Shaper Profile Select the option

Service Queue Stats Select the option

Force Delete Select the option

Control Packet Statistics

PPPoE

DHCPv4

DHCPv6

1. service - iptv

Service Name * iptv

UNI Port Id * ISKT429D7B1D-10-PPTP-ETHERNET-1 x

Uni Port Type Select the option

CPE MAC

AES Encryption * True

Remote Id Type Select the option

Data Rate Attribute DISABLED

CPE IP Type NONE

Close **Create**

- Activate the service for the subscriber. See [Activating and Deactivating the Service for the Subscriber \(on page 467\)](#).

Verification

Verify that the service is activated for the subscriber.

- Navigate to **Configuration > Subscriber > Service or Monitor > Services > Subscriber Service**.
 - Verify the admin and operational state of the service.
- The **Operational State** for the service must be **UP**, indicating that the service is up and running for the subscriber, and the **Admin State** of the service must be **ACTIVE** indicating that the service is activated for the subscriber.

Figure 267. Subscriber Service Status

Service List [Subscriber - sub1]

Show 10 entries

Search

Create Export

Name Admin State Operational State Creation Time Action

ser-202 ACTIVE UP May 31, 2023, 12:31:04 PM

Showing 1 to 1 of 1 entries

3. Navigate to **Monitor > Events**.
4. Verify the SERVICE-UP event is reported in RMS to confirm the service activation for the subscriber is successful, or the service status is UP.

Related information

[Workflow for Activating a Service for the Subscriber \(on page 36\)](#)

Example: Configuring Whole Home Digital Video Recording

This example shows how to configure and activate WHDVR for the subscriber.

- [Overview \(on page 857\)](#)
- [WHDVR Activation Workflow \(on page 857\)](#)
- [WHDVR Configuration \(on page 858\)](#)
- [Service Activation \(on page 865\)](#)
- [Verification \(on page 865\)](#)

Overview

Whole Home Digital Video Recording (WHDVR), is a technology that allows users to record and store television programming content on a central server or DVR device and then access that content from any television connected to the same network within their home.

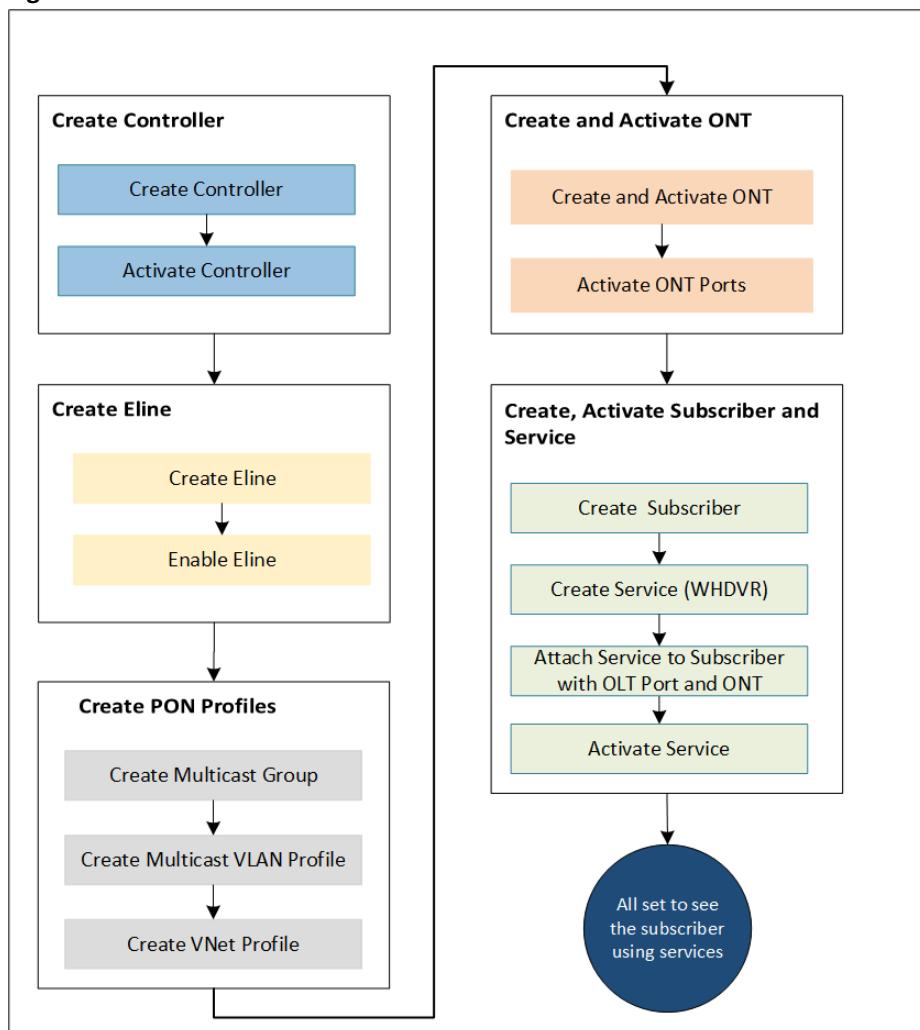


Note: The WHDVR is supported in limited ONT models with specific firmware version.

WHDVR Activation Workflow

The following diagram illustrates the workflow for creating and activating the WHDVR for the subscriber.

Figure 268. WHDVR Activation Workflow



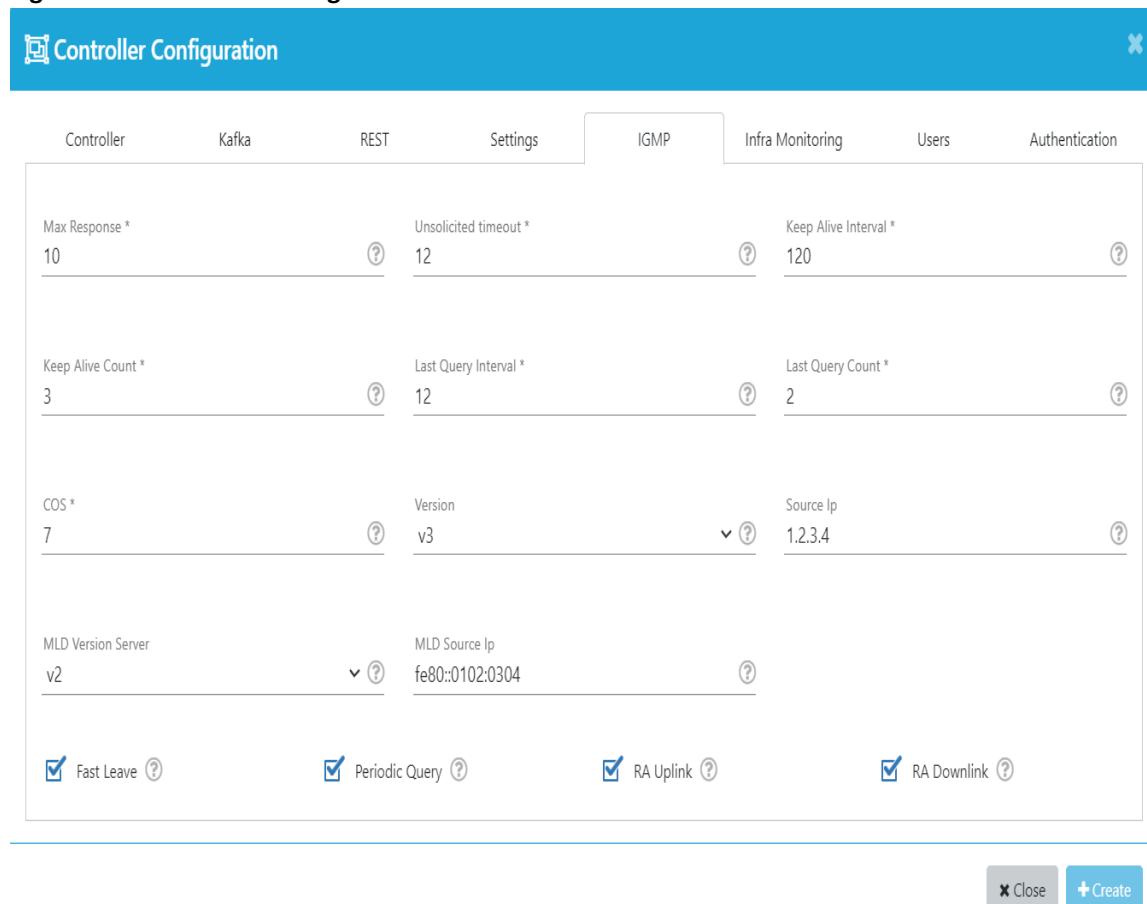
WHDVR Configuration

This section involves the configuration steps to create WHDVR.

1. Create a controller with IGMP configuration. See [Creating Controller Configuration \(on page 297\)](#).



Note: Select IGMP version as v3.

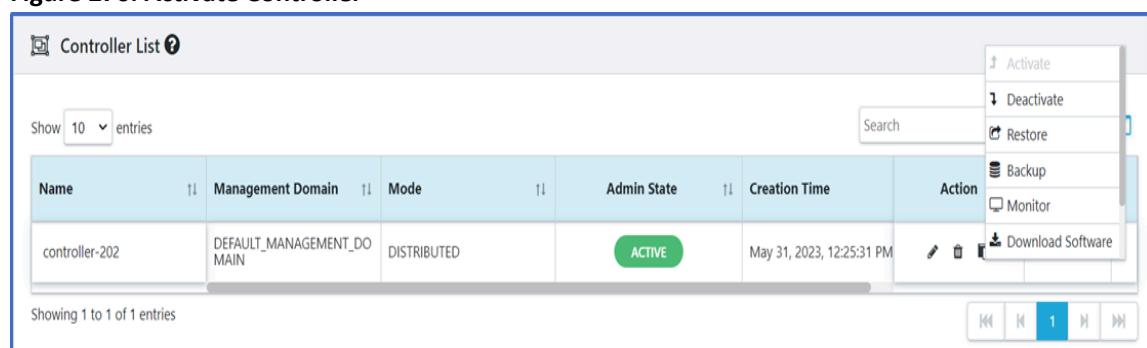
Figure 269. Controller Configuration


The screenshot shows the 'Controller Configuration' page with the 'IGMP' tab selected. The interface includes a navigation bar with tabs: Controller, Kafka, REST, Settings, IGMP (selected), Infra Monitoring, Users, and Authentication. The main content area contains several configuration fields with validation markers (asterisks and question marks):

- Max Response *: 10
- Unsolicited timeout *: 12
- Keep Alive Interval *: 120
- Keep Alive Count *: 3
- Last Query Interval *: 12
- Last Query Count *: 2
- COS *: 7
- Version: v3
- Source Ip: 1.2.3.4
- MLD Version Server: v2
- MLD Source Ip: fe80::0102:0304
- Checkboxes at the bottom: Fast Leave (checked), Periodic Query (checked), RA Uplink (checked), RA Downlink (checked).

At the bottom right are 'Close' and 'Create' buttons.

2. Activate a controller. See [Activating the Controller \(on page 305\)](#).

Figure 270. Activate Controller


The screenshot shows the 'Controller List' page with a single entry: 'controller-202'. The table columns are: Name, Management Domain, Mode, Admin State, Creation Time, and Action. The 'Action' column for the entry has a context menu open with the following options: Activate, Deactivate, Restore, Backup, Monitor, and Download Software. The 'Search' field is empty.

| Name | Management Domain | Mode | Admin State | Creation Time | Action |
|----------------|---------------------------|-------------|-------------|---------------------------|--|
| controller-202 | DEFAULT_MANAGEMENT_DOMAIN | DISTRIBUTED | ACTIVE | May 31, 2023, 12:25:31 PM | <input type="button" value="Activate"/> <input type="button" value="Deactivate"/> <input type="button" value="Restore"/> <input type="button" value="Backup"/> <input type="button" value="Monitor"/> <input type="button" value="Download Software"/> |

Showing 1 to 1 of 1 entries

3. Create a ELine. See [Creating ELine Configuration \(on page 332\)](#).

Figure 271. ELine Configuration

ELine Configuration

Name *

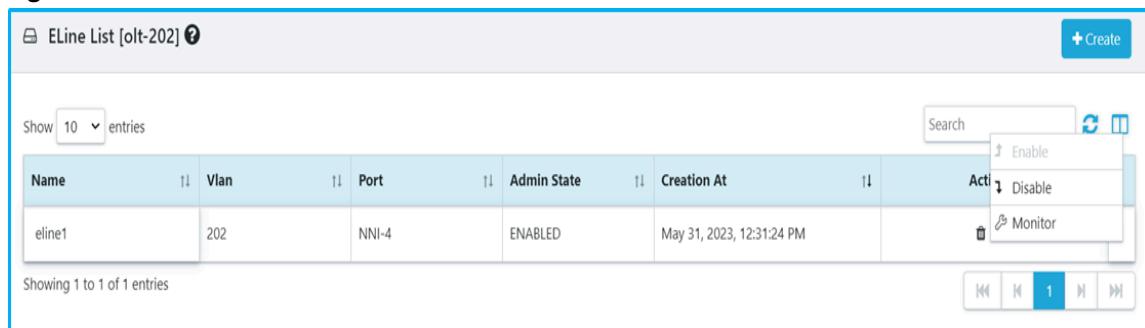
VLan Id *

Port *

NNI-2

Close **Create**

4. Enable ELine. See [Enabling and Disabling ELine Configuration \(on page 333\)](#).

Figure 272. Enable ELine

| Name | Vlan | Port | Admin State | Creation At | Action |
|--------|------|-------|-------------|---------------------------|---|
| eLine1 | 202 | NNI-4 | ENABLED | May 31, 2023, 12:31:24 PM | Enable Disable Monitor |

Showing 1 to 1 of 1 entries

5. Create an ONT Configuration by selecting Make, Model, and Device Profile. See [Creating ONT Configuration \(on page 427\)](#).



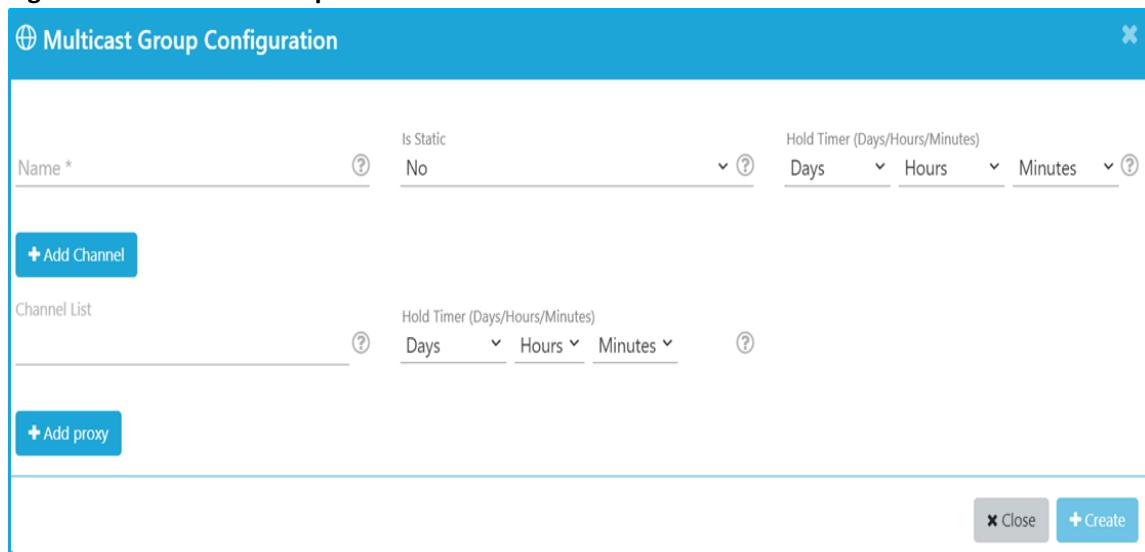
Note: The connectivity mode of the ONT must be N:MP or 1:MP mode.

Figure 273. ONT Configuration

6. Activate the ONT. See [Activating the ONT \(on page 431\)](#).

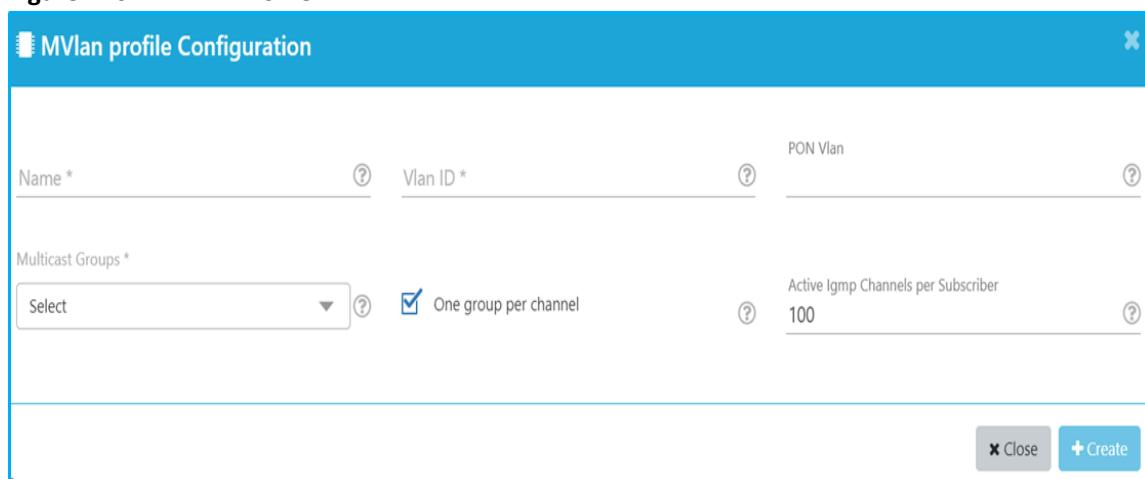
Figure 274. Activate ONT

7. Create a multicast group. See [Creating Multicast Group \(on page 431\)](#).

Figure 275. Multicast Group

The screenshot shows the 'Multicast Group Configuration' dialog box. At the top, there is a 'Name *' input field and an 'Is Static' dropdown set to 'No'. Below these are 'Hold Timer (Days/Hours/Minutes)' dropdowns for Days, Hours, and Minutes. A 'Channel List' section follows, with a 'Channel List' input field and its own 'Hold Timer' dropdowns. A 'Add Channel' button is located above the channel list. A 'Add proxy' button is also present. At the bottom right are 'Close' and 'Create' buttons.

8. Create a multicast VLAN (MVLAN) profile. See [Creating MVLAN Profile \(on page 568\)](#).

Figure 276. MVLAN Profile

The screenshot shows the 'MVLan profile Configuration' dialog box. It includes fields for 'Name *', 'Vlan ID *', and 'PON Vlan'. A 'Multicast Groups *' dropdown is set to 'Select'. A checkbox 'One group per channel' is checked. An 'Active Igmp Channels per Subscriber' input field is set to '100'. At the bottom right are 'Close' and 'Create' buttons.

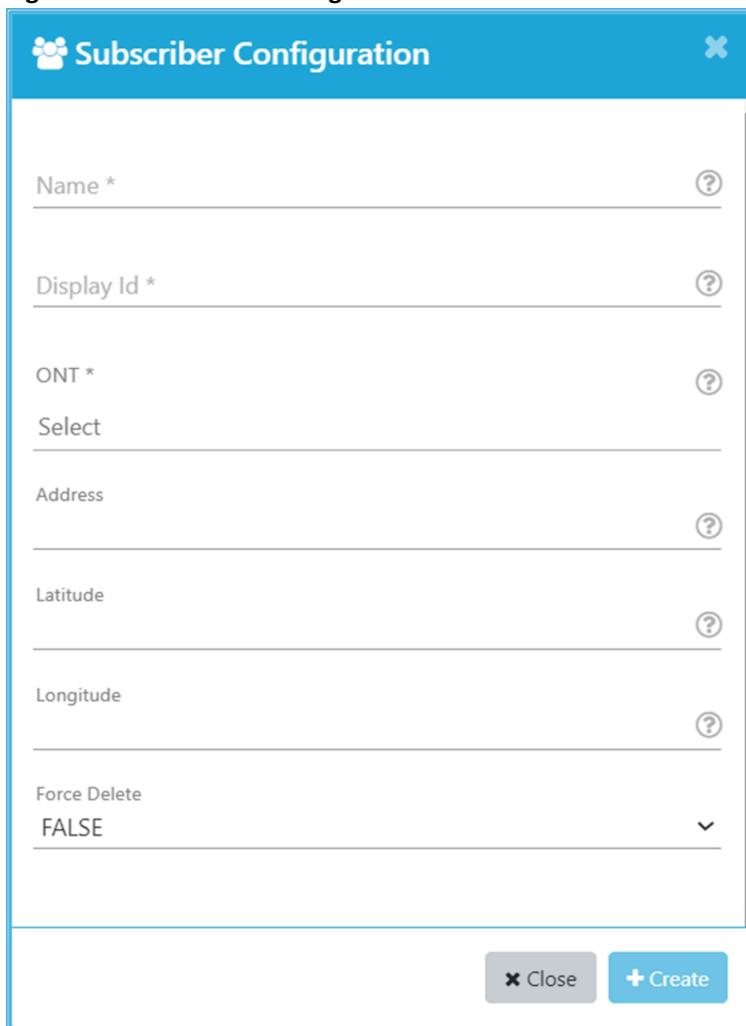
9. Create a VNet profile. See [Creating VNet Profile \(on page 577\)](#).



Note: Ensure that VLAN Control is ONU_CVLAN and MAC Learning Type is NONE.

Figure 277. VNet Profile Configuration

10. Create a subscriber. See [Creating Subscriber \(on page 455\)](#).

Figure 278. Subscriber Configuration

The image shows a 'Subscriber Configuration' dialog box. At the top is a title bar with the Radisys logo and the title 'Subscriber Configuration'. Below the title bar are several input fields: 'Name *' (with a question mark icon), 'Display Id *' (with a question mark icon), 'ONT *' (with a question mark icon), 'Select' (a dropdown menu), 'Address' (with a question mark icon), 'Latitude' (with a question mark icon), 'Longitude' (with a question mark icon), and 'Force Delete' (a dropdown menu with 'FALSE' selected). At the bottom of the dialog are two buttons: a grey 'Close' button and a blue '+ Create' button.

11. Create a service. See [Creating Service \(on page 459\)](#).

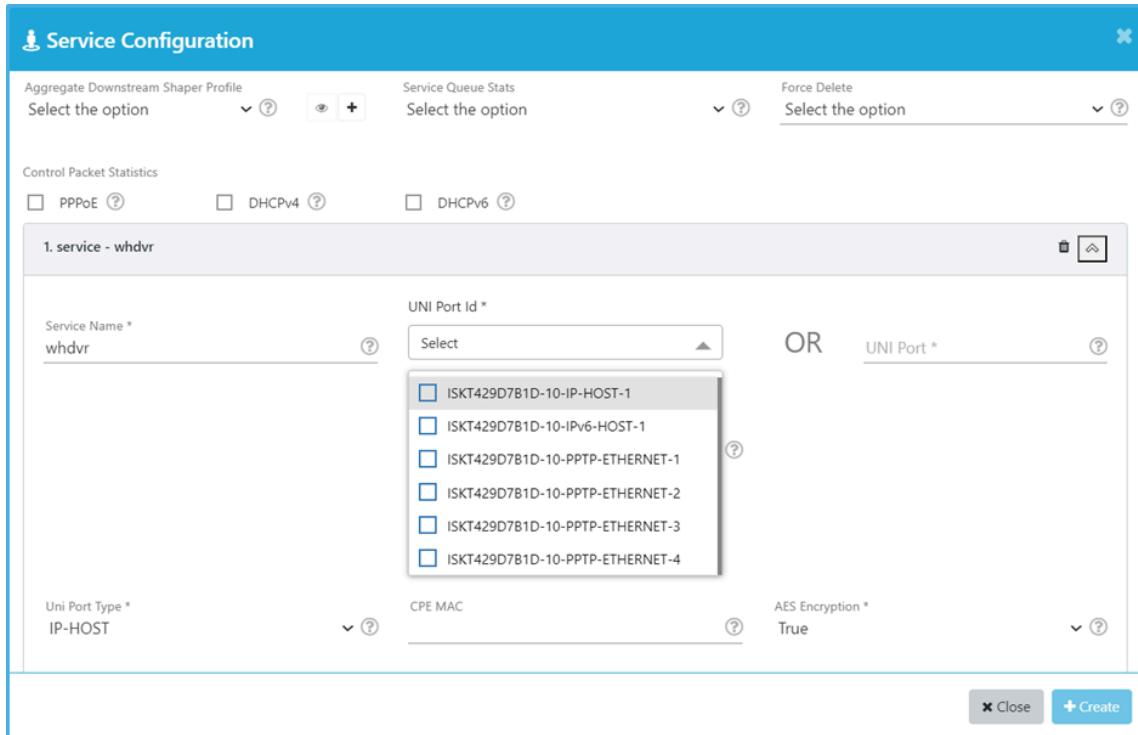
The following table describes the mandatory fields and values for WHDVR configuration.

Table 398. WHDVR Service Configuration

| Field | Values |
|----------------|--|
| AES Encryption | Select True from the list. |
| VLAN Control | Select ONU_CVLAN from the list. |

| Field | Values |
|-------|---|
| |  Note: SVLAN and CVLAN ID must be same if you select VLAN control as ONU_CVLAN. |

Figure 279. WHDVR Configuration



Service Activation

Service activation enables and grants access to specific services or features associated with a service plan or subscription. The service activation process ensures subscribers can start using the intended services and features as soon as possible, providing them with the intended connectivity and functionality based on their chosen service plan.

For more information on how to activate the service for the subscriber. See [Activating and Deactivating the Service for the Subscriber \(on page 467\)](#).

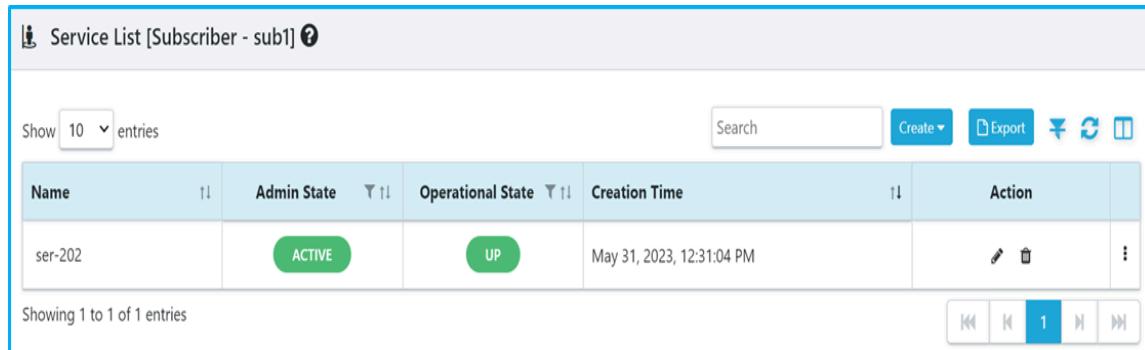
Verification

Verify that the service is activated for the subscriber.

1. Navigate to **Configuration > Subscriber > Service or Monitor > Services > Subscriber Service**.
2. Verify the admin and operational state of the service.

The **Operational State** for the service must be **UP**, indicating that the service is up and running for the subscriber, and the **Admin State** of the service must be **ACTIVE** indicating that the service is activated for the subscriber.

Figure 280. Subscriber Service Status



The screenshot shows a table titled "Service List [Subscriber - sub1]". The table has columns: Name, Admin State, Operational State, Creation Time, and Action. There is one entry: "ser-202" with Admin State "ACTIVE" and Operational State "UP". The Creation Time is "May 31, 2023, 12:31:04 PM". The Action column contains edit and delete icons. The table shows "Showing 1 to 1 of 1 entries".

| Name | Admin State | Operational State | Creation Time | Action |
|---------|-------------|-------------------|---------------------------|---|
| ser-202 | ACTIVE | UP | May 31, 2023, 12:31:04 PM |    |

3. Navigate to **Monitor > Events**.
4. Verify the SERVICE-UP event is reported in RMS to confirm the service activation for the subscriber is successful, or the service status is UP.

Related information

[Workflow for Activating a Service for the Subscriber \(on page 36\)](#)

Example: ONT Replacement

This example shows how to replace the ONT for the subscriber.

- [Overview \(on page 866\)](#)
- [ONT Replacement Workflow \(on page 866\)](#)
- [Configuration \(on page 867\)](#)
- [Verification \(on page 869\)](#)

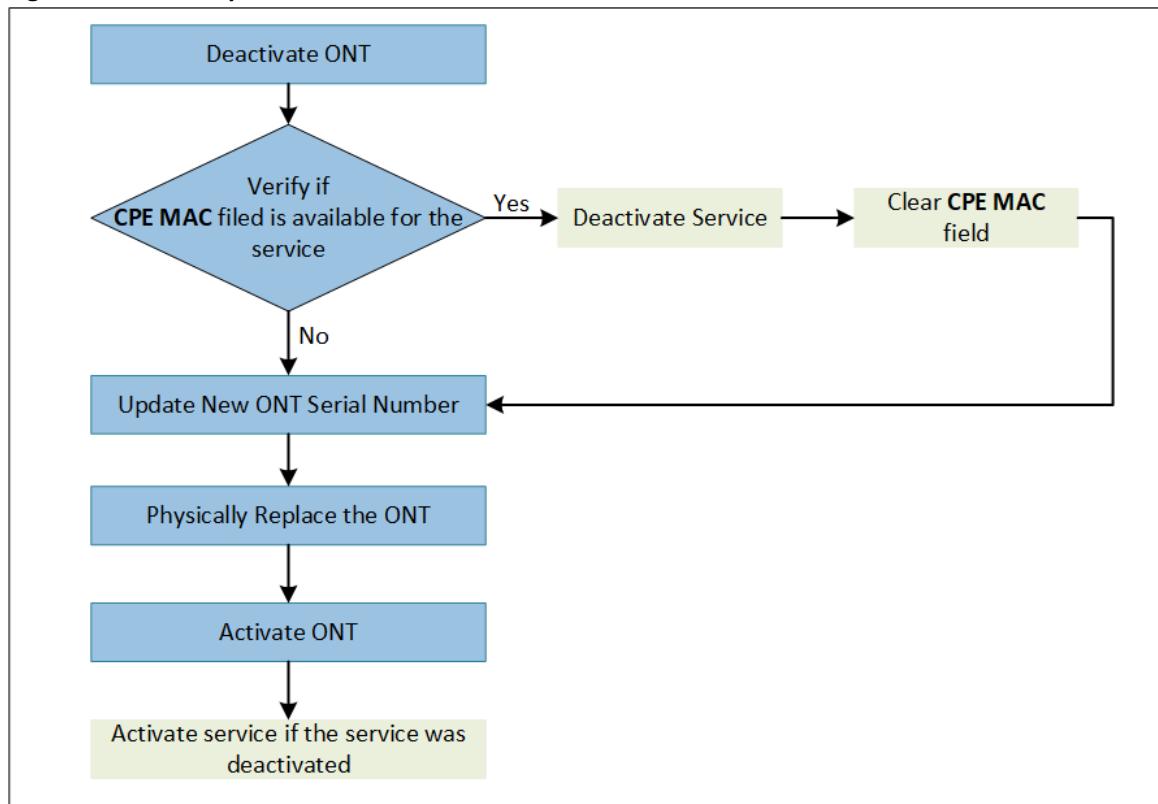
Overview

A user can replace the subscriber ONT if the ONT becomes non-functional due to hardware fault or any other reason.

ONT Replacement Workflow

The following diagram illustrates the workflow to replace the ONT for the subscriber.

Figure 281. ONT Replacement Workflow

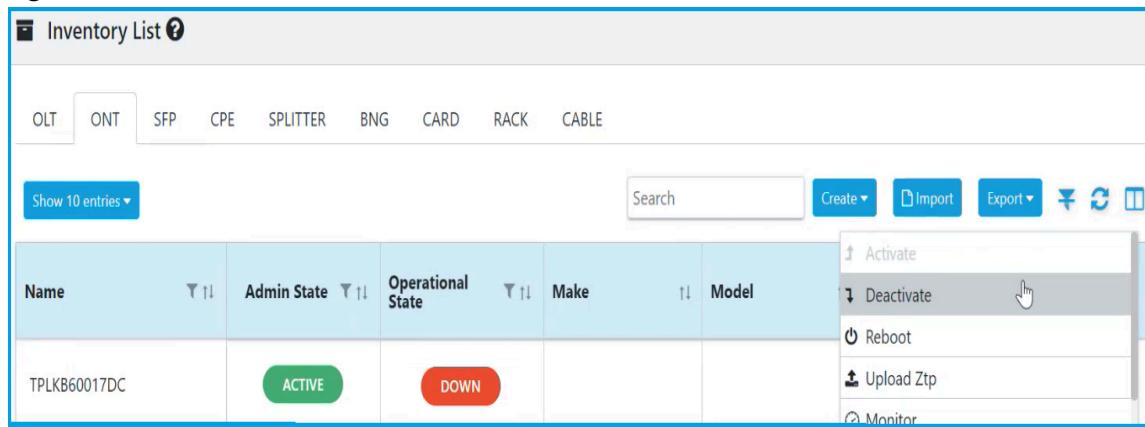


Configuration

This section covers the step-by-step procedure of ONT replacement.

1. Deactivate the ONT. See [Deactivating the ONT \(on page 431\)](#).

Figure 282. ONT Deactivation



2. Navigate to **Configuration > Subscriber > Service** and check if **CPE MAC** field is available.



Note: If **CPE MAC** field is not available, skip steps 3 (on page 868), 4 (on page 868), 5 (on page 868), and 9 (on page 869).

3. If **CPE MAC** field is available, deactivate the services attached to the ONT. See [Activating and Deactivating the Service for the Subscriber \(on page 467\)](#).

Figure 283. Deactivate Service

Service List [Subscriber - sub1]

Show 10 entries ▾

Search Create ▾

Actions

- Activate
- Deactivate (highlighted)
- Monitor
- Initiate Mac Dump
- Cancel Mac Dump
- Mac LookUp

| Name | Admin State | Operational State | Creation Time | Action |
|-------|-------------|-------------------|-------------------------|--|
| ser-1 | ACTIVE | DOWN | Feb 9, 2024, 9:18:10 AM | edit trash Mac LookUp |

Showing 1 to 1 of 1 entries

4. Clear the **CPE MAC** field for all the services.
5. Click **Save** to save the service configuration.
6. Edit ONT configuration and update the serial number for the new ONT. See [Common Operations \(on page 27\)](#).

Figure 284. New ONT Serial Number

ONT Configuration

OLT: olt-143 Port: SFPPON-11

Display Id: /rack=1/shelf=1/slot=LT-1/port=SFPON-11

Active Firmware Version: 1.22.0.033

Serial No. *: RDSYD9F27888

ONT Number: 1

Enable Time of Day: Select the option

Upstream FEC: ENABLED

Connectivity Mode: 1:MP map-filtering

Force Delete: FALSE

Mac Limit: 0

Close Save

7. Physically replace the faulty ONT with the new ONT.
8. Activate the new ONT. See [Activating the ONT \(on page 431\)](#).

Figure 285. Activate ONT

The screenshot shows the RMS 'Inventory List' for ONT devices. The table has columns for Name, Admin State, Operational State, Make, Model, Technology, and Display Id. One entry is visible: 'ont-202' with Admin State 'ACTIVE' and Operational State 'UP'. A context menu is open over this entry, with 'Activate' highlighted. Other options in the menu include 'Create', 'Deactivate', 'Reboot', 'Upload Ztp', 'Monitor', and a link to 'Logical Topology'.

- Activate all the services attached to the ONT if it is deactivated in step 3 (on page 868). See [Activating and Deactivating the Service for the Subscriber \(on page 467\)](#).

Verification

Verify the following.

Verify the ONT Activation

Perform the following steps to verify that the new ONT is active and up.

1. Navigate to **Configuration > Inventory > ONT**.
 2. Verify the admin and operational state of the ONT.
- The **Admin State** of the ONT must be **ACTIVE**, and the **Operational State** must be **UP**.

Figure 286. ONT Status

The screenshot shows the RMS 'Inventory List' for ONT devices. The table has columns for Name, Admin State, Operational State, Make, Model, Technology, Display Id, Serial No., and Action. One entry is visible: 'RDSYD9F2A274' with Admin State 'ACTIVE' and Operational State 'UP'. The 'Action' column for this entry contains a link to 'Logical Topology'.

3. Verify the ONT-UP event is reported in RMS to confirm that the ONT activation is successful.

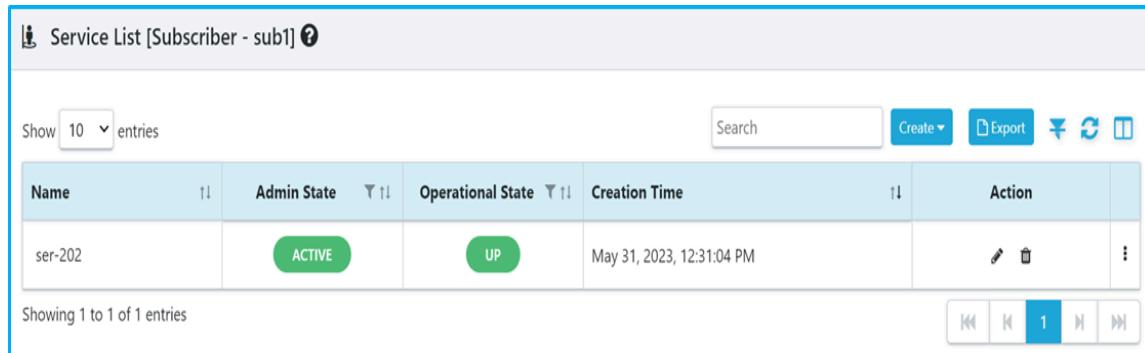
Verify the Service Activation

Perform the following steps to verify that the service is activated for the subscriber after activating the ONT.

1. Navigate to **Configuration > Subscriber > Service or Monitor > Services > Subscriber Service**.
2. Verify the admin and operational state of the service.

The **Operational State** for the service must be **UP**, and the **Admin State** of the service must be **ACTIVE** indicating that the service is activated for the subscriber.

Figure 287. Subscriber Service Status



| Name | Admin State | Operational State | Creation Time | Action |
|---------|-------------|-------------------|---------------------------|---|
| ser-202 | ACTIVE | UP | May 31, 2023, 12:31:04 PM |    |

3. Navigate to **Monitor > Events**.
4. Verify the SERVICE-UP event is reported in RMS to confirm the service activation for the subscriber is successful, or the service status is UP.

Example: Movement of ONT

This example shows how to move the ONT from one PON port to another PON port.

- [Overview \(on page 870\)](#)
- [ONT Movement Workflow \(on page 871\)](#)
- [Prerequisites \(on page 871\)](#)
- [Configuration \(on page 871\)](#)
- [Verification \(on page 872\)](#)

Overview

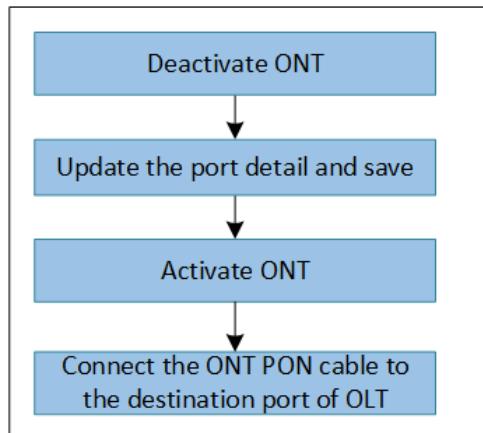
A user can move the subscriber services attached to the ONT from one PON port to another PON port under the same OLT. This is required when the PON port becomes non-functional due to SFP failure, PON hardware fault, or other reasons.

The ONT movement from one PON port to another PON is supported only within the same OLT. The failed and the new PON port must belong to the same OLT.

ONT Movement Workflow

The following diagram illustrates the workflow to move the ONT from one PON port to another PON port.

Figure 288. ONT Movement



Prerequisites

The following prerequisites must be fulfilled before the ONT movement.

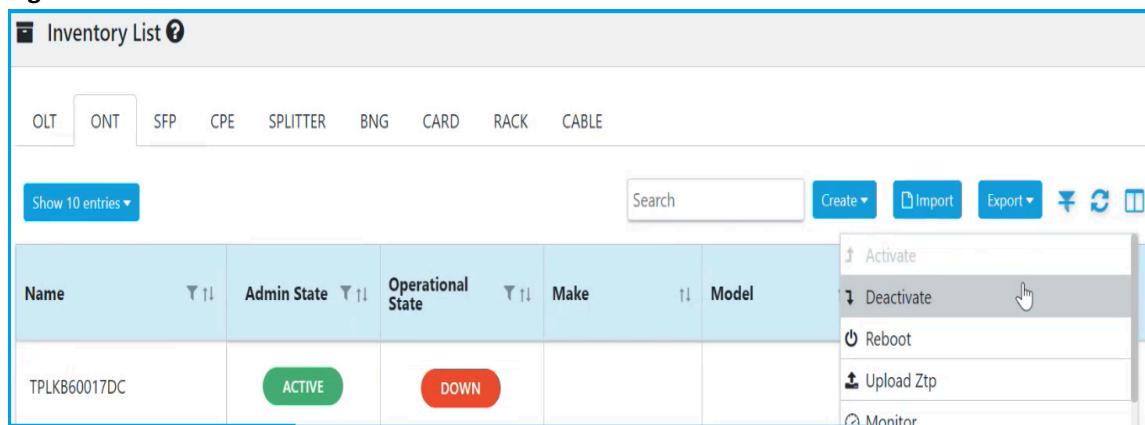
- The source PON port must be in a **DEACTIVE** state and the destination PON port must be in **ACTIVE** state.
- The source and destination PON ports must be in the same mode. For example, GPON, XGSPON, or CPON.

Configuration

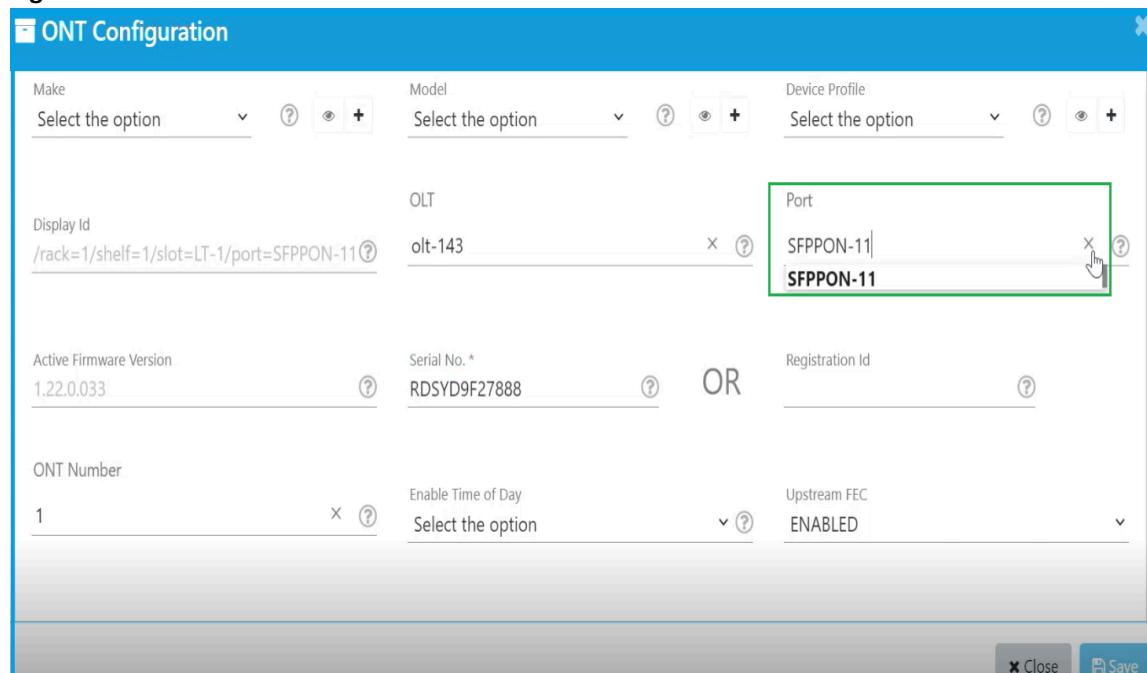
This section involves the steps to move the ONT from one PON port to another PON port.

1. Deactivate the ONT. See [Deactivating the ONT \(on page 431\)](#).

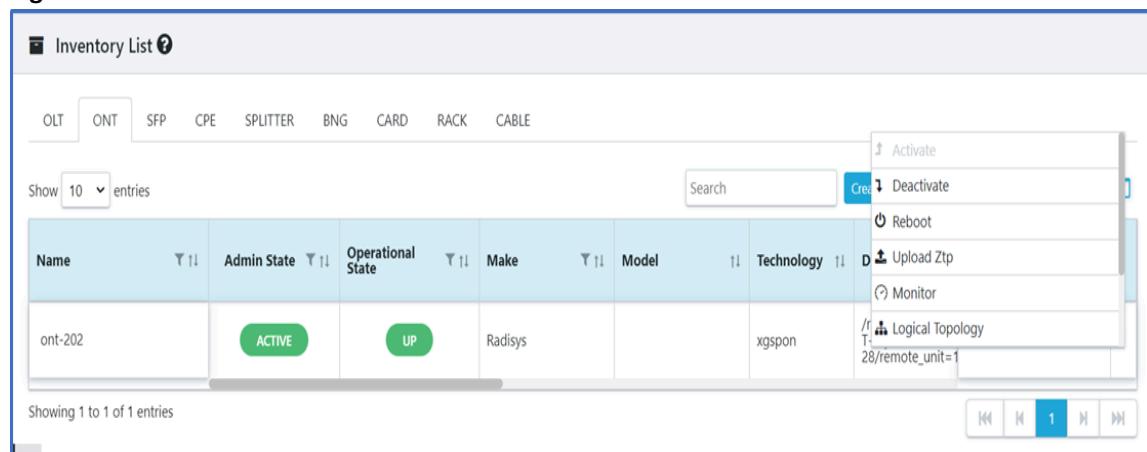
Figure 289. ONT Deactivation



2. Edit the **ONT Configuration** and update the port number to which you want to move the ONT. See [Common Operations \(on page 27\)](#).

Figure 290. Edit Port Number

3. Click **Save**.
4. Activate the ONT. See [Activating the ONT \(on page 431\)](#).

Figure 291. Activate ONT

5. Disconnect the ONT PON cable from the source port and connect it to the destination port of the OLT.



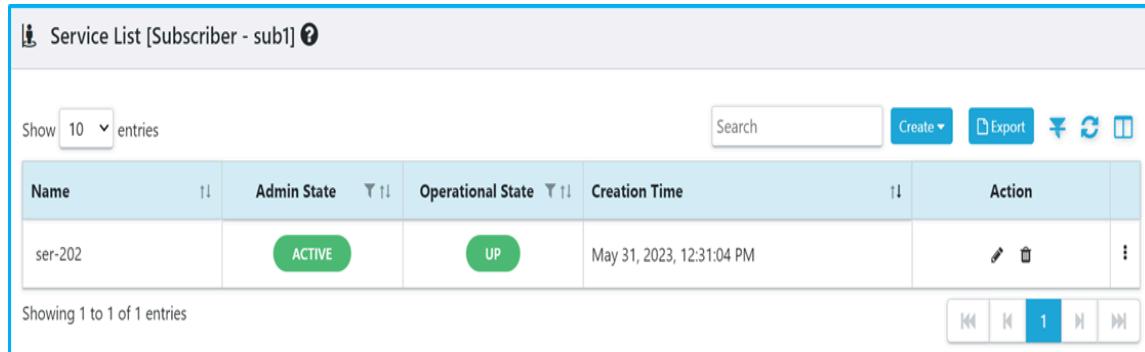
Note: You must perform this step where the OLT is located.

Verification

After connecting the ONT to the new PON port and activating the PON port, verify that the subscriber's service is activated.

1. Navigate to **Configuration > Subscriber > Service** or **Monitor > Services > Subscriber Service**.
2. Verify the admin and operational state of the service.
The **Operational State** for the service must be **UP**, and the **Admin State** of the service must be **ACTIVE** indicates that the service is activated for the subscriber.

Figure 292. Subscriber Service Status



The screenshot shows a table titled "Service List [Subscriber - sub1]". The table has columns: Name, Admin State, Operational State, Creation Time, and Action. There is one entry: "ser-202" with Admin State "ACTIVE" and Operational State "UP". The Creation Time is "May 31, 2023, 12:31:04 PM". The Action column contains icons for edit, delete, and more. The top of the table has a search bar, a "Create" button, and "Export" options. The bottom of the table shows "Showing 1 to 1 of 1 entries".

| Name | Admin State | Operational State | Creation Time | Action |
|---------|-------------|-------------------|---------------------------|---|
| ser-202 | ACTIVE | UP | May 31, 2023, 12:31:04 PM |    |

3. Navigate to **Monitor > Events**.
4. Verify the SERVICE-UP event is reported in RMS to confirm the service activation for the subscriber is successful, or the service status is UP.

Example: OLT Pre-Configuration

This example shows how to pre-configure the OLT for the subscriber.

- [Overview \(on page 873\)](#)
- [OLT Pre-Configuration Workflow \(on page 873\)](#)
- [Configuration \(on page 874\)](#)
- [Verification \(on page 884\)](#)

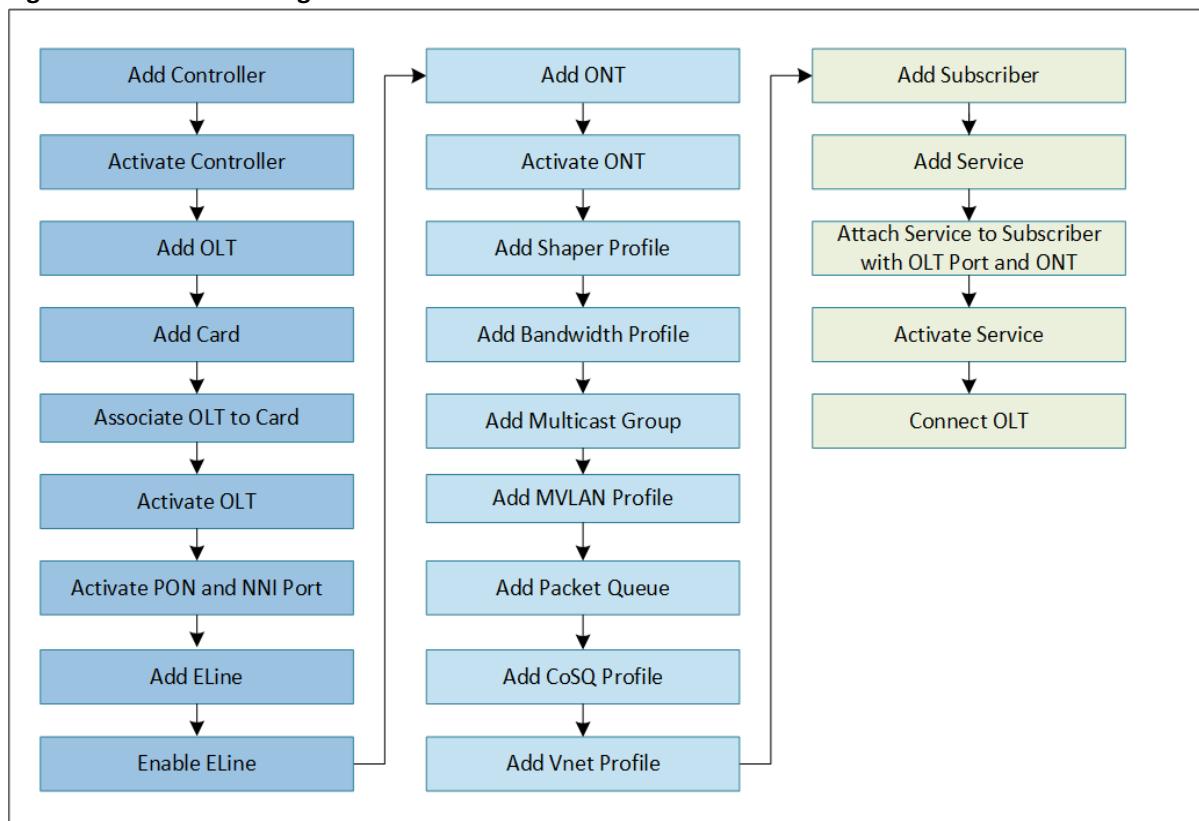
Overview

A user must complete all the configuration related to the OLT before adding the OLT to the network. The service comes up once the OLT is connected to the network.

OLT Pre-Configuration Workflow

The following diagram illustrates the workflow to pre-configure the OLT for the subscriber.

Figure 293. OLT Pre-Configuration Workflow



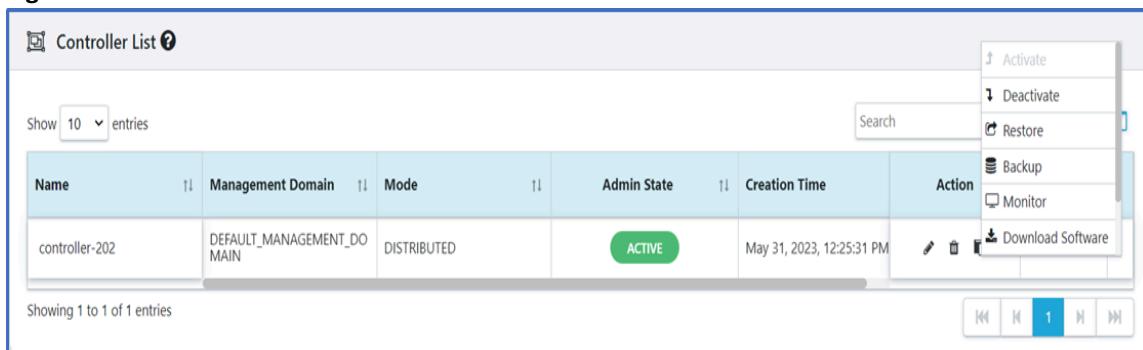
Configuration

This section covers the step-by-step procedure to pre-configure the OLT.

1. Create a controller configuration. See [Creating Controller Configuration \(on page 297\)](#).

Figure 294. Controller Configuration

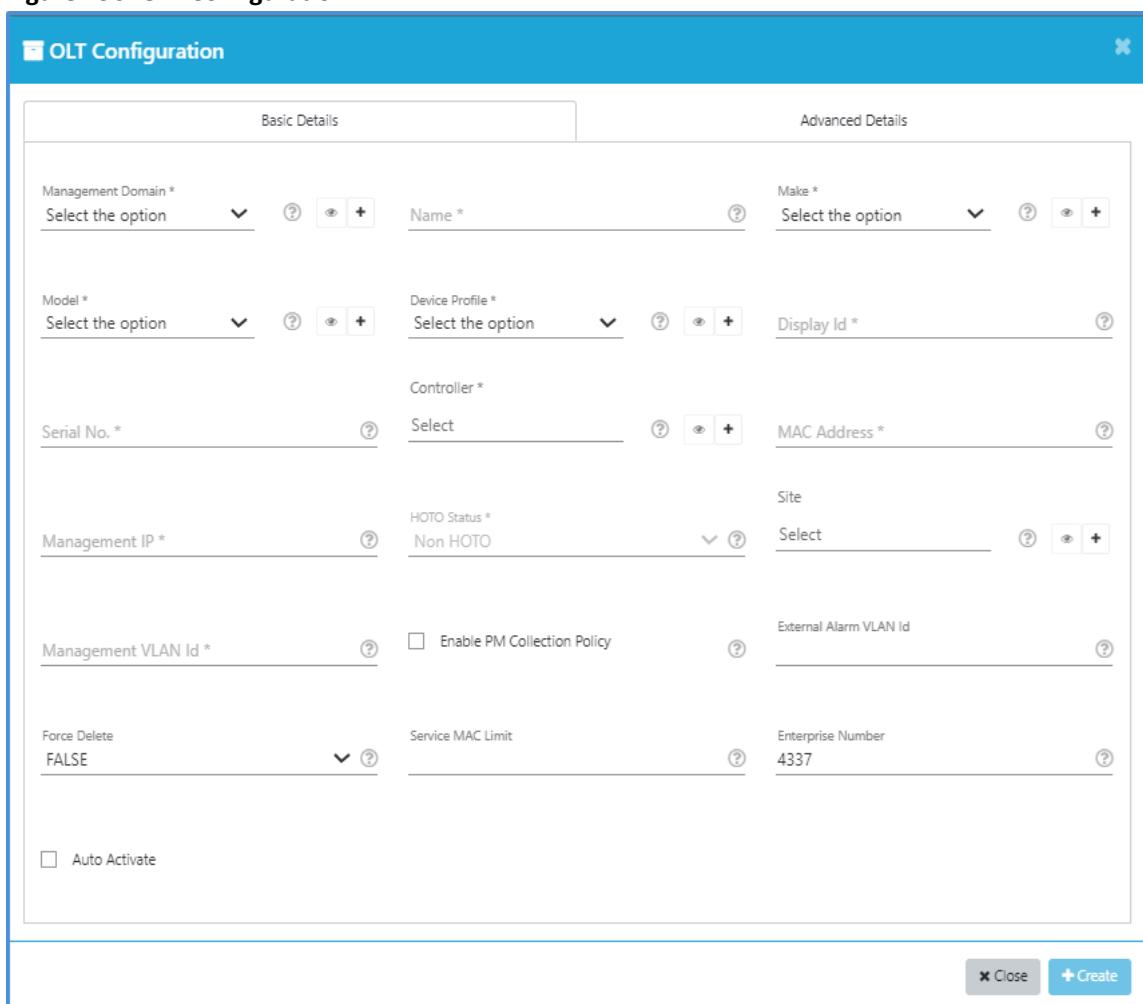
2. Activate a controller. See [Activating the Controller \(on page 305\)](#).

Figure 295. Activate Controller

| Name | Management Domain | Mode | Admin State | Creation Time | Action |
|----------------|---------------------------|-------------|-------------|---------------------------|--------|
| controller-202 | DEFAULT_MANAGEMENT_DOMAIN | DISTRIBUTED | ACTIVE | May 31, 2023, 12:25:31 PM | |

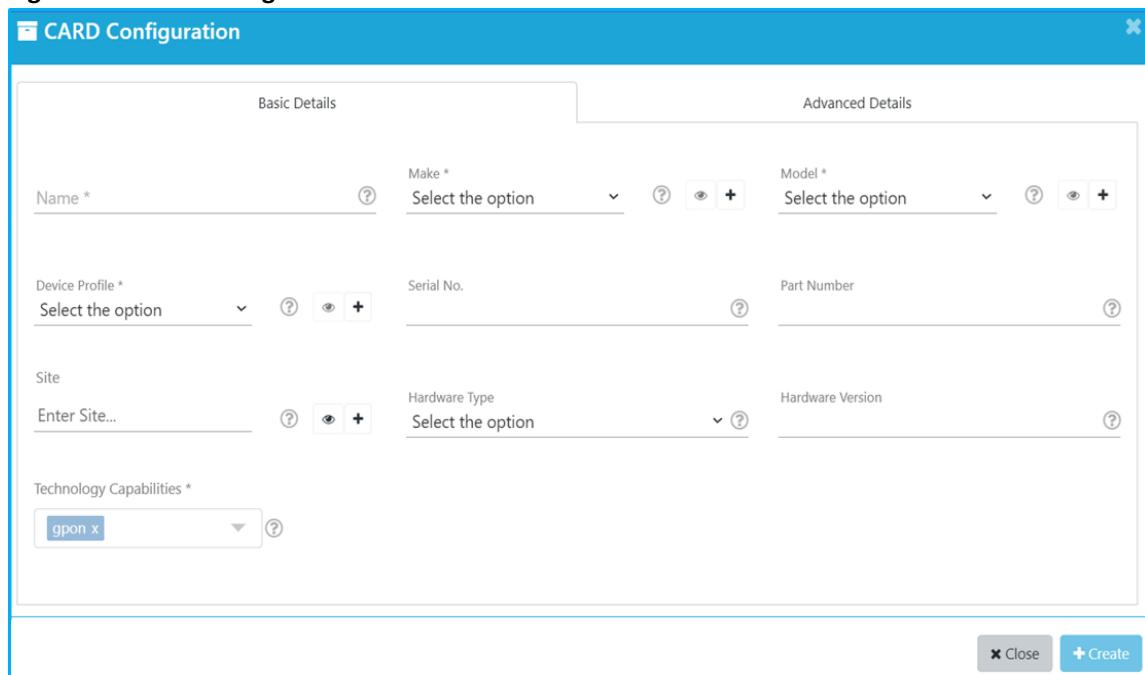
Showing 1 to 1 of 1 entries

3. Create an OLT. See [Creating OLT Configuration \(on page 318\)](#).

Figure 296. OLT Configuration

| | | | |
|--|--|-------------------|------------------------|
| Basic Details | | Advanced Details | |
| Management Domain * | Select the option | Name * | Make * |
| Model * | Select the option | Device Profile * | Display Id * |
| Serial No. * | Select | Controller * | MAC Address * |
| Management IP * | Non HOTO | Site | External Alarm VLAN Id |
| Management VLAN Id * | <input type="checkbox"/> Enable PM Collection Policy | Service MAC Limit | Enterprise Number |
| Force Delete | FALSE | 4337 | |
| <input type="checkbox"/> Auto Activate | | | |

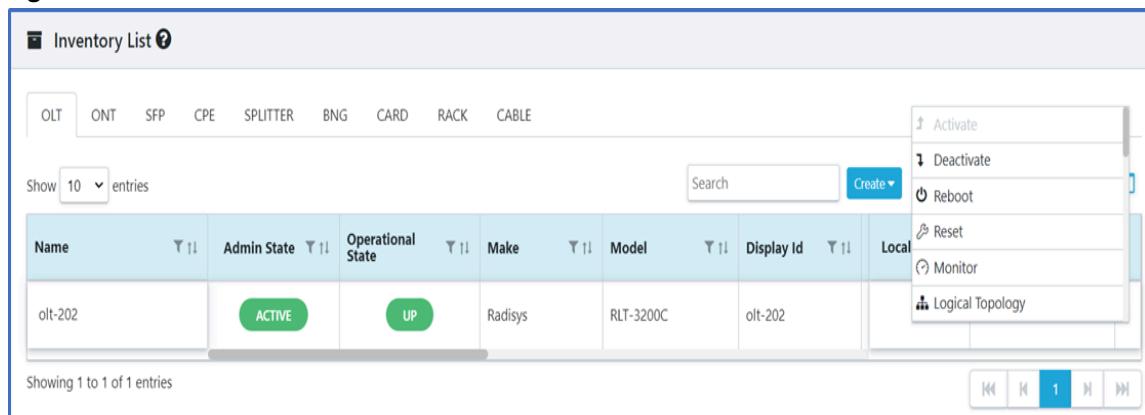
4. Create a card. See [Creating Card Configuration \(on page 444\)](#).

Figure 297. Card Configuration

| | | | |
|---------------------------|-------------------|-------------------|--|
| Basic Details | | Advanced Details | |
| Name * | Make * | Model * | |
| gpon x | Select the option | Select the option | |
| Device Profile * | Serial No. | Part Number | |
| Enter Site... | Hardware Type | Hardware Version | |
| Technology Capabilities * | | | |
| gpon x | | | |

Close **Create**

5. Associate the applicable OLT to the CARD. See [Creating Card Configuration \(on page 444\)](#).
6. Activate the OLT. See [Activating and Deactivating the OLT \(on page 324\)](#).

Figure 298. Activate OLT

| OLT | ONT | SFP | CPE | SPLITTER | BNG | CARD | RACK | CABLE |
|-----------------|--------|-----|---------|-----------|---------|------|------|-------|
| Show 10 entries | | | | | | | | |
| olt-202 | ACTIVE | UP | Radisys | RLT-3200C | olt-202 | | | |

Showing 1 to 1 of 1 entries

Activate
Deactivate
Reboot
Reset
Monitor
Logical Topology

7. Activate the PON and NNI port. See [Activating the PON and NNI Port \(on page 380\)](#).

Figure 299. Activate PON and NNI Port

| Ports List [Inventory - olt-202] | | | | | | |
|------------------------------------|-------------|-------------------|----------|--------------------------------------|---------------------------------------|--|
| Name | Admin State | Operational State | Media | Display Id | Action | |
| SFPPON-3 | DEACTIVE | UNKNOWN | PON | /rack=1/shelf=1/slot=LT-1/port=SFP1 | Activate | |
| SFPPON-2 | ACTIVE | DOWN | PON | /rack=1/shelf=1/slot=LT-1/port=SFP2 | Deactivate | |
| SFPPON-1 | DEACTIVE | UNKNOWN | PON | /rack=1/shelf=1/slot=LT-1/port=SFP1 | Logical Topology | |
| NNI-8 | ACTIVE | DOWN | ETHERNET | /rack=1/shelf=1/slot=LT-1/port=NNI-8 | Physical Link | |
| NNI-7 | ACTIVE | DOWN | ETHERNET | /rack=1/shelf=1/slot=LT-1/port=NNI-7 | Enable ONT Serial Number | |
| NNI-6 | ACTIVE | DOWN | ETHERNET | /rack=1/shelf=1/slot=LT-1/port=NNI-6 | Monitor | |
| NNI-5 | ACTIVE | DOWN | ETHERNET | /rack=1/shelf=1/slot=LT-1/port=NNI-5 | Monitor | |

8. Create a ELine. See [Creating ELine Configuration \(on page 332\)](#).

Figure 300. ELine Configuration

ELine Configuration

Name *

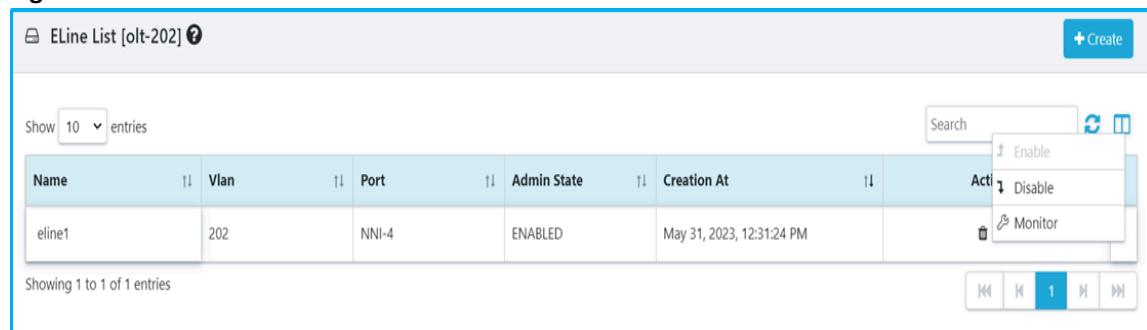
VLan Id *

Port *

NNI-2

Close Create

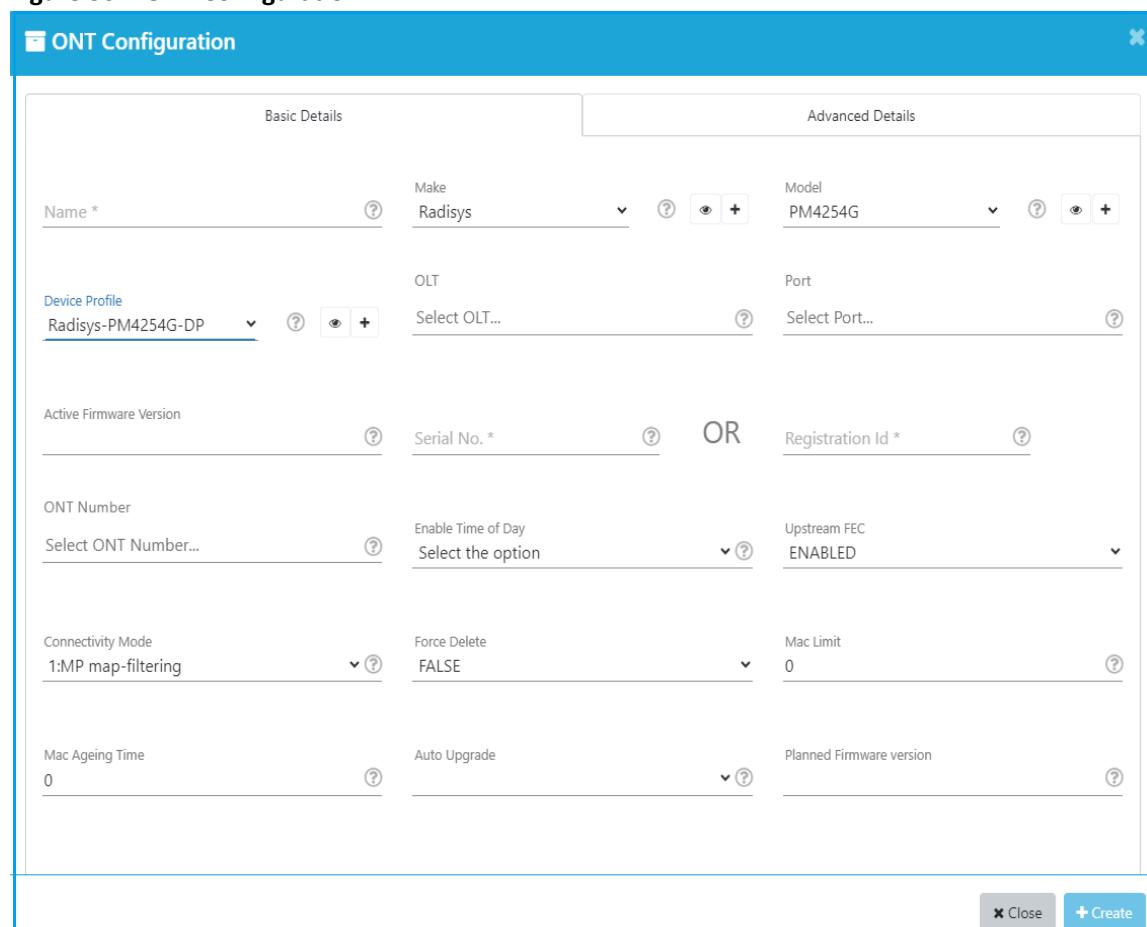
9. Enable ELine. See [Enabling and Disabling ELine Configuration \(on page 333\)](#).

Figure 301. Enable ELine

The screenshot shows a table titled "ELine List [olt-202]". The table has columns: Name, Vlan, Port, Admin State, Creation At, and Action. There is one entry: eLine1, Vlan 202, Port NNI-4, Admin State ENABLED, Creation At May 31, 2023, 12:31:24 PM. The Action column shows buttons for "Enable", "Disable", and "Monitor". The table has a "Search" field and a "Create" button in the top right. The bottom shows "Showing 1 to 1 of 1 entries".

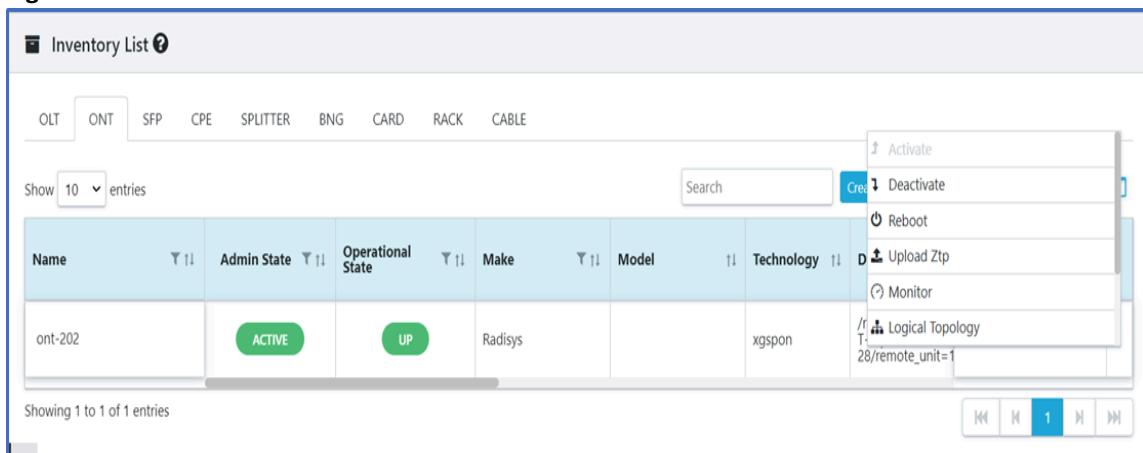
| Name | Vlan | Port | Admin State | Creation At | Action |
|--------|------|-------|-------------|---------------------------|---|
| eLine1 | 202 | NNI-4 | ENABLED | May 31, 2023, 12:31:24 PM |    |

10. Create an ONT Configuration. See [Creating ONT Configuration \(on page 427\)](#).

Figure 302. ONT Configuration

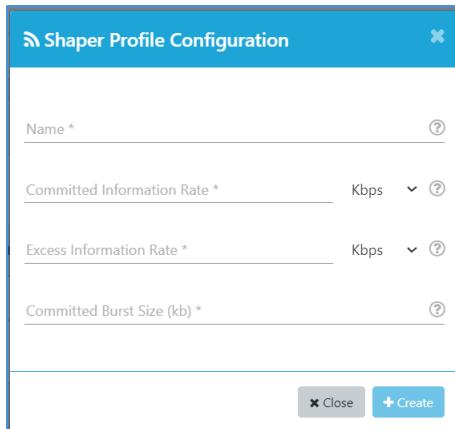
The screenshot shows the "ONT Configuration" dialog box. It has tabs for "Basic Details" and "Advanced Details". The "Basic Details" tab is active. It contains fields for Name (eLine1), Make (Radisys), Model (PM4254G), Device Profile (Radisys-PM4254G-DP), OLT (Select OLT...), Port (Select Port...), Active Firmware Version, Serial No. *, Registration Id *, ONT Number (Select ONT Number...), Enable Time of Day (Select the option), Upstream FEC (ENABLED), Connectivity Mode (1:MP map-filtering), Force Delete (FALSE), Mac Limit (0), Mac Ageing Time (0), Auto Upgrade, and Planned Firmware version. There are "OR" and "Close" buttons at the bottom.

11. Activate the ONT. See [Activating the ONT \(on page 431\)](#).

Figure 303. Activate ONT

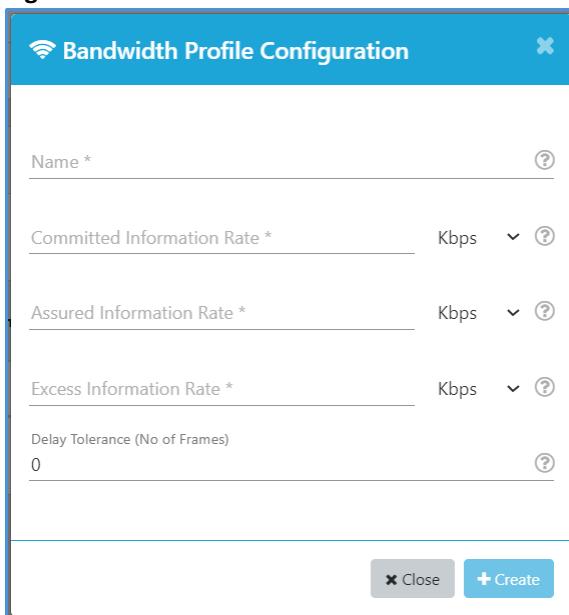
The screenshot shows the Radisys Inventory List interface. At the top, there are tabs for OLT, ONT, SFP, CPE, SPLITTER, BNG, CARD, RACK, and CABLE. The ONT tab is selected. Below the tabs, there is a search bar and a dropdown to 'Show 10 entries'. A context menu is open for the first entry, 'ont-202', which includes options: Activate, Deactivate, Reboot, Upload Ztp, Monitor, and Logical Topology (with a parameter '28/remote_unit=1'). The table columns are Name, Admin State, Operational State, Make, Model, and Technology. The entry 'ont-202' has Admin State as ACTIVE and Operational State as UP. The Make is Radisys, Model is xgspon, and Technology is not explicitly listed. At the bottom, it says 'Showing 1 to 1 of 1 entries'.

12. Create a shaper profile. See [Creating Shaper Profile \(on page 567\)](#).

Figure 304. Shaper Profile

The screenshot shows the 'Shaper Profile Configuration' dialog box. It has fields for 'Name *' (with a question mark icon), 'Committed Information Rate *' (with a dropdown for Kbps), 'Excess Information Rate *' (with a dropdown for Kbps), and 'Committed Burst Size (kb) *' (with a question mark icon). At the bottom, there are 'Close' and 'Create' buttons.

13. Create a bandwidth profile. See [Creating Bandwidth Profile \(on page 564\)](#).

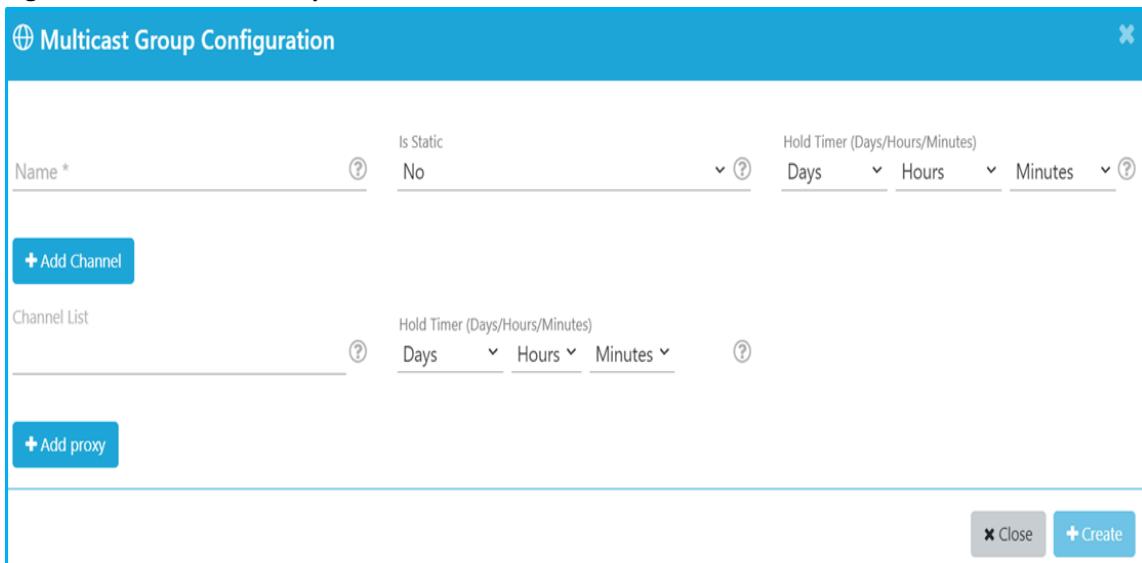
Figure 305. Bandwidth Profile

The dialog box is titled "Bandwidth Profile Configuration". It contains the following fields:

- Name *: A text input field with a question mark icon.
- Committed Information Rate *: A text input field followed by "Kbps" and a dropdown menu, with a question mark icon.
- Assured Information Rate *: A text input field followed by "Kbps" and a dropdown menu, with a question mark icon.
- Excess Information Rate *: A text input field followed by "Kbps" and a dropdown menu, with a question mark icon.
- Delay Tolerance (No of Frames): A text input field with a value "0" and a question mark icon.

At the bottom are two buttons: "Close" and "Create".

14. Create a multicast group. See [Creating Multicast Group \(on page 567\)](#).

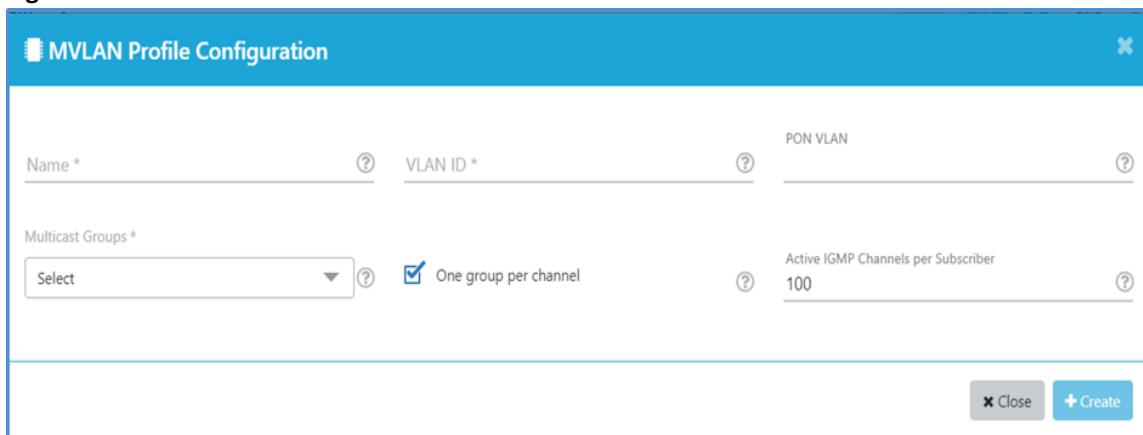
Figure 306. Multicast Group

The dialog box is titled "Multicast Group Configuration". It contains the following fields:

- Name *: A text input field with a question mark icon.
- Is Static: A dropdown menu with the value "No" and a question mark icon.
- Hold Timer (Days/Hours/Minutes): A dropdown menu with sub-options "Days", "Hours", and "Minutes" and a question mark icon.
- + Add Channel: A blue button.
- Channel List: A text input field with a question mark icon.
- Hold Timer (Days/Hours/Minutes): A dropdown menu with sub-options "Days", "Hours", and "Minutes" and a question mark icon.
- + Add proxy: A blue button.

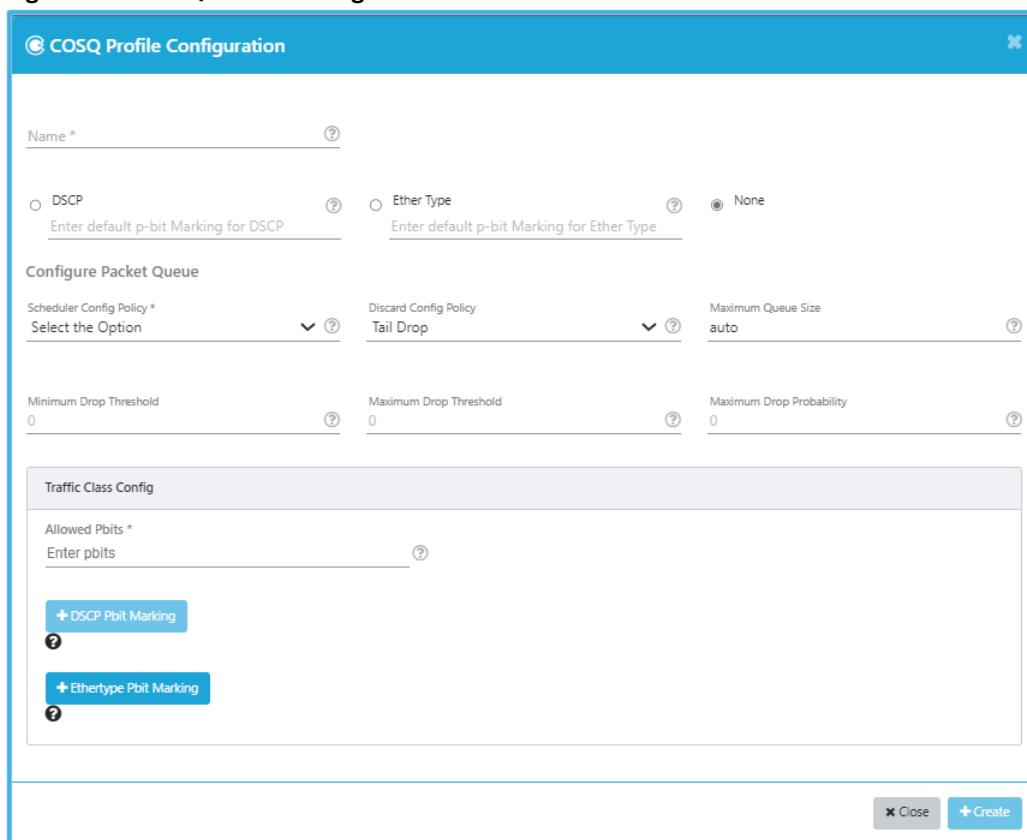
At the bottom are two buttons: "Close" and "Create".

15. Create a multicast VLAN (MVLAN) profile. See [Creating MVLAN Profile \(on page 568\)](#).

Figure 307. MVLAN Profile

The dialog box is titled "MVLAN Profile Configuration". It contains fields for "Name" (with a required asterisk), "VLAN ID" (with a required asterisk), and "PON VLAN" (with a question mark icon). Below these are sections for "Multicast Groups" (a dropdown menu with "Select" and a checkbox for "One group per channel") and "Active IGMP Channels per Subscriber" (set to 100). At the bottom are "Close" and "Create" buttons.

16. Create a Class of Service Queue (CoSQ) profile. See [Creating COSQ Profile \(on page 570\)](#).

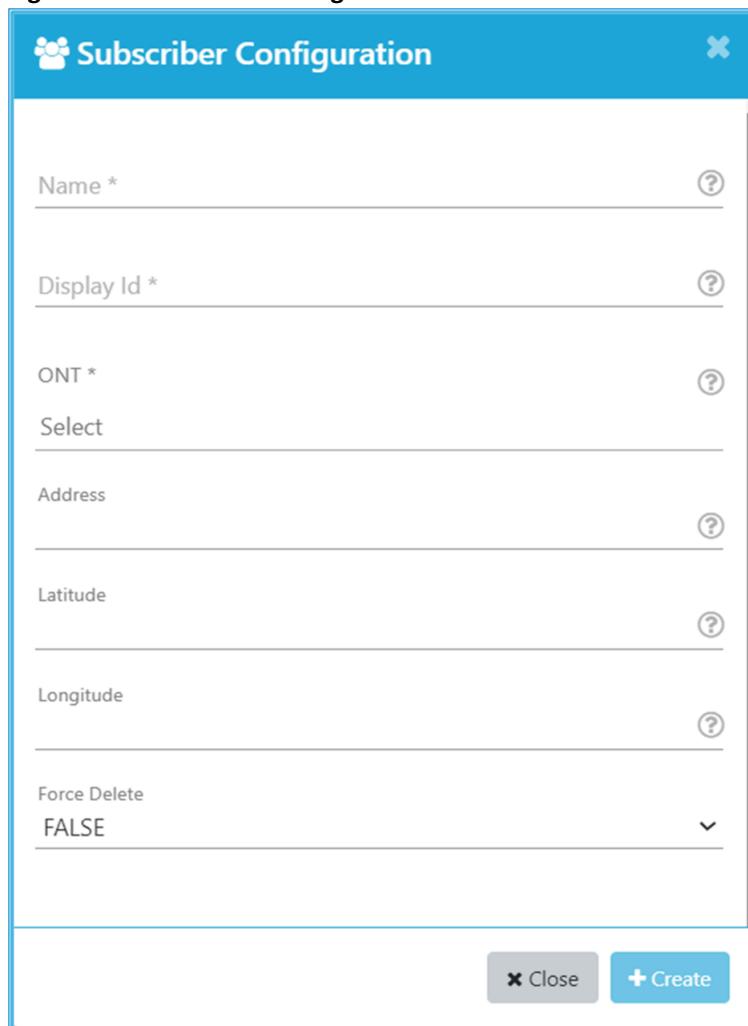
Figure 308. CoSQ Profile Configuration

The dialog box is titled "COSQ Profile Configuration". It includes fields for "Name" (with a required asterisk), "DSCP" (radio button, with "Enter default p-bit Marking for DSCP" below), "Ether Type" (radio button, with "Enter default p-bit Marking for Ether Type" below), and "None" (radio button). A "Configure Packet Queue" section contains "Scheduler Config Policy" (dropdown with "Select the Option"), "Discard Config Policy" (dropdown with "Tail Drop"), and "Maximum Queue Size" (set to "auto"). Below this are "Minimum Drop Threshold" (0), "Maximum Drop Threshold" (0), and "Maximum Drop Probability" (0). A "Traffic Class Config" section contains "Allowed Pbits" (with "Enter pbits" below) and two buttons: "+ DSCP Pbit Marking" and "+ Ethertype Pbit Marking". At the bottom are "Close" and "Create" buttons.

17. Create a VNet profile. See [Creating VNet Profile \(on page 577\)](#).

Figure 309. VNet Profile Configuration

18. Create a subscriber. See [Creating Subscriber \(on page 455\)](#).

Figure 310. Subscriber Configuration

The image shows a 'Subscriber Configuration' dialog box with a blue header and a white body. The header contains a 'Subscriber Configuration' title and a close button. The body contains several input fields: 'Name *' (with a question mark icon), 'Display Id *' (with a question mark icon), 'ONT *' (with a question mark icon), 'Select' (a dropdown menu), 'Address' (with a question mark icon), 'Latitude' (with a question mark icon), 'Longitude' (with a question mark icon), and 'Force Delete' (a dropdown menu set to 'FALSE'). At the bottom are 'Close' and 'Create' buttons.

| Subscriber Configuration | |
|--|---|
| Name * | (?) |
| Display Id * | (?) |
| ONT * | (?) |
| Select | (dropdown menu) |
| Address | (?) |
| Latitude | (?) |
| Longitude | (?) |
| Force Delete | (dropdown menu) FALSE |
| | |
| <input type="button" value="x Close"/> | <input type="button" value="+ Create"/> |

19. Create a service. See [Creating Service \(on page 459\)](#).

Figure 311. Service Configuration

- Activate the service for the subscriber. See [Activating and Deactivating the Service for the Subscriber \(on page 467\)](#).
- Connect to the OLT.

Verification

Verify the OLT Activation

Perform the following steps to verify that the OLT is active and up.

- Navigate to **Configuration > Inventory > OLT**.
 - Verify the admin and operational state of the OLT.
- The **Admin State** of the OLT must be **ACTIVE**, and the **Operational State** must be **UP**.

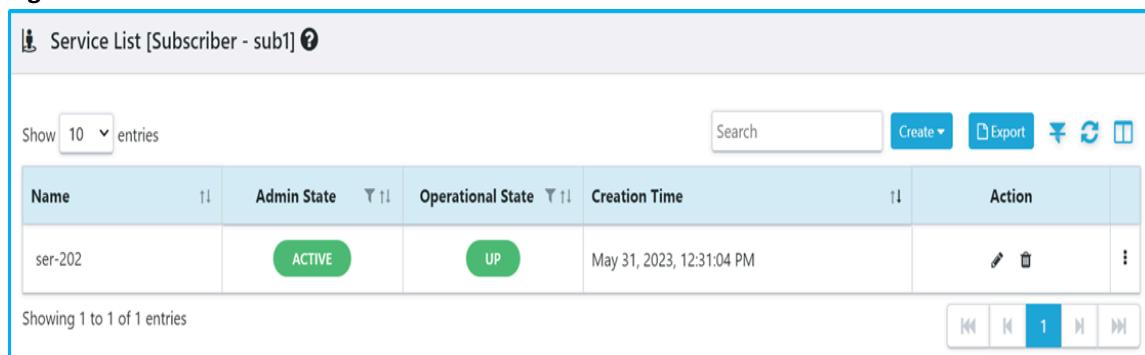
Figure 312. OLT Status

Verify the Service Activation

Perform the following steps to verify that the service is activated for the subscriber.

1. Navigate to **Configuration > Subscriber > Service or Monitor > Services > Subscriber Service**.
2. Verify the admin and operational state of the service.
The **Operational State** for the service must be **UP**, indicating that the service is up and running for the subscriber, and the **Admin State** of the service must be **ACTIVE** indicating that the service is activated for the subscriber.

Figure 313. Subscriber Service Status



The screenshot shows a table titled 'Service List [Subscriber - sub1]'. The table has columns: Name, Admin State, Operational State, Creation Time, and Action. There is one entry: 'ser-202' with Admin State 'ACTIVE' and Operational State 'UP'. The Creation Time is 'May 31, 2023, 12:31:04 PM'. The Action column contains icons for edit, delete, and more. The top of the table has a search bar, a 'Create' button, and export options. The bottom of the table shows 'Showing 1 to 1 of 1 entries'.

| Name | Admin State | Operational State | Creation Time | Action |
|---------|-------------|-------------------|---------------------------|---|
| ser-202 | ACTIVE | UP | May 31, 2023, 12:31:04 PM |    |

3. Navigate to **Monitor > Events**.
4. Verify the SERVICE-UP event is reported in RMS to confirm the service activation for the subscriber is successful, or the service status is UP.

Example: Pre-Provision of ONT

This example shows how to pre-provision the ONT for the subscriber.

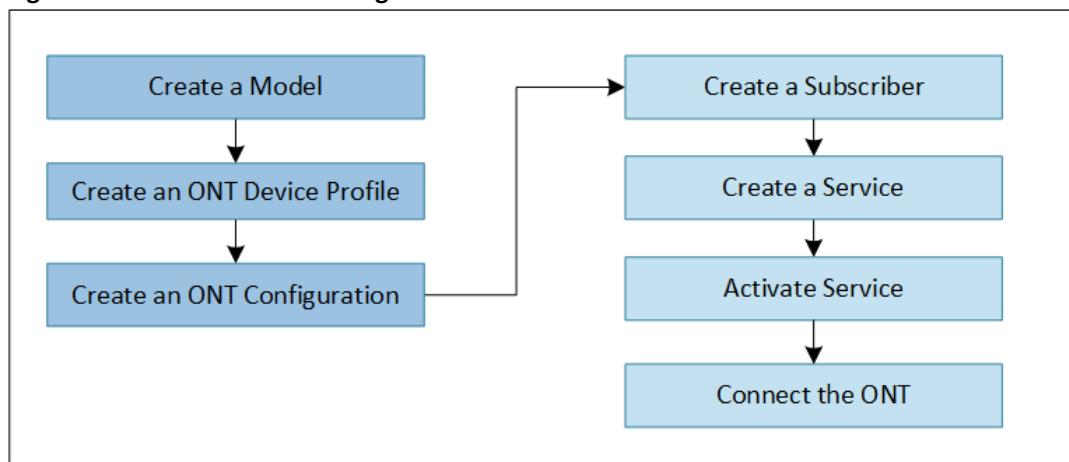
- [Overview \(on page 885\)](#)
- [Pre-provisioning Workflow \(on page 885\)](#)
- [Prerequisites \(on page 886\)](#)
- [Configuration \(on page 886\)](#)
- [Verification \(on page 890\)](#)

Overview

A user must complete all the configuration related to the ONT before adding the ONT to the network. The service comes up once the ONT is connected to the network.

Pre-provisioning Workflow

The following diagram illustrates the workflow to pre-provision the ONT for the subscriber.

Figure 314. ONT Pre-Provisioning Workflow

Prerequisites

The following configurations must be known before pre-provisioning the ONT.

- ONT Make and Model
- ONT Serial Number
- The plan purchased by the customer

Configuration

This section involves the configuration steps to pre-provision the ONT.

1. Create a model configuration for the ONT. See [Creating Model Configuration \(on page 610\)](#).



Note: You can use the existing model configuration or create a custom configuration.

Figure 315. Model Configuration

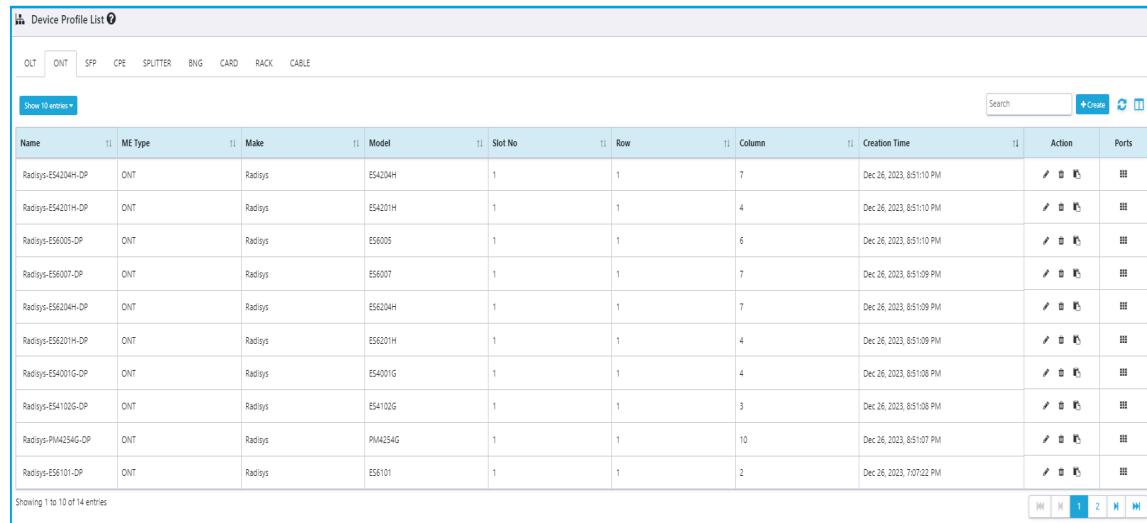
The screenshot shows the 'Model Configuration' dialog box. It has fields for 'Name *' (with a question mark icon), 'Type *' (a dropdown menu with 'Select the option' and a question mark icon), and 'Make *' (a text input field with 'Enter Make...' and a question mark icon). At the bottom are 'Close' and 'Create' buttons.

2. Create an ONT device profile. See [Creating ONT Device Profile \(on page 515\)](#).



Note: You can use the existing profile or create a custom ONT device profile. If you are creating a custom ONT device profile, create the applicable ports associated with the ONT device profile.

Figure 316. ONT Device Profile



The screenshot shows a web-based interface for managing device profiles. At the top, there is a navigation bar with tabs: OLT, ONT (which is selected), SFP, CPE, SPLITTER, BNG, CARD, RACK, and CABLE. Below the tabs, there is a search bar and a 'Create' button. The main area is a table titled 'Device Profile List' with the following columns: Name, ME Type, Make, Model, Slot No, Row, Column, Creation Time, Action, and Ports. The table contains 10 entries, each representing an ONT device profile. The entries are as follows:

| Name | ME Type | Make | Model | Slot No | Row | Column | Creation Time | Action | Ports |
|--------------------|---------|---------|---------|---------|-----|--------|--------------------------|--------|-------|
| Radisys-ES4204H-DP | ONT | Radisys | ES4204H | 1 | 1 | 7 | Dec 26, 2023, 8:51:10 PM | | |
| Radisys-ES4201H-DP | ONT | Radisys | ES4201H | 1 | 1 | 4 | Dec 26, 2023, 8:51:10 PM | | |
| Radisys-ES6005-DP | ONT | Radisys | ES6005 | 1 | 1 | 6 | Dec 26, 2023, 8:51:10 PM | | |
| Radisys-ES6007-DP | ONT | Radisys | ES6007 | 1 | 1 | 7 | Dec 26, 2023, 8:51:09 PM | | |
| Radisys-ES6204H-DP | ONT | Radisys | ES6204H | 1 | 1 | 7 | Dec 26, 2023, 8:51:09 PM | | |
| Radisys-ES6201H-DP | ONT | Radisys | ES6201H | 1 | 1 | 4 | Dec 26, 2023, 8:51:09 PM | | |
| Radisys-ES4001G-DP | ONT | Radisys | ES4001G | 1 | 1 | 4 | Dec 26, 2023, 8:51:08 PM | | |
| Radisys-ES4102G-DP | ONT | Radisys | ES4102G | 1 | 1 | 3 | Dec 26, 2023, 8:51:08 PM | | |
| Radisys-PM4254G-DP | ONT | Radisys | PM4254G | 1 | 1 | 10 | Dec 26, 2023, 8:51:07 PM | | |
| Radisys-ES6101-DP | ONT | Radisys | ES6101 | 1 | 1 | 2 | Dec 26, 2023, 7:07:22 PM | | |

3. Create an ONT Configuration by selecting Make, Model, and Device Profile. See [Creating ONT Configuration \(on page 427\)](#).

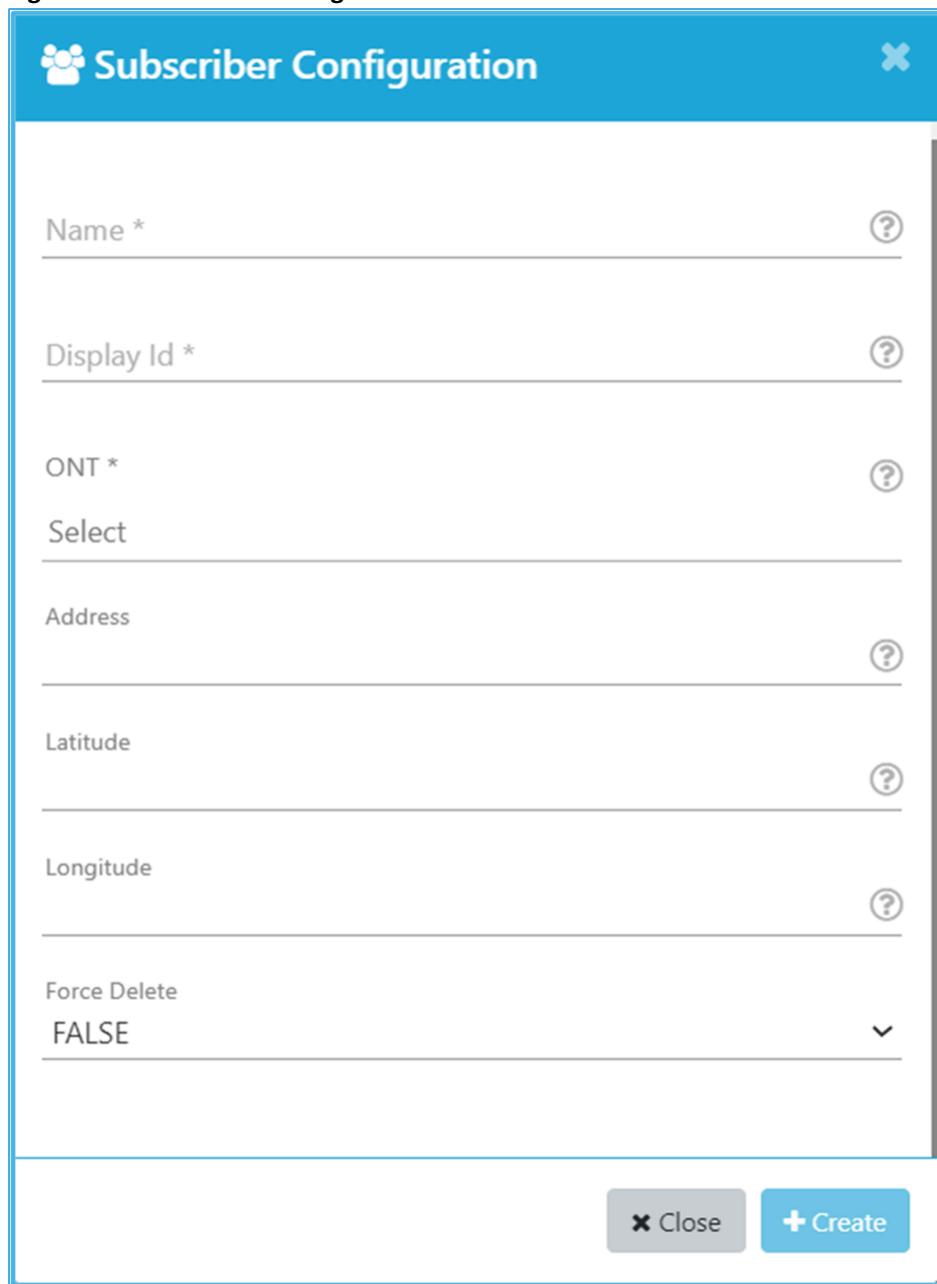
Figure 317. ONT Configuration

4. Activate the ONT. See [Activating the ONT \(on page 431\)](#).

Figure 318. Activate ONT

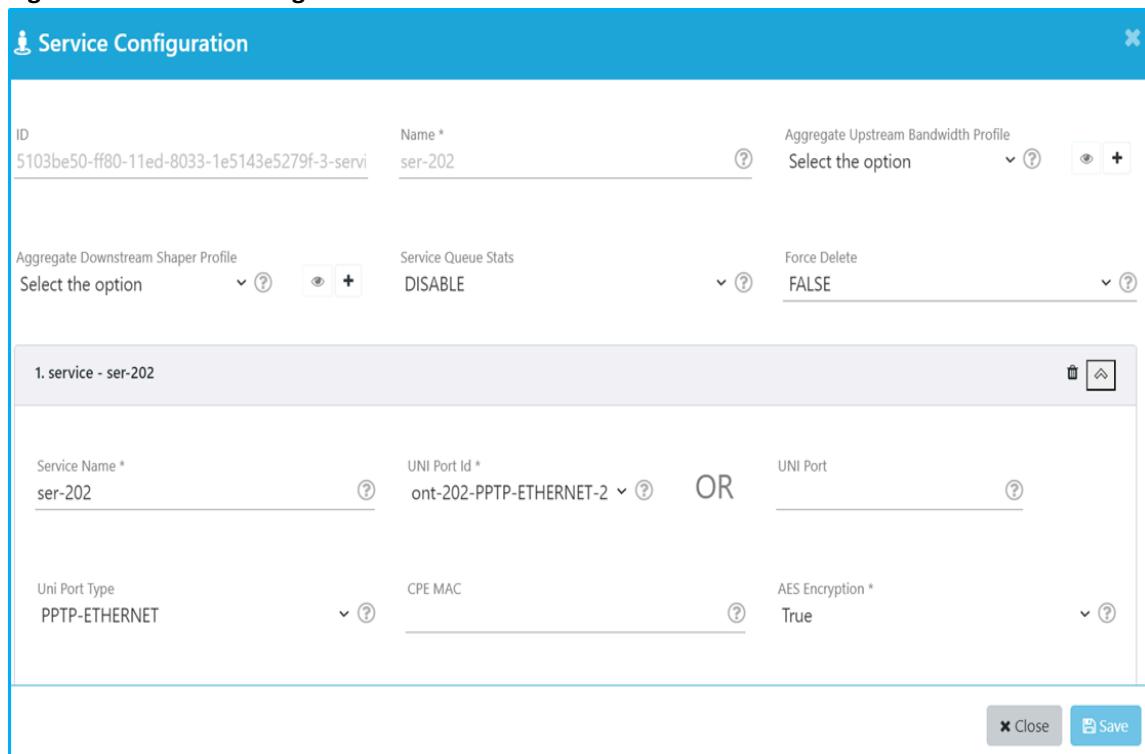
5. Create a subscriber on the ONT. See [Creating Subscriber \(on page 455\)](#).

Figure 319. Subscriber Configuration



The image shows a 'Subscriber Configuration' dialog box with a blue header and a white body. The header features a user icon and the text 'Subscriber Configuration' on the left, and a close button (X) on the right. The body contains several input fields with validation stars (*): 'Name' (with a question mark icon), 'Display Id' (with a question mark icon), 'ONT' (with a question mark icon), 'Select' (with a question mark icon), 'Address' (with a question mark icon), 'Latitude' (with a question mark icon), 'Longitude' (with a question mark icon), and 'Force Delete' (with a dropdown arrow icon). The 'Force Delete' field is set to 'FALSE'. At the bottom right are two buttons: a grey 'Close' button with a red X icon and a blue 'Create' button with a white plus sign icon.

6. Create a service. See [Creating Service \(on page 459\)](#).

Figure 320. Service Configuration

The screenshot shows the 'Service Configuration' dialog box. At the top, it displays the service ID (5103be50-ff80-11ed-8033-1e5143e5279f-3-service) and the service name (ser-202). It includes fields for 'Aggregate Upstream Bandwidth Profile' (with a dropdown menu 'Select the option'), 'Aggregate Downstream Shaper Profile' (with a dropdown menu 'Select the option'), 'Service Queue Stats' (set to 'DISABLE'), and 'Force Delete' (set to 'FALSE'). Below these, a list of services is shown: '1. service - ser-202'. The configuration section includes fields for 'Service Name' (ser-202), 'UNI Port Id' (ont-202-PPTP-ETHERNET-2), 'Uni Port Type' (PPTP-ETHERNET), 'CPE MAC', and 'AES Encryption' (True). At the bottom right, there are 'Close' and 'Save' buttons.

7. Activate the service for the subscriber. See [Activating and Deactivating the Service for the Subscriber \(on page 467\)](#).
8. Connect the ONT.



Note: Ensure that the PON ports are activated.

Verification

Verify that the service is activated for the subscriber after connecting the ONT and activating the PON port.

1. Navigate to **Configuration > Subscriber > Service or Monitor > Services > Subscriber Service**.
2. Verify the admin and operational state of the service.
The **Operational State** for the service must be **UP**, and the **Admin State** of the service must be **ACTIVE** indicates that the service is activated for the subscriber.

Figure 321. Subscriber Service Status

| Name | Admin State | Operational State | Creation Time | Action |
|---------|-------------|-------------------|---------------------------|--------|
| ser-202 | ACTIVE | UP | May 31, 2023, 12:31:04 PM | |

Showing 1 to 1 of 1 entries

3. Navigate to **Monitor > Events**.
4. Verify the SERVICE-UP event is reported in RMS to confirm the service activation for the subscriber is successful, or the service status is UP.

CBAC-D Upgrade

This section covers the steps to upgrade CBAC-D software as per the supported release path.

The following is the supported upgrade path for R3.2.1 release.

Table 399. CBAC Upgrade Path

| From | Direct Upgrade | Description |
|--------------------|----------------|---|
| R2.10.2 | Yes | Direct Upgrade |
| R3.1.X | Yes | Direct Upgrade |
| R3.2.X | Yes | Direct Upgrade |
| R3.0.X | No | Upgrade first to R3.1.X and then to R3.2.1 |
| All other releases | No | Contact customer support for the recommended upgrade path |

Setup Readiness

Perform the following steps to ensure the setup is ready.

1. Enable the 443 ACLs port on BNG to connect the OLT with the repository server.
2. Verify connectivity from OLT to the repository servers and the virtual IP.
3. Execute the following command to ensure NTP synchronization between the new repository and the NTP server. The NTP server must be co-located with the RMS cluster.

```
sudo ntpq -p
```

Figure 322. NTP Synchronization

```
oltausr@localhost:~$ date
Thu 20 Jul 2023 03:48:02 PM IST
oltausr@localhost:~$ sudo ntpq -p
      remote          refid      st t when poll reach   delay   offset   jitter
===== 
*1212::2:86    172.27.174.22    8 u 1000  512  376    0.192  -3.787  0.679
+1212::2:87    172.27.174.22    8 u 1055  512  376    0.225  -2.854  3.129
oltausr@localhost:~$
```

The following symbols can be displayed on the left of the server address.

- The asterisk (*) symbol indicates the server is successfully synchronized with the current source.
- The symbol x indicates that the synchronization server is unavailable.
- The symbol + indicates that the server is ready for an update.
- The symbol — indicates that the server is not recommended for synchronization.



Note: The output must show the symbol * before the server IP and under the remote parameter.

Prerequisites

The following requirements must be fulfilled before the CBAC-D upgrade.

1. RMS must be upgraded to the latest version.
2. There must not be any provisioning from the northbound on CBAC-D during the PE window upgrade.
3. Perform the following steps to update the repository server with the latest package.
 - a. Navigate to the <release_number_R3.x.x> file location on the /opt/CBAC_<release_number> repository.

Figure 323. SDPON Version in Repository

```
jmapprod@repo-server:~$ cd /var/www/html/sdpdon/
jmapprod@repo-server:/var/www/html/sdpdon$ ls
index.html  SDPON.1.12.72  SDPON.1.13.165
jmapprod@repo-server:/var/www/html/sdpdon$
```

- b. Navigate to the /opt/CBAC_<release_number> <SDPON.x.xx.xxx>/setup_repo folder.

Figure 324. Setup Repository

```
vmauser@ubuntu18:/opt/CBAC_R2.10.2/SDPON.1.14.183/setup_repo$ ls
acl_rules.sh          create_images_versions.sh      docker_repo_upgrade.sh  repo_verify.sh
apache-packages        create_new_version.sh        docker_ce_19.03.8~3~0~ubuntu-bionic_amd64.deb  run_node_exporter.sh
apt_repo.sh           cz_repo.sh                  docker_ce_19.03.8~3~0~ubuntu-bionic_amd64.deb  setup_local_repo.sh
certs                 debian_repo.sh            docker_ce_19.03.8~3~0~ubuntu-bionic_amd64.deb  update_docker_repo.sh
check_custom_image.sh  docker_repo.sh            docker_ce_19.03.8~3~0~ubuntu-bionic_amd64.deb  update_image_to_registry.sh
cleanup_repo.sh        docker_repo.sh            nginx                         yq
containerd.io_1.2.6-3_amd64.deb  docker_repo.sh            nginx-proxy.tar
vmauser@ubuntu18:/opt/CBAC_R2.10.2/SDPON.1.14.183/setup_repo$
```

- c. Execute the following command to update the SDPON repository.

```
sudo ./setup_local_repo.sh --sdpon-version <SDPON.x.xx.xxx> --repo-ip
<ip-address>
--update-repo
```

4. Perform the following steps if the OLT setup is executed using the offline installation.



Note: CBAC does not download a few artifacts required for the OLT upgrades.

Execute the following steps if the controller is already activated. The **SDPON version** and the **CBAC release version** fields on the **Monitor > Controller** page are blank.

- Log in to the corresponding OLT.
- Execute the following command to verify if <CBAC-Rx.x.x> release folder <SDPON.x.xx.xxx> exists in the /mnt/onl/sdpon/data/msm path. The folder must not exist.

```
oltausr@localhost:~$ ls /mnt/onl/sdpon/data/msm/<SDPON.x.xx.xxx>
```

- Execute the following command to verify if the repository server is reachable from the OLT.

```
oltausr@localhost:~$ sudo ping <repoip>
```

- Execute the following command to verify if the latest **SDPON** package exists in the repository. If not, update the repository with the latest **SDPON** package.

```
vmauser@reposerver:~$ ls /var/www/html/sdpon
```

- Execute the following command to retrieve the POD name.

```
sudo kubectl get pods | grep msm
```

- Execute the following command to delete the MSM POD.

```
sudo kubectl delete pod <msm-pod-name>
```

- After deleting the MSM POD, wait a minute and execute the following command to verify if the latest **SDPON** package folder exists.

```
oltausr@localhost:/mnt/onl/sdpon/data/msm$ ls /mnt/onl/sdpon/data/msm/
```

Command Output:

```
running SDPON.x.xx.xxx
```

- If the controller is already activated in RMS, deactivate and activate the controller.

- Verify if the **SDPON Version** and the **CBAC Release Version** details are populated correctly in the **Monitor > Controller** page.

Figure 325. Controller Details

| Controller Details | |
|--|--------------------------------------|
| Details Topology Reconciliation Troubleshooting Users Devices Alarms Events More | |
| Name | controller-185 |
| Admin State | ACTIVE |
| Kafka Host | 172.27.172.185 |
| Kafka Port | 30000 |
| Kafka Alarm Topic | EMSFAULT |
| Kafka Notification Topic | EMSNOTIFICATION |
| Kafka KPI Topic | EMSKPINOTIFICATION |
| Kafka Current KPI Topic | EMSLIVEKPI |
| CBAC Release Version | CBAC-R4.1.0 |
| Monitoring Endpoint Port | |
| Monitoring Endpoint IP | |
| Operational State | UP |
| REST | UP |
| Kafka | UP |
| Adaptor | SDPON |
| Management Domain | DEFAULT_MANAGEMENT_DOMAIN |
| REST Base Url | https://172.27.172.185:31082/sdpn/v1 |
| Last Backup Time | |
| Mode | DISTRIBUTED |
| Upgrade Status | UPGRADE-SUCCESSFUL |
| CBAC Build Version | SDPON.1.21.90 |
| Grafana Port | |
| Grafana IP | |

- If the OLT is configured with the incorrect repository server IP address, perform the following steps.
- Execute the following commands to verify the current repository IP configured on the OLT.

```
oltausr@localhost:~$ cat /etc/hosts
127.0.0.1 localhost localhost.localdomain
::1 localhost6 localhost6.localdomain
# Ansible inventory hosts BEGIN
172.27.174.134 localhost.cluster.local localhost
# Ansible inventory hosts END
172.27.173.132 docker-registry.com
oltausr@localhost:~$ sudo helm get values msm
USER-SUPPLIED VALUES:
hostname:
  worker1: '''localhost'''
repo_ip: <172.xx.xxx.xxx>
sdpn_version: <SDPON.x.xx.xxx>
timezone:
  enabled: true
  zoneinfo: /usr/share/zoneinfo/Asia/Kolkata
volumePath: /mnt/onl/sdpn
```

- Perform the following steps if the repository IP configuration differs from **helm get values msm** output.
- Login to the OLT and execute the following command.

```
sudo vi update_repo_ip.sh
```

- Copy the following script to the OLT.

```
#!/bin/bash
new_repo_ip=$1
echo "##### REPO IP CHANGE ######"
echo "Changing the repo ip to : $new_repo_ip"
# Update msm with the new repo
status=`sudo helm ls | grep 'msm' | tail -1| awk '{print $8}'`
```

```
if [ $status == 'deployed' ]
then
  sudo helm get values msm > /tmp/msm.yaml
  sed -i "s/repo_ip.*/repo_ip: $new_repo_ip/g" /tmp/msm.yaml
  sudo helm upgrade -f /tmp/msm.yaml
  msm /mnt/onl/sdpon/templates/platform-services/
  charts/msm
  if [ $? -ne 0 ]; then
    echo "ERROR: Helm Upgrade Failed, Proceeding to rollback !!"
    sudo helm rollback msm
    exit
  fi
  else
    echo "ERROR: Updating repo ip failed for msm..exiting!!"
    exit;
  fi
# Update /etc/hosts
sudo sed -i "s/.* docker-registry.com/$new_repo_ip
  docker-registry.com/g" /etc/hosts
# Update inventory
sudo sed -i "s/repo_ip.*/repo_ip:
  $new_repo_ip/g" /mnt/onl/sdpon/deployment_ansible/
  inventory/group_vars/all
echo "REPO IP Change is Done !!"
```

- e. Execute the following command to modify the repository IP.

```
$ bash update_repo_ip.sh <new_repo_ip>
```

Example:

```
bash update_repo_ip.sh 172.27.173.111
```

Figure 326. Repository IP Change

```
oltausr@localhost:~$ bash update_repo_ip.sh 172.27.173.111
#####
# REPO IP CHANGE #####
Changing the repo ip to : 172.27.173.111
Release "msm" has been upgraded. Happy Helming!
NAME: msm
LAST DEPLOYED: Fri Jul 21 13:00:37 2023
NAMESPACE: default
STATUS: deployed
REVISION: 7
TEST SUITE: None
REPO IP Change is Done !!
```

- f. Execute the following commands to verify the repository IP change.

```
oltausr@localhost:~$ sudo helm get values msm
USER-SUPPLIED VALUES:
hostname:
worker1: '''localhost'''
repo_ip: 172.xx.xxx.xxx
sdpon_version: SDPON.x.xx.xxx
timezone:
enabled: true
zoneinfo: /usr/share/zoneinfo/Asia/Kolkata
volumePath: /mnt/onl/sdpon
```

```

oltausr@localhost:~$ cat /etc/hosts
127.0.0.1 localhost localhost.localdomain
::1 localhost6 localhost6.localdomain
# Ansible inventory hosts BEGIN
172.27.174.134 localhost.cluster.local localhost
# Ansible inventory hosts END
172.xx.xxx.xxxx docker-registry.com
oltausr@localhost:~$
cat/mnt/onl/sdpn/deployment_ansible/inventory/group_vars/all
#REPO_IP: IPV4/IPv6 or dns address of the repo that contains the SDPON docker
images
repo_ip: 172.xx.xxx.xxxx

```

- Verify if the log server IP is configured from RMS.

Pre-Upgrade

Perform the following task to minimize the CBAC-D upgrade time.

- OLT Health ([on page 896](#))
- Redis AOF File Size Verification ([on page 897](#))
- Logstash PV Size Verification ([on page 897](#))
- K8s Cluster Health ([on page 897](#))
- OLT and Repository Server Connectivity ([on page 898](#))
- CBAC and ONL Image Download ([on page 898](#))

OLT Health

The following verification determine the OLTs health and ensure if the OLT is ready for the upgrade.

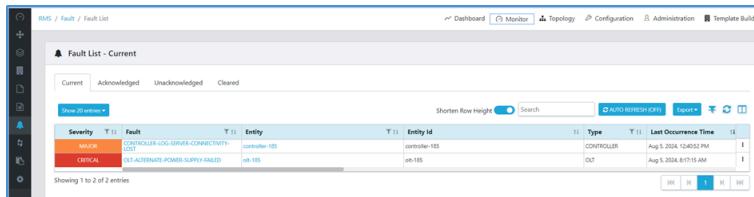
- Ensure the connectivity between RMS and the repository server is established.
- Ping the repository server and RMS worker node from the OLT shell.



Note: Ping the IPv6 IP of the repository and RMS nodes.

- Navigate to **Monitor > Faults** from the RMS GUI to check the alarm for disk and log server connectivity.

Figure 327. Alarms



- Login to the log server and check if logs for the OLT are relayed to the log server.
- If logs are relayed to the log server, continue to execute the rest of the steps for verification.

6. Perform the following steps to verify if the OLT disk size is under limits.
 - a. Login to the OLT using `oltausr` credentials.
 - b. Execute the following commands to verify the disk utilization of the OLT.

```
cd /var
df -h | grep var | awk '{print $5}' | head -n 1 | tr -d "%"
```

```
cd /mnt/onl/sdpon
df -h | grep "/mnt/onl/sdpon" | awk '{print $5}' | head -n 1 | tr -d "%"
```



Note: The command output must be less than or equal to 70.

Redis AOF File Size Verification

Execute the following command to verify the size of the Redis Append-only file.

```
du -sh /mnt/onl/sdpon/data/redis/appendonly.aof
```



Note: Output of the above command must be less than 5 GB.

Logstash PV Size Verification

Execute the following command to verify the size of the logstash PV.

```
du -sh /mnt/onl/sdpon/data/logstash/
```



Note: Output of the above command must be less than 3 GB.

K8s Cluster Health

Perform the following steps to check the Kubernetes cluster health.

1. Execute the following command to list all the PODs running on the Kubernetes cluster.



Note: All PODs must be running.

```
sudo kubectl get pods -A -o wide
```

2. Execute the following command to fetch the current state of all nodes.

```
sudo kubectl get nodes
```

Command Output:

| NAME | STATUS | ROLES | AGE | VERSION |
|-----------|--------|-----------------------|-------|---------|
| localhost | Ready | control-plane, master | 2d17h | v1.21.5 |

3. Execute the following command to check the health of the Kubernetes cluster.

```
"JSONPATH='range .items[*] {@.metadata.name}: {range
@.status.conditions[*] {@.type}={@.status}}; {end} {end}' && sudo kubectl get
nodes -o jsonpath="$JSONPATH" | grep "Ready=True"
```

Command Output:

```
localhost:NetworkUnavailable=False;MemoryPressure=False;DiskPressure=False;PIDPress
ure=
False;Ready=True;
```

OLT and Repository Server Connectivity

Execute the following command to verify the connectivity from OLT to the repository server on port 443.

```
sudo wget https://<repo-ipv6>:443
```

Figure 328. Server Connectivity

```
Linux localhost 4.19.81-OpenNetworkLinux #1 SMP Fri Nov 25 09:41:26 UTC 2022 x86_64
Last login: Thu Jul 20 14:25:42 2023 from 2405:200:824:1009::504
oltausr@localhost:~$ 
oltausr@localhost:~$ sudo wget https://[2405:200:824:1009::509]:443
[sudo] password for oltausr:
--2023-07-20 14:33:42-- https://[2405:200:824:1009::509]/
Connecting to [2405:200:824:1009::509]:443... connected.
ERROR: The certificate of '2405:200:824:1009::509' is not trusted.
ERROR: The certificate of '2405:200:824:1009::509' doesn't have a known issuer.
The certificate's owner does not match hostname '2405:200:824:1009::509'
oltausr@localhost:~$
```

CBAC and ONL Image Download

Perform the following steps to initiate the CBAC and ONL image download.

1. After updating the repository with a new package, navigate to the **Monitor > Events** page and view the latest event **SDPON-NEW-SOFTWARE-VERSION-AVAILABLE** to check the latest software version.

Figure 329. Events

| Events | | | | | | |
|--------------------------------------|----------------|----------------|-------------|-------------|------------|--------|
| Event Code | Entity | Entity Id | Entity Type | Parent Name | Error Code | Search |
| ME-LOGOUT | olt-105 | olt-105 | OLT | N/A | N/A | |
| ME-LOGOUT | olt-105 | olt-105 | OLT | N/A | N/A | |
| ME-SOFTWARE-COMMIT-SUCCESSFUL | olt-105 | olt-105 | OLT | N/A | N/A | |
| CONTROLLER-AUTHENTICATION-SUCCESSFUL | controller-105 | controller-105 | CONTROLLER | N/A | N/A | |

2. Perform the following steps to download the OLT (ONL) software from RMS.

- a. Create an OLT model configuration. See [Creating Model Configuration \(on page 610\)](#).
- b. Create an OLT model version configuration with the following details.
 - **Version**. Enter the applicable version. For example, 1.14.197.
 - **Image Path**. Enter the image path.

For example,

- To download from SFTP, `sftp://[2405:0200:0824:1009::509]/
ONL/ONL-SDPON_ONL-OS10_2023-06-05.0523
44a8d7a_AMD64_DSDPON_RSYS_1.14.197_INSTALLED_INSTALLER.`
- To download from HTTP, `http://[2405:0200:0824:1009::509]/
ONL/ONL-SDPON_ONL-OS10_2023-06-05.0523
44a8d7a_AMD64_DSDPON_RSYS_1.14.197_INSTALLED_INSTALLER.`
- **MD-5-SUM**. Enter the md5sum information.

For example, `8b5a1d8f2536381e2eeb99d64434c41a`.

Figure 330. Software Version Configuration



- c. Navigate to **Configuration > Maintenance > Task**.
- d. Complete the task configuration according to the guidelines provided in the following table.

Table 400. Software Upgrade Task Configuration

| Field | Description |
|-------------------|---|
| Name | Enter a unique name for the task. You can use any number of alphanumeric characters. Only the following special characters are supported. <ul style="list-style-type: none">▪ Underscore (_)▪ Hyphen (-)▪ Space |
| Type | Select the task type as “OLT Software Upgrade”. |
| Short Description | Enter a meaningful short description for the task. |

- e. Click **Create**.
- f. Complete the configuration according to the guidelines provided in the following table.

Table 401. OLT Software Upgrade Task

| Field | Description |
|------------------------|--|
| Configure | |
| Type | Select the device type. Example: OLT |
| Make | Select the make from the list. Example: Radisys |
| Model | Select the model from the list. Example: RLT-3200G |
| Select Actions: | You must select the Download Software checkbox and enter the Version applicable for the OLT. |

Figure 331. OLT Software Download

Select Actions : ?

Download Software

Activate Software

Commit Software

Rollback Software

Version *
RLT-1600C-ver-RSYS_1.14.197

g. Click **Next** and select the OLT devices you want to upgrade the software.

h. Select **Immediate** and click on **Submit**.

A **ME-SOFTWARE-DOWNLOAD-SUCCESSFUL** event is generated in the **Monitor > Events** tab.

CBAC-D Upgrade

This section covers the step to upgrade the CBAC and OLT software (Planned Event Window).

CBAC Upgrade

Perform the following steps to upgrade the CBAC.

1. Create a backup for the controller configuration. See [Backup Controller Configuration \(on page 307\)](#).

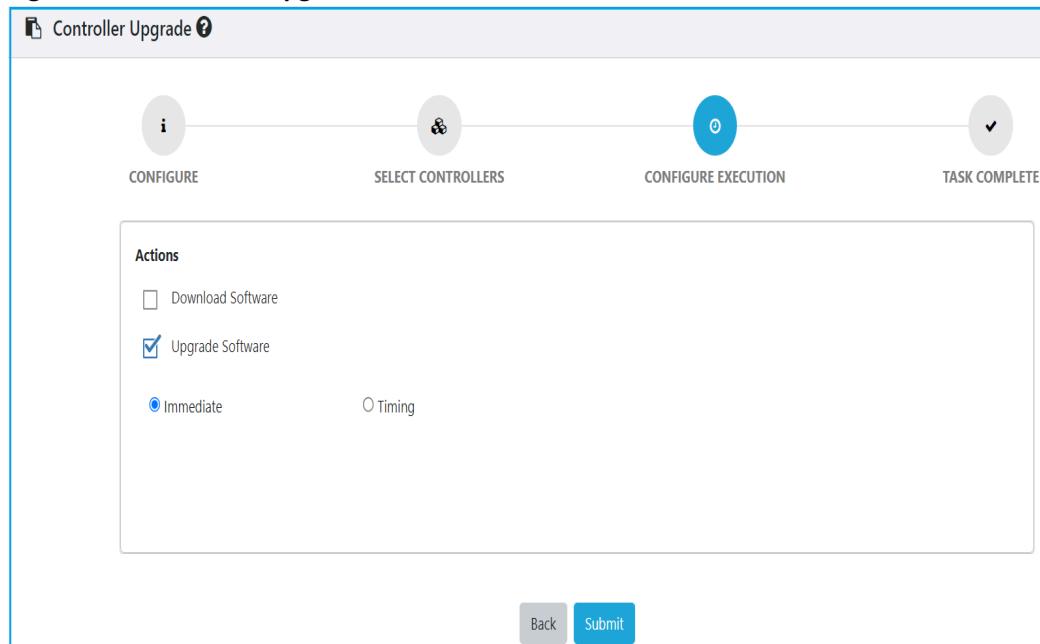


Note:

- Ensure the backup files are uploaded to the SFTP server co-located with the RMS cluster.
 - The backup path for CBAC is `ftp://[2405:200:824:1009::50e]/HPOO/CBAC_Backup`.
2. Upgrade the controller software. See [Creating Task for Single or Bulk Controller Software Upgrade \(on page 669\)](#).

**Note:**

- The RMS supports on-demand download and upgrade of CBAC. You must initiate the CBAC upgrade after receiving the **SDPON-NEW-SOFTWARE-VERSION-AVAILABLE** event notification, as CBAC is still on the older version.
- Ensure the latest controller version is available.
- An **SDPON-SOFTWARE-UPGRADE-SUCCESSFUL** event is generated after a successful controller upgrade.
- If the CBAC upgrade fails, CBAC falls back to the previous version of CBAC, and an event is raised for the failed upgrade.

Figure 332. Controller Upgrade

3. Verify the following from RMS.
- a. Controller state
 - b. OLT and Port states
 - c. Log in to the OLT and execute the following command to verify all microservices are running.

```
sudo kubectl get pods -o wide
```

OLT Upgrade

Perform the following steps to upgrade the OLT.

1. Select **Activate Software**, **Commit Software**, and **Rollback on Commit Failed** for the OLT software. See [Creating Task for Single or Bulk OLT Software Upgrade \(ONL or OLT BINS\) \(on page 647\)](#).



Note: The OLT image is already downloaded.

An **OLT-SOFTWARE-ACTIVATION-SUCCESSFUL** and **OLT-SOFTWARE-COMMIT-SUCCESSFUL** event is generated.

Figure 333. Activate and Commit

The screenshot shows the 'Activate and Commit' RMS task configuration screen. The top navigation bar has four steps: CONFIGURE, SELECT DEVICES, CONFIGURE EXECUTION, and TASK COMPLETE. The CONFIGURE step is active. The configuration fields are as follows:

- Type: OLT
- Make: Radisys
- Model: RLT-1600X

The 'Select Actions' section contains the following checkboxes:

- Download Software
- Activate Software
- Commit Software
- Rollback On Commit Failed
- Rollback Software

A 'Next' button is located at the bottom right of the configuration area.

2. Verify the following from RMS.
 - a. Controller state
 - b. OLT and Port states

Verifying CBAC-D Upgrade

Perform the following steps to verify the CBAC-D upgrade.

1. Ensure all subscribers and services are up and running.
2. Execute the following command to check the POD and node status.



Note: All the PODs must be running.

```
sudo kubectl get pods -A -o wide
```

3. Execute the following command to fetch the current state of all nodes.

```
sudo kubectl get nodes
```

Command Output:

| NAME | STATUS | ROLES | AGE | VERSION |
|-----------|--------|----------------------|-------|---------|
| localhost | Ready | control-plane,master | 2d17h | v1.21.5 |

4. Execute the following command to check the health of Kubernetes cluster.

```
"JSONPATH='range .items[*] {@.metadata.name}:range @.status.conditions[*] {@.type}={@.status};{end}{end}' && sudo kubectl get nodes -o jsonpath="$JSONPATH" | grep "Ready=True"
```

Command Output:

```
localhost:NetworkUnavailable=False;MemoryPressure=False;DiskPressure=False;PIDPressure=False;Ready=True;
```

5. Navigate to **Monitor > Controller** and verify the following in the RMS GUI.
 - The **SDPON Version** and **CBAC Release Version** must be the latest.
6. Navigate to the log path for CBAC and OLT and check the following logs.
 - CBAC application logs
 - OLT application logs
 - Audit and security logs for CBAC
 - Audit and security logs for OLT



Note:

- The log path for CBAC is */var/log/client_logs/CBAC-<OLT_inband_ip>*.
- The log path for OLT is */var/log/*.

Figure 334. Logs

```

-rw-r---- 1 syslog adm 1.7K Jul 19 22:08 oltinvpamlib.log
-rw-r---- 1 syslog adm 136 Jul 20 06:25 cracklib.log
-rw-r---- 1 syslog adm 347K Jul 20 07:35 TELEMETRY-LOG.log
-rw-r---- 1 syslog adm 160K Jul 20 12:29 MSM-LOG.log
drwxr-xr-x 24 syslog syslog 4.0K Jul 20 12:43 ..
-rw-r---- 1 syslog adm 95K Jul 20 13:00 systemd-udevd.log
-rw-r---- 1 syslog adm 212K Jul 20 13:00 containerd.log
-rw-r---- 1 syslog adm 166K Jul 20 13:00 dockerd.log
-rw-r---- 1 syslog adm 126K Jul 20 13:00 ntpd.log
drwxr-xr-x 2 syslog syslog 4.0K Jul 20 13:13 .
-rw-r---- 1 syslog adm 9.0M Jul 20 13:15 DEVICEMGR-LOG.log
-rw-r---- 1 syslog adm 18K Jul 20 13:15 smartd.log
-rw-r---- 1 syslog adm 14K Jul 20 13:16 root.log
-rw-r---- 1 syslog adm 760K Jul 20 13:17 dev_mgmt_daemon.log
-rw-r---- 1 syslog adm 7.2M Jul 20 13:19 EXTERNAL-KAFKA-LOG.log
-rw-r---- 1 syslog adm 546K Jul 20 13:23 systemd.log
-rw-r---- 1 syslog adm 16K Jul 20 13:23 oltpamlib.log
-rw-r---- 1 syslog adm 169K Jul 20 13:23 audit-parser.log
-rw-r---- 1 syslog adm 10K Jul 20 13:23 bash.log
-rw-r---- 1 syslog adm 18M Jul 20 13:23 INTERNAL-KAFKA0-LOG.log
-rw-r---- 1 syslog adm 2.8M Jul 20 13:24 MONMGR-LOG.log
-rw-r---- 1 syslog adm 377K Jul 20 13:25 CRON.log
-rw-r---- 1 syslog adm 1.2M Jul 20 13:25 EMSGW-LOG.log
-rw-r---- 1 syslog adm 605K Jul 20 13:25 SECURITY-LOG.log
-rw-r---- 1 syslog adm 97K Jul 20 13:25 SDPONSecurityAuditLogs.log
-rw-r---- 1 syslog adm 423K Jul 20 13:25 SDPONAuditLogs.log
-rw-r---- 1 syslog adm 943K Jul 20 13:25 openoltagent.log
-rw-r---- 1 syslog adm 6.7M Jul 20 13:25 OPENOLT-LOG.log
-rw-r---- 1 syslog adm 7.4M Jul 20 13:25 kubelet.log
-rw-r---- 1 syslog adm 5.0M Jul 20 13:25 NCM-LOG.log
-rw-r---- 1 syslog adm 28M Jul 20 13:25 ETCD0-LOG.log
-rw-r---- 1 syslog adm 16M Jul 20 13:25 kernel.log
vmauser@logserver1:/var/log/client_logs/CBAC-117::180:12$ █

```

- If the following alarms exist for the upgraded OLT, manually clear the alarms from the RMS GUI.
 - ONT-WINDOW-DRIFT
 - ONT-CHANNEL-DELINERATION

Figure 335. Alarm List

| Fault List - Current | | | | | | |
|----------------------|----------------------|------------------------------------|----------------------|----------------|----------------|------------|
| Fault | | Entity | | Last Occ. | | |
| Severity | Time | Fault | Time | Entity | Time | Type |
| MAJOR | Aug 5, 2024 11:11:11 | CONTROLLER-LOG-SERVER-CONNECTIVITY | Aug 5, 2024 11:11:11 | controller-105 | controller-105 | CONTROLLER |
| CRITICAL | Aug 5, 2024 11:11:11 | OLT-ALTERNATE-POWER-SUPPLY-FAILED | Aug 5, 2024 11:11:11 | olt-105 | olt-105 | OLT |

Showing 1 to 2 of 2 entries

- Ensure KPIs are generated by CBAC and processed by RMS. Verify PM dumps are generated at SFTP server level.

CBAC-D Rollback (PE Window)

The following section covers the rollback scenarios for CBAC and OLT.

CBAC Rollback

If the CBAC upgrade fails, it triggers an auto-rollback to the old version without any manual intervention. An **SDPON-SOFTWARE-UPGRADE-FAILED** alarm is raised to notify the user that the CBAC triggers the rollback.



Note: There are no alarms or event notifications for a successful rollback of CBAC software.

OLT Rollback

The OLT rollbacks to the older version in the following scenario.

1. If the OLT upgrade fails during the activation of the latest image, an auto-rollback to the older image is initiated. The CBAC-D raises **OLT-SOFTWARE-ACTIVATION-FAILED** alarm. After successful rollback to the older version, the **OLT-SOFTWARE-ROLLBACK-SUCCESSFUL** event is raised.
2. From RMS, if **Rollback upon commit Failed** is selected, RMS triggers a rollback to the older version if the commit of the latest version is failed. The **OLT-SOFTWARE-COMMIT-FAILED** alarm is raised. After successful rollback to the older version, the **OLT-SOFTWARE-ROLLBACK-SUCCESSFUL** event is raised.

Verifying CBAC-D Rollback

Perform the following steps to verify if the CBAC and OLT rollback is successful.

1. Execute the following command to check the POD and node status.



Note: All the PODs must be running.

```
sudo kubectl get pods -A -o wide
```

2. Execute the following command to fetch the current state of all nodes.

```
sudo kubectl get nodes
```

Command Output:

| NAME | STATUS | ROLES | AGE | VERSION |
|-----------|--------|-----------------------|-------|---------|
| localhost | Ready | control-plane, master | 2d17h | v1.21.5 |

3. Execute the following command to check the health of Kubernetes cluster.

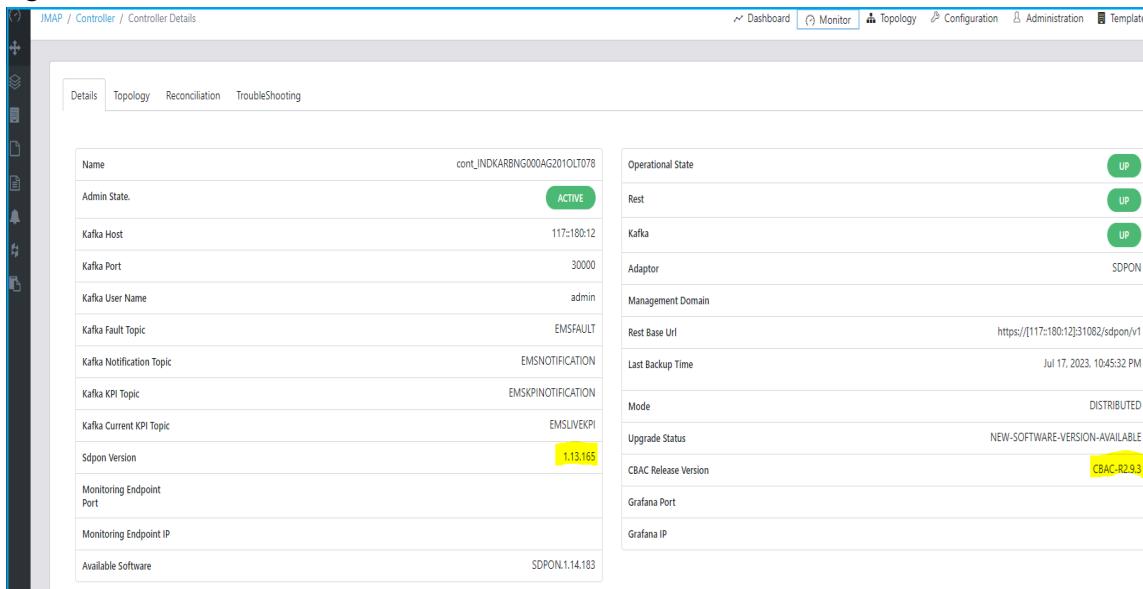
```
"JSONPATH='range .items[*]{@.metadata.name}:{range @.status.conditions[*]{@.type}={@.status};{end}}{end}' && sudo kubectl get nodes -o jsonpath="$JSONPATH" | grep "Ready=True"
```

Command Output:

```
localhost:NetworkUnavailable=False;MemoryPressure=False;DiskPressure=False;PIDPress
ure=
False;Ready=True;
```

4. Navigate to **Monitor > Controller** and verify the following in the RMS GUI.
 - The **SDPON Version** and **CBAC Release Version** must be the latest.

Figure 336. Controller Version



The screenshot shows the RMS (Radisys Management System) interface for a controller named 'cont_INDKARBNG000AG201OLT078'. The 'Details' tab is selected. The page displays various configuration parameters and their current values, along with operational status indicators (green 'UP' circles) and management domain assignments (SDPON). Key visible data includes:

| Parameter | Value | Status | Management Domain |
|--------------------------|------------------------------------|--------|-------------------|
| Name | cont_INDKARBNG000AG201OLT078 | | |
| Admin State | ACTIVE | UP | |
| Kafka Host | 117.180.12.31:1082 | UP | |
| Kafka Port | 30000 | UP | |
| Kafka User Name | admin | UP | |
| Kafka Fault Topic | EMSFault | UP | |
| Kafka Notification Topic | EMSNOTIFICATION | UP | |
| Kafka KPI Topic | EMSKPINOTIFICATION | UP | |
| Kafka Current KPI Topic | EMSLIVEKPI | UP | |
| Sdpn Version | 1.13.165 | UP | SDPON |
| Monitoring Endpoint Port | 31082 | UP | |
| Monitoring Endpoint IP | 117.180.12.31 | UP | |
| Available Software | SDPON.1.14.183 | UP | |
| Operational State | UP | UP | SDPON |
| Rest | https://117.180.12.31:1082/sdpn/v1 | UP | |
| Kafka | Jul 17, 2023, 10:45:32 PM | UP | |
| Adaptor | UP | UP | SDPON |
| Management Domain | DISTRIBUTED | UP | |
| Mode | UP | UP | |
| Upgrade Status | NEW-SOFTWARE-VERSION-AVAILABLE | UP | |
| CBAC Release Version | CBAC-R2.3 | UP | |
| Grafana Port | 3000 | UP | |
| Grafana IP | 117.180.12.31 | UP | |

5. Navigate to the log path for CBAC and OLT and check the following logs.
 - CBAC application logs
 - OLT application logs
 - Audit and security logs for CBAC
 - Audit and security logs for OLT

Topology and Recommendation

1. Subtended OLT
 - Upgrade subtended OLT
 - Post successful upgrade of subtended OLT, upgrade the main OLT.
2. OLTs that are in a ring must be upgraded simultaneously.
3. A number of OLTs can be upgraded simultaneously.

Appendix A: Alarms

The following table lists the alarms generated by CBAC and the RMS application.

Table 402. List of Alarms

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|------------------|---------------------|----------|--|--|
| ME-DOWN | OLT-CONNECTION-LOST | CRITICAL | Generated when RMS loses connection to the ME. | <ul style="list-style-type: none">• Raised<ul style="list-style-type: none">◦ The operational state of the ME is changed to DOWN and the fault count on ME is increased by one.◦ The ME health card is updated.◦ Full site hierarchy is updated with the fault count and levels.◦ ME-DOWN alarm raises automatically if the alarms ADAPTOR-KAFKA-CONNECTION-LOST and ADAPTOR-REST-CONNECTION-LOST are raised.• Cleared<ul style="list-style-type: none">◦ The operational state of the ME is changed to UP and the fault count on ME is decreased by one.◦ The ME health card is updated.◦ Full site hierarchy is updated with the fault count and levels. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|-------------------------|------------------------|----------|---|---|
| | | | | <ul style="list-style-type: none"> ◦ ME-DOWN alarm is cleared automatically if the alarms ADAPTOR-KAFKA-CONNECTION-LOST and ADAPTOR-REST-CONNECTION-LOST are cleared. |
| LOSS-OF-SIGNAL | LOSS-OF-SIGNAL | CRITICAL | Generated when the ONT loses the connection and the PON link fails or when the ONT is powered off. | <ul style="list-style-type: none"> • Raised <ul style="list-style-type: none"> ◦ The operational state of the port is changed to DOWN and the fault count on port is increased by one. ◦ Full site hierarchy is updated with the fault count and levels. • Cleared <ul style="list-style-type: none"> ◦ The operational state of the port is changed to UP and the fault count on port is decreased by one. ◦ Full site hierarchy is updated with the fault count and levels. |
| OLT- ETHERNET-LINK-DOWN | OLT-ETHERNET-LINK-DOWN | CRITICAL | Generated when the OLT loses the connectivity due to Network-to-Network Interface (NNI) link failure. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|-------------------------|-----------------------------|------------------------------|--|--|
| | | | | the fault count in the Monitor > Faults is decreased. |
| ONT-ETHERNET-LINK-DOWN | ONT-ETHERNET-LINK-DOWN | WARNING | Generated when the ONT Ethernet link goes down due to UNI port failure. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| HIGH-CPU-UTILIZATION | OLT-HIGH-CPU-UTILIZATION | CRITICAL/WARNING/MAJOR/MINOR | Generated when the CPU utilization of the OLT reaches the corresponding threshold value configured in the alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| HIGH-MEMORY-UTILIZATION | OLT-HIGH-MEMORY-UTILIZATION | CRITICAL/WARNING/MAJOR/MINOR | Generated when memory utilization of the OLT reaches the corresponding threshold value configured in the alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Site Group > Site. |
| HIGH-DISK-UTILIZATION | OLT-HIGH-DISK-UTILIZATION | CRITICAL/WARNING/ | Generated when the disk utilization of the OLT reaches the corresponding threshold | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|------------------|----------------------|---------------------------------|---|--|
| | | MAJOR/ MINOR | value configured in the alarm profile. | <ul style="list-style-type: none"> • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| HIGH-TEMPERATURE | OLT-HIGH-TEMPERATURE | CRITICAL/ WARNING/ MAJOR/ MINOR | Generated when the OLT temperature reaches the corresponding threshold value configured in the alarm profile. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| HIGH-FAN-SPEED | OLT-HIGH-FAN-SPEED | CRITICAL/ WARNING/ MAJOR/ MINOR | Generate when the fan speed of the OLT reaches the corresponding threshold value configured in the alarm profile. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| FAN-FAILURE | OLT-FAN-FAILURE | CRITICAL | Generated when the OLT reports a fan failure. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|------------------------------------|--|--|---|--|
| HIGH-UPLINK-UTILIZATION | OLT-NNI-UPSTREAM-TO-TOTAL-UTILIZATION OLT-PON-UPSTREAM-TOTAL-UTILIZATION | CRITIC AL/WARNING/ MAJOR OR/MINOR | Generated when the NNI/PON upstream bandwidth utilization of OLT reaches the corresponding threshold value configured in the alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| HIGH-DOWNLINK-UTILIZATION | OLT-NNI-DOWNSTREAM-AM-TOTAL-UTILIZATION OLT-PON-DOWNSTREAM-AM-TOTAL-UTILIZATION | CRITIC AL/WARNING/ MAJOR/MINOR | Generated when the NNI/PON downstream bandwidth utilization of OLT reaches the corresponding threshold value configured in the alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ME-NTP-SERVER-CONNECTIVITY-LOST | NTP-SERVER-CONNECTIVITY-LOST | WARNING | Generated when the ME loses the connection to the remote NTP server. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ME-RADIUS-SERVER-CONNECTIVITY-LOST | OLT-RADIUS | WARNING | Generated when the ME loses connection | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|---|------------------------------|----------|--|--|
| | | | | <ul style="list-style-type: none"> Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ME-PROVISIONING-FAILED | ONT-PROVISIONING-FAILED | CRITICAL | Generated when the ME provisioning fails due to an ME Management Control Interface (OMCI) error. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| CONTROLLER-LOG-SERVER-CONNECTIVITY-LOST | LOG-SERVER-CONNECTIVITY-LOST | WARNING | Generated when the ME loses the connection to the controller log server. | <ul style="list-style-type: none"> Raised. The fault is stored in the database. Cleared. Fault cleared status is changed to Yes. |
| ME-LOG-SERVER-CONNECTIVITY-LOST | LOG-SERVER-CONNECTIVITY-LOST | WARNING | Generated when the ME loses the connection to the remote log server. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-LOSS-OF-PLOAM-CHANNEL | ONT-LOSS-OF-PLOAM-CHANNEL | CRITICAL | Generated when the OLT requires the ONT to transmit the PLOAM message and the ONT goes offline. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|-----------------------------|------------------------------|----------|---|--|
| | | |  Note: Typically, the OLT raises this alarm after it fails to receive the PLOAM message from the ONT for consecutive times. | <ul style="list-style-type: none"> • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-PLOAM-CHANNEL-MIC-ERROR | ONT-PLOAM-CHANN-EL-MIC-ERROR | CRITICAL | Generated when RMS detects a PLOAM MIC error. PLOAM MIC error occurs when the message remains unparsable due to MIC error. This can happen both in upstream and downstream traffic. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-LOSS-OF-BURST | ONT-LOSS-OF-BURST | CRITICAL | Generated when the OLT fails to delineate CLOB of consecutive scheduled bursts from the ONT. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-STARTUP-FAILURE | ONT-STARTUP-FAILURE | CRITICAL | Generated when the ONT start up process fails due to ranging failures (Bad fiber, improper connection of fiber, signal strength, or quality) on | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|---------------------------|------------------------|----------|--|--|
| | | | the fiber or failure in the ONT bring up sequence. | <ul style="list-style-type: none"> Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-DYING-GASP | ONT-DYING-GASP | MINOR | Generated when the ONT loses power or the power cord is removed from the ONT. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| UNKNOWN-ME-DISCOVERED | UNKNOWN-ONT-DISCOVERED | MINOR | Generated when the OLT discovers an unknown ONT. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| CONTROLLER-ACCESS-BLOCKED | SDPON-USER-BLOCKED | WARNING | Generated when the user is blocked after multiple attempts to access RMS using invalid credentials. | <ul style="list-style-type: none"> Raised. The fault is stored in the database. Cleared. Fault cleared status is changed to Yes. |
| ONT-SIGNAL-FAIL | ONT-SIGNAL-FAIL | CRITICAL | Generated when the downstream Bit Error Rate (BER) value crosses the Signal Fail (SF) threshold value configured in the ANIG alarm profile. This alarm | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|------------------------|------------------------|----------|---|--|
| | | | is cleared when the BER value becomes lower than the SF value. | <ul style="list-style-type: none"> • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ME-SHUTDOWN | OLT-SHUTDOWN | CRITICAL | Generated when the maximum operating temperature of the OLT is exceeded, and the OLT is shutdown. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| OLT-FILESYSTEM-FAILURE | OLT-FILESYSTEM-FAILURE | MAJOR | Generated when the OLT detects the file system corruption or failure. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| OLT-RTC-FAILURE | OLT-RTC-FAILURE | MAJOR | Generated when the OLT's RTC experience the setting problem or excessive drift problem. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|----------------------------|--------------------------------|----------|--|--|
| SOFTWARE-DOWNLOAD-FAILED | OLT-SOFTWARE-DOWNLOAD-FAILED | MAJOR | Generated when the OLT software download process fails. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| SOFTWARE-ACTIVATION-FAILED | OLT-SOFTWARE-ACTIVATION-FAILED | MAJOR | Generated when the OLT software activation fails. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| SOFTWARE-COMMIT-FAILED | OLT-SOFTWARE-COMMIT-FAILED | MAJOR | Generated when the software commit operation fails on the OLT. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| SOFTWARE-ROLLBACK-FAILED | OLT-SOFTWARE-ROLLBACK-FAILED | CRITICAL | Generated when the software rollback process fails on the OLT. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|-----------------------------|----------------------------|----------|---|--|
| | | | | <ul style="list-style-type: none"> • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-DISCOVER ED- DUP-SL-NUM | ONT-DISCO VERED-DUP-SL-NUM | CRITICAL | Generated when the OLT discovers a duplicate ONT with an existing serial number. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| SFP-MISSING | SFP-MISSING | CRITICAL | Generated when the OLT detects that the SFP module is missing on the port during the port activation or when the SFP module is removed. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| SFP-INVALID-MODULE-ID | SFP-INVALID-MODULE-ID | MAJOR | Generated when the OLT detects an invalid SFP module is connected to the port. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|--|--|----------|--|--|
| PORT-EXCESSIVE-FCS-ERRORS-15-MIN-INTERVAL | PORT-EXCESSIVE-FCS-ERRORS-15-MIN-INTERVAL | MINOR | Generated when the number FCS errors on the PON port reaches the threshold value configured in the PON port alarm profile. RMS checks the FCS errors on the PON port at an interval of 15 minutes. This alarm is cleared when the number of FCS errors becomes lower than the threshold value configured in the alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| PORT-EXCESSIVE-FCS-ERRORS-1-DAY-INTERVAL | PORT-EXCESSIVE-FCS-ERRORS-1-DAY-INTERVAL | MAJOR | Generated when the number of FCS errors on the PON port reaches the threshold value configured in the PON port alarm profile. RMS checks the FCS errors on the PON port every day. This alarm is cleared when the number of FCS errors becomes lower than the threshold value configured in the alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| PORT-EXCESSIVE-DROP-OF-PACKETS-15-MIN-INTERVAL | PORT-EXCESSIVE-DROP-OF-PACKETS-15-MIN-INTERVAL | MINOR | Generated when the number of packet drops on the PON port reaches the threshold value configured in the PON port alarm profile. RMS checks packet drops on the PON port at an interval of 15 minutes. This alarm is cleared | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|---|--|------------------------------|---|--|
| | | | when the number of packet drops becomes lower than the threshold value configured in the alarm profile. | |
| PORT-EXCESSIVE-DROP-OF-PACKETS-1-DAY-INTERVAL | PORT-EXCESSIVE-DROP-OF-PACKETS -1-DAY-INTERVAL | MAJOR | Generated when the number of packet drops on the PON port reaches the threshold value configured in the alarm profile. RMS checks packet drops on the PON port every day. This alarm is cleared when the number of packet drops becomes lower than the threshold value configured in the alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| OLT-LAG-DOWNSTREAM-TOTAL-UTILIZATION | OLT-LAG-DOWNSTREAM-TOTAL-UTILIZATION | CRITICAL/WARNING/MAJOR/MINOR | Generated when the downstream bandwidth utilization of the LAG interface reaches the corresponding threshold value configured in the LAG alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| OLT-LAG-UPSTREAM-TOTAL- UTILIZATION | OLT-LAG-DOWNSTREAM-TOTAL-UTILIZATION | CRITICAL/WARNING/MAJOR/MINOR | Generated when the upstream bandwidth utilization of the LAG interface reaches the corresponding threshold value configured in the alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|--------------------------------------|---------------------------------------|----------|---|--|
| | | | | <ul style="list-style-type: none"> Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| SFP-TRANSMIT-FAILURE | SFP-TRANS MIT-FAILURE | CRITICAL | Generated when the transmit failure (TX_FAIL) signal is detected on the SFP module pins by the OLT. The transmit failure occurs due to faulty SFP module, pollution/damage on the optical interface, or Electrostatic discharge (ESD) damage. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| OLT-SW-PROGRAM-ABNORMALLY-TERMINATED | OLT-SW-PROGRAM-ABNORMAL LY-TERMINATED | MAJOR | Generated when the OLT detects that a critical software program has stops working. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-LOSS-OF-ACKNOWLEDGEMENT | ONT-LOSS-OF-ACKNOWLEDGEMENT | MAJOR | Generated when the OLT does not receive an acknowledgment from the ONT after a set of downstream messages that implies an upstream acknowledgment. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|----------------------------|----------------------------|----------|---|--|
| ONT-LOSS-OF-KEY | ONT-LOSS-OF-KEY | MAJOR | Generated when the ONT transmits the key in response to the “Request_Key” message to the OLT, and it fails three times consecutively. This alarm is cleared when the OLT receives a key from the ONT. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-LOSS-OF-OMCI-CHANNEL | ONT-LOSS-OF-OMCI-CHANNEL | MAJOR | Generated when three consecutive ONU Management and Control Interface (OMCI) packets are received with MIC errors and crosses the threshold value for asserting the Loss of OMCI channel (LOOCi) alarm. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| OLT-HW-CONFIG-READ-FAILURE | OLT-HW-CONFIG-READ-FAILURE | MAJOR | Generated when the OLT faces problem in reading OLT unit hardware properties such as serial number and ports. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| OLT-DISK-FAILURE | OLT-DISK-FAILURE | CRITICAL | Generated when the OLT detects the read/write failure on the disk. This alarm is cleared manually by the field engineer after the disk replacement. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|--|------------------------------|----------|---|--|
| | | | | <ul style="list-style-type: none"> • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-EXCESSIVE-DROP-OF-LOWER-TRAFFIC-CLASS-PACKETS-15-MIN- INTERVAL | NA | MINOR | Generated when the drop of packets for the lower traffic class for an ONT reaches the threshold value configured in the alarm profile. RMS checks packet drops on the ONT at an interval of 15 minutes. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-EXCESSIVE-DROP-OF-LOWER-TRAFFIC-CLASS-PACKETS-1-DAY-INTERVAL | NA | MAJOR | Generated when the drop of packets for the lower traffic class for an ONT reaches the threshold value configured in the alarm profile. RMS checks packet drops on the ONT at an interval of one day. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-REGISTRATION-ID-MISMATCH | ONT-REGISTRATION-ID-MISMATCH | CRITICAL | Generated when the ONT is discovered with different registration ID than the configured one. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|--------------------------|--------------------------|----------|--|--|
| ONT-SIGNAL-DEGRADE | ONT-SIGNAL-DEGRADE | MAJOR | Generated when the downstream Bit Error Rate (BER) value crosses the Signal Degrade (SD) threshold value configured in the alarm profile. This alarm is cleared when the BER value becomes lower than the SD value. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-DEACTIVATION-FAILURE | ONT-DEACTIVATION-FAILURE | CRITICAL | Generated by the OLT when the ONT does not respond for three “Deactivate_ONU-ID” or “Disable_Serial_Number” messages. This alarm is cleared by RMS when the offending ONU is successfully re-activated and remains positively controlled or is prevented from transmitting upstream. This alarm can also be cleared by the field engineer after the successful maintenance operations. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| DHCP-SERVER-TIMEOUT | DHCP-SERVER-TIMEOUT | CRITICAL | Generated when the ONT/RG sends the DHCP request and there is no response from the DHCP server for a defined time interval (5 min). This alarm is raised as per outer VLAN. | The Monitor > Faults page is updated. |
| SDPON-AUDIT-LOG-Failure | SDPON-AUDIT-LOG-Failure | MAJOR | Generated when you record audit log into | The Monitor > Faults page is updated. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|--|---|----------|---|--|
| | | | the database and the recording fails. | |
| SDPON-UPGRA DE- FAILED | SDPON-SOF TWARE- UPGRADE-F AILED | CRITICAL | Generated when the CBAC microservice upgrade is failed. | The Monitor > Faults page is updated. |
| SDPON-ROLLBA CK- FAILED | SDPON-SOF TWARE- ROLLBA CK-FAILED | CRITICAL | Generated when the CBAC microservice rollback operation is failed. | The Monitor > Faults page is updated. |
| REPOSITORY- SERVER- CONNECTIVITY- LOST | REPOSITO RY- SERVER- CONNECTIV ITY-LOST | MAJOR | Generated when CBAC node loses connectivity to the repository server. | The Monitor > Faults page is updated. |
| SDPON-DOCKER- IMAGE-DOWNLO AD- FAILED | SDPON-DO CKER- IMAGE-DO WNLOAD- FAILED | MAJOR | Generated when the docker image download process fails. | The Monitor > Faults page is updated. |
| ADAPTOR-KAF KA- CONNECTION-L OST | NA | MAJOR | Generated when RMS is not able to connect to the CBAC Kafka. | <ul style="list-style-type: none"> Raised. This alarm is raised automatically when the CBAC Kafka connection goes down. Cleared. This alarm is cleared automatically when the CBAC Kafka connection is established with RMS. |
| ADAPTOR-REST- CONNECTION-L OST | NA | MAJOR | Generated when RMS is not able to connect to the CBAC REST interface. | <ul style="list-style-type: none"> Raised. This alarm is raised automatically when the CBAC REST connection goes down. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|--|--|----------|---|--|
| | | | | <ul style="list-style-type: none"> Cleared. This alarm is cleared automatically when the CBAC REST interface connection is established with RMS. |
| ONT-DISCOVER ED- DUP- REGISTRATI ON-ID | ONT-DISCO VERED- DUP-REGIS TRATION- ID | CRITICAL | Generated when the OLT discovers a duplicate ONT with an existing registration ID. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| OLT-ERPS-F OP-PM | OLT-ERPS-F OP-PM | CRITICAL | Generated when the OLT reports Failure of Protocol - Provisioning Mismatch(FOR-PM). | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| OLT-ERPS-F OP-TO | OLT-ERPS-F OP-TO | CRITICAL | Generated when the OLT reports Failure Of Protocol - Time Out (FOP-TM). | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|--|--|----------|--|--|
| OLT- ERPS-INSTANCE-CONVERGENCE-FAILURE | OLT- ERPS-INSTANCE-CONVERGE NCE- FAILURE | CRITICAL | Generated when the OLT reports the ERPS instance convergence failure. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| CONTROLLER-DATABASE-FAILURE-CONFIGDB | SDPON-DATABASE-FAILURE-CO NFIGDB | CRITICAL | Generate when the database (Config DB) is not accessible, or read/write failures are encountered. RMS also reports this alarm when the health check fails consecutively (six times) in the interval of ten seconds. | The Monitor > Faults page is updated. |
| CONTROLLER-DATABASE-FAILURE-TSDB | SDPON-DATABASE-FAILURE-T SDB | CRITICAL | Generated when the database (Time Series Database (TSDB)) is not accessible, or read/write failures are encountered. RMS also reports this alarm when the health check fails consecutively (six times) in the interval of ten seconds. | The Monitor > Faults page is updated. |
| CONTROLLER-DATABASE-FAILURE-SUBSCRIBERDB | SDPON-DATABASE-FAILURE- SUBSCRIBE RDB | CRITICAL | Generated when the database (Subscriber Database) is not accessible, or read/write failures are encountered. RMS also reports this alarm when the health check fails consecutively | The Monitor > Faults page is updated. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|--------------------------------------|-------------------|----------|---|--|
| | | | (six times) in the interval of ten seconds. | |
| OLT-USER-BLOCKED | OLT-USER-BLOCKED | WARNING | Generated when the user is blocked after the multiple attempts (the default value is 3) to access the OLT using invalid credentials. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| USER-LOCKED | NA | MAJOR | Generated when the user is blocked after the multiple attempts (the default value is 3) to access RMS using invalid credentials. This alarm is cleared manually after 10 minutes. | The Monitor > Faults page is updated. |
| CURRENT-ALARMS-TABLE-SIZE-EXCEEDED | NA | CRITICAL | Generated when the current alarm table size exceeds than the threshold value (1000000) configured in RMS. | The Monitor > Faults page is updated. |
| HISTORICAL-ALARM-TABLE-SIZE-EXCEEDED | NA | CRITICAL | Generated when the historical alarm table size exceeds than the threshold value (1000000) configured in RMS. | The Monitor > Faults page is updated. |
| INVENTORY-TABLE-SIZE-EXCEEDED | NA | CRITICAL | Generated when the inventory table size exceeds than the threshold value | The Monitor > Faults page is updated. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|----------------------------|----------------------------|----------|---|--|
| | | | (1000000) configured in RMS. | |
| EVENT-TABLE-SIZE- EXCEEDED | NA | CRITICAL | Generated when the event table size exceeds than the threshold value (1000000) configured in RMS. | The Monitor > Faults page is updated. |
| ME-ACTIVATION- FAILURE | ONT-ACTIVATION- FAILURE | MINOR | Generated when you activate the managed element and the operation fails. | The Monitor > Faults page is updated. |
| EMS-BACKUP- FAILURE | NA | CRITICAL | Generated when the RMS database configuration operation fails. | The Monitor > Faults page is updated. |
| EMS-RESTORE- FAILURE | NA | CRITICAL | Generated when the OLT or controller restore operation fails. | The Monitor > Faults page is updated. |
| SFP-MISMATCH | NA | CRITICAL | Generated when there is a mismatch in the SFP attributes such as signal_range (reach) in the new SFP inserted, as compared to the previous SFP. | The Monitor > Faults page is updated. |
| FAN-MISSING | OLT-FAN-MISSING | CRITICAL | Generated when the OLT fan is missing. | The Monitor > Faults page is updated. |
| OLT- ALARM-PORT- LINK-DOWN | OLT- ALARM-PORT- LINK-DOWN | MAJOR | Generated when the OLT detects 'Alarm' port on the OLT link is operationally 'down'. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|--|--|----------|---|--|
| ONT-FIRMWARE-DOWNLOAD-ON-OLT-FAILED | ONT-FIRMWARE-DOWNLOAD-ON-OLT-FAILED | MAJOR | Generated when the firmware download process on the OLT is failed. The possible reasons are. <ol style="list-style-type: none"> 1. Firmware download failure. 2. A cyclic redundancy check (CRC32) checksum validation failure. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-FIRMWARE-DOWNLOAD-ON-ONT-FAILED | ONT-FIRMWARE-DOWNLOAD-ON-ONT-FAILED | MAJOR | Generated when the firmware download process on ONT fails. The possible reasons: <ol style="list-style-type: none"> 1. The firmware is not compatible with the ONT. 2. There are lot of errors in the OMCI channel while transferring the firmware. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-FIRMWARE-ACTIVATE-COMMIT- FAILED | ONT-FIRMWARE-ACTIVATE-COMMIT-FAILED | MAJOR | Generated when the firmware activation or commit operation fails. <ol style="list-style-type: none"> 1. The ONT came up with a wrong image instance 2. The ONT reports commit failure | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| OLT-CREATE-EXTERNAL-ALARML-VLAN-FAILED | OLT-CREATE-EXTERNAL-ALARML-VLAN-FAILED | WARNING | Generated when you create an external alarm VLAN and the operation is failed. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|--|--|----------|---|--|
| | VLAN-FAI LED | | | <ul style="list-style-type: none"> Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| OLT-DELETE-EXTERNAL-ALA RM-VLAN-FAILED | OLT-DELE TE-EXTERN AL-ALARM-VLAN-FAI LED | WARNING | Generated when you delete an external alarm VLAN and the operation is failed. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-PHYSICAL-EQUIPMENT-ERROR | ONT-PHYSICAL-EQUIPMENT-ERROR | MAJOR | Generated when the OLT receives a physical equipment error message from ONU. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-TRANSMISSION-INTERFERENCE-WARNING | ONT-TRANSMISSION-INTERFERENCE-WARNING | WARNING | Generated in the following condition. If there are N sequential bursts from a given ONU, the transmission drift exceeds the upper of two specified drift thresholds. This condition indicates that either the drift is occurring critically fast, or the attempt to correct the transmission phase through the Equalization | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|--------------------------|--------------------------|------------------------------|--|--|
| | | | Delay (EqD) update is failed. | |
| ONT-SFP-HIGH-TEMPERATURE | ONT-SFP-HIGH-TEMPERATURE | CRITICAL/WARNING/MAJOR/MINOR | Generated when the SFP temperature of the ONT reaches the corresponding high threshold value configured in the ME ANI-G alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-SFP-LOW-TEMPERATURE | ONT-SFP-LOW-TEMPERATURE | CRITICAL/WARNING/MAJOR/MINOR | Generated when the SFP temperature of the ONT reaches the corresponding low threshold value configured in the ME ANI-G alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-SFP-HIGH-VOLTAGE | ONT-SFP-HIGH-VOLTAGE | CRITICAL/WARNING/MAJOR/MINOR | Generated when the SFP voltage of ONT is more than the corresponding threshold value configured in the ME ANI-G alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-SFP-LOW-VOLTAGE | ONT-SFP-LOW-VOLTAGE | CRITICAL/WARNING/MAJOR/MINOR | Generated when the SFP voltage of the ONT is less than the corresponding threshold | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|-------------------------------|-------------------------------|---------------------------------|---|--|
| | | MAJOR/ MINOR | value configured in the ANI-G alarm profile. | <ul style="list-style-type: none"> • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-SFP-HIGH-BIAS-CURRENT | ONT-SFP-HIGH-BIAS-CURRENT | CRITICAL/ WARNING/ MAJOR/ MINOR | Generated when the SFP bias_current of the ONT is more than the corresponding threshold value configured in the ANI-G alarm profile. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-SFP-LOW-BIAS-CURRENT | ONT-SFP-LOW-BIAS-CURRENT | CRITICAL/ WARNING/ MAJOR/ MINOR | Generated when the SFP bias_current of the ONT is less than the corresponding threshold value configured in the ANI-G alarm profile. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-SFP-HIGH-RX-OPTICAL-POWER | ONT-SFP-HIGH-RX-OPTICAL-POWER | CRITICAL/ WARNING/ MAJOR/ MINOR | Generated when the SFP RX optical power of the ONT read is more than the corresponding threshold value configured in the ANI-G alarm profile. | <ul style="list-style-type: none"> • Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. • Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|---|--|--|---|--|
| ONT-SFP-L OW-RX-POWER | ONT-SFP-L OW-RX-POWER | CRITIC AL/WAR NING/ MAJOR/ MINOR | Generated when the SFP RX optical power of the ONT read is less than the corresponding threshold value configured in the ANI-G alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-SFP-HI GH-TX-OPTICAL-POWER | ONT-SFP-HI GH-TX-POWER | CRITIC AL/WAR NING/ MAJOR/ MINOR | Generated when the SFP TX optical power of ONT is more than the corresponding threshold value configured in the ANI-G alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| ONT-SFP-L OW-TX-POWER | ONT-SFP-L OW-TX-POWER | CRITIC AL/WAR NING/ MAJOR/ MINOR | Generated when the SFP TX optical power of the ONT is less than the corresponding threshold value configured in the ANI-G alarm profile. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |
| OLT-AUDIT-L OG-FILE-SIZE-LIM IT- EXCEEDED | OLT-AUD IT-LOG-FI LE-SIZE-LIM IT- EXCEEDED | CRITIC AL/WAR NING/ MAJ OR/MI NOR | Generated when the file size of the audit or security log on the OLT crosses 80% of the maximum file size. | The Monitor > Faults page is updated. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|---|---|------------------------------|--|--|
| OLT-UPDATE-E-LAN-FAILED | OLT-UPDA TE-E-LAN-FAILED | CRITICAL | Generated when you update the E-LAN configuration and it fails at the OLT. | The Monitor > Faults page is updated. |
| ACTIVE-CHANNELS-PER-PON-EXCEEDED | ACTIVE-CHANNELS-P ER-PON-EXCEEDED | CRITICAL/WARNING/MAJOR/MINOR | Generated when the active number of IGMP channels on the PON port exceeds the configured threshold value. | The Monitor > Faults page is updated. |
| ACTIVE-CHANNELS-PER-SUBSCRIBER-EXCEEDED | ACTIVE-CHANNELS-PER-SUBSCRIBER-EXCEEDED | CRITICAL | Generated when the number of active IGMP channels for a subscriber exceeds the configured limit. | The Monitor > Faults page is updated. |
| ROGUE-ONT-DETECTED | ROGUE-ONT-DETECTED | CRITICAL | Generated when a rogue ONT is detected during the rogue ONT detection cycle. | The Monitor > Faults page is updated. |
| PORT-ROGUE-TRANSMISSION-DETECTED | PORT-ROGUE-TRANSMISSION-DETECTED | MAJOR | Generated when the port rogue transmission is observed. However the burst transmission is too short to perform measurements on the ONT | The Monitor > Faults page is updated. |
| SERVICE-ACTIVATION-FAILURE | SERVICE-ACTIVATION-FAILURE | CRITICAL | Generated when the subscriber service configuration fails on the OLT or ONT. | <ul style="list-style-type: none"> Raised. The fault is stored in the database and the fault count in the Monitor > Faults is increased. Cleared. The fault status is changed to Yes and the fault count in the Monitor > Faults is decreased. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|--|---|----------|--|---|
| MULTICAST-STORM-CONTROL- EXCEEDED | MULTICAST-ST-STORM-CONTROL- EXCEEDED | CRITICAL | Generated when the multicast storm control is exceeded at the OLT. | The Monitor > Faults page is updated. |
| BROADCAST-STORM-CONTROL- EXCEEDED | BROADCAST-ST-STORM-CONTROL- EXCEEDED | CRITICAL | Generated when the broadcast storm control is exceeded at the OLT. | The Monitor > Faults page is updated. |
| UNKNOWN-UNICAST-STORM-CONTROL-EXCEEDED | UNKNOWN-UNICAST-ST-STORM-CONTROL-EXCEEDED | CRITICAL | Generated when the unknown unicast storm control is exceeded at the OLT. | The Monitor > Faults page is updated. |
| ONT-UNRESPONSIVE | ONT-UNRESPONSIVE | CRITICAL | Generated when the ONU OMCI channel goes down. | The Monitor > Faults page is updated. |
| TYPE-B-PROTECTION-SWITCHOVER- FAILED | TYPE-B-PROTECTION-ON-SWITCHOVER- FAILED | CRITICAL | Generated when the auto or manual type- B protection switchover is failed. | The Monitor > Faults page is updated. |
| TYPE-B-PROTECTION-NOT- AVAILABLE | TYPE-B-PROTECTION-ON-NOT- AVAILABLE | WARNING | Generated when any one of the PON ports of the type-B protection pair is operationally down due to PON loss of signal. | The Monitor > Faults page is updated. |
| TYPE-B-PROTECTION-PAIR- DOWN | TYPE-B-PROTECTION-ON-PAIR- DOWN | CRITICAL | Generated when both the PON ports of the type-B protection pair is operationally down due to PON loss of signal. | The Monitor > Faults page is updated. |
| OLT-ETHERNET-LINK-FLAPPING | OLT-ETHERNET- | CRITICAL | Generated when the OLT identifies the network connectivity issue due to | The Monitor > Faults page is updated. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|-------------------------------------|-------------------------------------|----------|--|---|
| | LINK-FLAPPING | | continuous flapping of the Network-to- Network Interface (NNI) link. | |
| OLT-ALTERNATE-POWER-SUPPLY-FAILED | OLT-ALTERNATE-POWER-SUPPLY-FAILED | CRITICAL | Generated when one of the OLT power supply terminals is not connected to the OLT. | The Monitor > Faults page is updated. |
| OLT-TACACS-SERVER-CONNECTIVITY-LOST | OLT-TACACS-SERVER-CONNECTIVITY-LOST | CRITICAL | Generated when the OLT loses the network connectivity with the Terminal Access Controller Access Control System (TACACS) server. | The Monitor > Faults page is updated. |
| OLT-CREATE-RING-FAILED | OLT-CREATE-RING-FAILED | CRITICAL | Generated when you create a ring, and the operation fails at the OLT. | The Monitor > Faults page is updated. |
| OLT-DELETE-RING-FAILED | OLT-DELETE-RING-FAILED | WARNING | Generated when you delete a ring, and the operation fails at the OLT. | The Monitor > Faults page is updated. |
| OLT-CREATE-ERPS-INSTANCE-FAILED | OLT-CREATE-ERPS-INSTANCE-FAILED | CRITICAL | Generated when you create an ERPS instance and the operation fails at the OLT. | The Monitor > Faults page is updated. |
| OLT-DELETE-ERPS-INSTANCE-FAILED | OLT-DELETE-ERPS-INSTANCE-FAILED | WARNING | Generated when you delete an ERPS instance and the operation fails at the OLT. | The Monitor > Faults page is updated. |
| OLT-UPDATE-ERPS-INSTANCE-FAILED | OLT-UPDATE-ERPS-INSTANCE-FAILED | CRITICAL | Generated when you update an ERPS instance and the operation fails at the OLT. | The Monitor > Faults page is updated. |
| OLT-UPDATE-RING-FAILED | OLT-UPDATE-RING-FAILED | CRITICAL | Generated when you update a ring, and the operation fails at the OLT. | The Monitor > Faults page is updated. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|-------------------------------|------------------------------|----------|---|---|
| PORT-ERPS-FW-STATE-BLOCKED | PORT-ER PS-FW-STATE-BLOCKED | CRITICAL | Generated when the ERPS forwarding is blocked on either the east or west port on an ERPS instance. | The Monitor > Faults page is updated. |
| OLT-BACKUP-CONFIG-FAILED | OLT-BACKUP-CONFIG-FAILED | MAJOR | Generated when the OLT database backup configuration operation fails. | The Monitor > Faults page is updated. |
| OLT-RESTORE-CONFIG-FAILED | OLT-RESTORE-CONFIG-FAILED | MAJOR | Generated when you restore the OLT database configuration, and the operation fails. | The Monitor > Faults page is updated. |
| ONT-DISCOVER ED-PORT-MISMATCH | ONT-DISCOVERED-PORT-MISMATCH | CRITICAL | Generated when the ONT is discovered with a different OLT and the PON port than the configured OLT and the PON port. | The Monitor > Faults page is updated. |
| SDPON-BACKUP-CONFIG-FAILED | SDPON-BACKUP-CONFIG-FAILED | MAJOR | Generated when the CBAC database backup configuration operation fails. | The Monitor > Faults page is updated. |
| SDPON-RESTORE-CONFIG-FAILED | SDPON-RESTORE-CONFIG-FAILED | MAJOR | Generated when you restore the CBAC database and the operation fails. | The Monitor > Faults page is updated. |
| MEP-LOSS-OF-CONNECTIVITY | MEP-LOSS-OF-CONNECTIVITY | CRITICAL | Generated when the local Managed End Point (MEP) is not receiving Continuity Check Message (CCM) from the remote MEP. | The Monitor > Faults page is updated. |
| ONT-REMOTE-DEFECT-INDICATION | ONT-REMOTE-DEFECT-INDICATION | MAJOR | Generated when the Remote Defect Indication (RDI) field of ONUi is | The Monitor > Faults page is updated. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|--------------------------------------|--------------------------------------|----------|---|---|
| | DEFECT-IN-DICATION | | asserted and the OLT transmission is received with defects at the ONUi. | |
| OLT-NTP-CLOCK-OUT-OF-SYNC | OLT-NTP-CLK-IS-OUT-OF-SYNC | MAJOR | Generated when the time of OLT is not synchronized with the network time servers configured in the NTP profile. | The Monitor > Faults page is updated. |
| OLT-ETHERNET-LAG-DOWN | OLT-ETHERNET-LAG-DOWN | CRITICAL | Generated when all the member ports of the LAG is down. | The Monitor > Faults page is updated. |
| OLT-FIRMWARE-ACTIVATION-FAILED | OLT-FIRMWARE-ACTIVATION-FAILED | MAJOR | Generated when the OLT firmware activation process is failed. | The Monitor > Faults page is updated. |
| OLT-HIGH-VOLTAGE | OLT-HIGH-VOLTAGE | CRITICAL | Generated when OLT operating voltage is not within the maximum threshold value. | The Monitor > Faults page is updated. |
| OLT-LOW-VOLTAGE | OLT-LOW-VOLTAGE | CRITICAL | Generated when OLT operating voltage is less than the minimum threshold value. | The Monitor > Faults page is updated. |
| OLT-HIGH-CURRENT | OLT-HIGH-CURRENT | CRITICAL | Generates when OLT operating electric current is not within the default threshold value. | The Monitor > Faults page is updated. |
| TYPE-B-PROTECTION-CONFIG-SYNC-FAILED | TYPE-B-PROTECTION-CONFIG-SYNC-FAILED | CRITICAL | Generates when the subscriber service configuration synchronization between the primary and secondary OLT of dual homed type-B protection pair fails. | The Monitor > Faults page is updated. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|--------------------------------|-----------------------------------|----------|---|---|
| OLT-HW-ASIC-DISCONNECT | OLT-HW-ASIC-DISCONNECT | CRITICAL | Generates when the OLT faces Aspen or Qumran chipsets disconnection (serial number and ports). | The Monitor > Faults page is updated. |
| SDPON-SOFTWARE-DOWNLOAD-FAILED | SDPON-SOFTWARE-DOWNLOAD-AD-FAILED | MAJOR | Generates when the software download process is failed. | The Monitor > Faults page is updated. |
| OLT-POWER-ON-REBOOT | OLT-POWER-ON-REBOOT | CRITICAL | Generates when the OLT gets rebooted due to power supply failures. | The Monitor > Faults page is updated. |
| OLT-ENABLE-VLAN-KPIS-FAILED | OLT-ENABLE-VLAN-KPIS-FAILED | WARNING | Generated when enabling the VLAN KPIs fails at the OLT. | The Monitor > Faults page is updated. |
| OLT-DISABLE-VLAN-KPIS-FAILED | OLT-DISABLE-VLAN-KPIS-FAILED | WARNING | Generated when disabling the VLAN KPIs fails at the OLT. | The Monitor > Faults page is updated. |
| ONT-LOSS-OF-FRAME | ONT-LOSS-OF-FRAME | MAJOR | Generated when the OLT receives consecutive invalid delimiters from the ONT. | The Monitor > Faults page is updated. |
| OLT-UPDATE-LAG-FAILED | OLT-UPDATE-LAG-FAILED | CRITICAL | Generated when the updated LAG fails at the OLT. | The Monitor > Faults page is updated. |
| PORT-MODE-CHANGE-FAILED | PORT-MODE-CHANGE-FAILED | CRITICAL | Generated when port mode change is failed at OLT. | The Monitor > Faults page is updated. |
| ONT-TYPE-CHANGE-DETECTED | ONT-TYPE-CHANGE-DETECTED | MAJOR | Generated when the ONU reports a different number of UNI ports from the last reboot. It happens when the ONU is upgraded to a new image | The Monitor > Faults page is updated. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|-----------------------------|-----------------------------|----------------|---|---|
| | | | that reports the change in the behavior of UNI ports. | |
| PON-LOS-DGi | PON-L OS-DGi | MAJOR | Generated by the OLT when PON LOS is detected due to last active ONU Dying Gasp. | The Monitor > Faults page is updated. |
| DATA-MIGRATION- FAILED | NA | CRITICAL | After the RMS upgrade, if there are any failures in the DB Migration this alarm is raised. For more information on DB migration failure, see Verifying the DB Migration Status (on page 21) . | The Monitor > Faults page is updated. |
| SDPON-PERF-ATTN- REQD | SDPON-PE RF-ATTN- REQD | MAJOR | Generated when OLT detects data path impact on the OLT resources like VLAN. | The Monitor > Faults page is updated. |
| SDPON-HIGH-AOF- UTILIZATION | SDPON-HIGH-AOF- UTILIZATION | MAJOR/CRITICAL | <p>Generated when the AOF size of the configuration database (REDIS) exceeds the configured threshold value.</p> <ul style="list-style-type: none"> • A major severity level alarm is reported when the AOF size exceeds 50% of the Manual Compaction Limit. • A critical severity level alarm is reported when the AOF size exceeds 70% of the maximum size of AOF at which the Liveness Probe is failing. | The Monitor > Faults page is updated. |

Table 402. List of Alarms (continued)

| Alarm Name (RMS) | Event Name (CBAC) | Severity | Description | RMS Behavior |
|-------------------------------------|-------------------------------------|----------|---|---|
| | | | At any point, only a single alarm with a severity level critical or major exists in the system. | |
| VNET-PROFILE-SERVICE-UPDATE-FAILURE | VNET-PROFILE-SERVICE-UPDATE-FAILURE | CRITICAL | Generated when the VNET profile update is failed for one or more associated admin enabled services. | The Monitor > Faults page is updated. |
| OLT-PACKET-CAPTURE-FAILED | OLT-PACKET-CAPTURE-FAILED | MAJOR | Generated when the packet capture (PCAP) job process fails at the OLT. | The Monitor > Faults page is updated. |
| EVENT-COLLECTION-FAILURE | NA | MAJOR | Generated when the event collection task is failed. | The Monitor > Faults page is updated. |
| FAULT-COLLECTION-FAILURE | NA | MAJOR | Generated when the fault collection task is failed. | The Monitor > Faults page is updated. |
| AUDITLOG-COLLECTION-FAILURE | NA | MAJOR | Generated when the auditlog collection task is failed. | The Monitor > Faults page is updated. |

Appendix B: Events

This following table lists the events generated by CBAC and the RMS application.

Table 403. List of Events

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|------------------|-------------------|---|--|
| ME-UP | OLT-UP | Generated when the ME activation is successful or when the ME connectivity is reestablished successfully. | The operational state of the ME is changed to UP and the ME activity log is updated. |
| ME-DOWN | OLT-DOWN | Generated when the ME activation fails due to unsuccessful GRPC connection establishment between the ME and RMS. The possible reasons are. <ul style="list-style-type: none"> • ME is powered off. • ME is unreachable to RMS. • Mismatch certificates between the ME and RMS • Deactivate ME from RMS. | The operational state of the ME is changed to DOWN and the ME activity log is updated. |
| ME-DISCOVERED | ONT-DISCOVERED | Generated when the ME discovers a known ONT. | <ol style="list-style-type: none"> 1. Creates a logical link if the link does not exist. 2. If the logical link exists with the discovered ONT, check if all the parameters (OLT Id, OLT port) are matching. If there is a mismatch, raises a <i>SERVICE_CONFIGURATION_MISMATCH</i> fault. 3. The ONT is visible in the monitoring of OLT/PON-PORT that are connected to the ONT. 4. The ONT activity log is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|-------------------------|-------------------|---|--|
| ME-UP | ONT-UP | Generated when the ME activation is successful. | The operational state of the ME is changed to UP and the ME activity log is updated. |
| ME-DOWN | ONT-DOWN | Generated when the ME activation fails due to unsuccessful OMCI connection establishment between the OLT and ONT. The possible reasons are. <ul style="list-style-type: none"> • ONT ranging failure. • Loss of Signal (LOS) at ONT. • PON link failure between the OLT and ONT. • Deactivate ONT from RMS. | The operational state of the ME is changed to DOWN and the ME activity log is updated. |
| INTERFACE-UP | PORT-UP | Generated when the port activation is successful. This is applicable for PON, NNI, and UNI ports. | The operational state of the port is changed to UP and the ME activity log is updated in the Monitor page. |
| INTERFACE-DOWN | PORT-DOWN | Generated when the port activation is failed. This is applicable for PON, NNI, and UNI ports. | The operational state of the port is changed to DOWN and the ME activity log is updated in the Monitor page. |
| SUBSCRIBER-SERVICE-DOWN | SERVICE-DOWN | Generated when one of the following conditions occur. <ul style="list-style-type: none"> • A service is successfully deactivated. • When you send the http status code 202 to the CBAC client to activate the service request and the service activation fails. • A service status becomes DOWN. | The operational state of the subscriber service is changed to DOWN. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|---------------------------------|---|---|---|
| SUBSCRIBER-SERVICE-UP | SERVICE-UP | Generated when the service activation for the subscriber is successful or the service status is UP. | The operational state of the subscriber service is changed to UP. |
| ME-REBOOTED | OLT-REBOOTED OLT-REBOOT-SUCCESSFUL NT-REBOOT-SUCCESSFUL | Generated when the ME is rebooting without a trigger from northbound (manual or software watchdog restart). | The software_reboot_status of the ME is changed to REBOOT-SUCCESSFUL and the activity log is updated. |
| ME-REBOOT-FAILED | OLT-REBOOT-FAILED ONT-REBOOT-FAILED | Generated when the ME reboot fails. | The software_reboot_status of the ME is changed to REBOOT-FAILED and the activity log is updated. |
| ME-SOFTWARE-DOWNLOAD-SUCCESSFUL | OLT-SOFTWARE-DOWNLOAD-SUCCESSFUL | Generated when the ME software download process is successful. | The ME activity log is updated. |
| ME-SOFTWARE-ROLLBACK-INITIATED | OLT-SOFTWARE-ROLLBACK-INITIATED | Generated when the ME software rollback process is initiated. | <ol style="list-style-type: none"> The software_rollback_status on the ME is changed as INITIATED. The ME activity log is updated. |
| ME-SOFTWARE-ROLLBACK-SUCCESSFUL | OLT-SOFTWARE-ROLLBACK-SUCCESSFUL | Generated when the ME cancel upgrade process is successful. | <ol style="list-style-type: none"> The software_rollback_status on the ME is changed as ROLL BACK-SUCCESSFUL. The ME activity log is updated. This event is processed only if the software_rollback_status is changed as INITIATED. |
| ME-SOFTWARE-DOWNLOAD-FAILED | ME-SOFTWARE-DOWNLOAD-FAILED | Generated when the ME software download process fails. | The ME activity log is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|--------------------------------------|---------------------------------|--|---|
| ME-CONFIG-UPDATE | OLT-CONFIG | Generated when the ME is activated. You can check the version of the components (Maple, ONT, and OpenOLT) running on the ME. | The ME activity log is updated. |
| ONT-CONFIG | ONT-CONFIG | Generated when the ONT is activated, ONT configuration details are reported. | The ME activity log is updated. |
| ME-SHUTDOWN | OLT-SHUTDOWN | Generated when the maximum operating temperature of the ME is exceeded, and the ME is shutdown. | The ME activity log is updated. |
| ME-LOGIN-SUCCESS | OLT-LOGIN-SUCCESS | Generated when a user logs in to the ME successfully. | The ME activity log is updated. |
| SUBSCRIBER-IP-ADDRESS | SUBSCRIBER-IP-ADDRESS | Generated when the IP address is allocated to the subscriber. | The IP address of the subscriber is updated. |
| ME-LOGIN-FAILED | OLT-LOGIN-FAILED | Generated when a user attempts to log in to the ME and the login fails due to unauthorized user access or invalid credentials. | The ME activity log is updated. |
| ME-RESET-FAILED | OLT-RESET-FAILED | Generated when the ME reset fails. | The ME activity log is updated. |
| ME-RESET-SUCCESSFUL | OLT-RESET-SUCCESSFUL | Generated when the ME reset is successful. | The ME activity log is updated. |
| CONTROLLER-ACTIVATED | NA | Generated when the controller activation is successful | The admin state of the controller is changed to ACTIVE. |
| CONTROLLER-DEACTIVATED | NA | Generated when the controller deactivation is failed. | The admin state of the controller is changed to DEACTIVE. |
| CONTROLLER-AUTHORIZATI ON- FAILED | SDPON-AUTHORIZATI ON- FAILED | Generated when the controller authorization is failed due to unauthorized user access. | The Monitor > Events page is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|---|---|---|---|
| CONTROLLER-AUTHENTICATION-SUCCESSFUL | SDPON-AUTHENTICATION-SUCCESSFUL | Generated when the controller authentication is successful. | The Monitor > Events page is updated. |
| CONTROLLER-AUTHENTICATION-FAILED | SDPON-AUTHENTICATION-FAILED | Generated when an unauthorized user tries to access the controller CLI/RMS.  Note: The event is not reported for the following scenarios. <ul style="list-style-type: none"> • When the idle session times out. • When the access token ID expires after one hour. | The Monitor > Events page is updated. |
| ME-UNTRUSTED-MGMT-ACCESS | OLT-UNTRUSTED-MGMT-ACCESS | Generated when the OLT receives a management access request from an untrusted subnet. | The Monitor > Events page is updated. |
| ASSOCIATE-ACL-PROFILE-TO-ME-SUCCESSFUL | ASSOCIATE-ACL-PROFILE-TO-ME-SUCCESSFUL | Generated when you associate the ACL profile to the managed element and the operation is successful. | The Monitor > Events page is updated. |
| ASSOCIATE-ACL-PROFILE-TO-ME-FAILED | ASSOCIATE-ACL-PROFILE-TO-ME-FAILED | Generated when you associate the ACL profile to the managed element and the operation fails. | The Monitor > Events page is updated. |
| DISSOCIATE-ACL-PROFILE-FROM-ME-SUCCESSFUL | DISSOCIATE-ACL-PROFILE-TO-FROM-SUCCESSFUL | Generated when you dissociate the ACL profile from the managed element and the operation is successful. | The Monitor > Events page is updated. |
| DISSOCIATE-ACL-PROFILE-FROM-ME-FAILED | DISSOCIATE-ACL- | Generated when you dissociate the ACL profile from the | The Monitor > Events page is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|-----------------------------------|-----------------------------------|--|---|
| | PROFILE-FR OM-ME- FAILED | managed element and the operation fails. | |
| ADD-LAG-SUCCESSFUL | ADD-LAG-SUCCESSFUL | Generated when you add the LAG configuration, and the operation is successful. | The Monitor > Events page is updated. |
| ADD-LAG-FAILED | ADD-LAG-FAI LED | Generated when you add the LAG configuration, and the operation fails. | The Monitor > Events page is updated. |
| DELETE-LAG-SUCCESSFUL | DELETE-LAG-SUCCESSFUL | Generated when the delete the LAG configuration and the operation is successful. | The Monitor > Events page is updated. |
| DELETE-LAG-FAI LED | DELETE-LAG-FAI LED | Generated when you delete the LAG configuration, and the operation fails. | The Monitor > Events page is updated. |
| ENABLE-LAG-SUCCESSFUL | ENABLE-LAG-SUCCESSFUL | Generated when you enable the LAG, and the operation is successful. | The Monitor > Events page is updated. |
| ENABLE-LAG-FAI LED | ENABLE-LAG-FAI LED | Generated when you enable the LAG, and the operation fails. | The Monitor > Events page is updated. |
| DISABLE-LAG-SUCCESSFUL | DISABLE-LAG-SUCCESSFUL | Generated when you disable the LAG, and the operation is successful. | The Monitor > Events page is updated. |
| DISABLE-LAG-FAI LED | DISABLE-LAG-FAI LED | Generated when you disable the LAG, and the operation fails. | The Monitor > Events page is updated. |
| LAG-UP | LAG-UP | Generated when the LAG port becomes operationally up. | The Monitor > Events page is updated. |
| LAG-DOWN | LAG-DOWN | Generated when the LAG port becomes operationally down. | The Monitor > Events page is updated. |
| ADD-MEMBER-PORT-TO-LAG-SUCCESSFUL | ADD-MEMBER-PORT-TO-LAG-SUCCESSFUL | Generated when you add a member port to LAG, and the operation is successful. | The Monitor > Events page is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|---|---|---|---|
| ADD-MEMBER-P ORT- TO-LAG-FAILED | ADD-MEMBER-P ORT- TO-LAG-FAILED | Generated when you add a member port to LAG, and the operation fails. | The Monitor > Events page is updated. |
| DELETE-MEMBER- PORT-FROM-L AG- SUCCESSFUL | DELETE-MEMBER- PORT-FROM-L AG- SUCCESSFUL | Generated when you delete a member port from LAG and the operation is successful. | The Monitor > Events page is updated. |
| DELETE-MEMBER- PORT-FROM-L AG- FAILED | DELETE-MEMBER- PORT-FROM-L AG- SUCCESSFUL | Generated when you delete a member port from LAG and the operation fails. | The Monitor > Events page is updated. |
| ENABLE-E-LINE- SUCCESSFUL | ENABLE-E-LINE- SUCCESSFUL | Generated when you enable E-Line, and the operation is successful. | The Monitor > Events page is updated. |
| ENABLE-E-LINE- FAILED | ENABLE-E-LINE- FAILED | Generated when you enable E-Line, and the operation fails. | The Monitor > Events page is updated. |
| DISABLE-E-LINE- SUCCESSFUL | DISABLE-E-LINE- SUCCESSFUL | Generated when you disable E-Line, and the operation is successful. | The Monitor > Events page is updated. |
| DISABLE-E-LINE- FAILED | DISABLE-E-LINE- FAILED | Generated when you disable the E-Line, and the operation fails. | The Monitor > Events page is updated. |
| ENABLE-E-LAN- SUCCESSFUL | ENABLE-E-LAN- SUCCESSFUL | Generated when you enable E-LAN, and the operation is successful. | The Monitor > Events page is updated. |
| ENABLE-E-LAN- FAILED | ENABLE-E-LAN- FAILED | Generated when you enable E-LAN, and the operation fails. | The Monitor > Events page is updated. |
| DISABLE-E-LAN- SUCCESSFUL | DISABLE-E-LAN- SUCCESSFUL | Generated when you disable E-LAN, and the operation is successful. | The Monitor > Events page is updated. |
| DISABLE-E-LAN- FAILED | DISABLE-E-LAN- FAILED | Generated when you disable the E-LAN, and the operation fails. | The Monitor > Events page is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|------------------------------------|-------------------------------------|--|---|
| SDPON-VERSISON- AVAILABLE | SDPON-VERSISON- AVAILABLE | Generated when CBAC is informed when the new CBAC version is available. | The Monitor > Events page is updated. |
| SDPON-UPGRADE- SUCCESSFUL. | SDPON-SOFTWARE- UPGRADE- SUCCESSFUL | Generated when the CBAC software upgrade is successful. | The Monitor > Events page is updated. |
| UPDATE-ERPS - INSTANCE- SUCCESSFUL | UPDATE-ERPS - INSTANCE- SUCCESSFUL | Generated when you update the ERPS instance the operation is successful. | The Monitor > Events page is updated. |
| UPDATE-ERPS - INSTANCE-FAILED | UPDATE-ERPS - INSTANCE-FAILED | Generated when you update the ERPS instance the operation fails. | The Monitor > Events page is updated. |
| CREATE-ERPS - INSTANCE- SUCCESSFUL | CREATE-ERPS - INSTANCE- SUCCESSFUL | Generated when you create the ERPS instance the operation is successful. | The Monitor > Events page is updated. |
| CREATE-ERPS- INSTANCE-FAILED | CREATE-ERPS- INSTANCE-FAILED | Generated when you create the ERPS instance the operation fails. | The Monitor > Events page is updated. |
| ERPS-INSTANCE- STATE-CHANGE | ERPS-INSTANCE- STATE-CHANGE | Generated when the ERPS instance state is changed. | The Monitor > Events page is updated. |
| CREATE-MEP- INSTANCE-FAILED | CREATE-MEP- INSTANCE-FAILED | Generated when you create the MEP instance, and the operation fails. | The Monitor > Events page is updated. |
| CREATE-MEP- INSTANCE- SUCCESSFUL | CREATE-MEP- INSTANCE- SUCCESSFUL | Generated when you create the MEP instance, and the operation is successful. | The Monitor > Events page is updated. |
| DELETE-MEP- INSTANCE-FAILED | DELETE-MEP- INSTANCE-FAILED | Generated when you delete the MEP instance, and the operation is successful. | The Monitor > Events page is updated. |
| DELETE-MEP- INSTANCE- SUCCESSFUL | DELETE-MEP- INSTANCE- SUCCESSFUL | Generated when you delete the MEP instance, and the operation fails. | The Monitor > Events page is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|---|---|---|---|
| TYPE-B-PROTECTION-SWITCHOVER-SUCCESSFUL | TYPE-B-PROTECTION-SWITCHOVER-SUCCESSFUL | Generated when the auto or manual type-B protection switchover is successful. | The Monitor > Events page is updated. |
| TYPE-B-PROTECTION-TRAFFIC-RESUME-SUCCESSFUL | TYPE-B-PROTECTION-TRAFFIC-RESUME-SUCCESSFUL | Generated when the traffic is successfully resumed after an automatic or manual type-B protection switchover. | The Monitor > Events page is updated. |
| TYPE-B-PROTECTION-TRAFFIC-RESUME-FAILED | TYPE-B-PROTECTION-TRAFFIC-RESUME-FAILED | Generated when the traffic resume fails after an automatic or manual type-B protection switchover. | The Monitor > Events page is updated. |
| CREATE-ERPS-RING-SUCCESSFUL | CREATE-ERPS-RING-SUCCESSFUL | Generated when you create an ERPS ring and the operation is successful. | The Monitor > Events page is updated. |
| ONT-FIRMWARE-DOWNLOAD-ON-OLT-SUCCESSFUL | ONT-FIRMWARE-RE-DOWNLOAD-ON-OLT-SUCCESSFUL | Generated when the ONT firmware download on OLT process is successful. | The Monitor > Events page is updated. |
| PORT-SFP-INVENTORY | PORT-SFP-INVENTORY | Generated when the port addition operation is successful and the SFP information is available for the port. | The Monitor > Events page is updated. |
| ONT-FIRMWARE-DOWNLOAD-ON-ONT-SUCCESSFUL | ONT-FIRMWARE-RE-DOWNLOAD-ON-ONT-SUCCESSFUL | Generated when the ONT firmware download on ONT is successful. | The Monitor > Events page is updated. |
| ONT-FIRMWARE-ACTIVATE-COMMIT-SUCCESSFUL | ONT-FIRMWARE-RE-ACTIVATE-COMMIT-SUCCESSFUL | Generated when the ONT firmware activate and commit on ONT is successful. | The Monitor > Events page is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|---|---|---|---|
| OLT-CREATE-EXTERNAL-ALA RM-VLAN-SUCCESS FUL | OLT-CREATE-EXTERNAL-ALA RM-VLAN-SUCCESS FUL | Generated when you create an external alarm VLAN and the operation is successful. | The Monitor > Events page is updated. |
| OLT-DELETE-EXTERNAL-ALA RM-VLAN-SUCCESS FUL | OLT-DELETE-EXTERNAL-ALA RM-VLAN-SUCCESS FUL | Generated when you delete an external alarm VLAN and the operation is successful. | The Monitor > Events page is updated. |
| CREATE-RING-SUCCESSFUL | CREATE-RING-SUCCESSFUL | Generated when you create an ERPS ring and the operation is successful. | The Monitor > Events page is updated. |
| DELETE-RING-SUCCESSFUL | DELETE-RING-SUCCESSFUL | Generated when you delete an ERPS ring and the operation is successful. | The Monitor > Events page is updated. |
| CREATE-ERPS-INSTANCE-SUCCESSFUL | CREATE-ERPS-INSTANCE-SUCCESSFUL | Generated when you create an ERPS instance and the operation is successful. | The Monitor > Events page is updated. |
| CREATE-ERPS-INSTANCE-FAI LED | CREATE-ERPS-INSTANCE-FAI LED | Generated when you create an ERPS instance and the operation fails. | The Monitor > Events page is updated. |
| DELETE-ERPS-INSTANCE-SUCCESSFUL, | DELETE-ERPS-INSTANCE-SUCCESSFUL, | Generated when you delete an ERPS instance and the operation is successful. | The Monitor > Events page is updated. |
| DELETE-ERPS-INSTANCE-FAI LED | DELETE-ERPS-INSTANCE-FAI LED | Generated when you delete an ERPS instance and the operation fails. | The Monitor > Events page is updated. |
| OLT-ENABLE-E-LINE- FAILED | OLT-ENABLE-E-LINE- FAILED | Generated when you enable E-LINE, and the operation fails at the OLT. | The Monitor > Events page is updated. |
| OLT-DISABLE-E-LINE- FAILED | OLT-DISABLE-E-LINE- FAILED | Generated when you disable E-LINE, and the operation fails at the OLT. | The Monitor > Events page is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|--|--|--|---|
| OLT-CREATE-MEP-INSTANCE-FAILLED | OLT-CREATE-MEP-INSTANCE-FAILLED | Generated when you create an MEP instance and the operation fails at the OLT. | The Monitor > Events page is updated. |
| OLT-DELETE-MEP-INSTANCE-FAILLED | OLT-DELETE-MEP-INSTANCE-FAILLED | Generated when you delete an ERPS instance and the operation fails at the OLT. | The Monitor > Events page is updated. |
| OLT-ADD-MEMBER-PORT-TO-LAG-FAILED | OLT-ADD-MEMBER-PORT-TO-LAG-FAILED | Generated when you add member port to LAG, and it fails at the OLT. | The Monitor > Events page is updated. |
| OLT-DELETE-MEMBER-PORT-TO-LAG-FAILED | OLT-DELETE-MEMBER-PORT-TO-LAG-FAILED | Generated when you delete the member port associated with LAG and it fails at the OLT. | The Monitor > Events page is updated. |
| OLT-ADD-LAG-FAILED | OLT-ADD-LAG-FAILED | Generated when you add LAG, and the operation fails at the OLT. | The Monitor > Events page is updated. |
| OLT-DELETE-LAG-FAILED | OLT-DELETE-LAG-FAILED | Generated when you delete LAG, and the operation fails at the OLT. | The Monitor > Events page is updated. |
| JOIN-UNSUCCESSFUL | JOIN-UNSUCCESSFUL | Generated when an IGMP join request is received from a subscriber, but the IGMP join is not sent to BNG. | The Monitor > Events page is updated. |
| QUERY-EXPIRED | QUERY-EXPIRED | Generated when the CBAC does not receive any responses for the IGMP queries sent to the subscriber. | The Monitor > Events page is updated. |
| PORT-ONT-ENABLE-SERIAL-NUMBER-SUCCESSFUL | PORT-ONT-ENABLE-SERIAL-NUMBER-SUCCESSFUL | Generated when the enable serial number operation is successful. | The Monitor > Events page is updated. |
| PORT-ONT-SERIAL-NUMBER-AL- | PORT-ONT-SERIAL-NUMBER-AL- | Generated when the ONT serial number is disabled to put the | The Monitor > Events page is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|--|--|---|---|
| NUMBER-DISABLED-LED | NUMBER-DISABLED-LED | ONT into the emergency stop state. | |
| PORT-UPDATED | PORT-UPDATED | Generated to indicate that the port configuration is updated. In type-B configuration, when the primary port configuration is updated, the secondary port configuration is automatically updated by CBAC. This event info Content Specification to update the secondary port configuration. | The Monitor > Events page is updated. |
| SERVICE-UPDATE-BULK | SERVICE-UPDATE-BULK | Generated when a service is updated by execution of some command from the CBAC CLI, and to synchronize the data with RMS or when the OLT name is changed from RMS, and it reports the updated circuit IDs of the services. | The Monitor > Events page is updated. |
| SERVICE-DOWN-BULK | SERVICE-DOWN-BULK | Generated when a list of services are impacted by certain operations, such as service VLAN migration. | The Monitor > Events page is updated. |
| SERVICE-UP-BULK | SERVICE-UP-BULK | Generated when a list of services are impacted by certain operations, such as service VLAN migration. | The Monitor > Events page is updated. |
| ASSOCIATE-STORM-CONTROL-PROFILE-TO-ME-SUCCESSFUL | ASSOCIATE-STORM-CONTROL-PROFILE-TO-ME-SUCCESSFUL | Generated when you associate the storm control profile to the managed element (ME), and the operation is successful. | The Monitor > Events page is updated. |
| ASSOCIATE-STORM-CONTROL-PROFILE-TO-ME-FAILED | ASSOCIATE-STORM-CONTROL-PROFILE-TO-ME-FAILED | Generated when you associate the storm control profile to the managed element (ME), and the operation fails. | The Monitor > Events page is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|--|--|--|---|
| DISSOCIATE-STO RM- CONTROL-PROFI LE- FROM-ME- SUCCESSFUL | DISSOCIATE-STO RM- CONTROL-PROFI LE- FROM-ME- SUCCESSFUL | Generated when you dissociate the storm control profile from the managed element (ME), and the operation is successful. | The Monitor > Events page is updated. |
| DISSOCIATE-STO RM- CONTROL-PROFI LE- FROM-ME- FAILED | DISSOCIATE-STO RM- CONTROL-PROFI LE- FROM-ME- FAILED | Generated when you dissociate the storm control profile from the managed element (ME), and the operation fails. | The Monitor > Events page is updated. |
| LAG-MEMB ER-UP | LAG-MEMB ER-UP | Generated when the LAG member port becomes active-up after LACP association. | The Monitor > Events page is updated. |
| LAG-MEMBER-D OWN | LAG-MEMBER-D OWN | Generated when the LAG memberport becomes active-down and hence it fails to participate in handling the LAG traffic. | The Monitor > Events page is updated. |
| EMS-BACKUP- SUCCESSFUL | NA | Generated after successful backup of RMS database. | The Monitor > Events page is updated. |
| EMS-RESTORE- SUCCESSFUL | NA | Generated after successful restore of RMS database. | The Monitor > Events page is updated. |
| OLT-PON- MOVEMENT- COMPLETED | OLT-PON- MOVEMENT- COMPLETED | Generated when the PON movement procedure is completed. | The Monitor > Events page is updated. |
| TYPE-B- PROTECTION- CONFIG-SYNC- SUCCESSFUL | TYPE-B- PROTECTION- CONFIG-SYNC- SUCCESSFUL | Generated when the subscriber services configurations are synchronized successfully on the secondary CBAC controller on a dual homed type-b protection pair. | The Monitor > Events page is updated. |
| MAC-DUMP- COMPLETED | MAC-DUMP- COMPLETED | Generated when the MAC dump is successfully collected on the given resource. | The Monitor > Events page is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|---|---|--|---|
| OLT-FIRMWARE-DOWNLOAD-SUCCESSFUL | OLT-FIRMWARE-DOWNLOAD-SUCCESSFUL | Generated when the OLT firmware download process is successful. | The Monitor > Events page is updated. |
| OLT-FIRMWARE-ACTIVATION-SUCCESSFUL | OLT-FIRMWARE-ACTIVATION-SUCCESSFUL | Generated when the OLT firmware activation process is successful. | The Monitor > Events page is updated. |
| ONT-FIRMWARE-AUTO-DOWNLOAD-AD-INITIATED | ONT-FIRMWARE-AUTO-DOWNLOAD-AD-INITIATED | Generated when the ONT firmware download on ONTs is initiated by CBAC based on auto-upgrade rules. | The Monitor > Events page is updated. |
| PORT-CONFIGURED | PORT-CONFIGURED | Generated when CBAC reports this event to update the NNI port configuration and the configuration is changed from the network services. This indication is applicable for the NNI port. | The Monitor > Events page is updated. |
| SDPON-SOFTWARE-DOWNLOAD-SUCCESSFUL | SDPON-SOFTWARE-DOWNLOAD-SUCCESSFUL | Generated when the software download process is successful for the CBAC upgrade. | The Monitor > Events page is updated. |
| SDPON-API-VERSION- INFORMATION | SDPON-API-VERSION- INFORMATION | Generated when CBAC reports the following events. <ol style="list-style-type: none"> 1. CBAC software upgrade is successful. 2. RMS notifies CBAC on its version change. 3. CBAC restore across releases. | The Monitor > Events page is updated. |
| ONT-FIRMWARE-UPGRADE-JOB-REPORT | ONT-FIRMWARE-UPGRADE-JOB-REPORT | Generated when the ONT firmware upgrade completed on ONTs. | The Monitor > Events page is updated. |
| ENABLE-VLAN-KPIS-SUCCESSFUL | ENABLE-VLAN-KPIS-SUCCESSFUL | Generated when the VLAN KPIs are enabled, and the operation is successful. | The Monitor > Events page is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|-------------------------------------|--------------------------------------|---|---|
| DISABLE-VLAN-K PIS- SUCCESSFUL | DISABLE-VLAN-K PIS- SUCCESSFUL | Generated when the VLAN KPIs are disabled, and the operation is successful. | The Monitor > Events page is updated. |
| ONT-ENABLED | ONT-ENABLED | Generated when the ONT is enabled at CBAC from the CLI SYNC mode. | The Monitor > Events page is updated. |
| ONT-DISABLED | ONT-DISABLED | Generated when the ONT is disabled at CBAC from the CLI SYNC mode. | The Monitor > Events page is updated. |
| PORT-DISCOVE RED | PORT-DISCOVE RED | Indicates the initial state of the NNI port when the OLT is activated. This indication is applicable for NNI and alarm ports. | The Monitor > Events page is updated. |
| PORT-ENABLED | PORT-ENABLED | Generated when the UNI port is implicitly activated by CBAC based on the subscriber service activation. CBAC reports this event when PON or NNI port is activated from CBAC- CLI in the CLI-SYNC mode. | The Monitor > Events page is updated. |
| PORT-DISABLED | PORT-DISABLED | Generated when the UNI port is implicitly deactivated by CBAC based on the subscriber service deactivation. CBAC reports this event when PON or NNI port is deactivated from CBAC-CLI in the CLI-SYNC mode. | The Monitor > Events page is updated. |
| PORT-CONFIGU RED | PORT-CONFIGU RED | Generated when the NNI port configuration is updated and configuration is changed from the network services. This notification is applicable to the NNI port. | The Monitor > Events page is updated. |
| PORT-MODE- CHANGE- SUCCESSFUL | PORT-MODE- CHANGE- SUCCESSFUL | Generated when the port mode change is successful and RMS | The Monitor > Events page is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|--------------------------------------|--------------------------------------|--|---|
| | | updates the port mode. For example, GPON to XGSPON. | |
| ME-DOWN-BULK | ME-DOWN-BULK | Generated when the OLT is deactivated or rebooted. | The Monitor > Events page is updated. |
| SERVICE-UPDATERED | SERVICE-UPDATERED | Generated when a service is updated by execution of some command from the CBAC CLI, and to synchronize the data with RMS or when the OLT name is changed from RMS, and it reports the updated circuit IDs of the services. | The Monitor > Events page is updated. |
| SERVICE-ENABLED | SERVICE-ENABLED | Generated when the service is activated. | The Monitor > Events page is updated. |
| SERVICE-DISABLED | SERVICE-DISABLED | Generated when the service is deactivated. | The Monitor > Events page is updated. |
| PON-HARDWARE-RESET | PON-HARDWARE-RESET | Generated when the PON hardware is reset due to some hardware issue. | The Monitor > Events page is updated. |
| DATA-MIGRATION-SUCCESS | NA | After the RMS upgrade, this event is raised if the DB Migration is successfully completed. For more information on DB Migration Status, see Verifying the DB Migration Status (on page 21) . | The Monitor > Events page is updated. |
| OLT-APP-RESTARTED | OLT-APP-RESTARTED | Generated when the OLT application is restarted automatically without an OLT reboot. | The Monitor > Events page is updated. |
| VNET-PROFILE-SERVICE-UPDATED-SUCCESS | VNET-PROFILE-SERVICE-UPDATED-SUCCESS | Generated when VNET profile is updated and change(s) are applied to all associated services successfully. | The Monitor > Events page is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|--------------------------------|--------------------------------|---|---|
| OLT-PACKET-CAPTURE-COMPLETE | OLT-PACKET-CAPTURE-COMPLETE | Generated when the packet capture for the OLT is successful. | The Monitor > Events page is updated. |
| ME-LOGOUT | OLT-LOGOUT | Generated when the ME logout is successful. | The Monitor > Events page is updated. |
| CONTROLLER-USER-LOGOUT | SDPON-USER-LOGOUT | Generated when the controller logout is successful. | The Monitor > Events page is updated. |
| LOAD-BALANCE-CONFIG-SUCCESSFUL | LOAD-BALANCE-CONFIG-SUCCESSFUL | Generated when you update LAG load balance config, and the operation is successful. | The Monitor > Events page is updated. |
| LOAD-BALANCE-CONFIG-FAILLED | LOAD-BALANCE-CONFIG-FAILLED | Generated when you update LAG load balance config, and the operation fails. | The Monitor > Events page is updated. |
| ME-BACKUP-CONFIG-SUCCESSFUL | OLT-BACKUP-CONFIG-SUCCESSFUL | Generated when the OLT backup configuration process is successful. | The Monitor > Events page is updated. |
| ME-RESTORE-CONFIG-SUCCESSFUL | OLT-RESTORE-CONFIG-SUCCESSFUL | Generated when the OLT restore configuration process is successful. | The Monitor > Events page is updated. |
| ADD-ACE-SUCCESSFUL | ADD-ACE-SUCCESSFUL | Generated when you add ACE and the operation is successful. | The Monitor > Events page is updated. |
| ADD-ACE-FAILED | ADD-ACE-FAILLED | Generated when you add ACE and the operation fails. | The Monitor > Events page is updated. |
| CREATE-RING-FAILED | CREATE-RING-FAILED | Generated when you create a ring and the operation fails. | The Monitor > Events page is updated. |
| DELETE-RING-FAILED | DELETE-RING-FAILED | Generated when you delete a ring and the operation fails. | The Monitor > Events page is updated. |
| UPDATE-RING-SUCCESSFUL | UPDATE-RING-SUCCESSFUL | Generated when you update a ring and the operation is successful. | The Monitor > Events page is updated. |
| UPDATE-RING-FAILED | UPDATE-RING-FAILED | Generated when you delete a ring and the operation fails. | The Monitor > Events page is updated. |

Table 403. List of Events (continued)

| Event Name (RMS) | Event Name (CBAC) | Description | RMS Behavior |
|-----------------------------------|------------------------------------|---|---|
| ME-SOFTWARE-ACTIVATION-SUCCESSFUL | OLT-SOFTWARE-ACTIVATION-SUCCESSFUL | Generated when the OLT software activation process is successful. | The Monitor > Events page is updated. |
| ME-SOFTWARE-DOWNLOAD-SUCCESSFUL | OLT-SOFTWARE-DOWNLOAD-SUCCESSFUL | Generated when the OLT software download process is successful. | The Monitor > Events page is updated. |
| ME-FIRMWARE-ACTIVATION-SUCCESSFUL | OLT-FIRMWARE-ACTIVATION-SUCCESSFUL | Generated when the OLT firmware activation process is successful. | The Monitor > Events page is updated. |
| ME-SOFTWARE-COMMIT-SUCCESSFUL | OLT-SOFTWARE-COMMIT-SUCCESSFUL | Generated when you commit the OLT software and the operation is successful. | The Monitor > Events page is updated. |
| ME-SOFTWARE-ROLLBACK-INITIATED | OLT-SOFTWARE-ROLLBACK-INITIATED | Generated when the OLT software rollback operation is initiated. | The Monitor > Events page is updated. |
| ME-SOFTWARE-ROLLBACK-SUCCESSFUL | OLT-SOFTWARE-ROLLBACK-SUCCESSFUL | Generated when you perform the OLT software rollback operation and the operation is successful. | The Monitor > Events page is updated. |

Appendix C: Kubernetes Log Dump Script

This section explains the procedure to collect all Kubernetes and application logs running on the K8s cluster.

Prerequisites

Execute the following command to ensure the *jq* package is installed in the master node where the script is running.

```
sudo apt-get install jq -y
```

Generating Log Dump

Execute the following steps in any of the master nodes to generate the log.

1. Ensure that the RMS Kubernetes-installation package is available in the master node.
2. Execute the following command from the *kubernetes-installation* directory to collect the logs.

```
sudo ansible-playbook log_collection.yml
```

3. Once the above command is executed, playbook initiates a script to collect all K8s and application logs at location */tmp/logdumps/* in the K8s-SYSTEM-LOGS-TIMESTAMP format.
4. In the *playbook(log_collection.yaml)*, you can mention the hosts where you want to run the script and collect the logs, and the same host must be updated in the *inventory/host file*. The default value is localhost. Change the **hosts** details from **localhost** to **all** in the *log_collection.yml* file to collect all K8 log levels.
5. By default, log dump collects all the Kubernetes related logs only. If you want to collect application logs, then specify *collect_pods_logs* bool as true (*collect_pods_logs: true*) in the *inventory/group-var/all* files.