



MicroClimate Management System

PON Manager User Guide

MCMS 6.2

323-1961-302 - Standard - Revision A

March 2026

Copyright© 2024 - 2026 Ciena® Corporation. All rights reserved.

Contents

LEGAL NOTICES	xi
CHAPTER 1	
Overview	17
CHAPTER 2	
MicroClimate Management System for MCMS PON networks	19
MCMS PON Manager	20
MCMS REST API	21
MCMS NETCONF server	21
MCMS PON Controller	22
MCMS PON Controller host processing software	22
MCMS gNMI streaming telemetry server	22
MongoDB datastore	22
CHAPTER 3	
Architecture	25
MCMS PON Manager web app	25
MCMS PON Manager web server and API	25
Private APIs	25
MongoDB	26
CHAPTER 4	
Installation	27
Installation overview	27
Requirements and dependencies	27
Package contents	30
Installation methods	32
Linux package	32
List of procedures	32
Procedure 1 Preparing to install the MCMS PON Manager using the Debian package	33
Procedure 2 Preparing to install the MCMS PON Manager using Docker	34
Procedure 3 Installing the MCMS PON Manager using Debian package	35
Procedure 4 Configuring alternate certificates for the PON Manager installed using Debian package	37
Procedure 5 Validating the installation of the PON Manager installed using the Debian package	38
Procedure 6 Configuring the MCMS PON Manager installed using Docker	39
Procedure 7 Configuring alternate certificates for the PON Manager installed using Docker	43
Procedure 8 Installing the MCMS PON Manager using Docker	45
Procedure 9 Restarting a Docker container	47
Procedure 10 Starting a Docker container	48
Procedure 11 Stopping a Docker container	49
Procedure 12 Uninstalling the PON Manager using the Debian package	50

CHAPTER 5	
Apache configuration	51
OpenStreetMap content security policies	51
Denial of service	52
CHAPTER 6	
Security	55
TCP/IP ports and network services	55
Role based access control	56
HTTPS	57
Authentication	57
External RADIUS authentication	57
RADIUS protocol message requirements	58
Access request	59
Access challenge	60
Access response	61
Authentication methods priority	61
Local User Authentication and Session Establishment	63
Radius user authentication and session establishment	64
Two-factor radius user authentication and session establishment	65
Authentication for Existing Session	66
Authentication failure	67
Encrypted keyring credential storage	67
Encrypted MongoDB authentication and email recovery credentials	67
Client-side field level encryption	68
Django key	69
List of procedures	69
Procedure 13 Configuring an encrypted keyring	70
Procedure 14 Configuring the encrypted MongoDB authentication and email recovery credentials	71
Procedure 15 Configuring client-side field level encryption	72
CHAPTER 7	
PON Manager	75
Auto refresh	75
Site navigation	75
Switch and router	76
Switch and router summary tab	76
Switch and Router identification tab	77
PON Controller	79
PON Controller summary	79
PON Controller identification	80
Authentication tab	80
Firmware tab	82
Monitoring tab	82
Operations tab	83
Protection tab	84
Automation tab	84
Alarms summary	87

Automation summary	88
System status	90
Creating and managing accounts	91
Password requirements	91
Logging out	93
Update the PON Manager user interface branding	93
Idle session timeout out from the PON Manager session	93
Update ONU IDs, alloc IDs, and LLIDs in the inventory	93
Automation tab	93
Statistics	95
Displaying graphs	96
Real-time statistics	97
ONUs under OLT statistics	99
Grafana	100
PON automation device controls	102
Device configuration overrides	103
Rogue ONU tasks	104
Site customization	104
Version	105
List of procedures	107
Procedure 16 Configuring the PON Controller image	108
Procedure 17 Configuring the switch name	110
Procedure 18 Configuring the switch image	111
Procedure 19 Configuring location coordinates for the PON Controller	113
Procedure 20 Configuring location coordinates for the switch	114
Procedure 21 Configuring the PON Controller name	115
Procedure 22 Deleting a PON Controller	116
Procedure 23 Configuring PON Automation name	117
Procedure 24 Logging in to MCMS for the first time with a configured database and no users	118
Procedure 25 Logging in to MCMS for the first time with a configured database with users	119
Procedure 26 Logging out from a PON Manager session	120
Procedure 27 Deleting a PON automation override	121
Procedure 28 Upgrading from R3.0.X and earlier to R3.1.0 and later	122
CHAPTER 8	
Dashboard	123
CHAPTER 9	
Network	131
Devices	131
Device navigation tree	132
ONU device states	135
Hierarchy view	135
PON automation	136
PON automation summary	137
PON automation identification	138
Logs tab	139
Operations tab	139
List of procedures	142
Procedure 29 Adding the network VLAN to the inventory	143

- Procedure 30 Adding an ONU to the inventory 144
- Procedure 31 Removing the network VLAN from the inventory 145
- Procedure 32 Removing the ONU from the inventory 146
- Procedure 33 Upgrading ONU firmware 147

CHAPTER 10

ONU configuration

149

- ONU summary tab 149
- Registration state 151
- ONU identification tab 152
- Associate provisioning 152
- ONU firmware tab 154
- Provisioned bandwidth summary 156
- ONU services tab 157
- ONU ports tab 160
- CPEs on this ONU 162
- ONU monitoring 162
- ONU operations tab 164
- Automation tab 165
- List of procedures 167
 - Procedure 34 Configuring the ONU name 168
 - Procedure 35 Configuring the ONU image 169
 - Procedure 36 Upgrading ONU firmware 170
 - Procedure 37 Disabling an ONU firmware upgrade 171
 - Procedure 38 Resetting bit error rate values 172
 - Procedure 39 Setting the ONU service configuration 173
 - Procedure 40 Resetting the ONU 174
 - Procedure 41 Allowing ONU registration from the ONU 175
 - Procedure 42 Disabling the ONU laser through the ONU 176
 - Procedure 43 Deleting an ONU 177
 - Procedure 44 Resetting the MIB ONU on GPON devices 178
 - Procedure 45 Adding an ONU to an OLT inventory 179
 - Procedure 46 Disabling an ONU serial number through OLT to disable ONU transmit laser 180
 - Procedure 47 Removing the ONU from the inventory 182

CHAPTER 11

OLT configuration

183

- OLT summary tab 183
- OLT identification tab 186
- OLT firmware tab 187
- OLT services tab 187
 - OLT services 189
 - Source MAC Verify 190
- OLT ports tab 190
- OLT NNI networks tab 192
 - OLT config tab 192
 - PON flood type 194
 - CPE tab 195
- ONU inventory for OLT 196
- OLT monitoring tab 197

ONUs stats tab	199
OLT operations tab	200
OLT protection tab	202
OLT automation tab	202
OLT Bandwidth tab	203
List of procedures	204
Procedure 48	Configuring an OLT protection partner 206
Procedure 49	Enabling automatic switchover for OLT active and standby 208
Procedure 50	Enabling automatic switchover with OLT toggle 209
Procedure 51	Disabling automatic switchover for OLT active and standby 210
Procedure 52	Forcing a switchover from active OLT to standby OLT 211
Procedure 53	Enabling OLT service ports on the ONU 212
Procedure 54	Enabling OLT service ports 213
Procedure 55	Configuring the downstream QoS map on the ONU 214
Procedure 56	Configuring an SLA for an OLT service on the ONU 215
Procedure 57	Configuring VLAN tagging for an OLT service on an ONU 216
Procedure 58	Configuring VLAN priority 217
Procedure 59	Adding a VLAN tag 218
Procedure 60	Removing a VLAN tag 220
Procedure 61	Enabling DHCP relay 221
Procedure 62	Adding an OLT to the switch inventory 222
Procedure 63	Deleting switch or router data 224
Procedure 64	Removing the ONU from the inventory 225
Procedure 65	Synchronizing automatic assigned in the inventory 226
Procedure 66	Assigning next free block of consecutive ALLOC IDs to a specified number of OLT service ports 227
Procedure 67	Adding an OLT to an inventory 228
Procedure 68	Removing an OLT from an inventory 229
Procedure 69	Upgrading OLT firmware 230
Procedure 70	Disabling OLT firmware upgrade 232
Procedure 71	Adding an NNI network to an OLT 233
Procedure 72	Adding a new NNI network to the inventory 234
Procedure 73	Removing an NNI network from the inventory 235
Procedure 74	Adding static MAC addresses to the network VLAN 236
Procedure 75	Enabling source MAC verify 237
Procedure 76	Disabling source MAC verify 239
Procedure 77	Enabling PPPoE on NNI networks 240
Procedure 78	Resetting the OLT 241
Procedure 79	Deleting OLT data 242
Procedure 80	Allowing ONU registration on the OLT 243
Procedure 81	Enabling the ONU serial number to enable transmit laser 244
Procedure 82	Configuring the OLT image 245
Procedure 83	Configuring the OLT name 246

CHAPTER 12

Accounts

247

Personal	247
Administration	249
Users	249

Roles	249
View Permissions	250
Modify an Existing Role's Permissions	250
Modify an Existing Role's Session Expiry Age	252
Display preferences	253
Logs	254
Sessions	256
Authentication	258
Radius authentication	258
API Documentation	259
Open Street Location	262
Collapse navigation panel	262

CHAPTER 13**Global configuration****263**

Alarms	263
SLAs tab	264
Services tab	265
Profiles tab	265
Downstream QoS Map tab	266
Files tab	267
Service configuration file	268
Databases tab	270
Initialize	270
Update tab	271
Manage tab	272
Device tab	272
Global configuration automation tab	273
PON Auto switches and routers	275
ONU Service Packages	275
OLTs	276
ONUs	277
Firmware Upgrade Scheduler	278
Search tab	280
Bulk updating	281
Bulk deleting	281
Monitoring tab	282
Alarms	282
Alarm count graphics	282
List of procedures	283
Procedure 84 Creating an alarm configuration	285
Procedure 85 Deleting an alarm configuration	286
Procedure 86 Editing an SLA profile configuration	287
Procedure 87 Creating an SLA profile configuration	288
Procedure 88 Deleting an SLA profile configuration	289
Procedure 89 Viewing a service profile configuration	290
Procedure 90 Creating a service profile configuration	291
Procedure 91 Deleting a service profile configuration	292
Procedure 92 Creating a downstream QoS mapping	293

Procedure 93	Creating subscriber provisioning	294
Procedure 94	Viewing a downstream QoS mapping	296
Procedure 95	Uploading a picture to the database	297
Procedure 96	Uploading an OLT firmware image to the database	298
Procedure 97	Uploading an ONU firmware image to the database	299
Procedure 98	Uploading the ONU firmware onto the PON Manager	300
Procedure 99	Uploading a service configuration to the database	301
Procedure 100	Editing a picture type in the database	302
Procedure 101	Deleting a picture from the database	303
Procedure 102	Editing service configuration details in the database	304
Procedure 103	Deleting a service configuration from the database	305
Procedure 104	Creating a database connection	306
Procedure 105	Editing a database connection	307
Procedure 106	Clearing statistics for a database connection	308
Procedure 107	Cloning a database connection	309
Procedure 108	Deleting a database connection	310
Procedure 109	Replacing an OLT	311
Procedure 110	Replacing an ONU	312
Procedure 111	Configuring PON auto switches and routers to skip tasks	313
Procedure 112	Creating a new template	314
Procedure 113	Editing a template	315
Procedure 114	Creating a user	316
Procedure 115	Editing user information	317
Procedure 116	Deleting a user	318
Procedure 117	Creating a user role	319
Procedure 118	Editing user role assignments	322
Procedure 119	Deleting a user role	323
Procedure 120	Editing user password requirements	324
Procedure 121	Creating an upgrade job	325
Procedure 122	Editing an existing upgrade job	329
Procedure 123	Cloning an upgrade job	330
Procedure 124	Pausing an upgrade job	331
Procedure 125	Canceling an upgrade job	332
Procedure 126	Deleting an upgrade job	333
Procedure 127	Exporting the alarms table	334

LEGAL NOTICES

THIS DOCUMENT CONTAINS CONFIDENTIAL AND TRADE SECRET INFORMATION OF CIENA CORPORATION AND ITS RECEIPT OR POSSESSION DOES NOT CONVEY ANY RIGHTS TO REPRODUCE OR DISCLOSE ITS CONTENTS, OR TO MANUFACTURE, USE, OR SELL ANYTHING THAT IT MAY DESCRIBE. REPRODUCTION, DISCLOSURE, OR USE IN WHOLE OR IN PART WITHOUT THE SPECIFIC WRITTEN AUTHORIZATION OF CIENA CORPORATION IS STRICTLY FORBIDDEN. EVERY EFFORT HAS BEEN MADE TO ENSURE THAT THE INFORMATION IN THIS DOCUMENT IS COMPLETE AND ACCURATE AT THE TIME OF PUBLISHING; HOWEVER, THE INFORMATION CONTAINED IN THIS DOCUMENT IS SUBJECT TO CHANGE.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing CIENA PROVIDES THIS DOCUMENT “AS IS” WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice. For the most up-to-date technical publications, visit www.ciena.com.

GAI Use Restriction. Unless expressly authorized in writing by Ciena on a case-by-case basis, you may not enter or use any Ciena Documentation in any Generative AI system, or include such information in the data for training such a system.

Copyright© 2024-2026 Ciena® Corporation All Rights Reserved

Use or disclosure of data contained in this document is subject to the Legal Notices and restrictions in this section and, unless governed by a valid license agreement signed between you and Ciena, the Licensing Agreement that follows.

The material contained in this document is also protected by copyright laws of the United States of America and other countries. It may not be reproduced or distributed in any form by any means, altered in any fashion, or stored in a data base or retrieval system, without express written permission of the Ciena Corporation.

Security

Ciena® cannot be responsible for unauthorized use of equipment and will not make allowance or credit for unauthorized use or access.

Contacting Ciena

Corporate Headquarters	410-694-5700 or 800-921-1144	www.ciena.com
Customer Technical Support/Warranty		www.ciena.com/support/

Sales and General Information	North America: 1-800-207-3714 International: +44 20 7012 5555	E-mail: sales@ciena.com
In North America	410-694-5700 or 800-207-3714	E-mail: sales@ciena.com
In Europe	+44-207-012-5500 (UK)	E-mail: sales@ciena.com
In Asia	+81-3-3248-4680 (Japan)	E-mail: sales@ciena.com
In India	+91-22-42419600	E-mail: sales@ciena.com
In Latin America	011-5255-1719-0220 (Mexico City)	E-mail: sales@ciena.com
Training		E-mail: learning@ciena.com

For additional office locations and phone numbers, please visit the Ciena web site at www.ciena.com.

READ THIS LICENSE AGREEMENT (“LICENSE”) CAREFULLY BEFORE INSTALLING OR USING CIENA SOFTWARE OR DOCUMENTATION. THIS LICENSE IS AN AGREEMENT BETWEEN YOU AND CIENA COMMUNICATIONS, INC. (OR, AS APPLICABLE, SUCH OTHER CIENA CORPORATION AFFILIATE LICENSOR) (“CIENA”) GOVERNING YOUR RIGHTS TO USE THE SOFTWARE. BY INSTALLING OR USING THE SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AND AGREE TO BE BOUND BY IT.

1. License Grant. Ciena may provide “Software” to you either (1) embedded within or running on a hardware product (together with Software, “Product”) or (2) as a standalone application, and Software includes upgrades acquired by you from Ciena or a Ciena authorized reseller. The terms of this License apply to your use of the Software and associated documentation whether such has been provided by Ciena, an affiliate of Ciena, or by means of an authorized reseller or distributor. Subject to these terms, and payment of all applicable License fees including any usage-based fees, Ciena grants you, as end user, a non-exclusive, non-transferable, personal License to use the Software only in object code form, subject to any applicable authorized use, activation requirements, usage levels, scope of functionality and release level of the Software, as set forth in the applicable quote accepted by Buyer upon Buyer's issuance of an acceptable purchase order (“Order”), and in accordance with the detailed ordering information in the Ciena's generally available, applicable, Product documentation as of the date of such Order. Unless the context does not permit, Software also includes associated documentation. Where an Order is for a (a) perpetual license, you may use the Software and associated documentation for as long as you use the Product for internal business use, or a (b) subscription license, you may only use the Software and associated documentation during the subscription term. A subscription license includes Software upgrades and/or technical support Services during the subscription term (that are not included in a perpetual license), in accordance with the Order and as further described in the applicable Ciena's service description as of the date of the applicable Order. Prior to the expiration of each subscription term, Ciena will send you a quote for the annual renewal fee(s). To renew the subscription Software license(s) for additional subscription terms, you issue an Order in advance of the then-current expiration date of such subscription term.

2. Open Source and Third Party Licenses. If any Software is subject to an open-source license that provides the end user with rights that are broader than this License, then such rights shall take precedence. Ciena warrants that using Software in accordance with its documentation will

not subject you to any obligation to disclose, distribute or license your own software that interacts with Software.

3. Title. You are granted no title or ownership rights in or to the Software. Unless specifically authorized by Ciena in writing, you are not authorized to create any derivative works based upon the Software. Title to the Software, including any copies or derivative works based thereon, and to all copyrights, patents, trade secrets and other intellectual property rights in or to the Software, are and shall remain the property of Ciena and/or its licensors. Ciena's licensors are third party beneficiaries of this License. Ciena reserves to itself and its licensors all rights in the Software not expressly granted to you.

4. Confidentiality. The Software contains trade secrets of Ciena. Such trade secrets include, without limitation, the design, structure and logic of individual Software programs, their interactions with other portions of the Software, internal and external interfaces, and the programming techniques employed. The Software and related technical and commercial information, and other information received in connection with the purchase and use of the Software that a reasonable person would recognize as being confidential, are all confidential information of Ciena ("Confidential Information").

5. Obligations. You shall:

- i) Hold the Software and Confidential Information in strict confidence for the benefit of Ciena using your best efforts to protect the Software and Confidential Information from unauthorized disclosure or use, and treat the Software and Confidential Information with the same degree of care as you do your own similar information, but no less than reasonable care;
- ii) Keep a current record of the location of each copy of the Software you make;
- iii) Use the Software only in accordance with the authorized usage level;
- iv) Preserve intact any copyright, trademark, logo, legend or other notice of ownership on any original or copies of the Software, and affix to each copy of the Software you make, in the same form and location, a reproduction of the copyright notices, trademarks, and all other proprietary legends and/or logos appearing on the original copy of the Software delivered to you; and
- v) Issue instructions to your authorized personnel to whom Software is disclosed, advising them of the confidential nature of the Software and provide them with a summary of the requirements of this License.

6. Restrictions. You shall not:

- i) Use the Software or Confidential Information a) for any purpose other than your own internal business purposes; and b) other than as expressly permitted by this License;
- ii) Allow anyone other than your authorized personnel who need to use the Software in connection with your rights or obligations under this License to have access to the Software;
- iii) Make any copies of the Software except such limited number of copies, in machine readable form only, as may be reasonably necessary for execution in accordance with the authorized usage level or for archival purposes only;
- iv) Make any modifications, enhancements, adaptations, derivative works, or translations to or of the Software;
- v) Reverse engineer, disassemble, reverse translate, decompile, or in any other manner decode the Software;

vi) Make full or partial copies of the associated documentation or other printed or machine-readable matter provided with the Software unless it was supplied by Ciena in a form intended for reproduction;

vii) Export or re-export the Software and/or the associated documentation from the country in which it was received from Ciena or its authorized reseller unless authorized by Ciena in writing; or

viii) Publish the results of any benchmark tests run on the Software.

7. Audit: Upon Ciena's reasonable request you shall permit Ciena to audit the use of the Software to ensure compliance with this License.

8. U.S. Government Use. The Software is provided to the Government only with restricted rights and limited rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in FAR Sections 52-227-14 and 52-227-19 or DFARS Section 52.227-7013(C)(1)(ii), as applicable. The Software and any accompanying technical data (collectively "Materials") are commercial within the meaning of applicable Federal acquisition regulations. The Materials were developed fully at private expense. U.S. Government use of the Materials is restricted by this License, and all other U.S. Government use is prohibited. In accordance with FAR 12.212 and DFAR Supplement 227.7202, the Software is commercial computer software and the use of the Software is further restricted by this License.

9. Term of License. This License is effective until the applicable subscription term expires or the License is terminated. You may terminate this License by giving written notice to Ciena. This License will terminate immediately if (i) you breach any term or condition of this License or (ii) you become insolvent, cease to carry on business in the ordinary course, have a receiver appointed, enter into liquidation or bankruptcy, or any analogous process in your home country. Termination shall be without prejudice to any other rights or remedies Ciena may have. Upon any termination of this License, you shall destroy and erase all copies of the Software in your possession or control, and forward written certification to Ciena that all such copies of Software have been destroyed or erased. Your obligations to hold the Confidential Information in confidence, as provided in this License, shall survive the termination of this License.

10. Compliance with laws. You agree to comply with all laws related to your installation and use of the Software. Software is subject to U.S. export control laws and may be subject to export or import regulations in other countries. If Ciena authorizes you to import or export the Software in writing, you shall obtain all necessary licenses or permits and comply with all applicable laws.

11. Limitation of Liability. ANY LIABILITY OF CIENA SHALL BE LIMITED IN THE AGGREGATE TO THE AMOUNTS PAID BY YOU TO CIENA OR ITS AUTHORIZED RESELLER FOR THE SOFTWARE. THIS LIMITATION APPLIES TO ALL CAUSES OF ACTION, INCLUDING WITHOUT LIMITATION BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS. THE LIMITATIONS OF LIABILITY DESCRIBED IN THIS SECTION ALSO APPLY TO ANY LICENSOR OF CIENA. NEITHER CIENA NOR ANY OF ITS LICENSORS SHALL BE LIABLE FOR ANY INJURY, LOSS OR DAMAGE, WHETHER INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL INCLUDING WITHOUT LIMITATION ANY LOST PROFITS, CONTRACTS, DATA OR PROGRAMS, AND THE COST OF RECOVERING SUCH DATA OR PROGRAMS, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

12. General. Ciena may assign this License to an affiliate or to a purchaser of the intellectual property rights in the Software. You shall not assign or transfer this License or any rights hereunder, and any attempt to do so will be void. This License shall be governed by the laws

of the State of New York without regard to conflict of laws provisions. The U.N. Convention on Contracts for the International Sale of Goods shall not apply hereto. This License constitutes the complete and exclusive agreement between the parties relating to the license for the Software and supersedes all proposals, communications, purchase orders, and prior agreements, verbal or written, between the parties. If any portion hereof is found to be void or unenforceable, the remaining provisions shall remain in full force and effect.

CHAPTER 1

Overview

This document describes the architecture, installation, setup, security features, and usage information for the MCMS PON Manager.

The following table lists the chapters in this document.

Table 1 Chapters in MCMS PON Manager user guide

Chapter	Description
MicroClimate Management System	Provides an overview of the primary components of the MicroClimate™ Management System (MCMS).
Architecture	Describes the MCMS web app, API, database, and related servers.
Installation	Describes the debian package and Docker container methods for installing and configuring the PON Manager.
Apache configuration	Instructs the reader to refer to a separate document--the MCMS installation guide--for information on the MongoDB installation, setup, and operation.
Security	Describes the security features that are designed into the PON Manager.
PON Manager	Describes the features that are designed into the PON Manager.
Dashboard	Describes PON Controller dashboard.
Network	Describes the top-level management entities within the PON network.
ONU configuration	Describes the ONU configuration.
OLT configuration	Describes the OLT configuration.
Accounts	Describes how to create, edit, view, and manage user profiles and roles.
Global configuration	Describes how to execute global configurations.

Audience

This document is intended for engineers, planners, and system administrators who will operate the MCMS PON Manager software.

Readers and users should be familiar with:

- Debian concepts
- Docker concepts
- MongoDB concepts

- Provisioning features and users

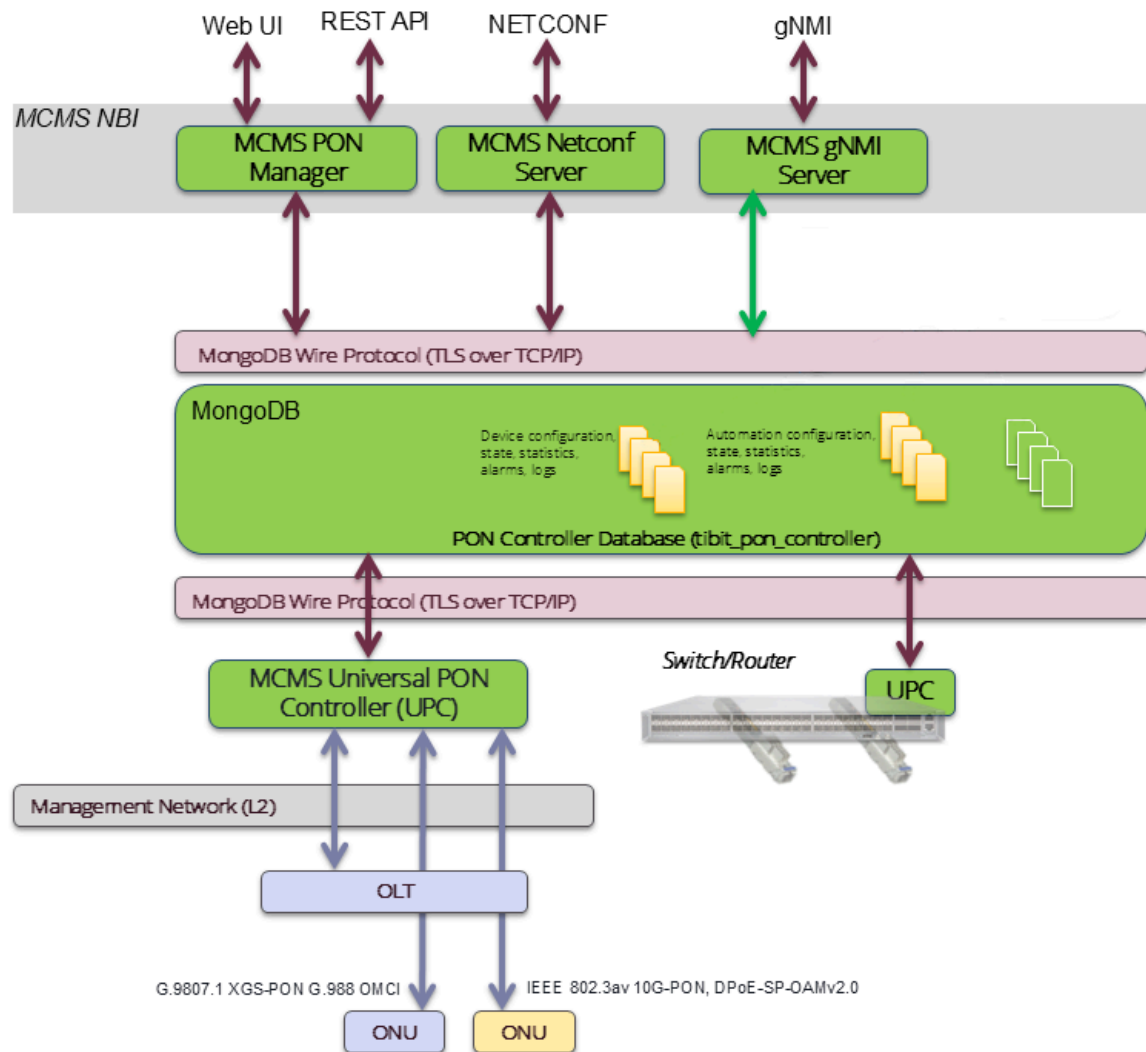
Trademark and copyright acknowledgments

Ciena®, Tibit™ MicroPlug™ OLT, and Tibit™ MicroClimate Management System® (MCMS) are registered trademarks of Ciena Corporation.

CHAPTER 2

MicroClimate Management System for MCMS PON networks

The MCMS is the management solution for MCMS PON networks. The following figure illustrates the MCMS.

Figure 1 MicroClimate Management System

MCMS PON Manager

The MCMS PON Manager is a single-page web application (Web App) and an accompanying REST API that provides a graphical user interface for managing the PON network. The Web App is built on the Angular web application framework, which provides an HTML and JavaScript frontend user interface. The REST API accompanies the Web App for the purposes of providing access to MongoDB for managing MCMS PON Manager users and the PON Network.

The MCMS PON Manager has the following features:

- Alarm management
- Dashboard view with a summary of PON network conditions
- Device monitoring and statistics
- Device provisioning and management

- Service configuration, including VLANs, service level agreements (SLAs), 802.1X authentication, DHCP relay, and PPPoE
- Logging for diagnostics and troubleshooting
- A Polyglot graphical OMCI (and future 10G EPON OAM) service configuration tool
- MCMS PON Controller database management
- MCMS PON Manager user management

MCMS REST API

The MCMS REST API is a component of the PON Manager that provides an application programming interface over HTTPS for managing PON devices for the Tibit solutions. The network operator can build device provisioning, service configuration, performance monitoring, logging collection, and other applications on top of the API for managing the PON network. In addition to customer applications, the PON Manager web app uses the API's PON and user management interfaces. The API implements a JSON interface that aligns directly with the PON Controller data model and interfaces with the MongoDB datastore for accessing configuration, state, statistics, logging, and file collections.

The MCMS REST API implements endpoints for managing the following:

- Device configuration and the status for PON Controllers, OLTs, ONUs, and switches and routers
- Service configuration, including ONU service configuration (SRV-CFG), VLANs, service level agreements (SLAs), 802.1X authentication, DHCP relay, and PPPoE
- Performance management statistics
- Device logs
- File management, including OLT firmware, ONU firmware, and device pictures

MCMS NETCONF server

The MCMS NETCONF server provides a standard NETCONF interface and customer facing API for managing the PON network.

The NETCONF server provides a standard NETCONF interface and customer facing API for managing the PON network.

The NETCONF server is built on the ConfD framework and interfaces with MongoDB.

Tibit YANG defines data models for provisioning and management of PON controllers, OLTs, ONUs, SLAs, service configuration and other elements of the PON network. For example:

- PON Controllers
- OLTs
- ONUs
- SLAs
- service configuration

MCMS PON Controller

The MCMS PON Controller is a stateless management controller and device driver application for configuring and monitoring the end points in a Tibit MicroPlug OLT PON network. It runs at customer-configurable intervals.

MongoDB serves as the northbound application programming interface for the PON Controller. The PON Controller applies the configuration to OLT and ONU devices from documents stored in MongoDB.

At each polling cycle, the PON Controller also collects state information, statistics, alarms, and logs from devices and reports the information to higher layer applications through MongoDB.

The PON Manager and NETCONF interfaces manage the PON Controller through MongoDB.

The PON Controller's southbound interface is the Tibit API, which is a Python API used to program OLTs using the Tibit OLT Management Interface (TOMI) protocol and ONUs (OMCI/DPoE).

MCMS PON Controller host processing software

The MCMS PON Controller software includes host processing components for control protocol functions that are typically required for deploying PON access networks.

Host processing includes support for 802.1X authenticator with RADIUS, DHCPv4 relay agent, DHCPv6 relay agent, and PPPoE intermediate agent.

Host processing provides functions such as DHCPv4 relay agent option 82 insertion and insertion of PPPoE BBF circuit ID and remote ID vendor tags.

The host processing software is packaged with and deployed alongside the PON Controller software.

MCMS gNMI streaming telemetry server

The MCMS gNMI Server provides a standards-based, asynchronous subscription interface to access MCMS data collected and stored in the MongoDB datastore. External gNMI clients, including 3rd party IT systems, can subscribe to configuration monitors, statistics, and/or alarms in the MCMS MongoDB.

The gNMI implementation enables gNMI *capabilities* and *subscribe* requests over a TLS transport interface. Data returned to the client from subscriptions is json encoded. The gNMI server supports *sample* and *on-change* subscription requests.

MongoDB datastore

The mongo database (MongoDB) provides the datastore for the MCMS. The MongoDB datastore contains all of the configuration, state, statistics, alarms, and logging data for the devices in the PON network. Northbound interfaces, such as the MCMS PON Manager, MCMS NETCONF Server, and customer applications interface with MongoDB to provision and retrieve monitoring information for devices in the PON network. The MongoDB serves as the interface

between the PON Manager and NETCONF and the PON Controller. The PON Controller defines the format and schema of the documents in the database.

Provisioning data generally flows downstream through the management network. The PON Manager and NETCONF interfaces write device configurations to MongoDB. The PON Controller reads the configuration data from MongoDB and programs the OLT and ONU devices accordingly.

Monitoring data, including device state, statistics, alarms, and logging, is collected and flows upstream through the management network. The PON Controller periodically collects state information from devices in the PON network and writes the monitoring data to MongoDB. The PON Manager reads the monitoring data from MongoDB for display in the web app.

CHAPTER 3

Architecture

The MCMS PON Manager software is composed of a graphical user front-end Web App and a RESTful interface (REST API) that provides access to the MongoDB datastore.

These software components integrate with the Apache2 web server and Django REST framework.

MCMS PON Manager web app

The core of the MCMS PON Manager web app is built on the Angular 17 framework and Bootstrap web front-end toolkit, along with libraries that support specific elements of the user interface. The Cytoscape library provides network visualization uses for graphical tools such as the Polyglot OMCI editor. Device statistics charts and graphs are built using the D3 graphs package and ngx-charts library. The font awesome library provides icons and fonts for the user interface.

MCMS PON Manager web server and API

The MCMS PON Manager web server is built on the ubiquitous Apache HTTP server, with Django running as a WSGI plugin and exposing a REST API. The REST API is a Tibit-created interface to the MCMS PON Controller database being hosted in MongoDB.

The PON Manager utilizes the user, group, permissions, and session management features of the Django REST framework to provide secure access and authorization for the web interface. See the security and accounts sections for more information on the PON Manager [Chapter 6](#), “Security” and [Chapter 12](#), “Accounts” management features.

By default, Django does not support integration with non-relational databases. Custom MongoEngine models are used to communicate with MongoDB. As HTTP requests are received, they are handled by Django accordingly but are mapped to the custom models for database operations instead of Django's default ORM.

Private APIs

The REST API implements a number of private endpoints that are intended to be used by the PON Manager Web App only. These private APIs are not published in customer documentation

and should not be used in customer applications. Private endpoints are not considered stable APIs and are subject to change from release to release.

MongoDB

Mongo database provides the datastore for the MicroClimate™ Management System, and is used to store PON device provisioning and monitoring information collected by the PON Controller. The MongoDB is an open source, secure database (www.mongodb.com) that employs a NoSQL architecture.

In addition to the PON device configuration and monitoring information, MongoDB is also used to store users, permissions, and session information used by the Django REST framework. The PON Controller defines the data model used to manage the PON network.

CHAPTER 4

Installation

There are two ways to install and configure the PON Manager: Debian package installation and Docker container. It is assumed that the MongoDB server is already configured.

Note: Native support for non-secure HTTP was deprecated for MCMS PON Manager version R2.2.0 and beyond, due to its inherent security vulnerabilities.

Installation overview

The two primary methods for installing and configuring the PON Manager are the debian package method and the Docker container method. This setup guide assumes that you have already set up a MongoDB server as described in the installation guide.

Note 1: Native support for non-secure HTTP has been deprecated for MCMS PON Manager version R2.2.0 and beyond, due to its inherent security vulnerabilities.

Note 2: Verify lighttpd or another web server is not already installed on the system before installing PON Manager. Also, verify that web servers and other services are not listening on TCP ports 80, 443, and 8013. Uninstall lighttpd and other web servers prior to installing PON Manager.

Requirements and dependencies

The following sections describe the requirements and dependencies for the PON Manager.

Supported browsers

PON Manager supports the following browsers:

Table 2 PON Manager supported browsers

Browser	Version
Firefox	94.x.x and later
Chrome	99.x.x and later

Supported operating systems

PON Manager supports the following operating systems:

Table 3 PON Manager supported operating systems

Operating system	Version
Ubuntu	22.04 and 24.04
Red Hat Enterprise Linux	8

Required packages

The following Linux apt packages are installed by the Debian package.

Refer to the [“Installation methods” on page 32](#) for instructions.

Note: MongoDB is not installed by the Debian/RPM package.

Table 4 Ubuntu

Ubuntu package	Ubuntu 22.04	Ubuntu 24.04
Apache2	2.4.52	2.4.52
Libapache2-mod-wsgi-py3	4.9.0	4.9.0
Libjpeg8-dev	8.0.0	8.0.0
Lsb-release	11.1.0	11.1.0
Mongo	6.0	8.0
Openssl	3.0.2	3.0.2
Pip3	22.0.2	22.0.2
Python	3.10.12	3.10.12
Python3-dev	3.10.6	3.10.6
Python3-venv	3.10.6	3.10.6
Systemd	249.11	249.11
Zlib1g-dev	1.2.11	1.2.11

Table 5 Red Hat Enterprise Linux

Package	RHEL 8
Audit	3.1.2
bash	8.30
coreutils	8.30
coreutils-single	8.30
httpd	2.4.37

Package	RHEL 8
mod_ssl	2.4.37
Mongo	6.0
spython3.11-devel	3.11.11
python3.11-mod-wsig	3.11.11
python3.11-setuptools	65.5.1

Python package dependencies

The following Python 3 packages are installed with Python package dependencies (pip3) by the Debian package within an MCMS PON Manager-specific Python virtual environment. Refer to the Debian installation instructions.

Table 6 Python package dependencies

Package	Version
dataclasses	0.6
Django	4.2.17
django-cors-headers	4.3.1
django-rest-swagger	2.2.0
django-rest-framework	3.15.2
django	1.2.30
drf-spectacular	0.27.2
jinja2	3.1.4
jsondiff	2.0.0
jsonschema	4.18.0
setuptools	70.0.0
Pillow	10.3.0
pymongo	4.7.2
python-resize-image	1.1.20
certifi	2024.12.14
requests	2.32.2
urllib3	2.2.3
simplejson	3.19.2
sqlparse	0.5.0
zxcvbn	4.4.28
cffi	1.16.0
python-snappy	0.7.1

30 Installation

Package	Version
httpagentparser	1.9.5
pyrad	2.4
future	1.0.0
watchdog	4.0.1
mongoengine	0.28.2
keyring	25.2.1
jsonref	1.1.0
jsonpatch	1.33
pymongocrypt	1.14.1
mergedeep	1.3.4
cramjam	2.10.0
tzlocal	5.3.1

Package contents

The MCMS PON Manager software is provided as a .zip file. The contents of the package are described in the table below.

Table 7 Package contents

File/Directory	Description
tibit-ponmgr_R6.2.0_all.deb , tibit-ponmgr-R6.2.0-1.el8.x86_64.rpm Debian or RPM	Debian or RPM Package based MCMS PON Manager application.
docker/	Directory containing Docker container and configuration files.
docker/databases.json	Docker container-based MCMS PON Manager configuration file. See Docker.
docker/docker-compose.yml	Contains the VM install parameters to be utilized by docker compose.
docker/generate_django_key.py	Python 3 script to generate a randomized Django key. See "Django key" on page 69 .
docker/ponmgr-api.conf	Docker container based MCMS PON Manager configuration file.
docker/ponmgr-web.conf	Docker container based MCMS PON Manager configuration file.
docker/Dockderfile	Responsible for building docker image.
dockder/README.txt	Quick startup guide for installing and configuring PON Manager Docker container.
docker/recovery_email_configuration.json	Specifies the Docker container based MCMS PON Manager configuration file. See Docker.

File/Directory	Description
docker/set_keyring_passwd.py	Python 3 script to generate a keyring and set the credentials for MongoDB and recovery email server authentication. See “Encrypted keyring credential storage” on page 67 .
docker/user_database.json	Docker container-based MCMS PON Manager configuration file. See Docker.
examples/	Directory containing example REST API query requests.
legacy_uninstall.py	Uninstallation script for MCMS PON Manager versions R1.2.0 and below.
LICENSES.txt	Lists the licensing information for third party software used.
mongodb_install.sh	Installs MongoDB.
mongodb_start.sh	Starts forked MongoDB instance.
mongodb_uninstall.sh	Removes mongodb application, logs, configuration, and databases.
README.txt	Quick startup guide for installing and configuring the PON Manager debian package.
tibit_ponmgr_selfsigned_cert_req.conf	Configuration file for self-signed certificate created during installation.
tools/	Directory containing tools and utilities relating to MCMS PON Manager.
tools/generate_django_key.py	Python 3 script to generate a randomized Django key. See “Django key” on page 69 .
tools/bulk_configure/	Directory containing bulk configuration utility.
tools/bulk_configure/bulk_configure.py	Bulk configuration Python 3 script.
tools/bulk_configure/olt_bulk_config.csv	File where OLT device info to be pre-provisioned is configured.
tools/bulk_configure/onu_bulk_config.csv	File where ONU device info to be pre-provisioned is configured.
tools/bulk_configure/README.txt	Guide for utilizing the bulk configuration utility.
tools/csfl_key_manager/	Directory containing CSFLE configuration utility.
tools/csfl_key_manager/key_manager.py	Python 3 script to generate a CSFLE CMK and DEK.
tools/db_import/	Directory containing the database import utility.
tools/db_import/db_import.py	Database import Python 3 script, which imports device firmware, pictures, and ONU service configuration files into MongoDB.
tools/special_scripts/	Directory containing scripts to update database schema, merging syslog and stats collections, and dropping the outdated collections.
tools/branding/	Contains the script and files for creating a custom branded PON Manager.
tools/set_keyring_passwd.py	Contains the Python 3 script to generate a keyring and set the credentials for MongoDB and recovery email server authentication. See “Encrypted keyring credential storage” on page 67 .

File/Directory	Description
tools/set_keyring_secrets.py	Python 3 script to generate an encrypted keyring and associated key on the filesystem and store secrets in an encrypted format. See “Encrypted keyring credential storage” on page 67.
version.txt	Version information.

Installation methods

This section describes the steps to install and uninstall the MCMS PON Manager software using the provided installation scripts.

Note: Read all steps including the notes section prior to installing the software.

Linux package

The RPM and Ubuntu packages handle installation of all dependencies except for Python.

List of procedures

Procedures for Installation are:

- [Procedure 1, “Preparing to install the MCMS PON Manager using the Debian package”](#)
- [Procedure 2, “Preparing to install the MCMS PON Manager using Docker”](#)
- [Procedure 3, “Installing the MCMS PON Manager using Debian package”](#)
- [Procedure 4, “Configuring alternate certificates for the PON Manager installed using Debian package”](#)
- [Procedure 5, “Validating the installation of the PON Manager installed using the Debian package”](#)
- [Procedure 6, “Configuring the MCMS PON Manager installed using Docker”](#)
- [Procedure 7, “Configuring alternate certificates for the PON Manager installed using Docker”](#)
- [Procedure 8, “Installing the MCMS PON Manager using Docker”](#)
- [Procedure 9, “Restarting a Docker container”](#)
- [Procedure 10, “Starting a Docker container”](#)
- [Procedure 11, “Stopping a Docker container”](#)
- [Procedure 12, “Uninstalling the PON Manager using the Debian package”](#)

Procedure 1 Preparing to install the MCMS PON Manager using the Debian package

Complete the prerequisites for installing the MCMS PON Manager software using the Debian package as required by the network plan.

Steps

- 1 Ensure that you have an active internet connection.
- 2 Ensure that you have the MongoDB Server running to manage user authentication and serve as the default database.

Note: It is recommended to use the MongoDB server host 127.0.0.1 if it is running locally.

- 3 Ensure you have the latest Ubuntu updates.
- 4 Uninstall MCMS PON Manager: prior to R1.3.0, you must uninstall MCMS PON Manager before continuing with installation, see [Procedure 12, "Uninstalling the PON Manager using the Debian package"](#).

Note: When upgrading from an earlier release to R3.1.0 and later, additional post installation steps may be required after upgrading the PON Controller and PON manager packages. For more information, see [Procedure 3, "Installing the MCMS PON Manager using Debian package"](#) and [Procedure 28, "Upgrading from R3.0.X and earlier to R3.1.0 and later"](#).

Procedure 2 Preparing to install the MCMS PON Manager using Docker

Complete the prerequisites for installing the MCMS PON Manager software using Docker as required by the network plan.

Steps

- 1 Ensure that you have an active internet connection.
- 2 Ensure that you have the MongoDB server running to manage user authentication and serve as the default database.

Note 1: Use the MongoDB server host 127.0.0.1 if it is running locally.

Note 2: The MongoDB server is not provided as part of the PON Manager package or Docker container.

- 3 Install the following packages:

Required package	Version
Docker	28.0.0+ or higher
Docker Compose	2.30.0+ or higher

Procedure 3 Installing the MCMS PON Manager using Debian package

Use this procedure to install the MCMS PON Manager using Debian package.

Requirements

Before starting this procedure, ensure that you have performed [Procedure 1, “Preparing to install the MCMS PON Manager using the Debian package”](#).

Overview

The tibit-ponmgr_R6.2.0_all.deb package handles installation of all dependencies except for Python.

Note 1: By default, the MCMS PON Manager deploys over HTTPS using a self-signed certificate created during installation--this is not safe for a production environment. When installing the MCMS PON Manager for any other use than evaluation, use legitimate certificates. For information about how to configure alternate certificates, see [Procedure 4, “Configuring alternate certificates for the PON Manager installed using Debian package”](#).

Note 2: When upgrading from an earlier release to R3.1.0 and later, additional post installation steps may be required after upgrading the PON Controller and PON Manager packages. R3.1.0 introduced a database schema change that allows for better scalability of both system logs and statistics data collection. After upgrading from R3.0.X and earlier to R4.0.0, users are encouraged to run two scripts located in the “tools/ directory. The merge_collections.py script merges the old per device collections into the new consolidated per device type collections. After verifying the statistics and logs were merged properly, use the delete_collections.py script to delete the old collections from the database. Directions are located in the README.txt file in the MCMS PON Manager package.

Steps

- 1 Open a shell and change to the root directory of the MCMS PON Manager application.
- 2 Optional: If required, you can configure the self-signed certificate created during installation by modifying the configuration file within this package directory: tibit_ponmgr_selfsigned_cert_req.conf. There are two sections that may be modified:
 - a. [req_distinguished_name]

countryName	Country code. Ex: 'US' (United States), etc.
ST	State or province
localityName	City or locality
organizationName	Name of organization
organizationalUnit Name	Name of group/unit within organization

CN	Fully Qualified Domain Name of system
----	---------------------------------------

b. [alt_names]

DNS. *number*	Name to access web server. Configure additional names by adding more DNS.x lines with increasing numbers in place of x in the example above. Ex: DNS.1 = tibitdev-web DNS.2 = tibitdev-api DNS.3 = www.MCMS.com
IP.*number*	IP of machine. Configure additional interfaces by adding more IP.x lines with increasing numbers in place of x in the example above. Ex: IP.1 = 127.0.0.1 IP.2 = 10.1.10.225

3 Install the package:

- a.** Use the following command to install PON Manager with the default self-signed certificate:

Ubuntu: sudo apt install ./tibit-ponmgr_R6.2.0_all.deb

./tibit-ponmgr_R6.2.0_all.deb Red Hat: sudo dnf install ./tibit-ponmgr-R6.2.0-1.el8.x86_64.rpm

- b.** Optional: Use the following command to install PON Manager with the customized self-signed certificate configured in Step 2:

Ubuntu: sudo TIBIT_PONMGR_CERT_REQ=/path/to/file.conf apt \ install ./tibit-ponmgr_R6.2.0_all.deb\ install ./tibit-ponmgr_R6.2.0_all.deb

Red Hat: sudo TIBIT_PONMGR_CERT_REQ=/path/to/file.conf dnf \ install ./tibit-ponmgr-R6.2.0-1.el8.x86_64.rpm

Procedure 4 Configuring alternate certificates for the PON Manager installed using Debian package

Use this procedure to replace the default self-signed certificate and key with alternates for the PON Manager software installed using the Debian package as required by the network plan.

Requirements

A valid certificate and private key.

Steps

- 1 Navigate to `/etc/tibit/ponmgr/`.
- 2 Modify the following in the `ponmgr-api` file, within the `HTTPS Options` section:
 - a. Replace the existing value of the `SSLCertificateFile` directive with the path to a valid certificate.
 - a. Replace the existing value of the `SSLCertificateKeyFile` directive with the path to a valid private key.
- 3 Modify the following in the `tibitdev-web.conf` file, within the `HTTPS Virtualhost` section, modify the following:
 - a. Replace the existing value of the `SSLCertificateFile` directive with the path to a valid certificate.
 - a. Replace the existing value of the `SSLCertificateKeyFile` directive with the path to a valid private key.
- 4 Restart Apache.

Procedure 5 Validating the installation of the PON Manager installed using the Debian package

Validate the PON Manager software installed using the Debian package as required by the network plan.

Steps

- 1 Navigate to `https://<IP address of the server>` in a web browser.

For example: `https://10.1.10.255`

Note: The default port for serving web pages is 443; therefore any requests made over the non-secure port 80 are redirected to port 443.

Procedure 6 Configuring the MCMS PON Manager installed using Docker

Configure the MCMS PON Manager software installed using Docker as required by the network plan.

Requirements

Ensure that the MongoDB server that manages user authentication is running.

Overview

By default, MCMS PON Manager deploys over HTTPS using a self-signed certificate created during installation. This is not safe for a production environment. When installing the MCMS PON Manager for any use other than evaluation, use legitimate certificates. For information about how to configure alternate certificates, see [Procedure 7, “Configuring alternate certificates for the PON Manager installed using Docker”](#).

Note: Native support for non-secure HTTP is deprecated for MCMS PON Manager version R2.2.0 and higher due to its inherent security vulnerabilities.

Steps

- 1 Open a shell and change to the root directory of the MCMS PON Manager application.
- 2 Open the shell in the `docker/directory` directory that contains the `docker-compose.yml` file, and then edit the following PON Manager configuration files using a text editor:
 - a. `user_database.json`

Stores configuration details for database user authentication.

Key	Description
<code>host</code>	The hostname or IP address of the MongoDB server hosting the user's database.
<code>name</code>	Name of the user's database. The default name is <code>tibit_users</code> . Note: If the user's database name does not exist, a name is created.
<code>port</code>	The MongoDB port number.
<code>auth_enable</code>	A Boolean value to verify if the MongoDB server at <code>host : port</code> uses authentication.
<code>auth_db</code>	The name of the MongoDB authentication database.

Key	Description
	Note: This is used when <code>auth_enabled = true</code> .
username	The username used to authenticate the MongoDB user. Note: This is used when <code>auth_enabled = true</code> .
password	The password for the specified MongoDB user. Note: This is used when <code>auth_enabled = true</code> .
tls_enable	A Boolean value that indicates if the MongoDB server at <code>host:port</code> uses encryption.
ca_cert_path	The local path of the encryption certificate.
compression	A Boolean value that specifies whether snappy compression for MongoDB connections is enabled or not.
dns_srv	A Boolean value that indicates if the MongoDB server uses a DNS seed list.
db_uri	The raw MongoDB connection URI. Note: If this key is used, all other fields are ignored.
replica_set_enable	A Boolean value that specifies if the MongoDB server is running as a replica set.
replica_set_name	The name of the MongoDB replica set. Note: This is used when <code>replica_set_enabled = true</code> .
replica_set_hosts	A list of hosts to be used as the MongoDB replica set. Note: This is used when <code>replica_set_enabled = true</code> .
django_key	Cryptographic key used by Django. The field format is a free-form string, but Django recommends a minimum length of 50 characters, with at least five of them being unique. For more information on the Django Key, see “Django key” on page 69 .

Key	Description
	Note: A randomized key is generated during installation if the <code>django_key</code> field is not present.

b. databases.json

Stores the list of all available PON databases in the PON Manager.

Key	Description
host	The hostname or the IP address of the MongoDB server hosting the PON Controller database.
name	Name of the PON Controller database. The default name is <code>tibit_pon_controller</code> . Note: If the PON Controller database name does not exist, a name is created.
port	The MongoDB server port number.
auth_enable	A Boolean value to verify if the MongoDB server at <code>host:port</code> uses authentication.
auth_db	The name of the MongoDB authentication database. Note: This is used when <code>auth_enabled = true</code> .
username	The username used to authenticate the MongoDB user. Note: This is used when <code>auth_enabled = true</code> .
password	The password for the specified MongoDB user. Note: This is used when <code>auth_enabled = true</code> .
tls_enable	A Boolean value to indicate if the MongoDB server at <code>host:port</code> uses encryption.
ca_cert_path	The local path of the encryption certificate.
dns_srv	A Boolean value that indicates if the MongoDB server uses a DNS seed list.
db_uri	The raw MongoDB connection URI.

Key	Description
	Note: If this key is used, all other fields are ignored.
replica_set_enable	A Boolean value that specifies if the MongoDB server is running as a replica set.
replica_set_name	The name of the MongoDB replica set. Note: This is used when replica_set_enabled = true.
replica_set_hosts	List of hosts to be used as the MongoDB replica set. Note: This is used when replica_set_enabled = true.

c. recovery_email_configuration.json

Configures SMTP email server for sending user password recovery emails.

Key	Description
host	The host used for sending emails.
port	A string type value that specifies the port used for the SMTP server.
use_tls	Used to specify if the TLS connections must be set to true or false. This key uses a string type value.
user	The username for the SMTP server.
password	The password for the user.

3 Restart Apache using the following command:

Ubuntu: `sudo systemctl restart apache2.service`

Red Hat: `sudo systemctl restart httpd.service`

Red Hat: `sudo systemctl restart apache2.service`

Note: If you run into problems after updating the configuration files and restarting Apache, try clearing your browser's cache.

Procedure 7 Configuring alternate certificates for the PON Manager installed using Docker

Use this procedure to replace the default self-signed certificate and keys with alternates for the PON Manager software installed using Docker as required by the network plan.

Requirements

A valid certificate and private key.

Steps

- 1 From the MCMS PON Manager package root, navigate to `docker/`, then modify the configuration files mentioned in the subsequent steps.
- 2 Bind the certificate and key to a location within the Docker container by adding two additional bind volumes in `docker-compose.yml`, as shown in the following examples.

Example 1:

```
- type: bind
  source: ./ponManager.crt
  target: /etc/ssl/certs/ponManager.crt
```

Example 2:

```
- type: bind
  source: ./ponManager.key
  target: /etc/ssl/private/ponManager.key
```

The following table contains the keys and their descriptions.

Table 8 PON Manager's keys and descriptions

Key	Description
type	Type of volume. (Use bind)
source	Path to the file on host machine
target	Path where the file will be located on Docker container

- 3 Modify the following in the `ponmgr-api.conf` file, within the HTTPS Options section:
 - a. Replace the existing value of the `SSLCertificateFile` directive with the path to a valid certificate, as defined as `target` in `docker-compose.yml`.
 - a. Replace the existing value of the `SSLCertificateKeyFile` directive with the path to a valid private key, as defined as `target` in `docker-compose.yml`.

- 4 Modify the following in the `ponmgr-web.conf` file, within the `HTTPS Virtualhost` section:
 - a. Replace the existing value of the `SSLCertificateFile` directive with the path to a valid certificate, as defined as `target` in `docker-compose.yml`.
 - a. Replace the existing value of the `SSLCertificateKeyFile` directive with the path to a valid private key, as defined as `target` in `docker-compose.yml`.
- 5 Restart Apache

Procedure 8 Installing the MCMS PON Manager using Docker

Install the MCMS PON Manager software using Docker as required by the network plan.

Requirements

Before starting this procedure, complete [Procedure 2, “Preparing to install the MCMS PON Manager using Docker”](#).

Overview

The Docker file handles installation of dependencies and the configuration of Apache within the containerized virtual machine (VM).

Note 1: If you use the Docker setup as well as the Debian package setup on the same server, there is a possibility of conflict on port binding. This can occur even after an uninstallation, due to the presence of two Apache servers listening on port 80. In such a case, stop the Apache service that is running on the host.

Note 2: When upgrading MCMS PON Manager using the Docker, a new MCMS PON Manager container must be established with the new version. Upgrading an existing container version is not supported.

Steps

- 1 Open a shell in the docker /directory.
- 2 Install or upgrade the existing Docker package to version 28.0.0+ or higher.
- 3 If you want to update the certificate configuration file provided in the package root directory, you must update the Docker file to include the environment variable TIBIT_PONMGR_CERT_REQ, as shown in the following table.

Existing command	Replace with
RUN apt get update && apt get install -y && apt get install systemd -y && apt get install ./t tbit-ponmgr_R6.2.0_all. deb -y	RUN apt get update && apt get install -y && apt get install systemd -y && TIBIT_PONMGR_ CERT_REQ=tibit-ponmgr_ install/tibit_ponmgr_ selfsigned_cert_req.conf apt get install ./tibit- ponmgr_R6.2.0_all.deb -y

- 4 Build the Docker image used by the MCMS PON Manager container using the following Docker compose:


```
docker compose build
```
- 5 Set the Apache user as the owner of the databases . json configuration file, as follows:

```
chown www-data:www-data databases.json
```

- 6 Create, install, and start the container using the following docker-compose:

```
docker compose up -d
```

The software is installed in the following location: /opt/tibit/ponmgr, /etc/tibit/ponmgr, /var/www/html (symbolic links)

Procedure 9 Restarting a Docker container

Restart a running Docker container as required by the network plan.

Steps

- 1 Open the shell, and then navigate to the `docker-compose.yml` file.
- 2 Run the following command:
`docker compose restart`

Procedure 10 Starting a Docker container

Start a Docker container as required by the network plan.

Steps

- 1 Open the shell, and then navigate to the `docker-compose.yml` file.
- 2 Run the following command:
`docker compose up -d`

Procedure 11 Stopping a Docker container

Stop a running Docker container as required by the network plan.

Steps

- 1 Open the shell, then then navigate to the `docker-compose.yml` file.
- 2 Run the following command:
`docker compose down`

Procedure 12 Uninstalling the PON Manager using the Debian package

Uninstall the PON Manager software using the Debian package as required by the network plan.

Steps

- 1 Uninstall the PON Manager software using any one of the following options:
 - To uninstall PON Manager and retain the configuration files, run the following command:

Ubuntu: `sudo apt remove tibit-ponmgr`

Red Hat: `sudo dnf remove`

The PON Manager software is uninstalled without deleting the configuration files.
 - To uninstall PON Manager and also delete the configuration files, run the following command:

Ubuntu: `sudo apt remove tibit-ponmgr --purge`

Red Hat: n/a

The PON Manager software is uninstalled and the configuration files are also deleted.
 - To uninstall PON Manager release R1.3.0 and other previous versions, run the following command:

`sudo ./legacy_uninstall.py`

PON Manager version R1.3.0 and earlier versions are removed.

CHAPTER 5

Apache configuration

Modify the Apache configuration to enable multi-processing and to change thread count.

The configuration file is generated on PON Manager installation and can be found at '/etc/tibit/ponmgr/tibitdev-api.conf'. Locate the following line in tibitdev-api.conf:WSGIDaemonProcess localhost python-home=/opt/tibit/ponmgr processes=1 threads=15

To set up multi-process, simply change the 'process' variable to a number greater than one. Likewise, thread count can be updated by changing the 'threads' variable. The following is an example of a common use case for an Apache configuration with eight processes and fifteen threads:

```
WSGIDaemonProcess localhost python-home=/opt/tibit/ponmgr processes=8 threads=15
```

Apache must be restarted after any configuration file updates in order for the changes to take effect. Restart Apache with the command:

Ubuntu: `sudo systemctl restart apache2.service`

Red Hat: `sudo systemctl restart httpd.service`

OpenStreetMap content security policies

If Open Street Map Location Services are being used, the Apache configuration must be updated to enable Content Security Policies (CSP) to allow connections to the OpenStreetMap service <https://www.openstreetmap.org/>.

To enable OpenStreetMap CSPs, edit the PON Manager Apache configuration /etc/tibit/ponmgr/ponmgr-web.conf. Locate the comment "Open Street Map Location Enable/Disable" in this file, which provides a commented out example configuration containing the OpenStreetMap CSPs. Update the Content-Security-Policy with the OpenStreetMap URLs shown in the example. (For convenience, comment out the existing Content-Security-Policy and uncomment the Content-Security-Policy line containing the OpenStreetMap URLs. Restart Apache to enable the changes. Refer to *Global Configuration* chapter for additional information on Open Street Location.

```
# Open Street Map Location Enable/Disable
```

```
# Header setifempty content-security-policy "default-src 'none';
script-src 'self' Header setifempty Content-Security-Policy "default-src 'none'; script-src
'self';
```

Denial of service

Apache has built-in protections against denial of service (DoS) attacks. The RequestReadTimeout, Timeout, and KeepAliveTimeout directives limit the time allotted for certain actions and help mitigate these attacks.

Waiting for a client to send a request or waiting for subsequent requests before closing a connection are a few examples of these actions. Additionally, the following directives are responsible for limiting resource usage for activity triggered by a client:

- LimitRequestBody
- LimitRequestFields
- LimitRequestFieldSize
- LimitRequestLine
- LimitXMLRequestBody

Default values for Apache directives relevant to DoS protection are shown in the table below. If changes are desired, these settings should be carefully fine-tuned with consideration for the unique requirements and available resources of any system.

The following table describes the default Apache values.

Table 9 Default Apache values

Attribute	Default Value	Units
RequestReadTimeout	handshake=0 header=20-40,MinRate=500 body=20,MinRate=500	Seconds, bytes per second
Timeout	60	Seconds
KeepAliveTimeout	5	Seconds
KeepAlive	On	n/a
LimitRequestBody	1073741824	bytes
LimitRequestFields	100	number
LimitRequestFieldSize	8190	bytes
LimitRequestLine	8190	bytes
LimitXMLRequestBody	1000000	bytes
AcceptFilter	http data https data	n/a

Attribute	Default Value	Units
MaxRequestWorkers	400 Note: This value is the product of ServerLimit (default 16) and ThreadsPerChild (default 25)	integer

CHAPTER 6

Security

This chapter describes TCP/IP ports and network security.

TCP/IP ports and network services

MCMS PON Manager installs and is deployed over the Apache2 HTTP web server.

By default, the apache2 web service is configured to listen on the following TCP/IP ports.

The following table describes the Apache2 TCP/IP listening ports.

Table 10 Listening ports

Network service	TCP port	Description
HTTP	80	Listens for all HTTP traffic. Redirects all traffic to secure port 443.
HTTPS	443	Listens for all secure HTTPS traffic.
REST API	8013	Listens for all HTTPS traffic for MCMS PON Manager REST API.

In addition to providing network services, the MCMS PON Manager server requires network services from external systems to operate. PON Manager requires client access to the following network services.

The following table describes the client ports.

Table 11 Client ports

Network service	TCP port	Description
MongoDB	27017	Default TCP port of the MongoDB server that the PON Manager connects to.

Network service	TCP port	Description
Open Layers (Open Street Maps)	443	Disabled by default. Open Layers/OpenStreetMap render server that generates all geographic maps for PON Manager. DNS names are: • https://openlayers.org - • https://a.tile.openstreetmap.org - • https://b.tile.openstreetmap.org - • https://c.tile.openstreetmap.org -

Role based access control

MCMS HTTPS PON Manager utilizes user roles and permissions to control what actions each user may perform.

Every user is assigned a role by a system administrator. Each role within the system may have a set of permissions defined for what any user within that role may do. Each permission has an access type associated with it based on the create, read, update, and delete (CRUD) model. For example, a user role may be assigned the permission to read an OLT's configuration data, but may not be assigned permission to update it.

These permissions are enforced within the PON Manager REST API. For every call the web client makes to the server, the attached user session provides the REST API with the information needed to verify that user. After being verified to have an existing and valid session, that user permissions are then checked for the required permissions for that operation. If the user does not have the required permissions, the server takes no action and informs the web client that the user is not permitted to access the requested data. One exception is PON Manager login. A user will not have a valid session prior to login, so no permissions are checked. See [“Authentication” on page 57](#) for more information on session authentication.

The web client hides and disables content within the web application based upon the permissions of the current user. A user who only has read permissions, for example, will not have any save, create, add, or delete buttons available to them throughout the application. See [Chapter 12, “Accounts”](#) for more information on configuring users, roles, and permissions using the Web Client

HTTPS

PON Manager supports HTTPS for the REST API and for the web app through Apache configuration by default. HTTPS ensures the confidentiality, authenticity, and integrity of all PON Manager network traffic. Non-secure HTTP is not supported.

Authentication

This section includes topics related to MCMS PON Manager authentication.

Session expiration

A user session expires after a period of inactivity. The session expiration timeout (in minutes) is configured in the PON Manager user database. The session expiration timeout is configured on a user's role or globally for all sessions. The default global timeout period is 20 minutes after the last successful HTTP request. If a request is made with an expired session token, a 403 response is returned. The user will have to re-login and authenticate with PON Manager when their session expires.

Session purging

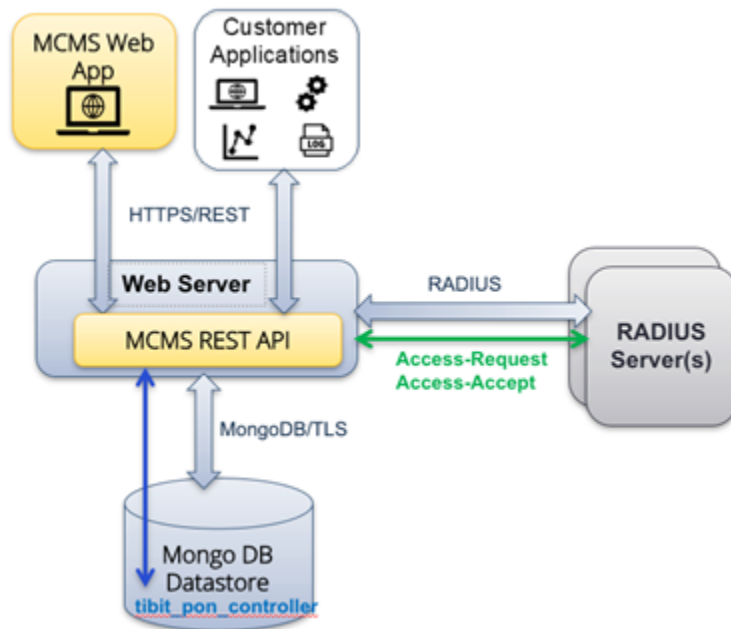
A new session object is created and stored in the MongoDB upon successful authentication. This is the case even if the user already has a previous session object(s) stored. Expired session objects are purged from MongoDB every 24 hours.

External RADIUS authentication

The PON Manager supports external authentication through the [RFC 2865] RADIUS protocol as an alternative to the local user authentication managed locally in MongoDB.

This feature enables PON Manager to authenticate users with an external radius server managed by the customer. The customer's radius server not only provides centralized authentication for the PON management interfaces but can also provide enhanced authentication services such as Multi-Factor Authentication.

The following figure shows the functional location of the external RADIUS server in a network with MCMS applications.

Figure 2 External RADIUS server in a network with MCMS applications

No per-user configuration is required in PON Manager when external radius authentication is used, where users are created in the customer's database instead of the PON Manager's local user database in MongoDB. However, the PON Manager does require the user's group/role name to be provided as part of the radius authentication exchange. The group/role name must be configured in the radius server by the customer for each RADIUS user. The customer database needs to match each radius user to a user role provisioned in PON Manager. User roles may include Administrators, Read Only, and others. The PON Manager supports a mix of local users and RADIUS users. At least one local administrator user must exist for essential PON Manager server management and for configuring and managing connections to the external RADIUS server.

Details on the interactions with the Radius server and how local and external authentication methods inter-operate are provided in the following sections.

RADIUS protocol message requirements

The PON Manager implements the standard RADIUS protocol exchange.

PON Manager sends Access-Request with user credentials to an external RADIUS server, and the RADIUS Server responds with either Access-Accept with user's group/role, or access-reject for unknown user, invalid password, or other authentication failure.

Access request

The access-request message sent by PON Manager includes RADIUS attributes for username, password, NAS Identifier, Service Type, and sometimes State. Details for each attribute and an example packet capture are shown below.

The following table shows the Access-Request message attributes.

Table 12 Access-Request message attributes

Attribute	Description
User-Name (1)	Specifies the username string (any format, not constrained to email address). Note: The PON Manager will continue to require an email address formatted username for local users.
User-Password (2)	Specifies the standard RFC 2865 MD hashed password.
NAS-Identifier (32)	Specifies the configurable value. The default is MCMS.
Service-Type (6)	Specifies the value hard-coded to "Login(1)."
State (24)	The session context created by the initial Access-Request. Note: This will only be included when following an Access-Challenge

The following figure shows an Access-Request message example packet.

Figure 3 Access-Request message example packet

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	mcms	radius-server	RADIUS	114	Access-Request id=233
2	0.000888	radius-server	mcms	RADIUS	84	Access-Accept id=233

Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)						
Ethernet II, Src: Cisco_d2:83:fa (14:a2:a0:d2:83:fa), Dst: RealtekU_3c:77:d9 (52:54:00:3c:77:d9)						
Internet Protocol Version 4, Src: mcms (10.3.8.126), Dst: radius-server (10.3.16.137)						
User Datagram Protocol, Src Port: 52729, Dst Port: 1812						
RADIUS Protocol						
Code: Access-Request (1)						
Packet identifier: 0xe9 (233)						
Length: 72						
Authenticator: celfe17c7c5cf16030f065238cd43b44						
[The response to this request is in frame 2]						
Attribute Value Pairs						
AVP: t=User-Name(1) l=22 val=radiususer@ciena.com						
AVP: t=User-Password(2) l=18 val=Encrypted						
AVP: t=NAS-Identifier(32) l=6 val=MCMS						
AVP: t=Service-Type(6) l=6 val=Login(1)						

0000	52 54 00 3c 77 d9 14 a2	a0 d2 83 fa 08 00 45 b8	RT <w... ..E
0010	00 64 c1 c0 40 00 3f 11	4c 04 0a 03 08 7e 0a 03	-d-@-?- L-...~
0020	10 89 cd f9 07 14 00 50	e0 0f 01 e9 00 48 ce 1f	P-...H-
0030	e1 7c 7c 5c f1 60 30 f0	65 23 8c d4 3b 44 01 16	·[·N·'0· e#·;D·
0040	72 61 64 69 75 73 75 73	65 72 40 63 69 65 6e 61	radiusus er@ciena
0050	2e 63 6f 6d 02 12 84 4c	b0 30 5e f1 da 22 f3 0b	.com...L·0^..."
0060	75 87 07 47 21 16 20 06	4d 43 4d 53 06 06 00 00	u-G!-· MCMS----
0070	00 01		..

Access challenge

PON Manager supports an Access challenge response from the RADIUS server when two-factor authentication is required. The Access challenge response is optional.

The following table shows the Access challenge message attributes.

Table 13 Access challenge message attributes

Attribute	Description
State (24)	Specifies the session context created by the initial Access-Request.
Reply-Message (18)	Specifies a string message that says the user must enter another token/password. Note: This message is displayed by the PON Manager in the 2FA input textbox.
Session-Timeout (27)	Specifies the number of seconds a user can enter their 2FA token before the session becomes stale. Note: This attribute is optional. If provided, the PON Manager displays the remaining time to enter their token.

The following figure shows the Access challenge response.

Figure 4 Access challenge response

No.	Time	Source	Destination	Protocol	Length	Info
→ 985	11.977394434	10.32.6.202	10.1.176.6	RADIUS	101	Access-Request id=87
← 986	12.035425465	10.1.176.6	10.32.6.202	RADIUS	113	Access-Challenge id=87
2768	36.597462930	10.32.6.202	10.1.176.6	RADIUS	119	Access-Request id=89
2769	36.648321985	10.1.176.6	10.32.6.202	RADIUS	108	Access-Accept id=89


```

> Frame 986: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface eth0, id 0
> Ethernet II, Src: ProxmoxServe_0c:f8:3a (bc:24:11:0c:f8:3a), Dst: JuniperNetwo_d1:f9:00 (40:71:83:d1:f9:00)
> Internet Protocol Version 4, Src: 10.1.176.6, Dst: 10.32.6.202
> User Datagram Protocol, Src Port: 1812, Dst Port: 48304
√ RADIUS Protocol
  Code: Access-Challenge (11)
  Packet identifier: 0x57 (87)
  Length: 71
  Authenticator: e286f5b2a73b787353e05447c247be41
  [This is a response to a request in frame 985]
  [Time from request: 0.058031031 seconds]
√ Attribute Value Pairs
  > AVP: t=State(24) l=18 val=6874466b4b4531323972796432364150
  > AVP: t=Reply-Message(18) l=27 val=Enter your TOKEN password
  > AVP: t=Session-Timeout(27) l=6 val=90

```

Access response

PON Manager requires the Access-response from the RADIUS server includes the RADIUS class attribute.

The Class attribute must be configured on the customer's RADIUS server. The Class attribute must include a string referencing a user role configured in the PON Manager. The group name string configured on the customer's RADIUS server must exactly match a User Role name provisioned in the PON Manager. Details for the Class attribute and an example packet capture are shown below.

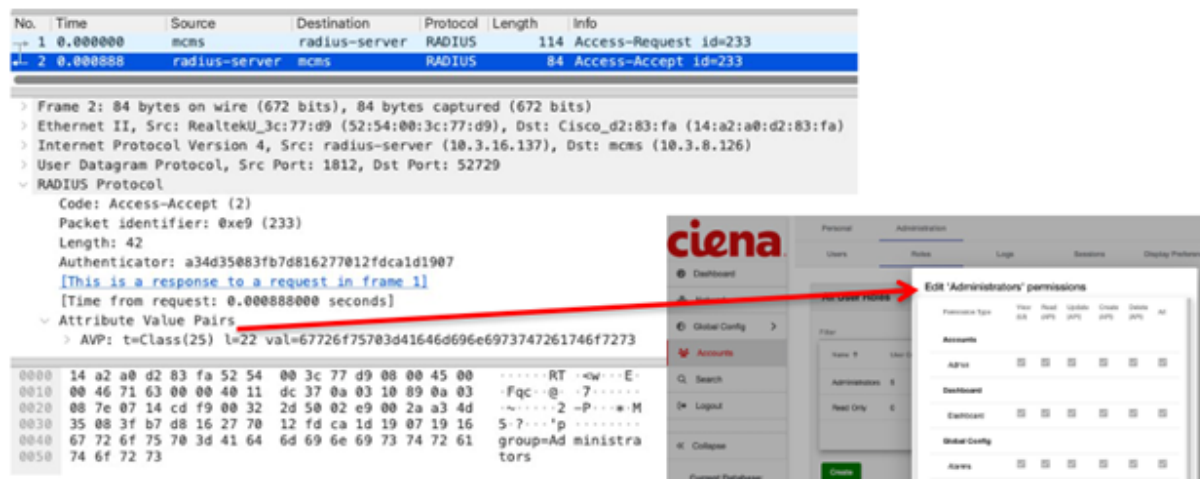
The following table describes the format for the RADIUS Class attribute.

Table 14 RADIUS Class attribute format

Attribute	Description
Class (25)	Encodes the PON Manager group/role assigned to the user with the format group=<PM Role>. For example, group=Administrators. Note: The customer configures the RADIUS Class attribute in the RADIUS server. The customer database must map the user to a PON Manager group/role.

The following figure shows a RADIUS Class attribute example packet.

Figure 5 RADIUS Class attribute example packet



Authentication methods priority

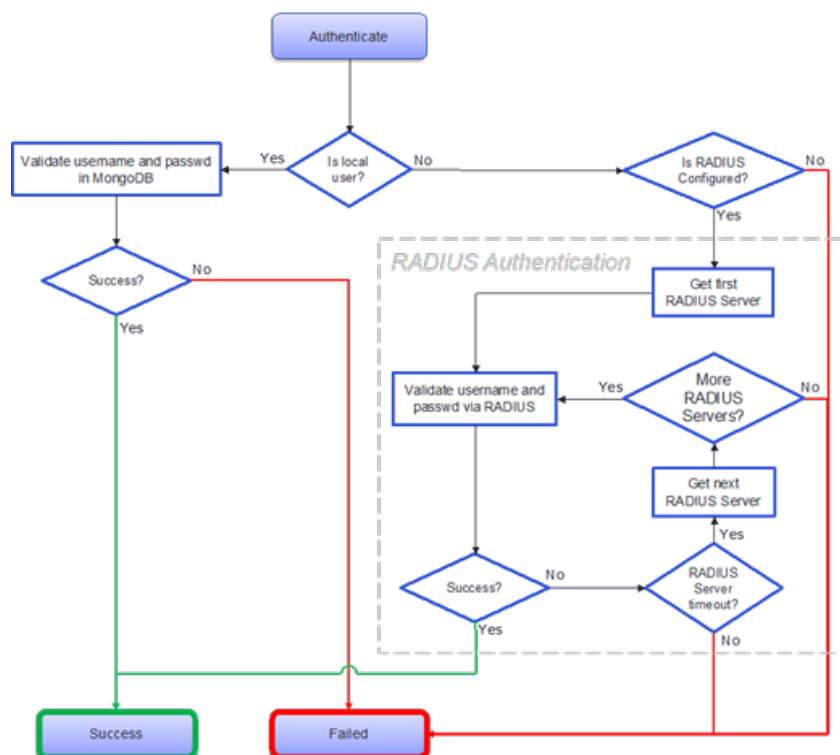
The PON Manager supports local user authentication simultaneously with external RADIUS authentication.

The authentication process is shown in the following flow chart. First, PON Manager authenticates users against the local users configured in MongoDB. If the same username is configured in both the local PON Manager database and the RADIUS server, only the local PON Manager configuration is used for authentication.

Next, if RADIUS authentication is enabled, PON Manager attempts to authenticate the user with the external RADIUS server. When multiple RADIUS servers are configured, the PON Manager attempts authentication with the server configured with the highest priority. If the first RADIUS authentication times out, the PON Manager attempts authentication with the next server. If both servers timeout, then the RADIUS authentication fails and PON Manager notifies the user of an authentication error.

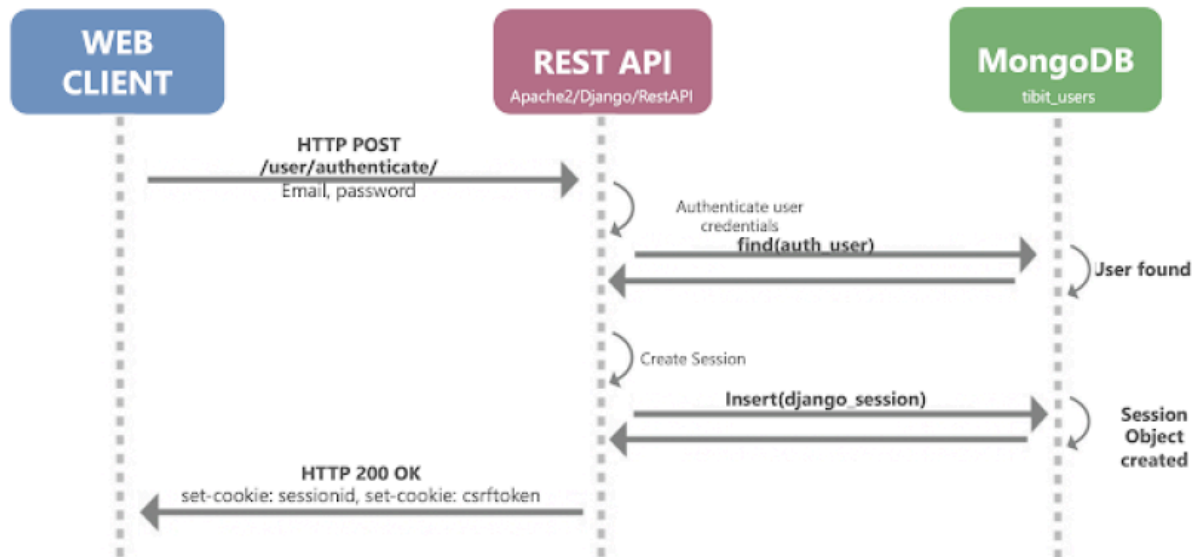
The following figure shows the authentication process.

Figure 6 Authentication process



Local User Authentication and Session Establishment

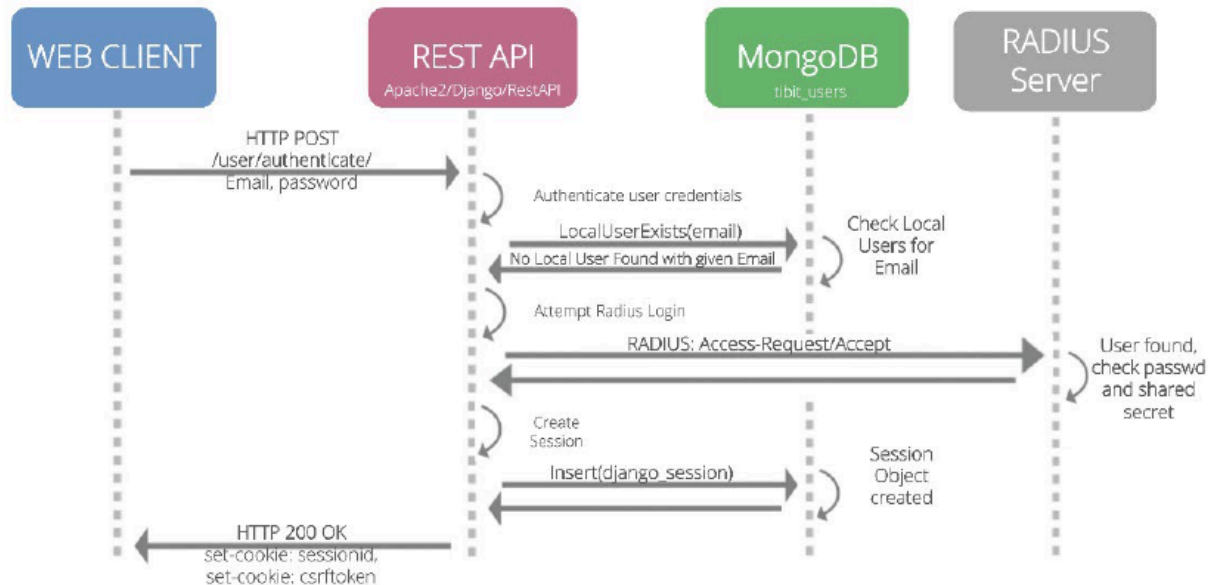
The following diagram displays the sequence of authenticating with the local user database and establishing a session for the user.



- **HTTP POST:** A user makes an HTTP request with a valid email and password combination to the REST API to authenticate.
- **find(auth_user):** The REST API queries the user collection, **tibit_users** in MongoDB to find and return the user profile matching the email address and password combination.
- **Insert(django_session):** The REST API creates a session associated with the authenticating user and inserts the session object into MongoDB.
- **HTTP 200 OK:** The user receives a successful response containing two set-cookie headers for the session identifier and csrftoken.

Radius user authentication and session establishment

The following diagram describes the sequence of authenticating with an external RADIUS server and establishing a session for the user.

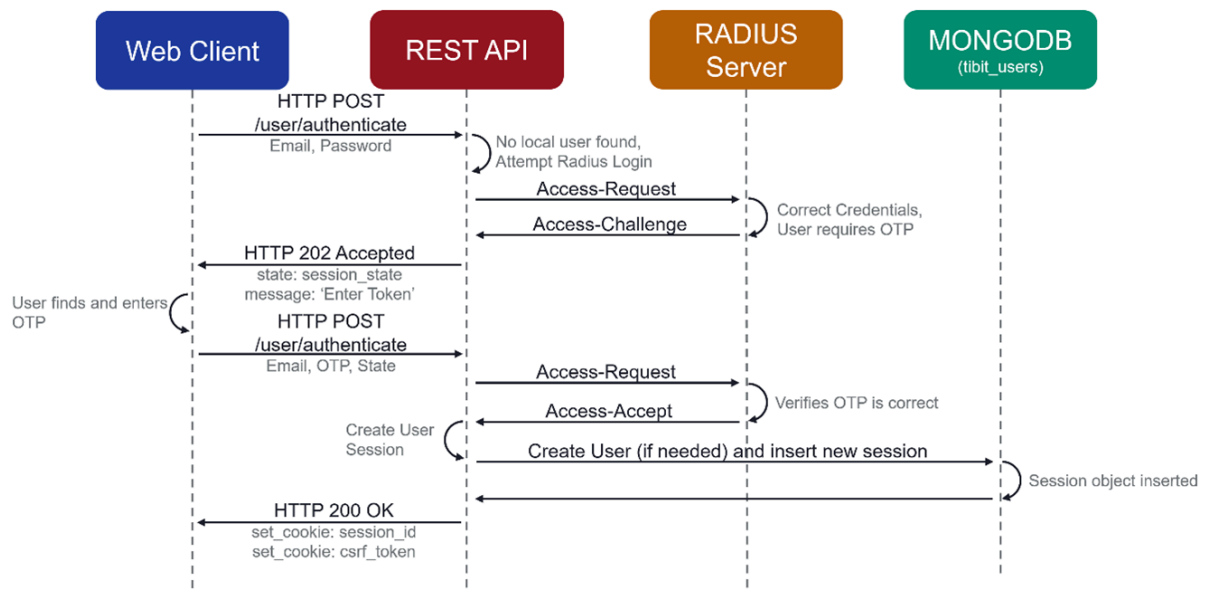


- **HTTP POST:** A user makes an HTTP request with a valid email and password combination to the REST API to authenticate.
- **LocalUserExists(email):** The REST API queries the user collection `tibit_users` if a local user exists with the given username and email address combination.
- **RADIUS: Access-Request/Accept:** The Radius server sends an access-request to the configured RADIUS server. The REST API returns an Access-Accept along with user role information if the username, password, and shared secret are correct.
- **Insert(django_session):** The REST API creates a session associated with the authenticating user and inserts the session object into MongoDB.
- **HTTP 200 OK:** The user receives a successful response containing two set-cookie headers for the session identifier and csrftoken.

Two-factor radius user authentication and session establishment

The following diagram displays the sequence of authenticating with a Two-Factor enabled external Radius server and establishing a session for the user.

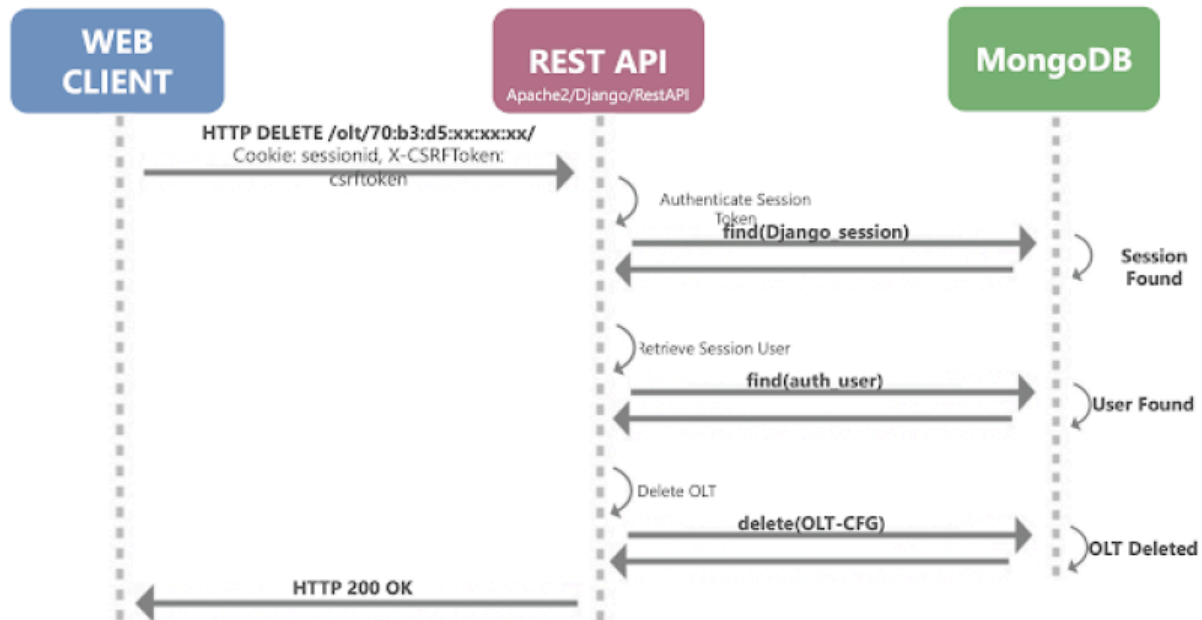
Figure 7 Two-factor radius user authentication sequence



- HTTP POST - a user makes an HTTP request with a valid email and password combination to the REST API to authenticate.
- Access-Request/Challenge - the REST API sends an Access-Request to the configured Radius server. The Radius Server returns an Access-Challenge along with the session state and a reply message.
- HTTP 202 Accepted - the user receives a 202 indicating the request has been received for processing, but the processing has not been completed. The body includes the session state and the reply message.
- HTTP POST - the user makes an additional HTTP request with their email, one-time password, and session state from the previous response.
- Access-Request/Accept - the REST API sends an Access-Request to the configured Radius server. The Radius server returns an Access-Accept along with user role information.
- Create User and Insert New Session - The REST API will create a local user in the database if one is not there. A session object will be created and inserted into MongoDB for the new user session.
- HTTP 200 OK - the user receives a successful response containing two 'set-cookie' headers for the session identifier and csrftoken.

Authentication for Existing Session

The following diagram describes the sequence of successfully authenticating with a valid user session.

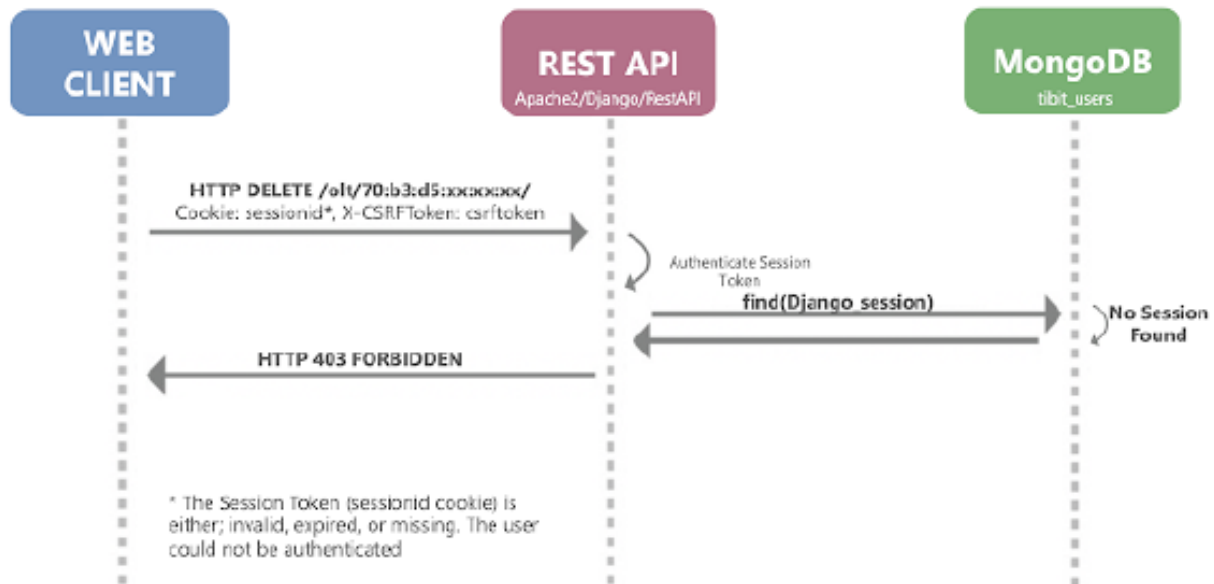


- **HTTP DELETE:** A user makes an HTTP request containing a valid sessionid and csrftoken cookie.
- **find(Django_session):** The REST API queries the session collection in MongoDB to find and return the session object with a matching sessionid.
- **find(auth_user):** The REST API queries the user collection tibit_users in MongoDB to find and return the user profile associated with the session object.
- **delete(OLT-CFG):** The authenticated request is performed.
- **HTTP 200 OK:** A successful response is returned to the user.

Authentication failure

The following diagram describes a failed authentication.

Figure 8 Authentication failure sequence



- HTTP DELETE: a user makes an HTTP request containing an invalid, expired, or missing sessionid cookie.
- find(Django_session): the REST API queries the session collection in MongoDB to find and return the session object with a matching sessionid. No valid session object is found.
- HTTP 403 FORBIDDEN: an unsuccessful, forbidden response is returned to the user.

Encrypted keyring credential storage

The file system for the PON Manager stores user names and passwords for accessing the MongoDB. An encryption keyring is used to store user names and passwords in a secure, encrypted, at-rest database.

The keyring stores the encrypted credential in a datafile that is stored on the file system. The keyring is secured with a keyring key that is also stored on the file system. Both the keyring data file and key are secured with strict root access permissions when created.

To encrypt the credentials, a raw Argon2 hash is generated from the keyring key. It is used to encrypt the plain text passwords in a GCM AES encryption scheme. The resulting encrypted credentials are persisted, together with the Argon2 salt, nonce and MAC.

Encrypted MongoDB authentication and email recovery credentials

When using MongoDB authentication or client-side field level encryption, credentials are required on the filesystem for the NETCONF server to access. Avoid storing these credentials

in plaintext in `NetconfInit.json`. An encrypted keyring mechanism can be used so the credentials are stored in a secure, encrypted at-rest datastore.

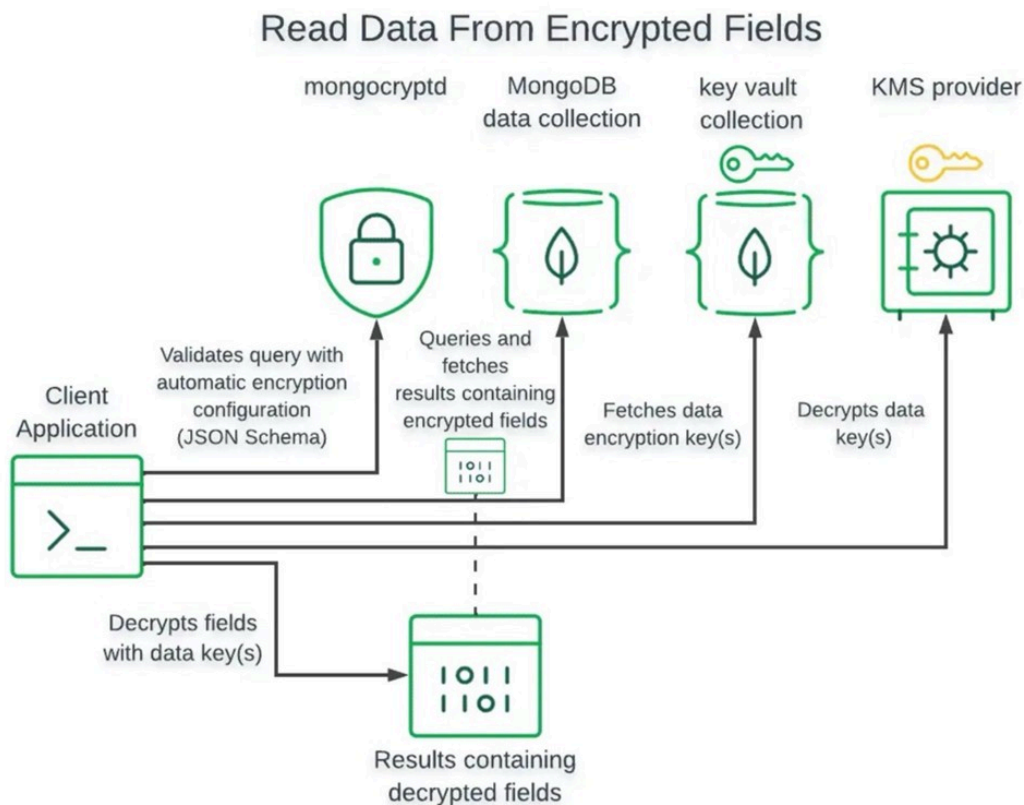
Client-side field level encryption

The PON Manager supports configuration and use of client side field encryption (CSFLE) to avoid storing secrets to the PON Controller database in plain text. CSFLE is a native MongoDB encryption mechanism that can encrypt and decrypt specific fields within the database.

CSFLE uses an envelope encryption strategy consisting of:

- A 96-byte Customer Master Key (CMK) used to encrypt or decrypt the Data Encryption Key (DEK)
- Data Encryption Key (DEK) used to encrypt or decrypt fields in MongoDB. This key is encrypted and stored in MongoDB in a unique database and cannot be directly used to decrypt MongoDB fields.
- Encrypted fields in MongoDB. The MongoDB field `CNTL-CFG.RADIUS.Shared Secret` supports encryption when CSFLE enabled.

Figure 9 CSLE encryption strategy



Django key

The Django REST API framework defines a 'SECRET_KEY' which is used for cryptographic signing within the Django framework.

The key is used by the framework for various internal cryptographic signing functions, such as signing session cookies and other serialized data. The key is not used for user password hashing, salting, or storage.

The Django key is user modifiable and is configured under the `django_key` field in `user_databases.json`. The key is automatically generated when the PON Manager package is installed if the field doesn't exist or it's empty. The `generate_django_key.py` script is provided with the PON Manager package in the 'tools/' directory and can be used to generate a new Django key value. The format of the field is a freeform string; however, Django recommends it be a minimum 50 characters with a minimum of 5 unique characters. The Apache web server must be restarted for changes to the Django Key to take effect. All active web sessions are invalidated when the key is changed, forcing users to re-authenticate.

When deploying multiple PON Managers that use the same user database, the `django_key` should be configured with the same value across all MCMS PON Manager instances. While it is possible to use multiple PON Manager instances using the same user database with different secret keys, this can result in unexpected behavior and is not recommended.

List of procedures

Procedures for Security are:

- [Procedure 13, "Configuring an encrypted keyring"](#)
- [Procedure 14, "Configuring the encrypted MongoDB authentication and email recovery credentials"](#)
- [Procedure 15, "Configuring client-side field level encryption"](#)

Procedure 13 Configuring an encrypted keyring

The encryption script creates the encrypted keyring and associated key on the file system and stores a user provided password in an encrypted format for use in the MongoDB authentication and the recovery email mechanism. Execute the script multiple times to set a new password and to rotate the key for the keyring as required by the network plan.

Overview

Execute the following script with root permissions.

The path to the keyring data file is in `user_database.json`. If it is not manually specified when executing the `set_keyring_passwd.py` script, the default location is `/etc/tibit/ponmgr/keyring.data` and `/etc/tibit/ponmgr/keyring.key` respectively.

Steps

- 1 Configure an encrypted keyring:

```
sudo /opt/tibit/ponmgr/tools/set_keyring_passwd.py -g -t mongodb
```

Procedure 14 Configuring the encrypted MongoDB authentication and email recovery credentials

Configure the encrypted MongoDB authentication and email recovery credentials as required.

Overview

The provided script creates the encrypted key ring and associated key on the file system and stores the user provided password in an encrypted format to use in MongoDB authentication. The script can be executed multiple times to set a new MongoDB password or to rotate the key for the keyring.

The path to the keyring data file and keyring must be provided in `user_database.json`. If not manually specified when executing the `set_keyring_passwd.py` script, the default location is `/etc/tibit/ponmgr/keyring.data` and `/etc/tibit/ponmgr/keyring.key` respectively.

Steps

- 1 Create the encrypted key ring and associated key on the file system:
`/opt/tibit/ponmgr/tools/set_keyring_passwd.py`

Note:

- 2 Provide the path to the key ring data file where the key ring must be in the `user_database.json`:

```
{
  "auth_enable": true,
  "auth_db": "tibit_users",
  "username": "authUser",
  "password": "",
  "password_opts": {
    "type": "keyring",
    "keyring_path": "/etc/tibit/ponmgr/keyring.data",
    "keyring_key_path": "/etc/tibit/ponmgr/keyring.key",
  },
}
```

Note 1: The values configured under "password_opts" in `user_database.json` apply to all MongoDB databases and the recovery email SMTP server.

Note 2: If the encrypted keyring is configured to be used in `user_database.json`, credentials for all MongoDB databases as well as the recovery email SMTP server are stored in the encrypted keyring.

Procedure 15 Configuring client-side field level encryption

Configure client-side field level encryption (CSFLE) as required.

Requirements

Every database that uses CSFLE must set keyring paths and configure CSFLE values in the `databases.json` file.

Steps

- 1 Generate a Customer Master Key and Data Encryption Key:
 - a. Create a CMK and DEK used for encryption and decryption. The executable can be executed multiple times to generate or rotate a new CMK/DEK.


```
/opt/tibit/ponmgr/tools/csfle_key_manager/key_manager.py --create -v 1 --database Default
```
 - b. Activate the python virtual environment located at:


```
/opt/tibit/ponmgr/bin
```
 - c. This executable generates a CMK that must be inserted into the encrypted keyring:


```
1:NonBeBIWpRz+DElIYNawTEHBeE7RSVqH0qmTGfDNcy08...
```
- 2 Generate the keyring and insert the CMK:
 - a. Create the encrypted keyring and associated key on the file system and stores the user provided CMK in an encrypted format


```
/opt/tibit/ponmgr/tools/set_keyring_secrets.py -g -c <CMK>
```

Note: Execute the script with root permissions to ensure secure file access permissions.
- 3 Configure `databases.json`
 - a. CSFLE configuration leverages the existing 'password_opts' 'keyring_path' and 'keyring_key_path' file paths. These must be set even if not using the encrypted MongoDB authentication credential.


```
{
    "Default": {
      "password_opts": {
        "keyring_path": "/etc/tibit/ponmgr/keyring.data",
        "keyring_key_path": "/etc/tibit/ponmgr/keyring.key"
      },
      "CSFLE": {
        "enable": true,
        "database": "encryption",
        "collection": "__keyVault",
        "cmk_storage": "keyring"
      }
    }
  }
```



```
},  
...  
},  
...  
}
```

4 Restart Apache:

- Ubuntu
 `sudo systemctl restart apache2.service`
- Red Hat:
 `sudo systemctl restart httpd`

CHAPTER 7

PON Manager

The PON Manager is designed to be backwards compatible supporting PON Controller database revisions R2.0.4 and greater

The web app only displays configuration parameters that are applicable and available for the version specified in the device configuration document stored in the database. When using older releases of the database or device configuration files, only configuration and state attributes for that version are displayed in the UI. Any attribute added after the configuration version the user is currently using will be hidden and not saved to the database when making configuration edits. This is observed on the network portion of the web interface and is for all devices.

The PON Manager uses the field CNTL.CFG Version in the device configuration document to determine what fields are shown in the UI. This field and the device configuration file is updated in the PON Manager by navigating to Global Config > Databases > Update.

Auto refresh

Automatic web page refresh occurs every 5 seconds. Pages that contain large amounts of data take 10-15 seconds. Very large pages that do not update automatically have a refresh button to refresh their page data. It is not required to refresh the browser to refresh the updated data for a tab.

Site navigation

After logging into the PON Manager, site navigation is visible on the left-hand side of the window. The current page selected is marked by the highlighted section of this navigation menu. The first view you see after logging in is the dashboard page. From anywhere on the site it is possible to transition between the dashboard, network, global config, accounts, and search pages. You can also collapse the PON Manager menu and log out of the PON Manager.

The ID of the current database in use is shown at the bottom of the menu.

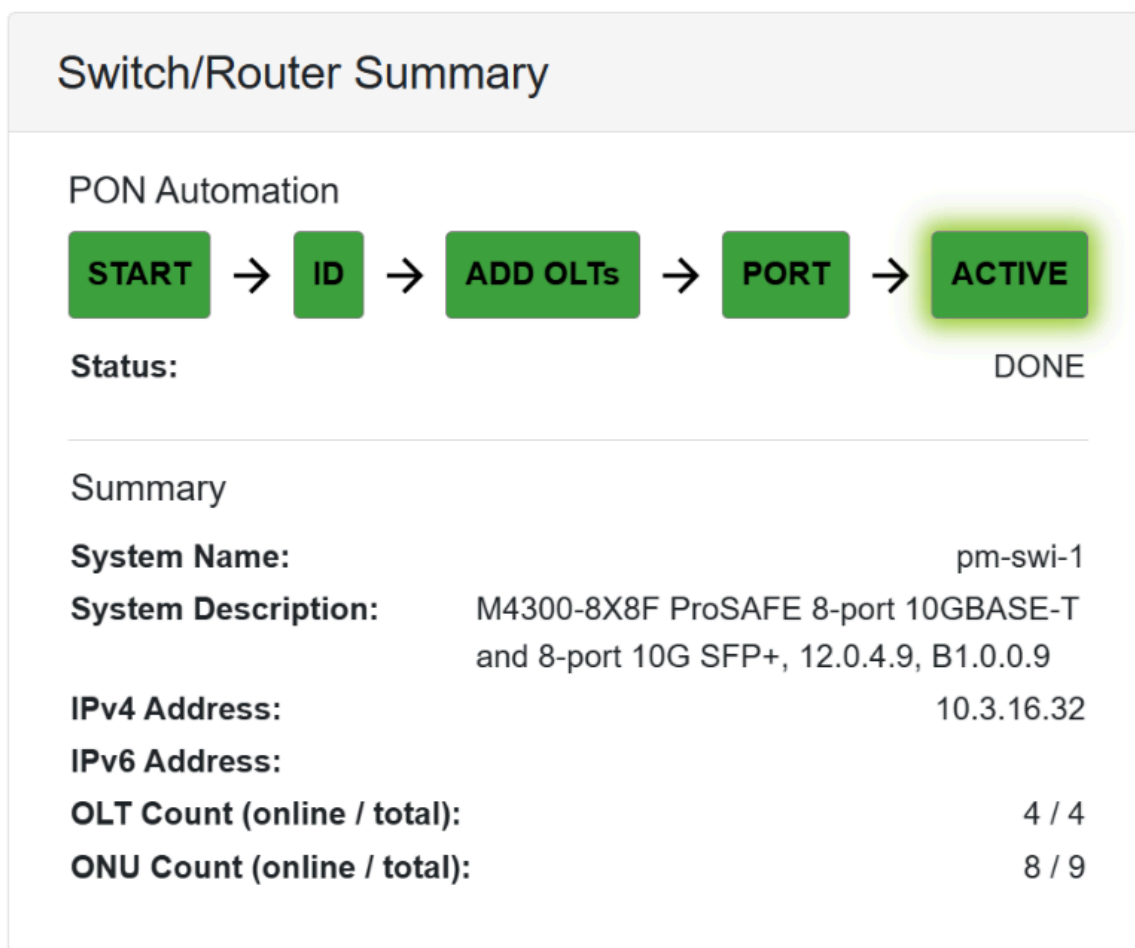
Switch and router

The switch and router's summary tab shows the switch's ID, system name, IPv4 and IPv6 addresses and OLT and ONU counts for quick reference.

The summary tile also displays a quick indication of the PonAuto status for this device at the top of the card. If PON automation is inactive or not used, text displays stating that the PON auto service is unavailable.

The following figure describes the Switch and Router Summary.

Figure 10 Switch and Router Summary



Switch and router summary tab

The Switch and Router summary tab displays information for the selected switch or router within the PON network.

The Summary tab displays the following information for the switch or router:

- The system ID as a MAC address

- The system name
- The system IPv4 or IPv6 address
- The PON automation status in a process flow diagram showing, start, ID, add OLTs, port and active stages with a status update.

Note: When PON Automation is inactive or not used, the PON automation status diagram, is replaced with text stating that the PON Automation service is unavailable.

Switch and Router identification tab

View and configure information for the switch.

The configurable fields are listed under the configuration heading, and the informational read-only fields are listed under state. If the switch's picture configuration is set to an image in the database, the image displays in place of the default blue icon.

The following figure describes the Switch and Router Identification tab

Figure 11 Switch and Router Identification tab



pm-swi-1

Chassis ID: 08:bd:43:72:e3:b1



Configuration

Picture:

Labels:

NETCONF Name:08:bd:43:72:e3:b1

Tag:

Create Date:2024-07-18 22:01:50.781171

Location Coordinates:

Address:

Region:Arizona

POP:Gilbert

State

System Name:pm-swi-1

System Description:M4300-8X8F ProSAFE 8-port 10GBASE-T and 8-port 10G SFP+, 12.0.4.9, B1.0.0.9

IPv4 Address:10.3.16.32

IPv6 Address:

Edit

PON Controller

Tabs related to PON Controller are used to configure the PON Controller and view information.

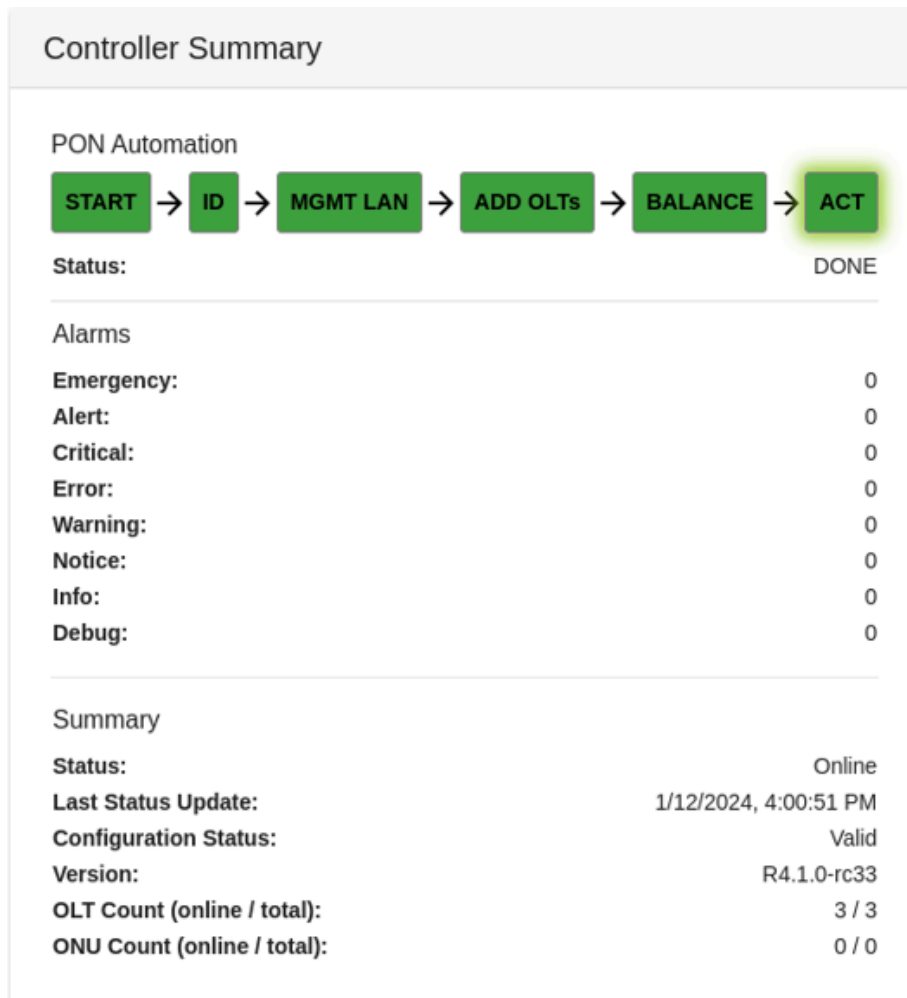
PON Controller summary

The summary tab displays information relevant to the current state and status of the device.

Values such as the total alarm count, MAC address, version, OLT and ONU counts, and status display. The time stamp indicating when the PON Controller's state was last updated also displays. A table displays the raised and unacknowledged alarms in more detail. The summary tile also displays a quick indication of PON auto status for this device at the top of the card. If PON automation is inactive or not used, the users instead see text stating that PON auto service is unavailable.

The following figure describes the Controller Summary.

Figure 12 Controller Summary



PON Controller identification

There are two tiles on the PON Controller identification page. The first displays identifying information about the controller such as its name, ID, picture, and more. Several of these items are configurable by clicking the edit button at the bottom of the tile. The second tile shows a table of all network interfaces on the PON Controller device.

Authentication tab

This tab allows for the configuration of the RADIUS settings on this PON Controller.

The RADIUS servers and user access monitoring settings can also be configured from this tab.

The following figure describes RADIUS Configurations.

Figure 13 RADIUS Configurations

RADIUS Configurations

Shared Secret:-

Revive Interval:0

Failure Threshold:4

Max Retry:0

Held Period:0

Quiet Period:0

Failure Period:0

Auth Retransmit Num:3

Auth Retransmit Timeout:5

Auth Retransmit Backoff Time:5

Servers

Server 1

IP Address:127.0.0.2

Port:1812

Priority:3

Status:

Total Auth Complete:

Total Auth Timeout:

Current Auth Complete:

Current Auth Timeout:

Revive Num:

Server 2

IP Address:-

Port:-

Priority:-

Status:

Total Auth Complete:

Total Auth Timeout:

Current Auth Complete:

Current Auth Timeout:

Revive Num:

Server 3

IP Address:-

Port:-

Priority:-

Status:

Total Auth Complete:

Total Auth Timeout:

Current Auth Complete:

Current Auth Timeout:

Revive Num:

User Access Monitoring

Username:-

Enable:false

Recover Threshold:2

Check Interval:60

Edit

Firmware tab

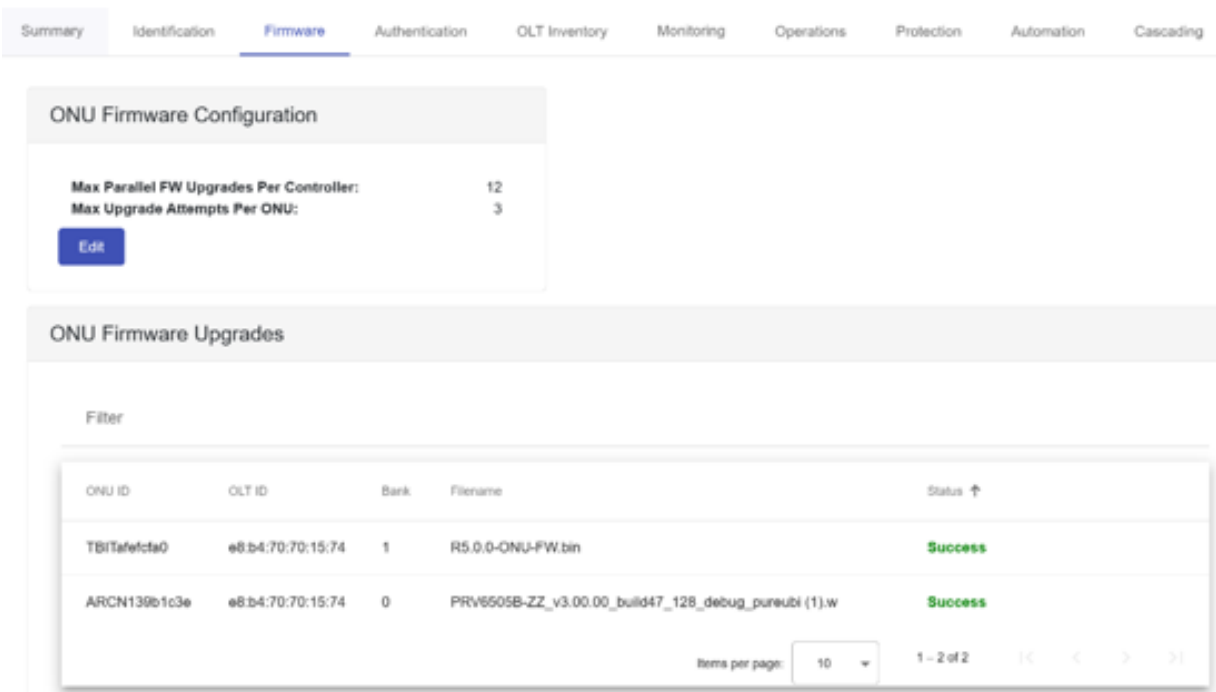
The PON Controller Firmware tab has two tiles.

The first is the ONU Firmware Configuration Tile. Click Edit to change this attribute.

The second tile lists all ONU firmware upgrades reported by the PON Controller. The table displays the ONU being upgraded, its parent OLT's ID, the firmware bank, filename, and the last available upgrade status. The status updates automatically and shows the progress of an active upgrade.

The following figure describes an ONU Firmware Upgrade

Figure 14 ONU Firmware Upgrade



The firmware bank pointer in the ONU firmware pane at the top is supported by the PON automation service. Refer to the PON automation documentation for more information on managing configuration for these fields.

Monitoring tab

The config sub-tab contains the configuration for the controller's alarm profile, statistics sample time, and all logging.

Logging levels may be set for various types of authentication, controller, OLT, TAPI, and UMT relay logs.

Operations tab

There are several fields describing the PON Controllers service. The PON Controller service can be paused for the Operations tab.

Configure the following in the Operations tab:

- auto create
- loop delay
- loop count
- last stop

Note: Auto create ONUs can only be set to true while Subscriber Provisioning is disabled. The following figure describes the Operational settings tab.

Figure 15 Operational settings tab

The image shows two tabs from the PON Manager interface. The top tab, 'Operational Settings', contains a table of configuration parameters and an 'Edit' button. The bottom tab, 'Delete PON Automation', contains a warning message and a 'Delete' button.

Operational Settings	
Pause:	false
Shutdown:	false
Mode:	active (primary)
Auto Create ONUs:	true
Loop Delay:	10
Loop Count:	109796
Last Loop:	4/14/2025, 2:17:00 PM

Edit

Delete PON Automation

Delete this PON Automation and it's records from the database

Delete

Use this tab to delete the PON Automation service from the system. The Delete action removes the following from the database for this PON Automation service.

- all configurations
- state
- statistics

- logging data

Note: This action cannot be undone.

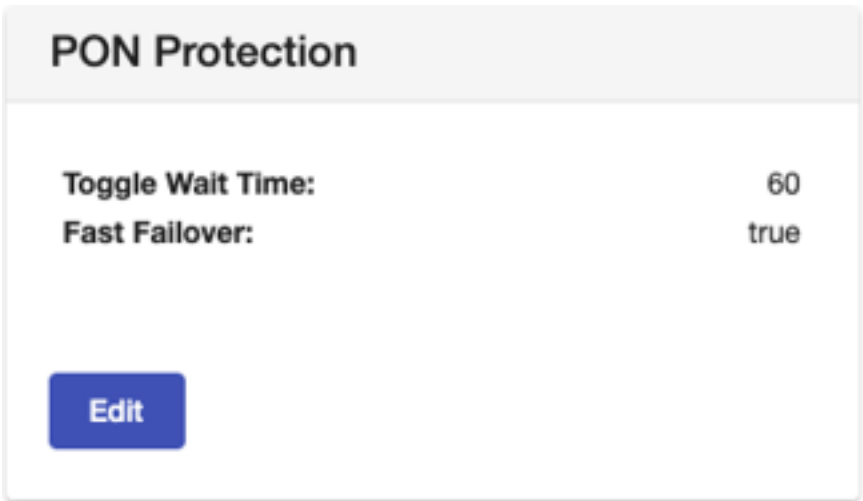
Protection tab

The PON protection tab has two configurable fields that assist with Type-B PON protection. These are global settings that apply to all OLTs managed by the PON Controller.

Toggle wait time is the attribute that specifies the maximum time the PON Controller waits for ONU discovery on an OLT in a protected pair. If no ONUs are registered within the configured time, the PON Controller initiates a switchover to the peer OLT and checks for registered ONUs. This toggle process continues until at least one ONU is registered on both OLTs in the protection group. Enabling fast failover allows ONUs to remain registered during a protection switch.

The following figure describes PON Protection

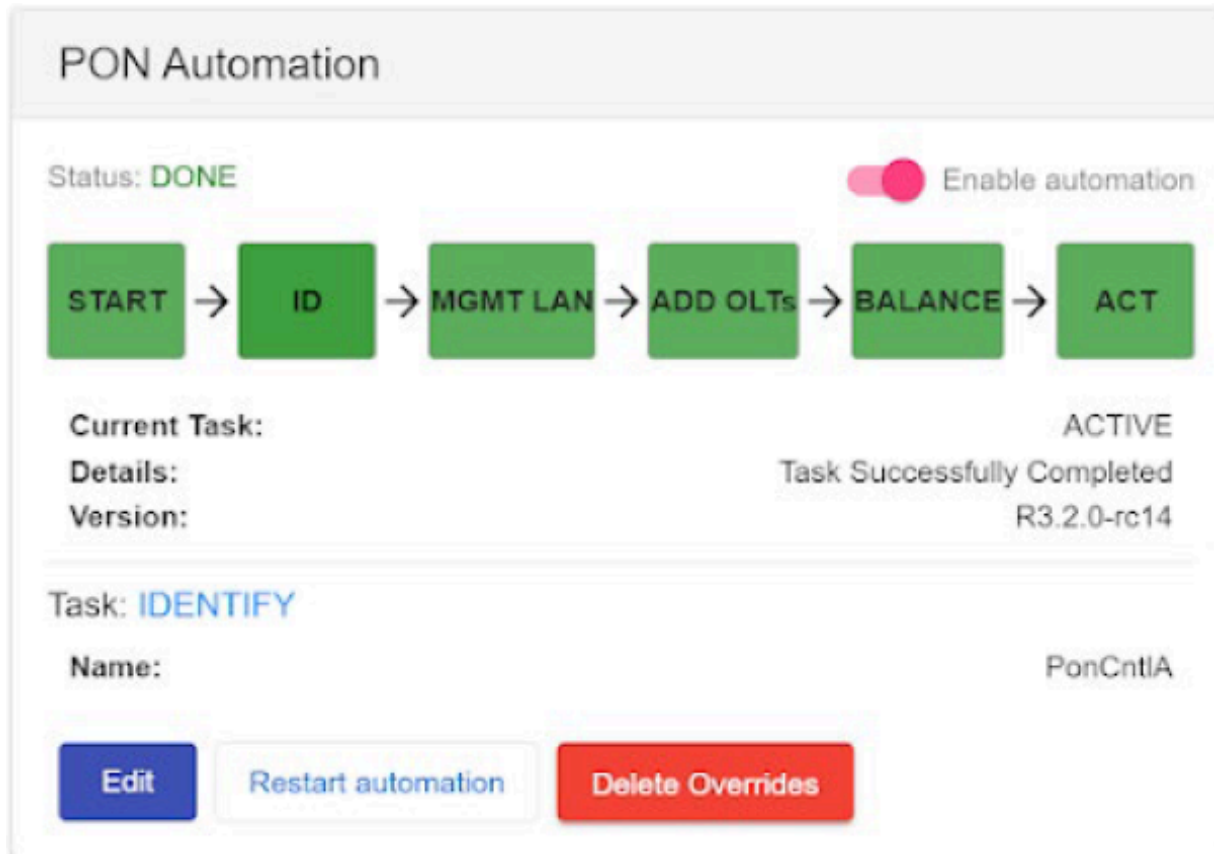
Figure 16 PON Protection



Automation tab

The automation tab contains a single tile displaying the PON Automation status, details, current task, the template used to configure the device, and controls to edit this device's PON automation configuration.

The following figure describes PON Automation.

Figure 17 PON Automation

The following table details the task color status for the PON automation box.

Table 15 Task color status for the PON automation box

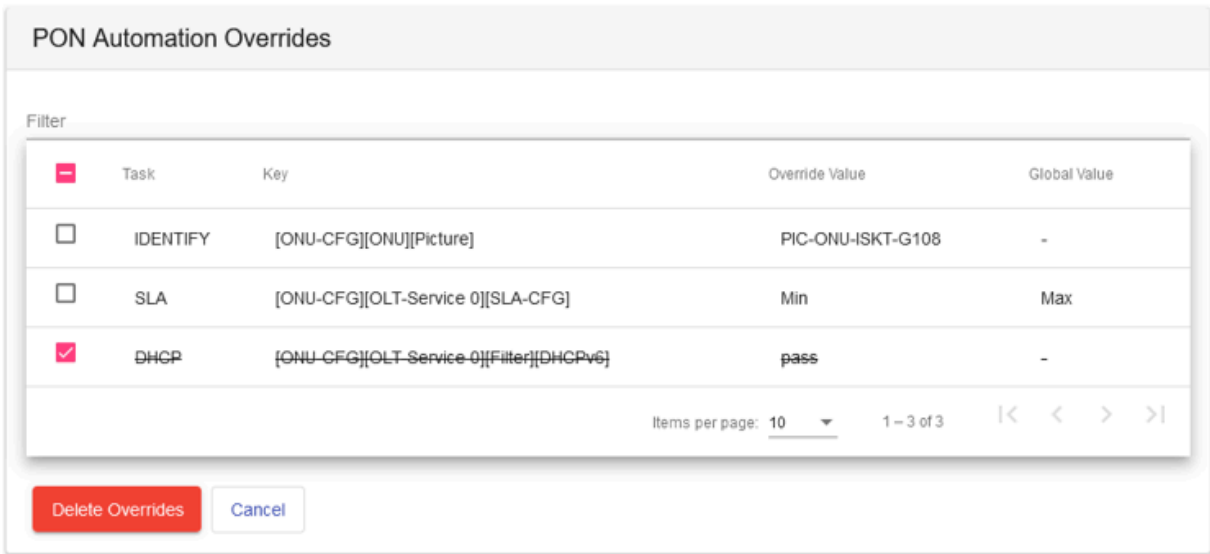
Color	Description
Green	Task completed successfully.
Orange	Task requires a field or fields as described in the details field.
Red	Task contains an error that PON automation cannot clear.
Gray	Task process is not complete.

The ID task is a clickable button. Click on a task to view and edit the configuration for a specific automation task. To update the device's PON automation configuration, select the task to view, and click Edit. By default, each field uses the value found in the PON automation state. To override the value for a field for this device, click the checkboxes next to each field. If overridden, the value reflects the new configuration value after saving. To pause or disable

Pon automation for a given device, toggle the Enable automation switch at the top of the tile. When it is disabled, PON automation will not make any updates to this device's configuration. All overrides are removed by clicking the Delete Overrides button.

The following figure describes PON automation overrides.

Figure 18 PON automation overrides

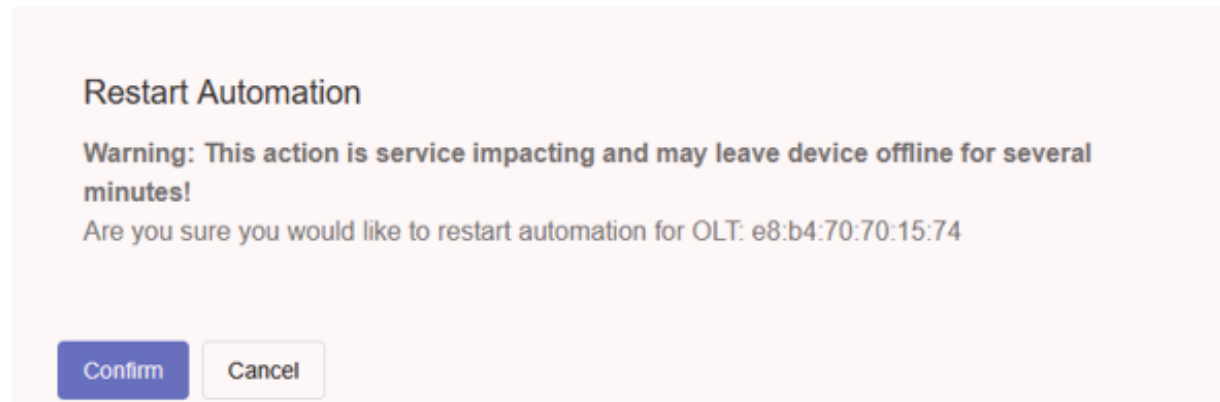


A PON Controller has one editable task for PON automation: Identify. Configure the PON Controller name here.

If PON automation is active on the current database, the button to restart Pon automation is enabled. Click restart automation to update the device's automation configuration.

When selecting the Restart Automation button, a warning pop-up appears indicating that the device may be offline for several minutes. Click Confirm to continue with the process or Cancel to go back.

The following figure describes the Restart Automation dialogue box.

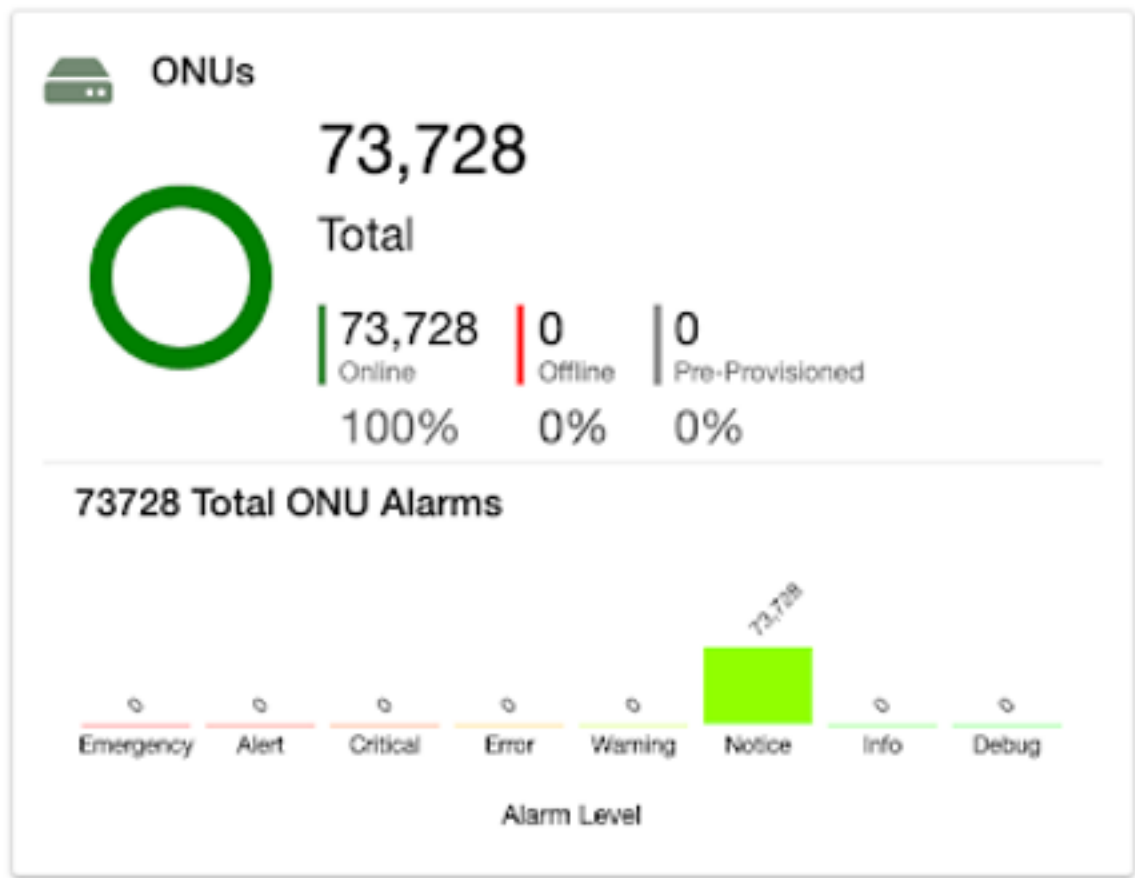
Figure 19 Restart Automation

Alarms summary

The alarm counts for a given device type are shown at the bottom of that device type's tile. The bars in these charts are clickable to see more detail for the selected alarm level. For example, after clicking the "Info" bar, a table of all Information level alarms populates below the device summary tiles.

The following figure describes the Alarms Summary.

Figure 20 Alarms Summary



The alarms table displays the ID of the device the alarm is associated with, followed by the time the alarm was reported, the alarm ID, and the IDs of the parent OLT and PON Controller.

Automation summary

The Automation States section on the dashboard displays a summary of the current PON automation status for each type of device: controller, switch, OLT and ONU. For each device type, counts are displayed showing the number of devices in each of the PON automation states.

Under the Automation States count is a set of Automation Task counts that reflect how many devices under each Automation State are in a certain Automation Task. Each Automation State is represented by a corresponding symbol, which is referenced in the Automation States counts.

Figure 21



The following table details the PON automation states.

Table 16 PON automation states

States	Description
Done	Automation has completed and the device is in the active state.
Start	Occurs on initial startup or restart of PON Automation. Several non-service impacting fields are set to default.
Error	Automation is unable to complete activation due to an error.
Waiting For Input	Automation is paused waiting for user input for a device.
Waiting For Device	Automation is waiting for the PON Controller to complete the configuration.
Disabled	Automation is disabled for a device.

The automation states count and the stacked horizontal bar can be clicked to display the list of devices in a specific state. The table displays the ID of a device, whether automation is enabled or not, the automation task it is currently on, and the automation state for the device. Clicking an ID takes you to the PON automation tab for that device.

The following figure displays automation summary.

Figure 22 Automation Summary

All ONU's on WAITING FOR DEVICE status and in 'IDENTIFY' task

Filter			
ID	Enable	Task	Status
Subscriber 4993A2	True	IDENTIFY	WAITING FOR DEVICE
TB/Tafel/560	True	IDENTIFY	WAITING FOR DEVICE
ac 44 76 71 78 20	True	IDENTIFY	WAITING FOR DEVICE
48 54 70 71 78 30	True	IDENTIFY	WAITING FOR DEVICE

Items per page: 5 1 - 4 of 4

System status

The System card lists MCMS services on the system along with a color indicator icon representing that status.

For online services, the (1/1) text indicator to the right of the service name indicates that there is 1 service online out of 1 total services found on the system.

The following image describes online service indicators.

Figure 23 online service indicators

-  Mongo DB (1/1)
-  PON Automation (0/1)
-  PON Manager (1/1)

The color of the icon changes depending on the service status.

The following table describes the different service health indicator colors.

Table 17 Service health indicator colors

Status	Indicator	Description
online		All nodes for this service are online.
Offline		The functional majority of nodes for this service are offline.
Combination		This service has a combination of online and offline nodes such that the service is not running in a fully redundant state.

Status	Indicator	Description
Unavailable		Could not retrieve data for nodes of this service type.

To get more details about a service, hover over the name or status indicator. On this system there is only one PON Automation service. The details show that the service is named "pm-dev-3" and it is currently offline.

The following figure describes a service indicator.

Figure 24 Service indicator



Creating and managing accounts

When a new MCMS PON Manager system is installed, the first user to access the Web App is prompted to create a user. This user account is an administrator by default.

Administrators are responsible for creating additional user accounts. This is done from the accounts tab.

Creating an account adds the new user to the user's database as configured in the user_database.json configuration file. Passwords are encrypted and are not stored in plain text.

Password requirements

Password requirements for user accounts are configurable for admin users on the user configuration tab. By default, user account passwords require the following:

- A minimum length of 12 characters
- A maximum length of 64 characters
- A password strength of 'weak' or higher
- Cannot contain user email or name

The following figure describes Minimum password requirements.

Figure 25 Minimum password requirements

Minimum Password Requirements

Minimum Length (Characters):	12
Maximum Length (Characters):	64
Minimum Lowercase Count (Characters):	0
Minimum Uppercase Count (Characters):	0
Minimum Number Count (Characters):	0
Minimum Special Character Count (Characters):	0
Excluded Characters:	';:"]}{[=+
Minimum Strength:	weak
Exclude Email:	true
Exclude Name:	true
ASCII Standard Characters Only:	false

[Edit](#)

When entering a password, a user is displayed a popup on the password field indicating the defined password requirements and current adherence to the requirements, via a red X or green check mark. If available, feedback is provided to the user within the popup indicating how the password may be improved.

If the password does not adhere to the configured requirements, a label below the field displays in red to indicate that the password is invalid and cannot be saved.

Note: Administrative users creating new users and modifying existing users are warned if a password does not adhere to the defined password requirements, but will be allowed to save a non-compliant password. In this case, a label below the password field will appear in orange to indicate that the password is invalid but can still be saved.

Logging out

The option to logout is accessible from the site navigation menu on the left of the PON Manager user interface. When it is selected, a confirmation dialog appears.

If a user is approaching the maximum allowable time period of inactivity, a warning is displayed to the user notifying them that they will be logged out. If no action is taken, the user will be logged out.

Update the PON Manager user interface branding

Update the PON Manager user interface branding after installation by adding custom logos and background to:

- the background of the login screen
- the logo of the login screen
- the corner logo visible after login
- the footer text

Note: Upload the recommended image sizes to ensure the logos and background display correctly.

Idle session timeout out from the PON Manager session

The system displays a warning, when the PON Manager session has been inactive for the idle session timeout duration. Perform a task on the PON Manager user interface to resume the session. If no action is taken, the system terminates the PON Manager session.

Update ONU IDs, alloc IDs, and LLIDs in the inventory

Sync automatically assigned” button appears if the configured settings do not match what is active in the OLT’s state. Clicking this button will set each input field to match their value from the OLT’s state upon saving. This action is only available when the configuration does not match what is active.

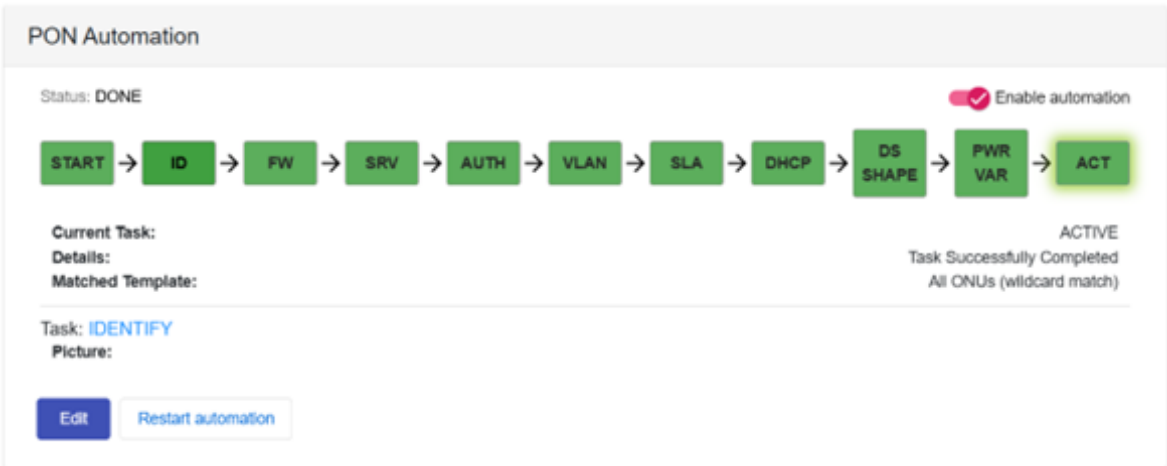
The “Assign next free block” button assigns consecutive ALLOC IDs for the number of service ports specified in the “Service Port Count” field.

Automation tab

The Automation tab contains a single tile displaying the PON auto status and configuration for this ONU device, and it is organized and functions similarly to the PON Controller automation tab.

The following figure describes ONU PON Automation

Figure 26 ONU PON Automation



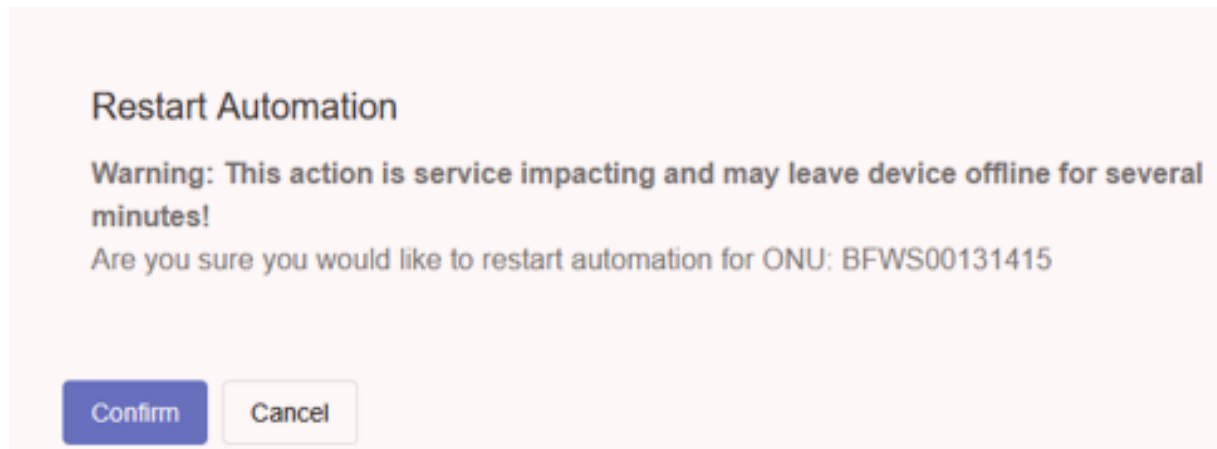
An ONU has several editable tasks for PON Auto: Identify, Disallowed ONU, Firmware, Service, VLAN, SLA, Active, DHCP, Downstream Shape, and Power Variation. The ONU's picture is in the identify task, as well as the firmware bank pointer and banks from the firmware task.

The service task allows the configuration of the PON auto ONU service package, service configuration file, and any values required by the chosen service configuration.

The authentication, VLAN, SLA, and Active sections all contain editable fields to update the RADIUS configuration, OLT and ONU VLAN settings, the SLA, and the DHCP settings of each OLT-Service for PON auto.

Click the Restart automation button to restart the PON Automation workflow back to the START task. A warning pop-up appears and notifies users that restarting automation on devices may leave them offline for several minutes. Click either Confirm to continue to reset automation, or Cancel to return to the PON Automation Screen.

The following figure describes Restart Automation.

Figure 27 Restart Automation

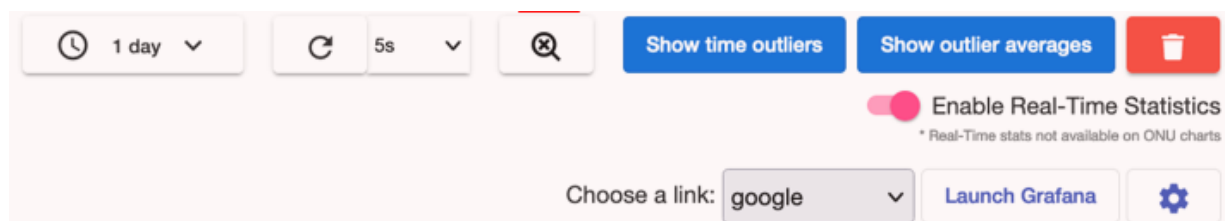
Power Variation is a Rogue ONU task for ONU Automation. If issues occur during Power Variation, the user has the ability to start Fast Recovery or Remediation by clicking the button under Rogue ONU Alarm Status.

Statistics

Statistics presents a view of the statistics generated about a device operations. All available statistics are shown within the statistics group.

The stats sub-tab is available under the Monitoring tab for PON Controllers, OLTs, and ONUs. To display the graph for any given statistic, mark the check-box next to the field name. Numerical values in the right column display the statistics' most recent value or for counter values, the accumulated value based on the selected time period.

The following figure describes the Statistics tab.

Figure 28 Statistics tab

The statistics tab has advanced controls for selecting the time range, refresh interval, and other statistics display controls.

- Time selection offers the following options to the user. A custom time range specified by selecting the start and end date. Choosing a set To date stops the graphs from automatically updating. Simple, predefined ranges from 15 minutes to the last month can be applied with one click.

- Refresh configures how often to refresh the statistics data.
- Reset zoom restores the X/Y axis zoom on graphs to default values.
- Show time outliers finds anomalies on the graph and display those times as a dotted line instead of a solid line. The PON Manager does this by finding the average time between stat gathering cycles for the selected time period and looks for times greater than twice the average.
- Show outlier averages uses the average period of time between stat cycles to fill the gap in time of the statistical outliers with estimated time periods of stat gathering where they should have occurred. It then uses however many new points that were created to fill the gap on the x-axis to find the average y-axis value and distribute that value between all the new points of data.
- Clear statistics clears all statistics for this device. This process cannot be undone.

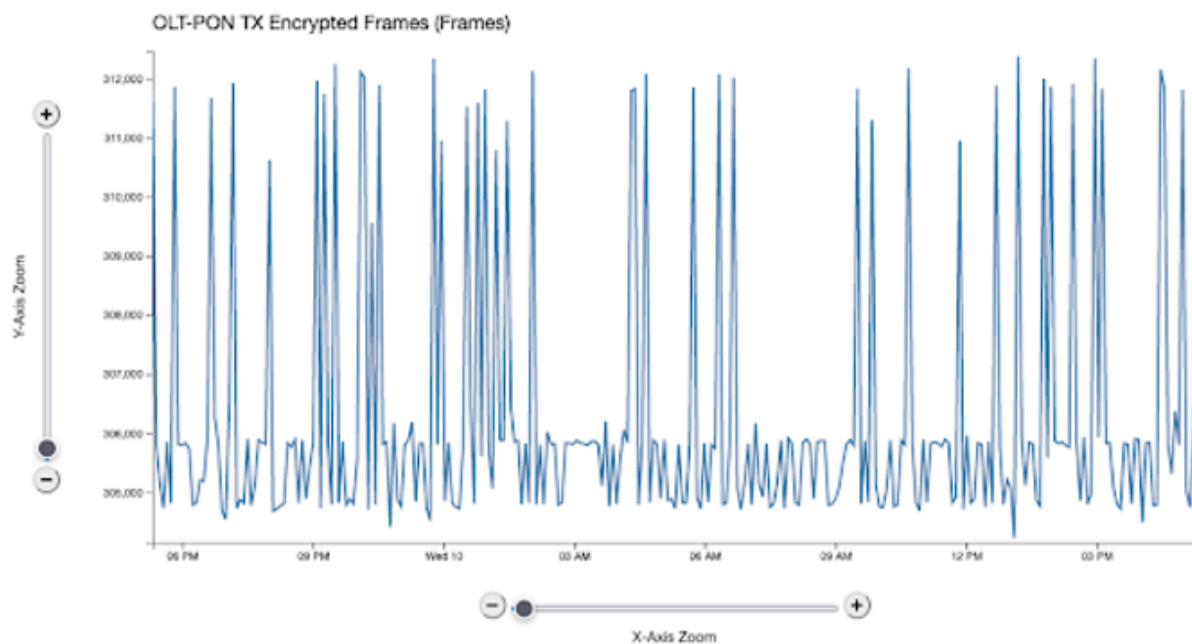
Displaying graphs

All graphs on the statistic's tab follow the same layout.

Each graph displays a single statistic, where the X-Axis is the date and time the statistic was reported, and the Y-Axis units depend on each individual statistic. For example, Y-Axis represents the number of frames counter for TX Encrypted Frames statistic.

The following figure describes a graph.

Figure 29 Graph



The following table describes the controls for zooming and viewing graph data.

Table 18 Controls for zooming and viewing graph data

Controls	Control location	Description
+ increase zoom - decrease zoom	Axis	When zoomed in on graph data, click and drag the graph to view different data in the series.
Vertical controls	Y-axis	Vertical click and drag is controlled individually for graphs.
Horizontal controls	X-axis	Horizontal click and drag controls are aligned and apply to all graphs that are displayed. Aids with troubleshooting by displaying multiple metrics aligned to the same point in time.

A red line is displayed on the graph if the statistics data extends outside the range of current zoom.

Alternatively, users can zoom and pan on the graphs by clicking anywhere inside of the graph area and then using their mouse to scroll in and out or to click and drag.

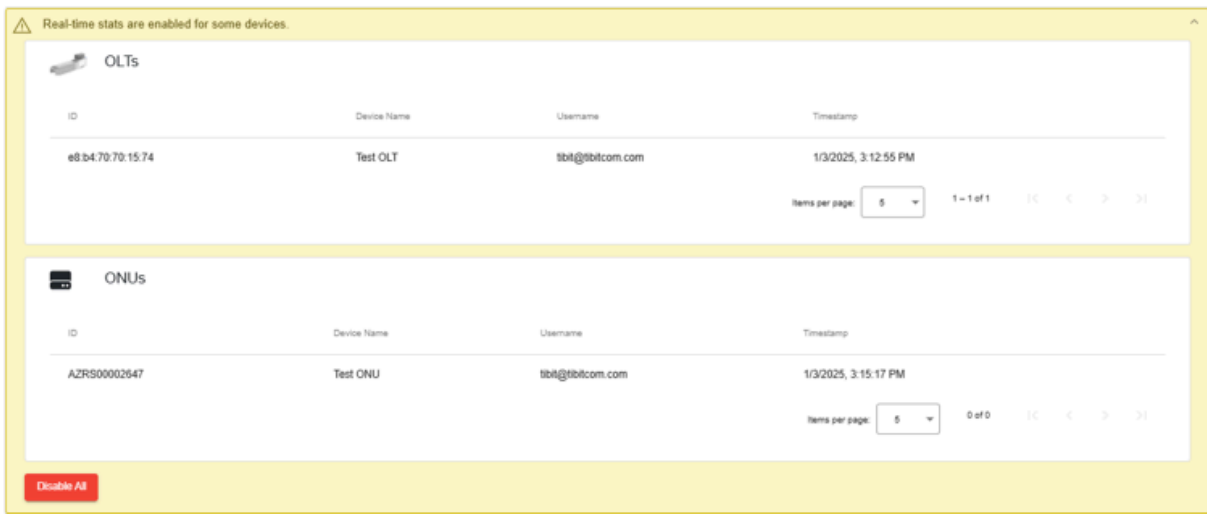
Real-time statistics

When Real-Time Statistics is enabled for a device, a banner displays globally in PON Manager. When the banner is clicked, it expands to provide the device's identifier and name, the user who enabled Real-Time Statistics on each device, and the timestamp for when each device was enabled.

To disable Real-Time Statistics for a single device, click on that device's identifier to navigate to its statistics page. Otherwise, bulk-disabling Real-Time Statistics for all devices is possible by clicking the 'Disable All' button.

The following figure describes the Real-time statistics banner.

Figure 30 Real-time statistics banner

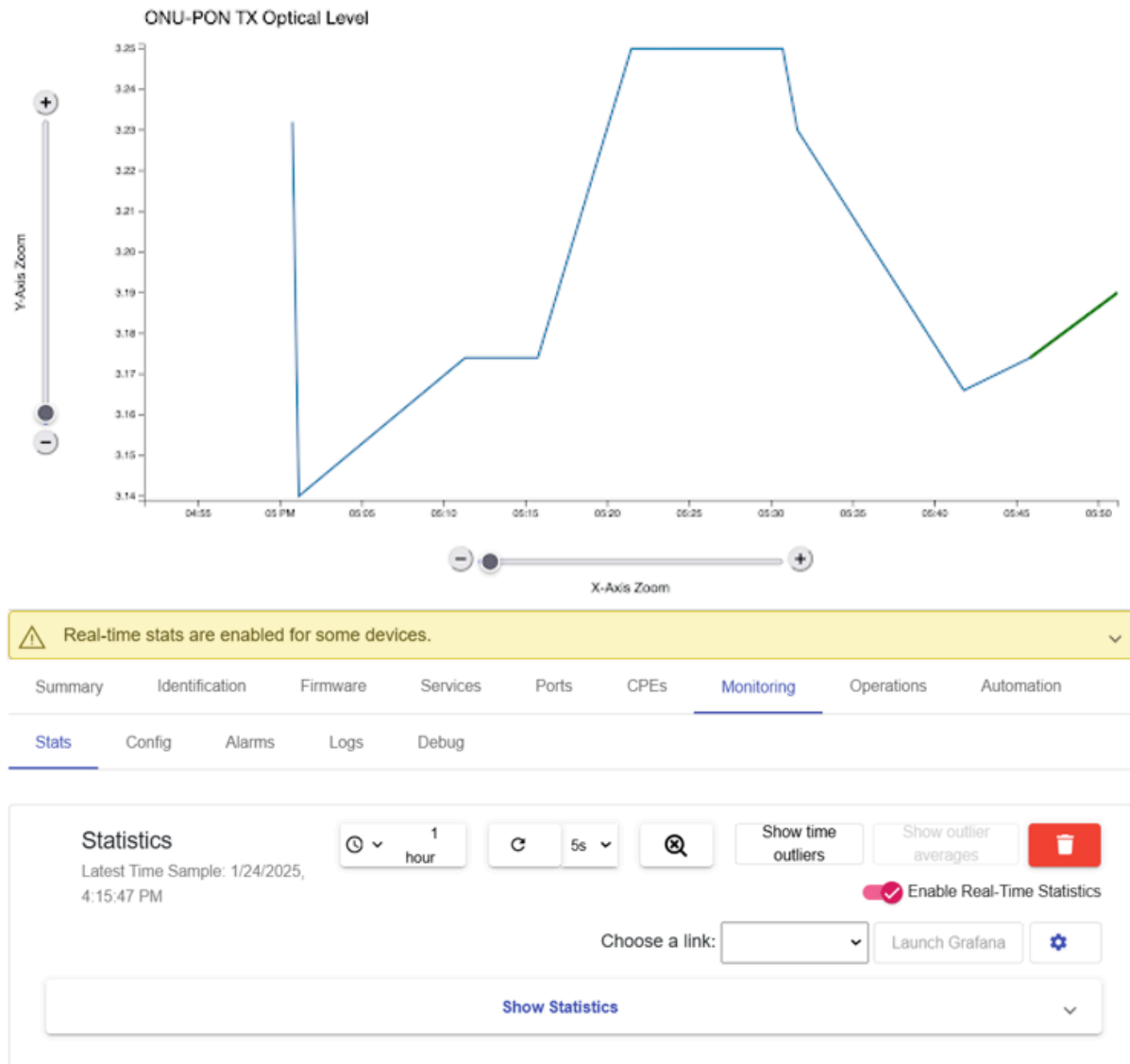


When viewing statistics for an ONU or OLT, there is an option to toggle real-time statistics. This option uses data gathered every interval (as defined by the PON Controller’s real-time statistics sample time) to update the view of the graphs and total statistic counts.

The total statistic count updates steadily as the current values are reported for each PON Controller real-time statistics sample interval. These are located next to the checkboxes for selecting which statistics to graph. On the graphs themselves, real-time statistics creates an extra data point that is connected to the graph by a green line. This value changes regularly and represents the accumulation of the value since the most recent collection of complete statistics by the PON Controller.

Note: It is not advisable to enable real-time stats on many devices. Enabling real-time statistics can affect the performance of the PON controller. A warning banner is displayed anytime real-time statistics are enabled.

The following figure describes Real-time statistics.

Figure 31 Real-time statistics

ONUs under OLT statistics

The OLT stats page displays the statistics of the ONUs that it manages.

A tab is located at the top of the page that allows users to navigate between the OLT statistics and the ONUs. The ONU statistics display both a line chart containing all the ONUs, and a bar chart that shows the accumulated values of each ONU for the selected time period. The colors of the lines on both the line and the bar chart will correspond with the outline around the list of ONUs at the top of the page. To remove one of the ONUs on the graph, click on its address at the top of the page.

Grafana

Grafana is an open source data visualization tool that runs separately from the MCMS.

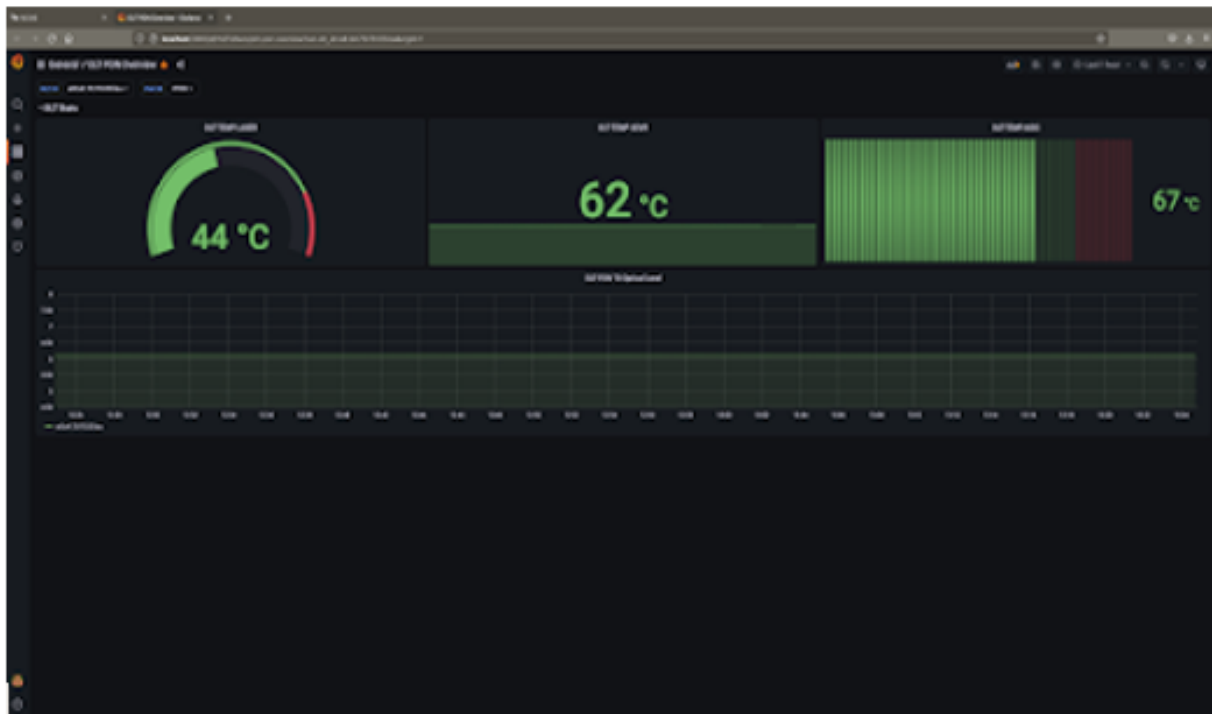
The statistics exporter in conjunction with prometheus, an open source data collection software tool kit, is available for MCMS users. The OLT and ONU statistics pages provide a way to link users to a Grafana server for a more in-depth view of statistics.

There are several prerequisites to using this feature in the PON Manager:

- Install the Grafana server on a supported operating system within the network accessible from the PON Manager.
- Install and configure the statistics exporter, which is packaged with the PON Controller.
- Create dashboards for OLT and ONU devices in Grafana that the PON Manager can link to.

The following figure describes Grafana,

Figure 32 Grafana



Grafana dashboard links

Create up to 50 links to preconfigured grafana dashboards.

When creating links, add query parameters to help pre-populate dashboards with the ONU and OLT's names and IDs. The query parameters automatically take information and include it in the link, so there's no need to specify devices when creating the links.

The following figure describes Grafana dashboard links.

Figure 33 Grafana dashboard links

Configure links to Grafana dashboards

How do links work? Links allow you to go directly to pre-configured Grafana dashboards from the PON Manager. There are several pre-defined query parameters that act as variables to help fill out the dashboards: `var-olt_id={{OLT ID}}` & `var-olt_name={{OLT NAME}}` (if you are on an ONU then you will also have `{{ONU ID}}` & `{{ONU NAME}}`). Variable query parameters for Grafana always start with `var-`. You can edit the variable names in the pre-defined query parameters that the PON Manager provides but **do not** edit the names within the brackets `{{ }}`, or the brackets themselves. The PON Manager replaces the `{{TAGS}}` with the appropriate information when launching Grafana.

Name	URL	Query Parameters	Delete
ONU Dashboard	http://localhost:3000/d/QAZ1y8Qnz/onu-pon-overview?var-olt_id={{OLT ID}}&var-olt_name={{OLT NAME}}&var-onu_id={{ONU ID}}&var-onu_name={{ONU NAME}}	☐ Include OLT ID ☐ Include OLT Name ☒ Include ONU ID ☒ Include ONU Name	

Save **Cancel** **+ Add**

Query parameters defined as part of the dashboard's URL and are surrounded by double braces `{{QUERY-PARAM}}`. PON Manager replaces the `{{QUERY-PARAM}}` with the device identifier or device name when clicking the launch Grafana to open a tab to the selected dashboard.

The format of the dashboard URL with example query parameters `{{OLT ID}}` and `{{ONU ID}}` is shown below. A description of the query parameters supported by PON Manager is listed in the table below.

`https://grafana-server:3000/d/QAZ1y8Qnz/pon?orgId=1&olt={{OLT ID}}&onu={{ONU ID}}`

PON Manager query parameter description option include OLT ID `{{OLT ID}}` MAC Address identifying the OLT device. Which are available when displaying OLT statistics. Include OLT Name `{{OLT Name}}` User configurable name identifying the OLT device (OLT-CFG.OLT.Name). Available when displaying OLT statistics.

Table 19 Query parameters supported by PON Manager

PON Manager Option	Query Parameter	Description
Include OLT ID	{{OLT ID}}	MAC address identifying the OLT device. Available when displaying OLT statistics.
Include OLT Name	{{OLT Name}}	User configurable name identifying the OLT device (OLT-CFG.OLT.Name). Available when displaying OLT statistics.
Include ONU ID	{{ONU ID}}	GPON serial number or EPON MAC address identifying the ONU device. Available when displaying OLT or ONU statistics.

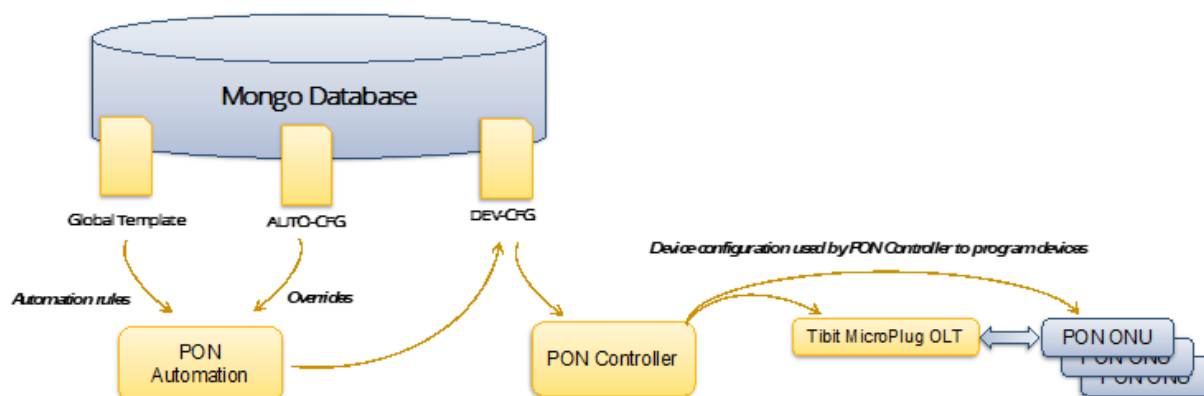
PON Manager Option	Query Parameter	Description
Include ONU Name	{{ONU Name}}	User configurable name identifying the ONU device (ONU-CFG. ONU.Name). Available when displaying OLT or ONU statistics.

PON automation device controls

When PON automation is in use, the OLT and ONU network configuration tabs provide a unified interface for configuration fields managed by PON automation and for fields managed directly by the PON Controller. Not all configuration fields are manageable through the PON automation service.

The following figure describes PON automaton device controls.

Figure 34 PON automation device controls



PON automation configuration is stored in the MongoDB along with the PON Controller's configuration, state, statistics, and log collections used to manage devices. A global template defines a set of rules used by the automation service along with a pre-defined set of algorithms (tasks) to compute device and service configuration values for a particular subscriber and device, for example, a VLAN ID assignment, SLA, and ONU SRV-CFG file. Automation allows overrides to these automatically computed values, which are configured in the device's AUTO-CFG. Automation takes the computed configuration, applies the overrides from the user, and combines this information to create configuration for the device used by the PON Controller to manage devices on the PON network.

When PON Automation is in use, OLT and ONU devices display automation values (AUTO-CFG) as well as the normal configuration (CFG) and state (STATE) values. Automation text is displayed under the config value and is denoted by a pink automation icon.

For each configuration field with automation support, the UI displays the source of the value. If the value was automatically computed by PON automation's global template rules, the UI displays (via global) next to the automation icon. Otherwise, if the current configuration value was overridden by the user, the UI displays (via override) next to the automation icon. If there is a mismatch between the automation value (AUTO-CFG) and the current device configuration

(CFG), the pending automation value is also displayed. The UI displays the pending value until the PON automation service completes the configuration processing for this device.

Table 20 PON automation terminology

Terminology	Managed by	Collection name	Document ID
Global	PON automation	{Device-Type}-AUTO-CFG	Global
Override	PON automation	{Device-Type}-AUTO-CFG	{Device ID}
Config	PON controller	{Device-Type}-CFG	{Device ID}
State	PON controller	{Device-Type}-STATE	{Device ID}
Default Config	PON controller	{Device-Type}-CFG	Default

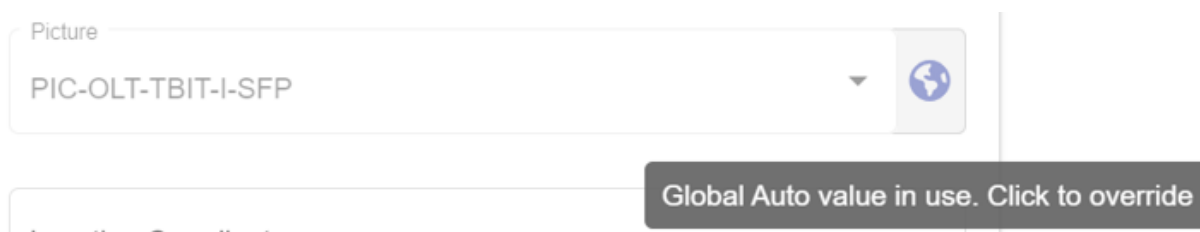
Device configuration overrides

Configuration values are based on the global template automation rules unless the value is overridden by the user. A device override is stored in a device specific document in an automation configuration collection (AUTO-CFG).

In edit mode, the user can override automation configuration values. By default, device configuration uses the value selected by automation's global template rules. The globe icon is configured to use the automation's global value or from the device. Default automation configuration is used when there's no global value. The UI does not allow the value to be modified by the user when global is selected. Clicking save while global is selected will delete any previous overrides to this field.

The following figure describes Device configuration overrides.

Figure 35 Device configuration overrides



Clicking the global icon changes it to a user icon and vice versa. When the user icon is selected, the field is now editable and able to be overridden by the user. Saving with the user icon selected will save the value as an override and to the device config.

Note: If the user icon is grayed out, the value is only saved to the config, because there's no global automation value to override.

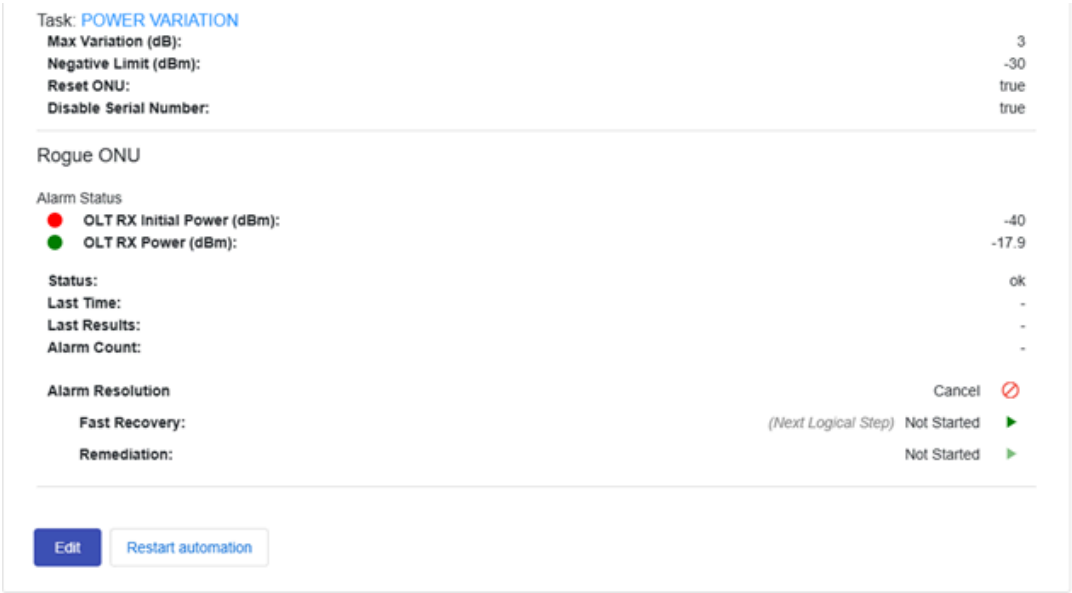
Rogue ONU tasks

Disallowed ONU and power variation are rogue ONU tasks for ONU Automation.

If problems occur during the Power Variation task, start fast recovery or remediation by clicking the green play button next to the status on the right side of the Alarm Resolution section. During Disallowed ONU, only fast recovery is available. Status of the operation is also displayed under the alarm resolution section. An operation can be canceled while in progress using the red cancel button that appears where the play button used to be.

The following figure describes Rogue ONU tasks.

Figure 36 Rogue ONU tasks



Site customization

- There are two options to customize the look and feel of the PON manager user interface:
- Create a package with custom branding that will be installed along with the PON Manager. To do this, follow the instructions provided in the README.txt file located in the tools/branding folder of the installation package. The README.txt contains detailed steps on running a script to customize the PON Manager package before installation.
 - If the PON Manager is already installed, you can make changes directly to the user interface after installation. The MCMS PON Manager provides the ability to add custom logos and backgrounds to make the site look more brand-specific. There are four places that the Web App provides the means to customize the appearance of the interface:
 - the background of the login screen
 - the footer text
 - logo of the login screen

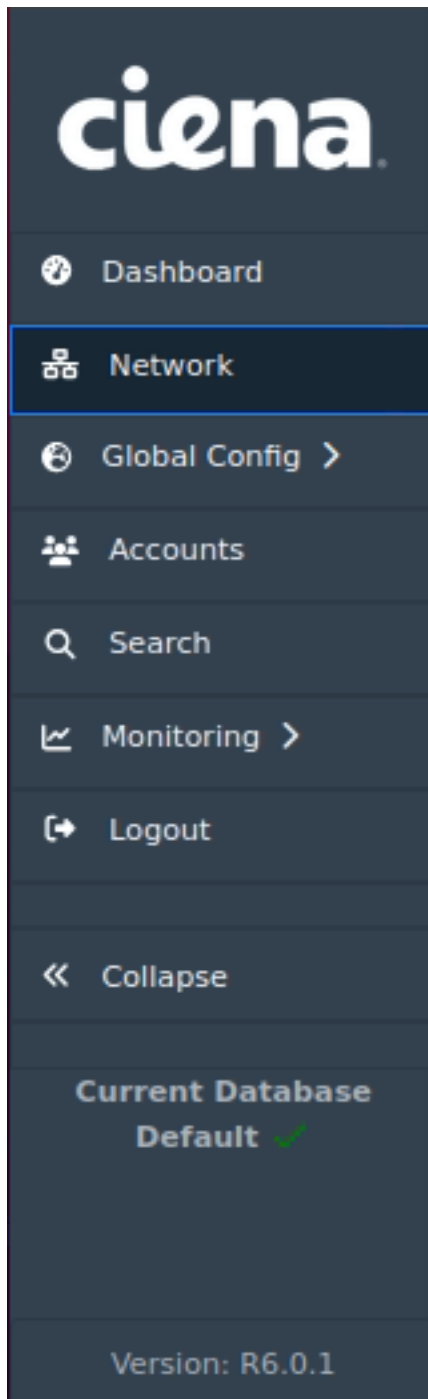
— the corner logo visible after login.

After logging into the Web App, any user can customize the look of the PDM by clicking on the TIBIT Communications logo on the upper left corner of the screen. After clicking on the logo, a popup appears showing the current images and a preview for the user of what the selected images would look like after saving.

Version

A user can see more about the version of the MCMS PON Manager by clicking on the “Version” label on the bottom of the Site Navigation menu.

The following figure describes the version label.

Figure 37 Version label

This button displays a popup that gives details on the current build being used as well as any third party software used in the creation of the MCMS PON Manager.

List of procedures

Procedures for Dashboard configuration are:

- [Procedure 16, “Configuring the PON Controller image”](#)
- [Procedure 17, “Configuring the switch name”](#)
- [Procedure 18, “Configuring the switch image”](#)
- [Procedure 19, “Configuring location coordinates for the PON Controller”](#)
- [Procedure 20, “Configuring location coordinates for the switch”](#)
- [Procedure 21, “Configuring the PON Controller name”](#)
- [Procedure 22, “Deleting a PON Controller”](#)
- [Procedure 23, “Configuring PON Automation name”](#)
- [Procedure 24, “Logging in to MCMS for the first time with a configured database and no users”](#)
- [Procedure 25, “Logging in to MCMS for the first time with a configured database with users”](#)
- [Procedure 26, “Logging out from a PON Manager session”](#)
- [Procedure 27, “Deleting a PON automation override”](#)
- [Procedure 28, “Upgrading from R3.0.X and earlier to R3.1.0 and later”](#)

Procedure 16 Configuring the PON Controller image

Configure an image for the PON Controller as required by the network plan.

Requirements

If you try to upload an image and receive the message “The selected file must have a unique name”, the image is already being used with a different Device Type. Create a copy of the image with a different file name. You’ll be instructed to select the corresponding Device Type for this new image in the steps below.

Overview

The Identification tab contains two tiles. The upper tile displays identifying information about the controller, such as its name, ID, image, and more. Several of these items, including the image, are configurable.

Steps

- 1 Click Network on the left navigation pane.
- 2 Navigate to the desired PON Controller.
- 3 Click the Identification tab.
- 4 Click Edit.
- 5 In the Picture field, click the arrow to display the available images.
- 6 Proceed as follows:

If	Then
You see the image you want to use:	Select the image. Click Save. STOP HERE. This procedure is complete.
You do not see the image you want to use:	Continue to Step 7.

- 7 From the left navigation pane, navigate to Global Config, Files, and click the Pictures tab.
- 8 In the displayed list, use the arrows to display the available images.
- 9 Proceed as follows:

If	Then
You see the image you want to use:	Click Edit. Continue to Step 10.

If	Then
You do not see the image you want to use:	Click Upload. In the window that displays, click Choose file. Locate and select the image, then click Open. Continue to Step 10.
10	In the Device Type field for the image, use the arrow to select CNTL.
11	Click Save.
12	Return to the Identification tab and click Edit.
13	In the Picture field, click the arrow to display the available images.
14	Select the image.
15	Click Save.

Procedure 17 Configuring the switch name

Configure the switch name as required by the network plan.

Overview

The Identification tab displays identifying information about the switch, such as its name, tag, location, image, and more. Several of these items, including the name, are configurable. There are no restrictions on creating the name for the switch.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired switch.
- 4 Click the Identification tab.
- 5 Click Edit.
- 6 In the Name field, enter a name for the switch.
- 7 Click Save.

The new name displays in the Name field and in the navigation panel.

Procedure 18 Configuring the switch image

Configure an image for a switch as required by the network plan.

Requirements

If you try to upload an image and receive the message “The selected file must have a unique name”, the image is already being used with a different Device Type. Create a copy of the image with a different file name. You’ll be instructed to select the corresponding Device Type for this new image in the steps below.

Overview

The Identification tab displays identifying information about the switch, such as its name, tag, location, image, and more. Several of these items, including the image, are configurable.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired switch.
- 4 Click the Identification tab.
- 5 Click Edit.
- 6 In the Picture field, click the arrow to display the available images.
- 7 Proceed as follows:

If	Then
You see the image you want to use:	Select the image. Click Save. STOP HERE. This procedure is complete.
You do not see the image you want to use:	Continue to Step 8.

- 8 From the left navigation pane, navigate to Global Config, Files, and then click the Pictures tab.
- 9 In the displayed list, use the arrows to display the available images.
- 10 Proceed as follows:

If	Then
You see the image you want to use:	Click Edit. Continue to Step 10.

If	Then
You do not see the image you want to use:	Click Upload. In the window that displays, click Choose file. Locate and select the image, then click Open. Continue to Step 10.

- 11** In the Device Type field for the image, use the arrow to select SWI.
- 12** Click Save.
- 13** Return to the Identification tab and click Edit.
- 14** In the Picture field, click the arrow to display the available images.
- 15** Select the image.
- 16** Click Save.

Procedure 19 Configuring location coordinates for the PON Controller

Configure location coordinates for the PON Controller as required by the network plan.

Overview

The Identification tab contains two tiles. The upper tile displays identifying information about the controller, such as its name, ID, picture, and more. Several of these items, including the location coordinates, are configurable.

The Location Coordinates field accepts decimal degrees (excluding direction designation and degree symbol) formatted as latitude, longitude with latitude first, followed by longitude, and separated with a comma and a space.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired switch.
- 4 Click the Identification tab.
- 5 Click Edit.
- 6 Enter latitude and longitude values for the controller in the Location Coordinates field.
- 7 Click Save.
- 8 To see the coordinates on a map, click the blue icon to the right of the Location Coordinates field.

Procedure 20 Configuring location coordinates for the switch

Configure the location coordinates for a switch as required by the network plan.

Requirements

This task is performed from the Identification tab, accessible from the left navigation pane by selecting Network / Topology, then drilling down to the switch device.

Overview

The Identification tab displays identifying information about the switch, such as its name, tag, location, image, and more. Several of these items, including the location coordinates, are configurable.

The Location Coordinates field accepts decimal degrees (excluding direction designation and degree symbol) formatted as latitude, longitude with latitude first, followed by longitude, and separated with a comma and a space.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired switch.
- 4 Click the Identification tab.
- 5 Click Edit.
- 6 In the Location Coordinates field, enter latitude and longitude values for the switch.
- 7 Click Save.
- 8 To see the coordinates on a map, click the blue icon to the right of the Location Coordinates field.

Procedure 21 Configuring the PON Controller name

Configure the name for the PON Controller as required by the network plan.

Overview

The Identification tab contains two tiles. The upper tile displays identifying information about the controller, such as its name, ID, picture, and more. Several of these items, including the name, are configurable. There are no restrictions on creating the name for the controller.

Steps

- 1 Click Network on the left navigation pane.
- 2 Navigate to the desired PON Controller.
- 3 Click the Identification tab.
- 4 Click Edit.
- 5 Enter a name for the controller in the Name field.
- 6 Click Save.

The new name displays in the Name field and in the navigation panel.

Procedure 22 Deleting a PON Controller

Delete a PON Controller as required by the network plan.

Requirements

This task is performed from the Operations tab, accessible from the left navigation pane by selecting Network / MGMT LANs, then drilling down to the controller device where the OLT resides.

Overview

When the PON Controller is deleted, all of its configuration records are deleted from the database. This action cannot be undone.

Steps

- 1 Click Network on the left navigation pane.
- 2 Navigate to the desired PON Controller.
- 3 Click the Operations tab.
- 4 Click Delete in the Delete Controller panel.

Procedure 23 Configuring PON Automation name

Configure the PON Automation name as required by the network plan.

Requirements

This task is performed from the PON Automation tab, accessible from the left navigation pane by selecting PON Automation, then drilling down to the specific instance that you need.

Overview

There are no restrictions on creating the name for the PON Automation instance.

Steps

- 1 Click Network on the left navigation pane.
- 2 Navigate to the desired PON Controller.
- 3 Click the Automation tab.
- 4 Click Edit.
- 5 Enter a name for the instance in the Name field.
- 6 Click Save.

The new name displays in the Name field and in the navigation panel.

Procedure 24 Logging in to MCMS for the first time with a configured database and no users

Log in to MCMS for the first time using a configured user database that has no users, as required by the network plan.

Requirements

If you are using the default self-signed or other untrusted certificate, a security exception must be added in the browser for both the PON Manager Web App and the REST API. The browser displays a warning regarding potential security risks, with options for addressing them. Note that if you activate the security exceptions, the HTTPS traffic is still encrypted.

Steps

- 1 Connect to the IP address for the Web App.
- 2 Click the Advanced button on the warning display.
- 3 Click the Accept the Risk and Continue button.
- 4 Follow the prompt to create the first administrative user.

Procedure 25 Logging in to MCMS for the first time with a configured database with users

Log in to MCMS for the first time using a configured user database with existing users, as required by the network plan.

Requirements

If you are using the default self-signed or other untrusted certificate, a security exception must be added in the browser for both the PON Manager Web App and the REST API. The browser displays a warning regarding potential security risks, with options for addressing them. Note that if you activate the security exceptions, the HTTPS traffic is still encrypted.

Steps

- 1 Connect to the IP address for the Web App.
- 2 Click the Advanced button on the warning display.
- 3 Click the Accept the Risk and Continue button.

Procedure 26 Logging out from a PON Manager session

Log out from a PON Manager session when the session is no longer required.

Steps

- 1 Open the site navigation menu on the left of the PON Manager user interface.
- 2 Select the Exit option.

Procedure 27 Deleting a PON automation override

Delete a PON automation override as required by the network plan.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired device.
- 4 Click the Automtion tab.
- 5 Click the Delete Overrides button.
- 6 Click Delete again.

Procedure 28 Upgrading from R3.0.X and earlier to R3.1.0 and later

Upgrade from R3.0.X and earlier to R3.1.0 and later to ensure access to data collected prior to the upgrade as required by the network plan.

Requirements

For detailed instructions for this process, refer to the README.txt file in the MCMS PON Manager package.

Overview

A database schema change was implemented in R3.1.0 that improves the scalability of the system logs and statistics data collection. After upgrading from R3.0.X and earlier to R4.0.0, users are encouraged to run several scripts located in the “tools/” directory to merge old collections and then delete them from the database. If this action is not performed, only data collected after the upgrade will be accessible. This action is required only once per database.

Steps

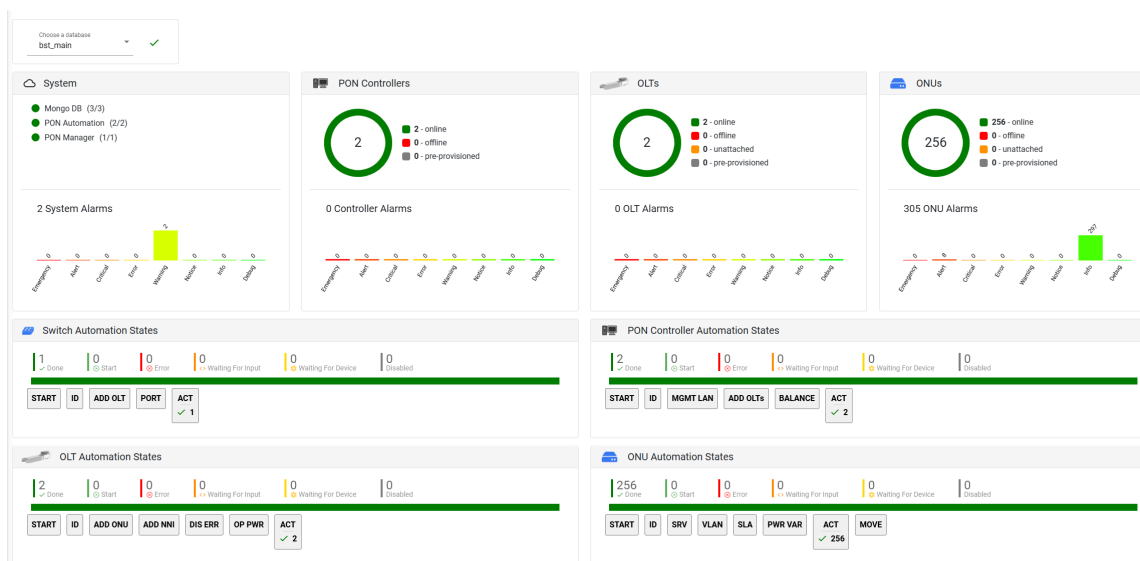
- 1 Navigate to the tools, directory.
- 2 Run the provided scripts to merge previous data collections and delete them from the database.

CHAPTER 8

Dashboard

The PON Manager dashboard displays user options available for performing various functions. The following figure describes the PON Manager Dashboard.

Figure 38 PON Manager Dashboard



The PON Manager Dashboard view displays an option to select a database for use, counts of devices in the database, counts of alarms for each device type, counts of alarms on the system, and counts of Automation States for each device type.

Database selection determines the source of the configuration, state, statistics, alarms, and logs presented in the dashboard, network, global configuration, and other portions of the user interface for this session. If the database is accessible, a green check mark displays as a button to choose the database. If the database is offline, a red "X" displays indicating that the database is not selectable.

The following actions can be performed on the dashboard:

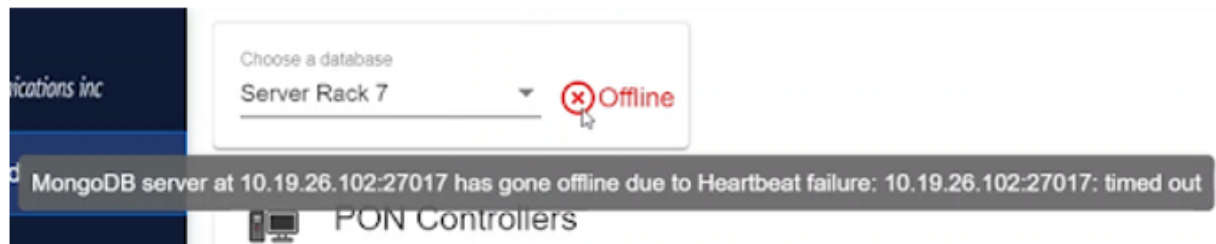
- Clicking an alarm level for a device displays those alarms in a table
- Clicking on a color in the donut chart or the specific status counts of devices in the database will display that specific device status in a table

- Clicking on the number in Automation States or the horizontal bar will show all the devices within that state in a table
- Clicking on a number or a Task label below the bar chart will filter all devices in the table that are within a specific state and task combination

The Automation tiles are only displayed if PON Auto has run on the database. The search filter can be used to look up specific information to display on the table. By default, tables are collapsed until the information is selected to display and tables can be collapsed by clicking on the header of the table card.

The following figure describes the Database Selection.

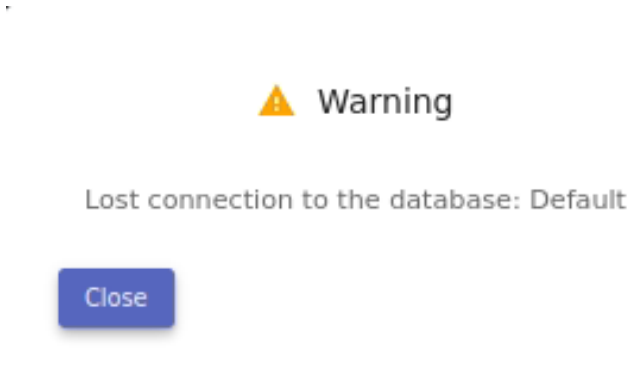
Figure 39 Database Selection



If a database becomes unreachable during its use, a warning message displays to the user to notify them of the problem.

The following figure describes the database unreachable warning.

Figure 40 Database unreachable



Dashboard device summary tiles

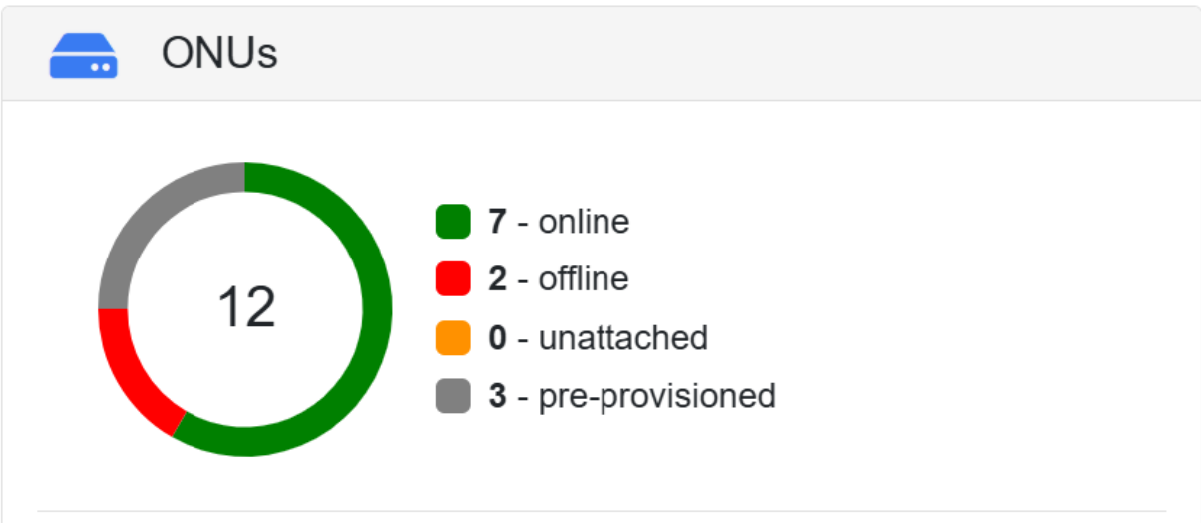
The dashboard shows one summary device tile for each of the following PON devices:

- PON Controller summary device tile
 - displays the total number of PON Controllers in the PON network by number and pie chart
 - displays the number of PON Controllers by device states by number and percentage
 - displays the number of alarms raised on the PON Controllers by alarm severity
 - displays PON Controller alarm tables by alarm severity

- OLT summary device tile
 - displays the total number of OLTs in the PON network by number and pie chart
 - displays the number of OLTs by device states by number and percentage
 - displays the number of alarms raised on the OLTs by alarm severity
 - displays OLT alarm tables by alarm severity
- ONU summary device tile
 - displays the total number of ONUs in the PON network by number and pie chart
 - displays the number of ONUs by device states by number and percentage
 - displays the number of alarms raised on the ONUs by alarm severity
 - displays ONU alarm tables by alarm severity

The following figure describes the Device Summary.

Figure 41 Device Summary



The following table details the PON device states.

Table 21 Device states for PON Controllers, OLTs and ONUs

Device states for PON Controllers, OLTs and ONUs	Description
Online	A device that is currently active in the PON network.
Offline	A device that has been provisioned and inventoried but not active in the PON network.
Unattached	A device that has its provisioning removed. A device that is not inventoried and is no longer active in the PON network.

Device states for PON Controllers, OLTs and ONUs	Description
Pre-provisioned	A device that has been configured and not active in the PON network.

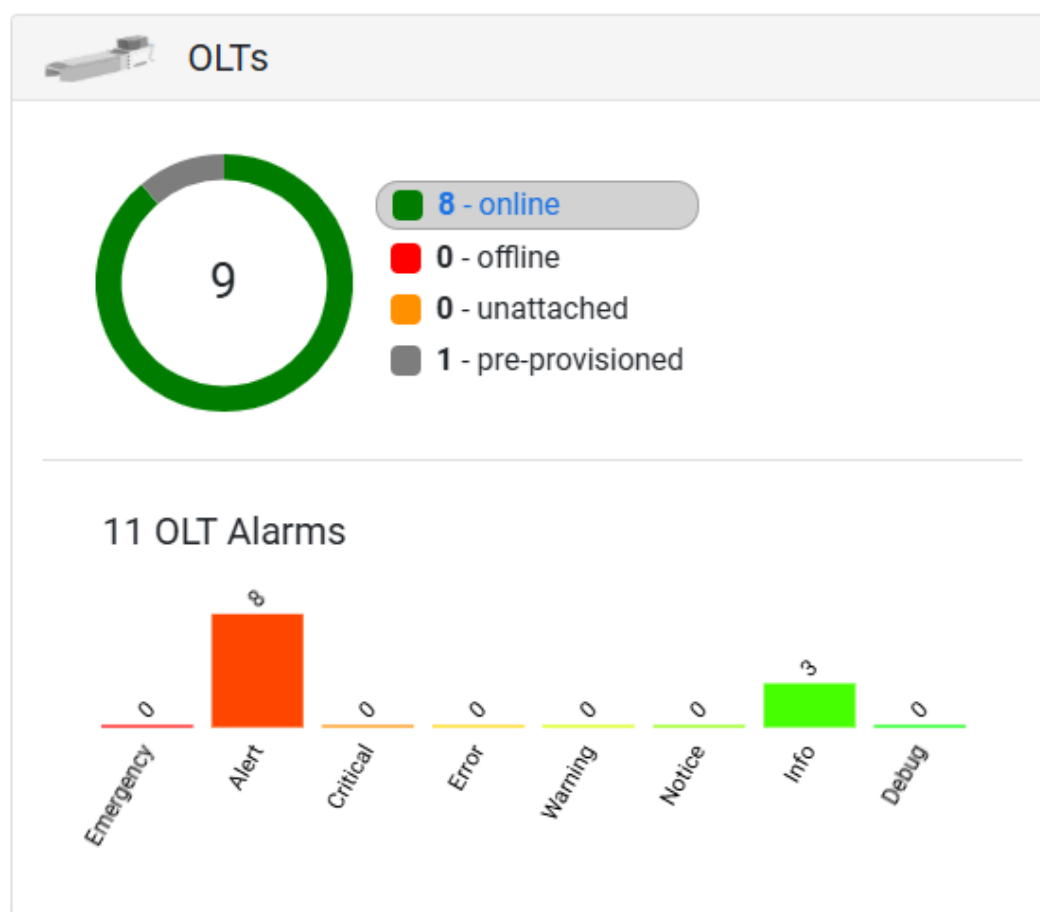
The Device Status table displays:

- the ID of the device
- the nickname of the device
- the last status time from the device
- the IDs of the parent OLT and PON Controller when applicable

To display the tables, click on a color on the donut chart on the left side of the device states panel, or any of the displayed states counts.

The following figure shows the device summary for OLTs

Figure 42 Device summary for OLTs



The following figure shows the OLT device statuses.

Figure 43 OLT device statuses

All Online OLTs

Filter

ID	Name	Status	Last Status Update	Parent Controller ID
e0:9b:27:f0:e9:ac	8112_2_OLT8	Primary	2/9/2026, 7:25:14 PM	0081:12:01:01:00
e0:9b:27:ec:ce:06	8112_1_OLT11	Primary	2/9/2026, 7:25:14 PM	0081:12:01:01:00
e0:9b:27:f0:e9:f4	8112_1_OLT8	Primary	2/9/2026, 7:25:14 PM	0081:12:01:01:00
e0:9b:27:f0:e9:f0	8112_1_OLT1	Primary	2/9/2026, 7:25:14 PM	0081:12:01:01:00
e0:9b:27:f5:d1:34	8112_2_OLT3	Primary	2/9/2026, 7:22:20 PM	0081:12:01:01:00
e0:9b:27:ec:ce:02	8112_2_OLT11	Primary	2/9/2026, 7:25:13 PM	0081:12:01:01:00
e0:9b:27:7e:8e:24	8112_1_OLT3	Primary	2/9/2026, 7:22:20 PM	0081:12:01:01:00
e0:9b:27:f5:d1:32	8112_2_OLT1	Primary	2/9/2026, 7:25:15 PM	0081:12:01:01:00

Items per page: 10 1 - 8 of 8

The alarms raised against the PON Controllers, OLTs and ONUs are bar graphed against the following alarm severity levels:

- emergency
- alert
- critical
- error
- warning
- notice
- info
- debug

Dashboard alarm tables

Selecting an alarm severity level generates an alarm table for that identifies the devices the alarm was raised against, the times when the alarms were raised and the identities of the alarms for that particular severity level. When applicable, the alarm table displays the identity of the parent OLT or PON Controller.

Dashboard automation states

The dashboard automation states displays the current PON automation states for each of the following PON devices:

- Switch
 - displays the total number of switches in the PON network that have completed automation and are in the active state as Done.
 - displays the number of switches that are unable to complete activation due to an error as Error.
 - displays the number of switches where automation is paused waiting for user input as Waiting For Input.
 - displays the number of switches that have automation waiting for the PON Controller to complete configuration as Waiting For Device.
 - displays the number of switches that have automation disabled as Disabled.

- displays switch automation tables for Done, Error, Waiting For Input, Waiting For Device and Disabled automation states.
- PON Controllers
 - displays the total number of PON Controllers in the PON network that have completed automation and are in the active state as Done.
 - displays the number of PON Controllers that are unable to complete activation due to an error as Error.
 - displays the number of PON Controllers that have automation paused waiting for user input as Waiting For Input.
 - displays the number of PON Controllers that are waiting to complete configuration as Waiting For Device.
 - displays the number of PON Controllers that have automation disabled as Disabled.
 - displays PON Controller automation tables for Done, Error, Waiting For Input, Waiting For Device and Disabled automation states.
- OLTs
 - displays the total number of OLTs in the PON network that have completed automation and are in the active state as Done.
 - displays the number of OLTs that are unable to complete activation due to an error as Error.
 - displays the number of OLTs that have automation paused waiting for user input as Waiting For Input.
 - displays the number of OLTs that have automation waiting for the PON Controller to complete configuration as Waiting For Device.
 - displays the number of OLTs that have automation disabled as Disabled.
 - displays OLT automation tables for Done, Error, Waiting For Input, Waiting For Device and Disabled automation states.
- ONUs
 - displays the total number of ONUs in the PON network that have completed automation and are in the active state as Done.
 - displays the number of ONUs that are unable to complete activation due to an error as Error.
 - displays the number of ONUs that have automation paused waiting for user input as Waiting For Input.
 - displays the number of ONUs that have automation waiting for the PON Controller to complete configuration as Waiting For Device.
 - displays the number of ONUs that have automation disabled as Disabled.
 - displays ONU automation tables for Done, Error, Waiting For Input, Waiting For Device and Disabled automation states.

Dashboard automation tables

Selecting a number or horizontal bar in the automation state generates a either an automation Done, Error, Waiting for Input, Waiting for Device or Disabled automation summary table. The table displays the identities of the devices, the automation states as enabled or disabled, the current automation tasks of the devices, and the automation states for the device.

Selecting a device identity takes you to that device's PON Automation tab.

CHAPTER 9

Network

This chapter describes the top-level management entities within the PON network.

Devices

There are several device types defined as top-level management entities within PON Manager. Each device is represented in the device navigation tree and is identified in the tree by an icon.

The following table identifies device types and their associated icons.

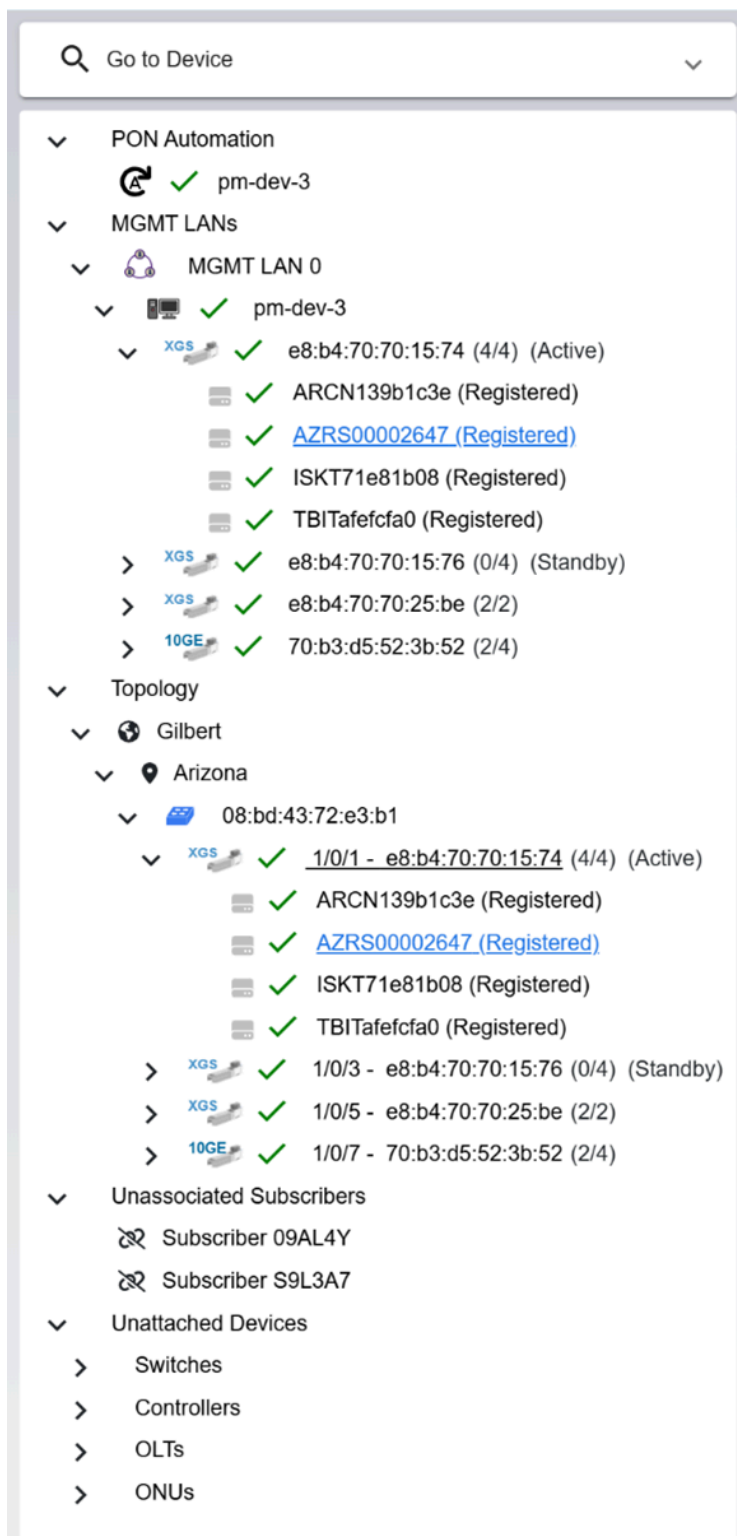
Table 22 Device types

Device	Icon	Description
Switch or Router		Network switch with respect to switch properties associated with PON. Switches are discovered by OLT devices through LLDP.
PON Controller		The PON Controller with respect to management of the application service, not the system hosting the Controller.
25GS OLT		25GS MicroPlug OLT device.
XGS OLT		XGS MicroPlug OLT device.
10G-EPON OLT		10G-EPON OLT MicroPlug OLT device.
ONU		ONUs compliant with the XGS-PON or 10G EPON standards.
PON Automation		The PON Automation service running against the current database. This is only be present when using PON Automation.

Device navigation tree

The device navigation tree has four root-level branches: PON automation, MGMT LANs, topology, and unattached devices. The PON automation branch only appears if the database has a PON automation service running against it. By default, one branch under the MGMT LANs branch is “Unnamed”. This name might change and others appear later if management LAN names are assigned to PON Controllers. Each named management LAN branch lists all of the PON Controllers using that name as sub-branches. Under controllers, OLTs are sorted by OLT MAC address.

The following figure describes the device navigation tree.

Figure 44 Device navigation tree

All identified switches appear under the topology branch organized by geographic labels if assigned. This provides a switch-based hierarchy to access the same OLT and subtended ONU devices that are found under the MGMT LAN hierarchy described previously. Under switches, OLTs are sorted and organized by the switch port number the OLT is plugged into. The OLT learns the switch port number from the switch using LLDP. An “Unknown Switch” appears if there are OLTs without LLDP information.

Unassociated subscribers lists out all subscriber provisioning that are not associated with a device. This tree only appears if the Subscriber Provisioning field is enabled in the Display Preferences tab.

Unattached devices lists all devices on the network that do not have a parent device. Many factors can determine when a device is listed as unattached. For example, the device's previous parent device may have been removed from the network.

Each device type is marked by its unique icon to help quickly identify the device type. All PON Controller, switch and router, OLT, and ONU branches also have a secondary icon indicating device status and alarms. This device tree automatically updates any open nodes. Each of these device branches lists the device's ID (Name if available) as clickable text to navigate to that device. Note that is not possible to navigate to a management LAN. Each OLT branch also displays the number of online ONUs out of the total ONUs beneath it, and every ONU also displays its current state.

The width of this tree pane may be adjusted by dragging the right border to the left or right. There is also a help icon at the bottom right that opens a window to explain the various icons and levels of the tree.

Active warnings and alarms for devices are displayed as icons on the tree nav next to their respective device. When hovering over the icon, a panel displays showing the alarm type and the number of current alarms of this type. Clicking the icon navigates users to the device's alarm page, and clicking the alarm type in the panel pre-filters the page's alarm table, showing only that type of alarm.

Device statuses in the tree are identified by the icons in the table below:

Table 23 Device Statuses

Status	Icon	Description
No alarms		Device is online with no active warnings or errors.
Offline		Device is offline. This icon displays as priority over errors or warnings.
Errors		Device has active errors. The sum of errors are shown within its badge in the icon. This icon takes priority over warnings on the same device.
Warnings		Device has active warnings. The sum of warnings are shown within its badge in the icon.

At the top of the navigation tree is the Go to Device section. By expanding this section, the user can select a criterion to search on. Enter the search text to find a specific device, and then select the arrow to navigate to that device. Selecting the Advanced Search navigates to the Search page for the application.

ONU device states

In the network device tree, the device state is displayed to the right of the ONU in parentheses. ONU device states display the current state of the ONU in relation to its parent OLT. The device states do not appear for ONUs in the unattached devices section of the tree, since these ONUs are not associated with any OLT.

The following table describes the ONU device states.

Table 24 ONU Device States

State	Description
Deregistered	The ONU is deregistered and inventoried in the OLT configuration file. This indicates a Loss-of-signal (LOS) condition for the ONU.
Disabled	GPON: a disable serial number PLOAM was sent to the ONU, disabling the serial number for the ONU. EPON: the upstream transmit laser is disabled for the ONU.
Disallowed Admin	The ONU is administratively disabled. The MAC address of the parent OLT was not found within the list of allowed MAC addresses for this ONU.
Disallowed Error	The ONU deregistered and is blocked from registering by the OLT due to excessive upstream errors.
Disallowed Reg ID	GPON: The expected ONU registration ID does not match the actual ONU registration ID.
Dying Gasp	The ONU deregistered due to dying gasp (loss of power).
Offline	The ONU is offline.
Pending Reset	A reset has been requested for the ONU.
Preprovisioned	The ONU is configured before being attached to the network and discovered by the PON Controller (CFG without a STATE).
Registered	The ONU is registered on the OLT and is inventoried in the OLT configuration.
Reset	The ONU is in the process of being reset.
Unprovisioned	The ONU is attempting to register with the OLT. New ONUs are in this state temporarily until they are configured on the OLT.
Unspecified	The ONU is registered on the OLT and is not inventoried in the OLT configuration.

Hierarchy view

The hierarchy view bar displays the current hierarchy of viewed devices.

Starting on the left with the management LAN, the selected PON Controller and switch or router, OLT and ONU display. The name, ID, MAC address, switch port (for OLTs), and the state (for ONUs) of the current hierarchy devices are all displayed. Each device listed, excluding the

MGMT LAN, is clickable to navigate to any device in the hierarchy. If a PON automation service is selected, PON automation is the only element displayed in the hierarchy. Only those selected devices display.

The following figure describes the Hierarchy View.

Figure 45 Hierarchy View

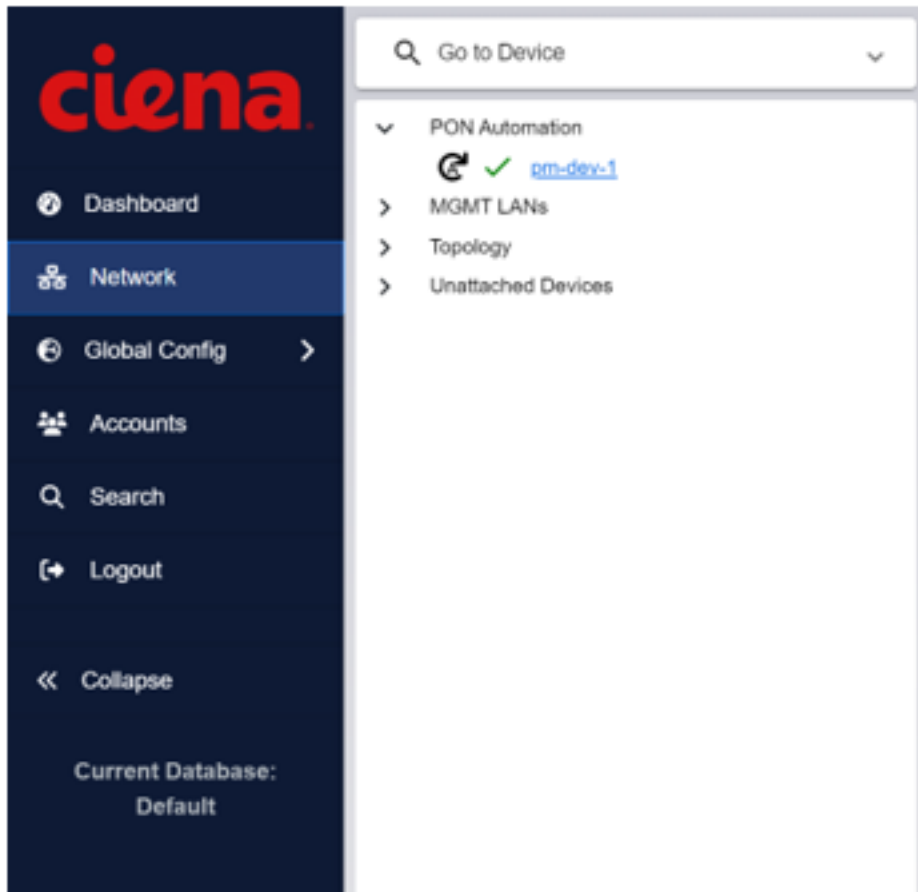


PON automation

PON automation is an optional MCMS service that runs alongside the PON Controller, PON Manager, and other MCMS software components.

When PON automation is in use, the service appears in the network device tree as a manageable entity. This section describes the management interface for the PON automation service.

The following figure describes PON automation.

Figure 46 PON Automation

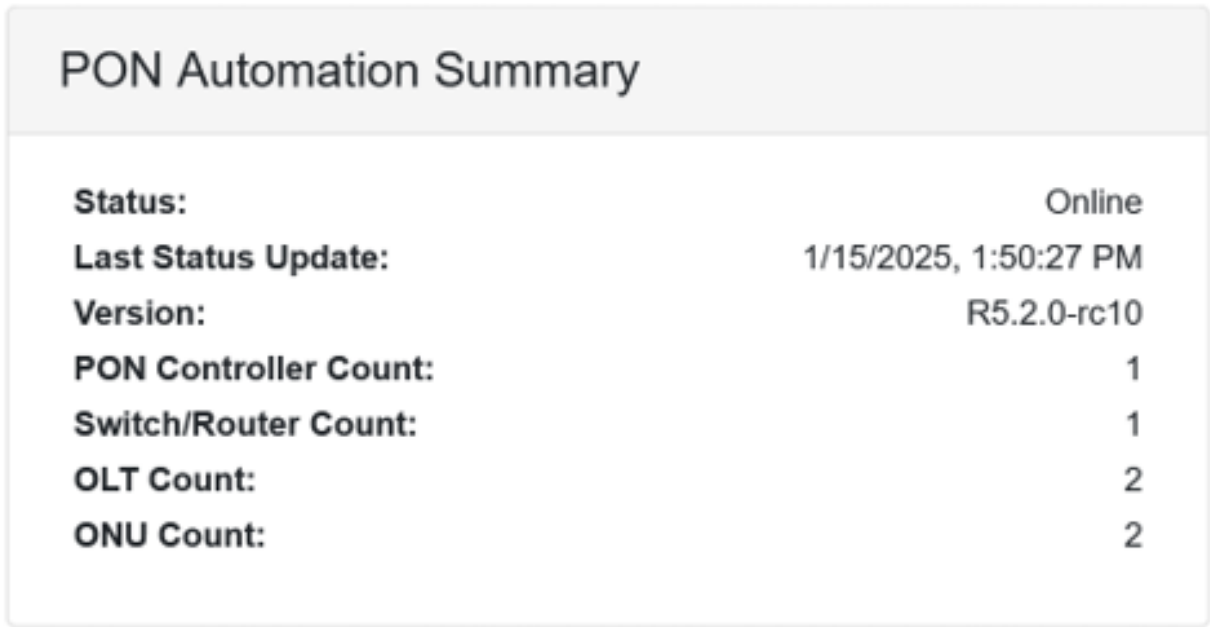
PON automation summary

The summary tab displays information relevant to the current state and status of the service.

Values such as the ID, version, PON Controller, switch and router, OLT, and ONU counts and status are displayed. The time stamp indicating when the PON automation service's state was updated is also displayed.

The following figure describes PON automation summary

Figure 47 PON automation summary



PON automation identification

There are two tiles on the PON automation identification page.

The first displays identifying information about the service, such as its name, ID, and more. The name is configurable by clicking Edit at the bottom of the tile. The second tile shows a table for the system that is supporting the PON automation feature. The table lists all the network interfaces on that system.

The following figure describes the network on this maching

Figure 48 Network on this machine



PON Automation Name

System Name: pm-dev-3

DB Config Version:

R5.2.0-rc10

Edit

Networks on this machine

Interfaces

Interface	MAC Address	IPv4 Address	IPv6 Address
eno1	18:66:da:7d:f4:fd	10.3.16.30/24	fe80::1a66:daff:fe7d:f4fd/64
br-c6ec0e3cca3a	02:42:74:b9:ab:7e	172.18.0.1/16	fe80::42:74ff:feb9:ab7e/64
docker0	02:42:c9:1e:d8:ef	172.17.0.1/16	fe80::42:c9ff:fe1e:d8ef/64
br-8d968516a17e	02:42:75:0d:30:8c	172.19.0.1/16	undefined/undefined
vetha9597b4	4a:16:a9:0f:f2:42		fe80::4816:a9ff:fe0f:f242/64
vethfb99d10	aa:c7:0c:e7:79:03		fe80::a8c7:cff:fe7:7903/64
veth139f3c0	22:0d:28:f7:a4:a6		fe80::200d:28ff:fe17:a4a6/64
veth37bc815	52:98:27:82:5e:fc		fe80::5098:27ff:fe82:5efc/64
eno2.4090	18:66:da:7d:f4:fe		fe80::1a66:daff:fe7d:f4fe/64

Logs tab

The Logs tab contains a table of logs the PON automation service has entered into the database. The logs track the following time ranges:

- One Hour
- Day
- Week
- Month
- Three Months

Sort the logs by time or severity. Filter the logs by time, severity, and message.

Click delete, to clear all logs for this PON automation service.

Operations tab

The Operations tab contains several fields describing a PON Controller's behavior. From the Operations tab, pause, reset, auto create ONUs or shutdown the PON Controller, configure the OLT timeout, management LAN name, and set the loop delay.

Note: Auto Create ONUs can only be set to true while Subscriber Provisioning is Disabled.

All data belonging to this controller may also be deleted. The delete action prompts for a confirmation and cannot be undone if confirmed.

The following figure describes operational settings.

Figure 49 Operational Settings

Operational Settings

Pause:	false
OLT Timeout:	300
MGMT LAN:	Unnamed
Loop Delay:	0
Loop Count:	171142
Last Loop:	8/26/2025, 4:45:56 PM
UMT Discovery Timeout:	2
UMT Relay	
Maximum CPEs Allowed	0
Maximum CPE Time	0
Expired Age Limit	65535

Edit

Reset Controller

Reset this Controller

Reset

Delete Controller

Delete this controller and it's records from the database

Delete

List of procedures

Procedures for PON network:

- [Procedure 29, "Adding the network VLAN to the inventory"](#)
- [Procedure 30, "Adding an ONU to the inventory"](#)
- [Procedure 31, "Removing the network VLAN from the inventory"](#)
- [Procedure 32, "Removing the ONU from the inventory"](#)
- [Procedure 33, "Upgrading ONU firmware"](#)

Procedure 29 Adding the network VLAN to the inventory

Add the network VLAN to the inventory as required.

Steps

- 1 Navigate to **Network**> **select OLT** > **NNI Networks** > **Config**
- 2 The NNI Networks section will display a check next to any Network VLANs that are inventoried under the Inventoried column.
- 3 Click on the **Edit** button
- 4 Click on **Add new** to add any network VLANs from inventory
- 5 Click on the **Save** button

Procedure 30 Adding an ONU to the inventory

Add an ONU to the inventory once the ONU completes the service configuration..

Overview

Adding an ONU to the inventory means that the AllocIDs and other related configurations for the ONU are stored in the database. This means after an ONU reset, the same AllocID and configurations is retrieved from the database and restored to the ONU prior to the reset.

Steps

- 1 Navigate to **Network > select OLT > ONU Inventory**
- 2 Any ONUs not inventoried will have ONU state of **Unspecified**
- 3 Click on the **Edit** button to inventory the ONUs
- 4 Click on the **Add** button for each ONU to be added to the inventory
- 5 Click on the **Save** button and wait for the ONUs to be added to the inventory

Procedure 31 Removing the network VLAN from the inventory

Remove the network VLAN from the inventory as required.

Overview

Inventorying Network VLANs and ONUs will save the configuration information, such as allocation IDs & XGEM ports IDs, in the database so that they are preserved after changes, such as OLT or ONU reboot. This should only be done for pre-provisioning or if the PON completes system configuration of all ONUs.

If pre-provisioning is not supported, Ciena recommends that all Network VLANs and ONUs be removed from inventory, especially for lab testing. This removes any limitation/restriction upon the PON Controller to use specific configurations that may potentially be in conflict with other ONUs.

Steps

- 1 Navigate to **Network> select OLT > NNI Networks > Config**
- 2 The NNI Networks section will display a check next to any Network VLANs that are inventoried under the Inventoried column.
- 3 Click on the **Edit** button
- 4 Click on **Remove** to remove any network VLANs from the inventory
- 5 Click on the **Save** button

Procedure 32 Removing the ONU from the inventory

Remove the ONU from the inventory as required.

Requirements

Before provisioning the service configuration for an ONU, it must not be inventoried. Inventorying the ONU means that an AllocID will be pre-assigned to it, which can potentially cause out-of-sync issues when the ONU is provisioned for service later.

Steps

- 1 Navigate to **Network > select OLT > ONU Inventory**
- 2 Any ONUs that are inventoried will have a check under the Inventoried column and have an ONU State of **Registered**.
- 3 Click on the **Edit** button to inventory the ONUs
- 4 Click on **Remove** button for each ONU to be removed from the inventory
- 5 Click on the **Save** button and wait for the ONU removal process to complete

Procedure 33 Upgrading ONU firmware

Upgrade ONU firmware as required by the network plan.

Overview

The Firmware tab contains two sub-tabs: OLT Firmware for managing the firmware on a given OLT, and ONU Firmware for monitoring the firmware status on subtended ONUs. This procedure is performed on the OLT Firmware sub-tab.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired ONU.
- 4 Click the Firmware menu.
- 5 Click Edit.
- 6 Click the arrow to select the number for the bank that should be active and used in the Bank Pointer State field. If the arrow is grayed out, click the globe icon to the right, then click the arrow.
- 7 Click the arrow in the Bank 0 State Version field to select the required firmware image. If the arrow is grayed out, click the globe icon to the right, then click the arrow.
- 8 Repeat Step 7 for the other bank.
- 9 Click Save.

CHAPTER 10

ONU configuration

ONU tabs are used to configure and monitor ONUs in the PON network.

ONU summary tab

The ONU summary tab contains two tiles with data about the ONU. The first tile shows the PON automation status for this ONU, the total alarm counts, status information, downstream and upstream statistics between the OLT and ONU, and the ONU's PON and UNI ports statuses. If PON automation is inactive or not used, users see text stating that the PON automation service is unavailable, instead of a diagram.

The downstream connection and upstream connection fields indicate the health of the connection, either green (healthy) or red (unhealthy). The first table below describes the conditions for the optical power measurements to be green or red. The next table describes the UNI Port status conditions for each color.

Table 25 ONU summary connection status health LED criteria

Field	Green	Red
OLT TX Power	greater than or equal to 3 dB	< 3 dB
ONU RX Power	greater than or equal to -30 dB	< -30 dB
ONU Bit Error Rate (BER)	Pre-FEC BER = 0 Post-FEC BER = 0	Post-FEC BER > 0
OLT RX Power	greater than or equal to -30 dB	< -30 dB
ONU TX Power	greater than or equal to 3 dB	< 3 dB
OLT Bit Error Rate (BER)	Pre-FEC BER = 0 Post-FEC BER = 0	Post-FEC BER > 0

At the bottom of the tab in the second tile, the alarms table lists all active alarms on the ONU in detail.

The following figure describes the ONU summary tab.

Figure 50 ONU summary tab



Registration state

The Registration State represents the current registration status of the ONU.

The registration state provides more detailed ONU status, such as provisioning failures, faults, resets, and firmware upgrades.

The following figure describes the ONU status.

Figure 51 ONU status

ONU Status	
Status:	Registered
Last Status Update:	4/30/2025, 10:55:11 AM
Online Duration:	50d, 19h, 36m
Since:	3/10/2025, 3:18:51 PM
Last Dereg Reason:	
Registration State:	Provisioned
Configuration Status:	Valid
Firmware Version:	3.2.36
Controller Version:	R6.0.0-rc6

The following table describes ONU registration states.

Table 26 ONU registration states

Status	Description
Provisioning	PON Controller is currently provisioning service for the ONU
Provisioned	Provisioning was successfully applied to the ONU
Provisioning Stalled	PON Controller provisioning the ONU is not converging. This can be due to an incompatibility between the ONU Service Configuration (SRV-CFG) and the ONU device
Provisioning Failed	OLT or ONU device returned an error while provisioning service for the ONU
Service Disabled	ONU Service configuration (SRV-CFG) is set to "Disabled"
Unreachable	(XGS-GPON Only) The ONU is not responding to management requests, based on attempts to get ONT Data OMCI ME Data Sync Interval
Suspended	Processing for the ONU has been suspended. Set when PON Controller waits for UMT Relay to clear its learning tables when Source Mac Verify is enabled
FW Upgrade	ONU Firmware is being upgraded
Reset	Commanded ONU reset occurred

ONU identification tab

The identification tab hosts the configurations for the ONU's identification details. This ID may be any string or ANY to allow any registration ID value. Beneath the configurable items are state details, including data about the ONU's model, vendor, manufacturer and more. A picture of the ONU can be displayed in place of the default blue icon.

The picture field is supported by the PON automation service. Refer to the PON automation documentation for more information on managing configuration for these fields.

The following figure describes the Identification tab.

Figure 52 Identification tab

ONU Name
ID: TBITafefcfa0

Configuration

Labels:
Picture: PIC-ONU-HiSense
Location Coordinates: ☐
Address:
NETCONF Name: TBITafefcfa0
Tag:
Create Date: 2023-12-12 18:23:27.362238
Allowed OLTs: ANY
Expected Registration ID: ANY

State

Registration ID: REGID-ONT-54424954-0000ac4afefcfa08
Vendor: TBIT
Model: HBG7100A
Manufacturer: TBITCOM
Hardware Version: v1.0
Equipment ID:
Logical ID:
Logical Password:
DB Config Version: R5.0.0
Parent PON Controller: 18:66:da:7d:14:1e
PON Controller Version: R5.0.0-rc20
OMCC Version: 0xa3

[Edit](#)

Associate provisioning

The Associate Provisioning button appears when subscriber provisioning is enabled and the ONU is not yet associated to a subscriber.

Clicking this button opens a popup with a stepper.

- The first step gives the option to associate with an existing provision that is available or to create one based on the default ONU automation document.
- The second step gives the option to connect the subscriber to the device by specifying the GPON FSAN Vendor ID/Serial Number or EPON MAC address of the ONU device.

GPON ONUs have an additional option to associate the subscriber provisioning to the ONU by GPON Registration ID.

The following figure describes Associate provisioning.

Figure 53 Associate provisioning

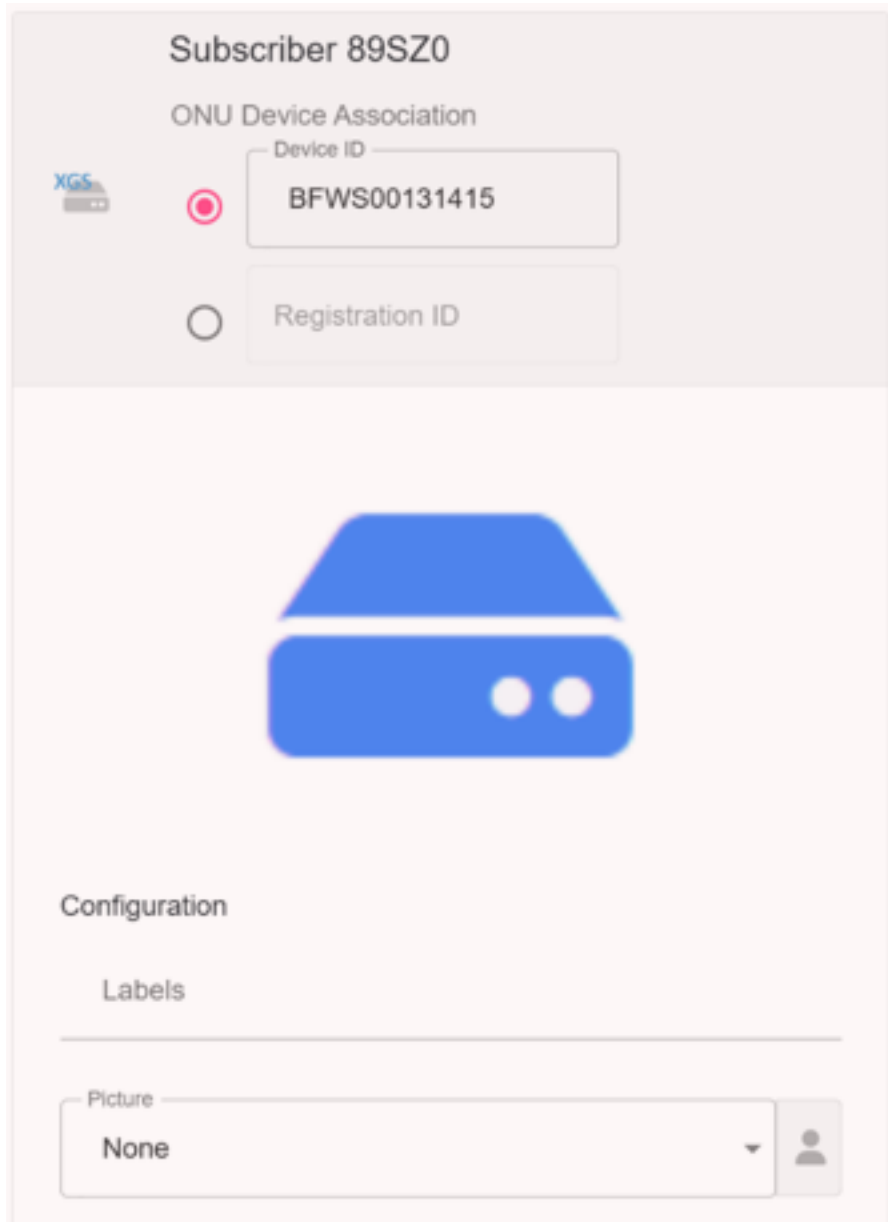
The figure consists of two side-by-side screenshots of a web interface titled "Associate Provisioning".

The left screenshot shows the "Subscriber Provisioning" step (indicated by a blue circle with the number 1). Under "Existing Provision", a dropdown menu is open showing "Subscriber S9L3A7". Below this, the "New Provision:" option is unselected, with a text input field labeled "New Provision Name". At the bottom are "Cancel" and "Next" buttons. A second step indicator (blue circle with the number 2) for "Device Identification" is visible at the bottom left.

The right screenshot shows the "Device Identification" step (indicated by a blue circle with the number 2). The "Subscriber Provisioning" step is now greyed out. Under "Serial Number: TBITafefcfa0", the "Registration ID: REGID-ONT-TBIT-0000ac4afefcfa08" option is unselected. At the bottom are "Back" and "Save" buttons.

When an ONU is associated with a subscriber, the Associate Provisioning button disappears. Click edit to modify the device association. The device identifier can be modified to connect the subscriber to a different device. The field can also be saved as blank to disassociate the subscriber from the ONU.

The following figure describes ONU device association.

Figure 54 ONU device association

Subscriber 89SZ0

ONU Device Association

☒ Device ID
BFWS00131415

☐ Registration ID



Configuration

Labels

Picture
None

ONU firmware tab

The ONU firmware tab contains two display tiles. The first tile enables users to view and configure the maximum parallel ONU upgrades on this OLT.

The second tile displays the ONU firmware upgrade status, which lists the ONU ID, the firmware bank the file was saved to, the filename, and the last reported status for the firmware upgrade.

The following figure describes the ONU firmware tab.

Figure 55 ONU firmware

ONU Firmware

Bank Pointer:

1

Bank 0:

File:

Version:

State: R5.0.0

Bank 1:

File:

R5.0.0-ONU-FW.bin

Version:

R5.0.0

OMCI Download Parameters

Max Window Size [bytes]:

64

Backoff Divisor:

2

Backoff Delay [Seconds]:

5

Max Retries:

4

End Download Timeout [Seconds]:

0

Download Format:

Baseline OMCI

State

Upgrade Status:

Successful

Failures:

0

Version Mismatches:

0

Upgrade Duration:

01m, 14s

Upgrade Time:

12/17/2024, 10:24:15 AM

Current Version:

R5.0.0

ONU Model:

HBG7100A

Equipment ID:

Hardware Version:

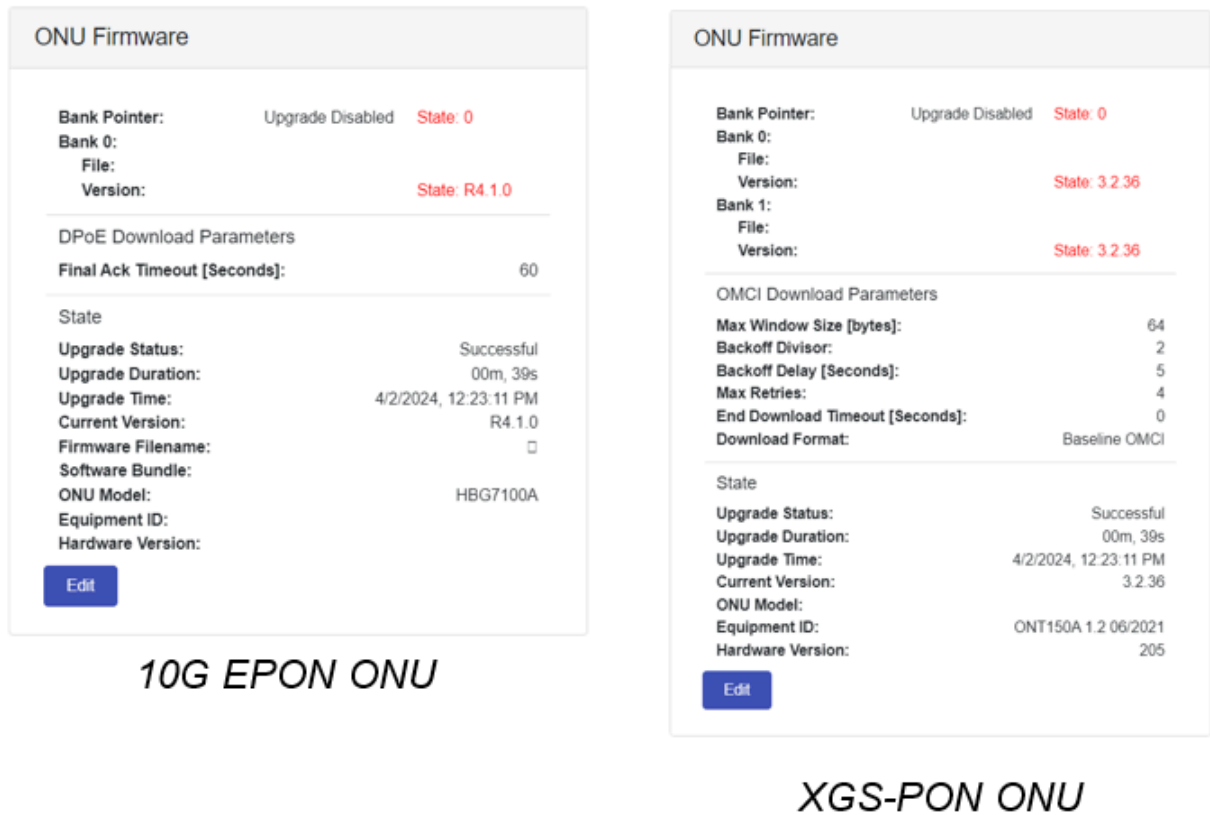
v1.0

Edit

Retry Upgrade

The following figure describes the 10G EPON ONU and the XGS-PON ONU.

Figure 56 10G EPON ONU and the XGS-PON ONU



Provisioned bandwidth summary

The Services Config sub-tab provisioned bandwidth tile provides a quick view of the ONUs and its parent OLT's guaranteed and best effort rates for both upstream and downstream bandwidth based on its configured SLAs.

The guaranteed row is a summation of the priority rows below it. The priority number comes from the configured priorities of each of the ONU's SLAs and are ordered 1-8. For the OLT Bandwidth column, each priority row is a summation of all ONUs on that OLT whose SLA has that priority.

The following figure describes the Provisioned bandwidth summary.

Figure 57 Provisioned bandwidth summary

Provisioned Bandwidth Summary		
Downstream		
SLA	ONU Bandwidth	OLT Bandwidth
Guaranteed:	128 Kbps	384 Kbps
Best Effort:	10 Gbps	30 Gbps
Total:	10 Gbps	30 Gbps
Upstream		
SLA	ONU Bandwidth	OLT Bandwidth
Fixed:	0	0
Guaranteed:	128 Kbps	384 Kbps
Priority 1:	128 Kbps	384 Kbps
Best Effort:	10 Gbps	30 Gbps
Total:	10 Gbps	30 Gbps

ONU services tab

The services tab contains all subscriber service-related configurations that applies to this ONU.

This includes selections of the GPON OMCI or EPON OLT service ports programmed on the ONU, Service level agreements enforced by the OLT, VLAN tag matching and manipulation, DHCP relay agent option 82, and 802.1X authentication configuration.

The services tab contains four tabs:

- Config
- MIB reset
- MIB config
- MIB current

The config tab displays the OLT services tile that includes a table with rows for each OLT service port (0 to 7). Each table tab displays different service port configuration categories.

For XGS-PON ONUs, the OLT service port has two modes, TCONT and XGEM or XGEM Only. In TCONT and XGEM mode, the service port operates as both a TCONT and an associated XGEM. In XGEM only mode, the service port operates as an XGEM port only. In this scenario, it

must reference a service port that is operating as a TCONT. This configuration supports multiple XGEM ports per TCONT.

PON automation services support the following fields:

- On the OLT service ports tab: Enable, Name, SLA
- On the DHCP relay tab: DHCPv4, DHCPv6, Remote Id, Circuit Id, Sub-Options
- On the 802.1x authenticator tab: 802.1x, NAS Identifier, NAS Port ID, User Name Override
- On the VLAN tagging tab: VLAN Tag Fields, Upstream Priority Value, NNI Networks, PON Networks.

The ONU services tile displays information about the service configuration programmed on the ONU. The UNI ports subsection is used to configure and to enable service for specific ports on the ONU. This configuration applies only when the ONU is configured for unmodified or add CTag built-in services. Virtual Ethernet interface ports (VEIPs) and physical ports available on the ONU are listed. Both virtual and physical ports might be present, depending on the type of ONU. In this case, the user is given the option to select between the virtual and physical ports for the service. The fields MIB reset on registration, and process service config once they are available for configuration on GPON devices.

The fields Skip OMCI Stats, Skip OMCI Tables, and SRV-CFG OMCI Stats are available for configuration on both GPON and EPON devices.

Note: SRV-CFG OMCI Stats is disabled when Service Configuration is set to Disabled, Unmodified, or Add C-Tag.

The service configuration, and service value fields are supported by the PON automation service.

The following table describes the settings for the default RS232 port parameters:

Table 27 Default RS232 port parameters

Service	Values
[SRV-CFG Valued][CircuitPack administrative_state]:	0
[SRV-CFG Valued][SshServerOperation server_action]:	1
[SRV-CFG Valued][Serial Port 1 Admin State]:	0
[SRV-CFG Valued][Serial Port 1 Baud Rate]:	0
[SRV-CFG Valued][Serial Port 1 Data Bits]:	0
[SRV-CFG Valued][Serial Port 1 Parity]:	0
[SRV-CFG Valued][Serial Port 1 Stop Bits]:	0
[SRV-CFG Valued][Serial Port 1 Flow Control]:	0
[SRV-CFG Valued][Serial Port 2 Admin State]:	0
[SRV-CFG Valued][Serial Port 2 Baud Rate]:	0

Service	Values
[SRV-CFG Valued][Serial Port 2 Data Bits]:	0
[SRV-CFG Valued][Serial Port 2 Parity]:	0
[SRV-CFG Valued][Serial Port 2 Stop Bits]:	0
[SRV-CFG Valued][Serial Port 2 Flow Control]:	0
[SRV-CFG Valued][Serial Port 3 Admin State]:	0
[SRV-CFG Valued][Serial Port 3 Baud Rate]:	0
[SRV-CFG Valued][Serial Port 3 Data Bits]:	0
[SRV-CFG Valued][Serial Port 3 Parity]:	0
[SRV-CFG Valued][Serial Port 3 Stop Bits]:	0
[SRV-CFG Valued][Serial Port 3 Flow Control]:	0
[SRV-CFG Valued][Serial Port 4 Admin State]:	0
[SRV-CFG Valued][Serial Port 4 Baud Rate]:	0
[SRV-CFG Valued][Serial Port 4 Data Bits]:	0
[SRV-CFG Valued][Serial Port 4 Parity]:	0
[SRV-CFG Valued][Serial Port 4 Stop Bits]:	0
[SRV-CFG Valued][Serial Port 4 Flow Control]:	0
[SRV-CFG Valued][IPv6 Address]:	
[SRV-CFG Valued][Default Router]:	
[SRV-CFG Valued][Primary DNS]:	
[SRV-CFG Valued][Secondary DNS]:	

The provisioned bandwidth summary tile displays the configured guaranteed and best effort rates for both upstream and downstream bandwidth, for both the ONU and its parent OLT. The rates are based on the configured SLAs. The guaranteed row provides a summation of the SLA priority rows below it, numbered 1–8. For the OLT bandwidth column, each priority row is a summation of all ONUs configured with that SLA priority on the associated OLT.

The MIB reset tab applies to GPON ONUs only, and does not have content for 10G EPON ONUs

The MIB config tab displays detailed information about the ONU's service configuration. If the ONU is assigned an SRV-CFG file, this tab displays the configuration using the same expandable tree structure as the MIB reset and MIB current tabs.

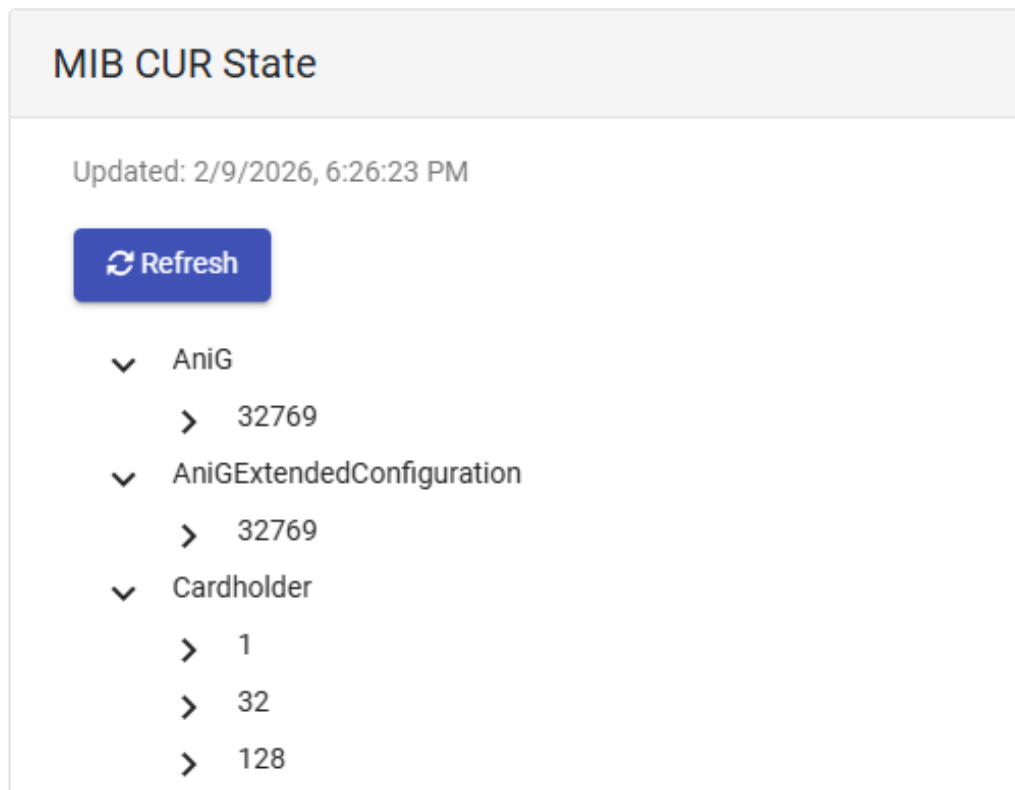
The MIB configuration does not display when the ONU service configuration is disabled or is using the built-in unmodified or add CTag services. The OMCI diagram depicting the data flow path for that service configuration displays under the MIB configuration tree tile.

Note that this sub-tab applies to GPON ONUs only, and does not have content for 10G EPON ONUs.

The MIB current tab displays MIB CUR State information. Click the Refresh button to refresh the information.

The following figure describes the MIB CUR State.

Figure 58 MIB CUR State



ONU ports tab

The ONU ports contains three tabs:

- PON
- UNI
- VOICE

The PON tab lists the values for bidirectional PHY delay and PON mode. It also lists encryption information.

The UNI tab shows a table of configurations for the UNI ports. DPoE Broadcast Rate Limit, ONU MAC Learning, and PHY Type configurations are also supported on 10G EPON ONUs. All

values except for state and ME ID are editable for each UNI port. The state and ME ID columns are hidden in edit mode.

The following figure describes ONU UNI ports.

Figure 59 ONU UNI ports

ONU UNI Ports

Port Number	Enabled	State	ME ID	Speed	Max Frame Size	Duplex	Loopback	PoE
UNI-ETH 1	true	unknown(no link)	257	Auto	2000	Auto	false	false
UNI-ETH 2	true	unknown(no link)	258	Auto	2000	Auto	false	false
UNI-ETH 3	true	unknown(no link)	259	Auto	2000	Auto	false	false
UNI-ETH 4	true	unknown(no link)	260	Auto	2000	Auto	false	false
UNI-ETH 5	true	unknown(no link)	261	Auto	2000	Auto	false	false

Edit

Note: Current values for a field in ONU State are shown in red, if different than configured value.

The VOICE tab appears for XGS-PON ONUs only. It displays two UNI-POTS for the user to configure if needed. This tab also displays state information such as the ME ID, state, and hook state.

The following figure describes the voice ports.

Figure 60 Voice ports

Tab	Value
PON	
UNI	
Voice	

Voice Ports

UNI-POTS 1

Enable:	true
ME ID:	769
State:	disabled
Hook State:	on

UNI-POTS 2

Enable:	true
ME ID:	770
State:	disabled
Hook State:	on

Edit

CPEs on this ONU

This tab displays the CPEs associated with this ONU.

If there are not any CPEs associated with a particular ONU, then the tab reads that there is no information to display.

ONU monitoring

The ONU monitoring contains five tabs:

- stats
- config
- alarms
- logs
- debug

The stats tab presents a view of the statistics related to the ONU's operation. Setting the value of "Use Descriptive Stats" in the PON Controller Monitoring Config page to "True" can categorize the ONU stats with more meaningful names. If not using the built-in service configurations, the service configuration in use with the ONU must have meaningful labels configured within it.

The config tab allows the user to view and edit the ONU's alarm profile.

The alarms tab displays the same table on the main summary tab for viewing the active alarms in detail. Refer to ONU alarms for more information.

The logs tab displays all logs for the ONU within the selected time range. The clear logs button clears all existing logs from the database for this ONU. After clicking the button, the user is prompted to confirm the deletion. If confirmed, all logs for this ONU are deleted. This cannot be undone. Refer to ONU Logs for more information.

The debug tab contains a single tile that allows the user to generate and download a JSON-formatted dump of the ONU debug information. Once it is generated, the download button is enabled. Clicking it downloads a zip folder of all directly-related debug information for that ONU.

Generating the OLT Debug Dump is a separate process. Clicking the generate OLT debug dump button alerts the parent OLT for the selected ONU and gathers its most recent debug information. The most recent timestamp of this dump is found at the bottom of the sub-tab and will be included in the debug generation process.

The following figure describes the OLT Debug options.

Figure 61 OLT Debug

OLT Debug Options

OLT Diagnostic Data:
Generate debug information for this OLT, it's controller and switch/router.

[Generate](#)[Download](#)

[Generate OLT Debug Dump](#)

*Note: Generate OLT Debug Dump is disabled when parent controller is paused/offline.

Last Debug Dump Time: 2024-03-27 17:32:07.202292

Logging Level: CRITICAL

[Edit](#)

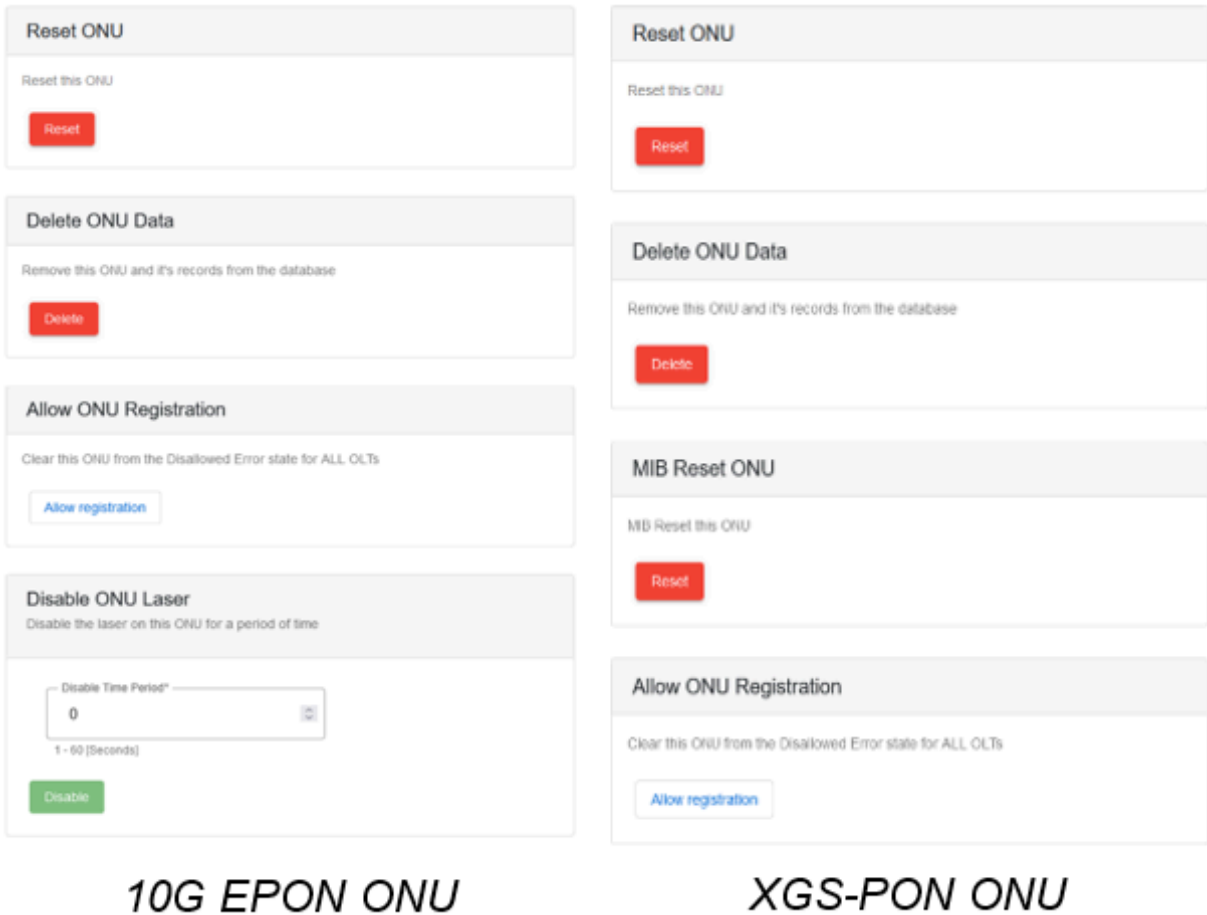
ONU operations tab

The operations tab displays up to five actions that can be performed on an ONU, depending on the PON mode:

- reset ONU
- allow ONU registration
- disable ONU laser on EPON
- restart ONU automation (supported when PON auto is enabled)
- delete ONU

The following figure describes ONU operations

Figure 62 ONU operations



Automation tab

The Automation tab contains a single tile displaying the PON auto status and configuration for this ONU device, and it is organized and functions similarly to the PON Controller automation tab.

The following figure describes ONU PON Automation

Figure 63 ONU PON Automation

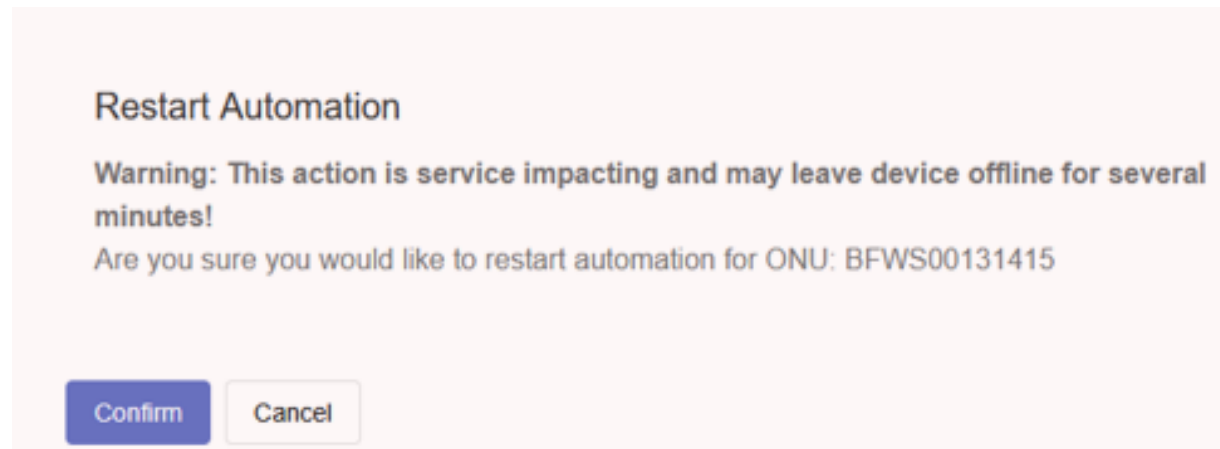
An ONU has several editable tasks for PON Auto: Identify, Disallowed ONU, Firmware, Service, VLAN, SLA, Active, DHCP, Downstream Shape, and Power Variation. The ONU's picture is in the identify task, as well as the firmware bank pointer and banks from the firmware task.

The service task allows the configuration of the PON auto ONU service package, service configuration file, and any values required by the chosen service configuration.

The authentication, VLAN, SLA, and Active sections all contain editable fields to update the RADIUS configuration, OLT and ONU VLAN settings, the SLA, and the DHCP settings of each OLT-Service for PON auto.

Click the Restart automation button to restart the PON Automation workflow back to the START task. A warning pop-up appears and notifies users that restarting automation on devices may leave them offline for several minutes. Click either Confirm to continue to reset automation, or Cancel to return to the PON Automation Screen.

The following figure describes Restart Automation.

Figure 64 Restart Automation

Power Variation is a Rogue ONU task for ONU Automation. If issues occur during Power Variation, the user has the ability to start Fast Recovery or Remediation by clicking the button under Rogue ONU Alarm Status.

List of procedures

Procedures for ONU configuration are:

- [Procedure 34, "Configuring the ONU name"](#)
- [Procedure 35, "Configuring the ONU image"](#)
- [Procedure 36, "Upgrading ONU firmware"](#)
- [Procedure 37, "Disabling an ONU firmware upgrade"](#)
- [Procedure 38, "Resetting bit error rate values"](#)
- [Procedure 39, "Setting the ONU service configuration"](#)
- [Procedure 40, "Resetting the ONU"](#)
- [Procedure 41, "Allowing ONU registration from the ONU"](#)
- [Procedure 42, "Disabling the ONU laser through the ONU"](#)
- [Procedure 43, "Deleting an ONU"](#)
- [Procedure 44, "Resetting the MIB ONU on GPON devices"](#)
- [Procedure 45, "Adding an ONU to an OLT inventory"](#)
- [Procedure 46, "Disabling an ONU serial number through OLT to disable ONU transmit laser"](#)
- [Procedure 47, "Removing the ONU from the inventory"](#)

Procedure 34 Configuring the ONU name

Configure the name for the ONU as required by the network plan.

Overview

The Identification tab contains two tiles. The upper tile displays identifying information about the ONU, such as its name, ID, picture, and more. Several of these items, including the name, are configurable. There are no restrictions on creating the name for the ONU.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired ONU.
- 4 Click the Identification menu.
- 5 Click the Edit button.
- 6 Enter a name for the ONU in the name field.
- 7 Click the Save button.

The new name displays in the Name field and in the navigation panel.

Procedure 35 Configuring the ONU image

Configure the ONU image as required by the network plan.

Overview

The Identification tab contains two tiles. The upper tile displays identifying information about the ONU, such as its name, ID, picture, and more. Several of these items, including the picture, are configurable.

If you try to upload an image and receive the message “The selected file must have a unique name,” the image is already being used with a different Device Type. Create a copy of the image with a different file name. You’ll be instructed to select the corresponding Device Type for this new image in the steps below.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired ONU.
- 4 Click the Identification menu.
- 5 Click the Edit button.
- 6 Click the Picture drop down list under Configuration.
- 7 Select the desired system.
- 8 Click Save.

Procedure 36 Upgrading ONU firmware

Upgrade ONU firmware as required by the network plan.

Overview

The Firmware tab contains two sub-tabs: OLT Firmware for managing the firmware on a given OLT, and ONU Firmware for monitoring the firmware status on subtended ONUs. This procedure is performed on the OLT Firmware sub-tab.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired ONU.
- 4 Click the Firmware menu.
- 5 Click Edit.
- 6 Click the arrow to select the number for the bank that should be active and used in the Bank Pointer State field. If the arrow is grayed out, click the globe icon to the right, then click the arrow.
- 7 Click the arrow in the Bank 0 State Version field to select the required firmware image. If the arrow is grayed out, click the globe icon to the right, then click the arrow.
- 8 Repeat Step 7 for the other bank.
- 9 Click Save.

Procedure 37 Disabling an ONU firmware upgrade

Disable the ONU firmware upgrade as required by the network plan.

Overview

This task is performed from the Firmware tab, accessible from the left navigation pane by selecting Network or Topology, then drilling down through the OLT to the ONU. Note that this action does not cancel a firmware upgrade that is already in progress.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired ONU.
- 4 Click the Firmware menu.
- 5 Click Edit.
- 6 Click the Bank Pointer State drop down arrow and then select Upgrade Disabled.
- 7 Click the arrow under Bank 0 State Version, and then select None.
- 8 Repeat the previous step for each of the other banks.
- 9 Click Save.

Procedure 38 Resetting bit error rate values

Resetting the bit error rate (BER) configures the following count values to 0: ONU Pre-FEC bit error rate, ONU Post-FEC bit error rate, OLT Pre-FEC bit error rate, and the OLT Post-FEC bit error rate. Both Downstream and Upstream connection BER values are reset. Rest the BER values as required by the network plan.

Overview

The following figure describes Bit error rate values.

Figure 65 Bit error rate valued

Downstream Connection		Reset BER
● OLT TX Power (dB):	5.6	
● ONU RX Power (dB):	-24.948	
● ONU Pre-FEC Bit Error Rate:	7.30e-11	
● ONU Post-FEC Bit Error Rate:	0.0	
Upstream Connection		Reset BER
● OLT RX Power (dB):	-26.4	
● ONU TX Power (dB):	5.232	
● OLT Pre-FEC Bit Error Rate:	6.86e-4	
● OLT Post-FEC Bit Error Rate:	0.0	

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired ONU.
- 4 Click the Summary menu.
- 5 Click reset BER under downstream connections or upstream connections.

Procedure 39 Setting the ONU service configuration

Set the ONU service configuration as required by the network plan.

Overview

The following table describes the parameter for setting the ONU service configuration.

Table 28 Parameter for setting the ONU service configuration

Parameter	Valid values	Description
service configuration	Disabled Unmodified Add CTag SRV-CFG file	Select one of the following: • Disabled: Disables service for this ONU. • Unmodified: Configures the ONU with a service that forwards customer traffic applying no VLAN tag modifications. • Add CTag: Configures the ONU to push/pop a C-Tag. If this service is selected, a CVID must be specified. • SRV-CFG file: All other values not listed above are SRV-CFG files stored in MongoDB. Depending on the file selected, additional Service Values may need to be configured.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired ONU.
- 4 Select the Services tab, and then click the Config sub-tab.
- 5 Click the Edit button under ONU Services.
- 6 Configure the ONU Services as desired.
- 7 Click the Save button.

Procedure 40 Resetting the ONU

Reset the ONU as required by the network plan.

Overview

This task is performed from the Operations tab, accessible from the left navigation pane by selecting Network or Topology, then drilling down through the OLT to the ONU.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired ONU.
- 4 Click the Operations menu.
- 5 Click Reset in the Reset ONU pane.
- 6 Click Reset again.

Procedure 41 Allowing ONU registration from the ONU

Allow ONU registration from the ONU as required by the network plan.

Requirements

This task is performed from the Operations tab, accessible from the left navigation pane by selecting Network or Topology, then drilling down through the OLT to the ONU.

Overview

This action clears an ONU from the Disallowed Error state and allows it to register on the PON.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired ONU.
- 4 Click the Operations menu.
- 5 Click Allow registration in the Allow ONU Registration pane.
 - **Note:** If the OLT is in the process of another ONU registration, a message to this effect displays and the Allow registration button is disabled. Wait for the OLT to complete the pending registration operation before attempting the operation for this ONU.

Procedure 42 Disabling the ONU laser through the ONU

Disable the ONU laser through the ONU as required by the network plan.

Requirements

The Disable ONU Laser operation is available for EPON devices only.

Overview

This task is performed from the Operations tab, accessible from the left navigation pane by selecting Network / Topology, then drilling down through the OLT to the ONU.

Steps

- 1 In the **Disable ONU Laser** pane, in the **Disable Time Period** field, enter the time period in seconds as an integer from 1 - 60.
- 2 Click **Disable**.

Procedure 43 Deleting an ONU

Delete an ONU as required by the network plan.

Overview

The Delete action removes all configuration, state, statistics, and logging data for this ONU from the database. It also removes the ONU from any OLT Inventories. This action cannot be undone.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired ONU.
- 4 Click the Operations menu.
- 5 Click delete in the Delete ONU Data pane to remove the ONU from the system.

Procedure 44 Resetting the MIB ONU on GPON devices

Reset the MIB ONU on GPON devices as required by the network plan.

Overview



CAUTION
MIB Reset action.

Once confirmed, this will trigger the ONU to restart.
This process can take several minutes.

Steps

- 1 Select Network on the left navigation pane.
- 2 Select Topology.
- 3 Navigate to the desired ONU.
- 4 Select the Operations menu.
- 5 Go to the MIB Reset ONU.
- 6 Select Reset.
A pop up window appears.
- 7 Confirm the MIB Reset ONU in the pop up window.
The ONU restarts.

Procedure 45 Adding an ONU to an OLT inventory

Add an ONU to an OLT inventory as required by the network plan.

Overview

This task is performed from the ONU Inventory tab, accessible from the left navigation pane by selecting Network or Topology, then drilling down to the OLT supporting the specified ONU.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired ONU.
- 4 Click the ONU Inventory menu.
- 5 Click Edit in the ONU Inventory table.
- 6 Perform one of the following options to add ONUs to the OLT's inventory:
 - To add a single ONU, click the Add button next to the ONU you want to add.
Note: The Add button is displayed only for ONUs that not inventoried.
 - To add all ONUs that are not inventoried, click Add all at the bottom of the window.
- 7 Click the globe icon in the ONU ID column, then change the ID or use the arrows to make a selection to configure an ONU ID.
Note: ONU IDs must be unique for each OLT.
- 8 Click the drop down arrow in the expand menu and make edits as needed to configure the ALLOC IDs or LLIDs, .
Note: ALLOC IDs and LLIDs must be unique for each OLT.
- 9 Click Save.

A green check mark replaces the red x in the Inventoried column for the ONU.

Procedure 46 Disabling an ONU serial number through OLT to disable ONU transmit laser

Disable an ONU serial number from the OLT inventory in order to disable the ONU's transmit laser as required by the network plan.

Overview

This task is performed from the ONU Inventory tab, accessible from the left navigation pane by selecting Network or Topology, then drilling down to the OLT supporting the specified ONU. The following figure describes a disabled serial number.

Figure 66 Disabled Serial Number

The screenshot displays the ONU Inventory interface. At the top, there are tabs: Active, Inventoried, Serial Number ↑, ONU Name, ONU State, ONU ID, ALLOC IDs, Disable Serial Number, and Expand. Below these tabs, a table lists ONU details. The first row shows a green checkmark, a green checkmark, a red 'Remove' button, the serial number 'ARCN139b1c3e', the state 'Registered', an 'ONU ID' dropdown set to '4' (with a range of '1 - 128'), the value '1530', a toggle switch for 'Disable Serial Number' (which is currently off and highlighted with a red box), and an expand icon. Below the table, the 'ALLOC IDs' section is visible. It includes a 'Service Port Count*' dropdown set to '1'. To the right of this are two buttons: 'Sync automatically assigned' and 'Assign next free block', both highlighted with red boxes. Below these are eight 'OLT-Service' dropdowns, labeled 'OLT-Service 0' through 'OLT-Service 7'. 'OLT-Service 0' is set to '1530' and has a green '(enabled)' status. Below it, the text '(Inventoried, Not Active)' is displayed. The other OLT-Service dropdowns are empty. At the bottom, the range '1154 - 1534 (excluding 1279)' is shown.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired ONU.
- 4 Click the ONU Inventory menu.
- 5 Click Edit.
- 6 Locate the desired ONU on the list.
- 7 Click the toggle button under disable serial number so that it moves to the right.

The toggle button changes from gray to pink.

- 8** Click Save.

Procedure 47 Removing the ONU from the inventory

Remove the ONU from the inventory as required.

Requirements

Before provisioning the service configuration for an ONU, it must not be inventoried. Inventorying the ONU means that an AllocID will be pre-assigned to it, which can potentially cause out-of-sync issues when the ONU is provisioned for service later.

Steps

- 1 Navigate to **Network > select OLT > ONU Inventory**
- 2 Any ONUs that are inventoried will have a check under the Inventoried column and have an ONU State of **Registered**.
- 3 Click on the **Edit** button to inventory the ONUs
- 4 Click on **Remove** button for each ONU to be removed from the inventory
- 5 Click on the **Save** button and wait for the ONU removal process to complete

CHAPTER 11

OLT configuration

OLT tabs are used to configure and monitor OLTs in the PON network.

OLT summary tab

The OLT summary tab contains three tiles with information about the OLT. The first tile displays OLT and ONU automation information as well as the PON protection and the summary information. The second tile displays provisioned bandwidth summary information. The third tile displays a list of raised and unacknowledged alarms.

The following figure describes the OLT Summary tab.

Figure 67 OLT Summary tab

OLT Summary
MAC: e8:b4:70:70:27:28

OLT PON Automation

Status: DONE

ONU PON Automation on this OLT

PON Protection

PON Protection Status:	Disabled
Automatic Switchover Status:	Disarmed
OLT Protection Partner:	-

Alarms

Emergency:	0
Alert:	0
Critical:	0
Error:	0
Warning:	0
Notice:	0
Info:	0
Debug:	0

Summary

Status:	Online
Last Status Update:	3/22/2022, 12:40:27 PM
Online Duration:	14d, 19h, 50m
Since:	3/7/2022, 3:50:37 PM
Uptime:	3d, 21h, 34m, 37s
Configuration Status:	Valid
Version:	R3.0.0-rc28
ONU Count (online / total):	1 / 1

☐ *Auto Boot Mode: OFF

*Note: This feature is not supported and should be disabled. Autoboot Mode cannot be re-enabled after disabling it.

Several details about the OLT are found on the first tile. The online duration field (located in the summary subsection) shows the duration of time that this OLT has been online. When the OLT

is offline, the summary tab displays both offline duration and last online duration. The offline duration shows how long the OLT has been offline. Last online duration displays the length of time the OLT was previously online before it went offline.

At the top of the main summary tile are indicators for PON auto status and PON protection status. Beneath the OLT PON automation subsection, the automation summary displays for all ONUs connected to this OLT. The ONU PON auto summary lists tasks with a floating count. The count indicates the number of ONUs in that task that are managed by this OLT. Each task is a clickable button that displays a table of the ONUs.

If PON automation is inactive or not used, text displays stating that the PON auto service is unavailable.

The provisioned bandwidth summary tile displays the OLT's configured guaranteed and best effort rates for both upstream and downstream bandwidth. The rates are based on the SLAs for each of the OLT's associated ONUs. The guaranteed row provides a summation of the SLA priority rows that follow it, numbered 1–8. Each priority row is a summation of all the ONUs configured with that SLA priority on the associated OLT.

The following figure describes the provisioned bandwidth summary tile.

Figure 68 Provisioned Bandwidth Summary

Provisioned Bandwidth Summary

Downstream

SLA	Bandwidth
Guaranteed:	128 Kbps
Best Effort:	10 Gbps
Total:	10 Gbps

Upstream

SLA	Bandwidth
Fixed:	0
Guaranteed:	128 Kbps
Priority 1:	128 Kbps
Best Effort:	10 Gbps
Total:	10 Gbps

OLT identification tab

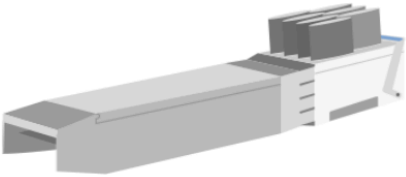
The OLT identification tab lists the hardware and firmware details. Configurable values include the name, picture, tags, and switch description. The picture field is supported by the PON automation service. The following figure describes the OLT Identification tab.

Figure 69 OLT Identification tab

10GE

OLT Name

MAC:e0:9b:27:7e:8e:28



Labels:

Vendor:

CIENA-BIT

Model:

XCVR-SGPL04

HW Rev:

001

Serial Number:

OLT-E09B277E8E28

FW Version:

R6.2.0-rc23

Production Code:

M3.4.1

Manufacturing Serial Number:

M2052418573

ASIC:

180713

Parent Controller:

bc:24:11:52:16:e9

PON Controller Version:

R6.2.0-rc26

DB Config Version:

R6.2.0-rc5

Create Date:

2025-10-10 10:21:59.231742

Picture:

Location Coordinates:

Address:

NETCONF Name:

e0:9b:27:7e:8e:28

Tag:

Allowed Switch/Router Ports:

ANY

Switch/Router Description

Chassis ID:

ac:89:d2:c7:60:20

System Name:

sw-5160-12-l6

Port ID:

1

IPv4 Address:

10.1.180.57

IPv6 Address:

2620:11b:d03f:f0b5:ae89:d2ff:fec7:6020

System Description:

Ciena 5160 Service Aggregation Switch

Port Description:

Edit

OLT firmware tab

The OLT firmware sub-tab shows configured settings and versions. It displays the current version and active versions in each bank.

Any available firmware version can be selected. Firmware bank pointer and image selections are supported by the PON automation service.

The following figure describes the OLT Firmware tab.

Figure 70 OLT Firmware tab

The screenshot shows the 'OLT Firmware' configuration interface. It displays the current version as R6.0.0 and the bank pointer as 3. Below this, it lists the firmware details for four banks (Bank 0 to Bank 3). Each bank entry includes the file name and the version number. An 'Edit' button is located at the bottom left of the configuration area.

OLT Firmware	
Current Version:	R6.0.0
Bank Pointer:	3
Bank 0:	
File:	R5.1.0-OLT-FW.bin
Version:	R5.1.0
Bank 1:	
File:	R5.2.0-OLT-FW.bin
Version:	R5.2.0
Bank 2:	
File:	R6.0.0-OLT-FW.bin
Version:	R6.0.0
Bank 3:	
File:	R6.0.0-OLT-FW.bin
Version:	R6.0.0
Edit	

OLT services tab

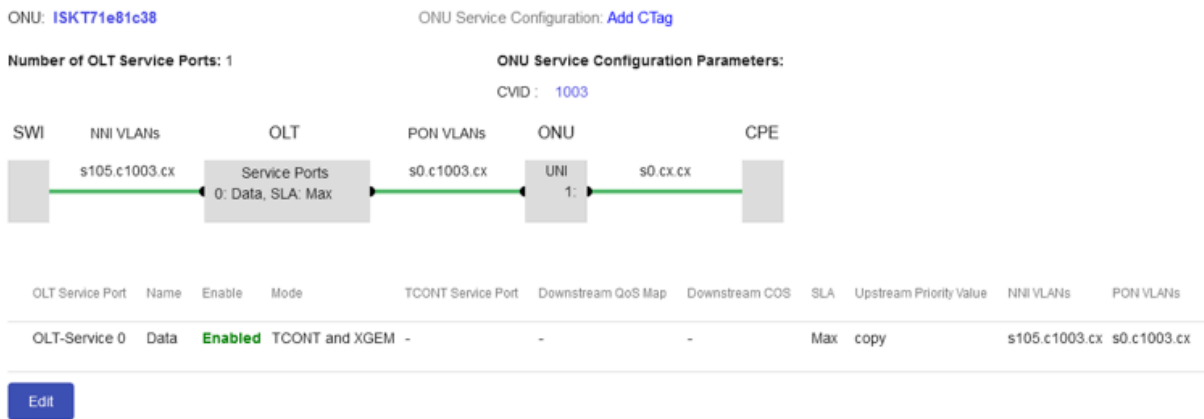
The services tab provides a summary of configured services on the OLT. It displays attached ONUs with dropdown panels.

Up to eight OLT services (0 to 7) can be configured per ONU, with up to 16 VLANs per service. Deletion of services and VLAN configurations can also be done on this tab.

The following figure describes OLT Services

Figure 71 OLT Services

A maximum of eight OLT Services (0..7) can be configured per ONU and up to 16 VLANs can be configured per service. Deleting an OLT Service or VLAN configuration can also be performed on this tab.

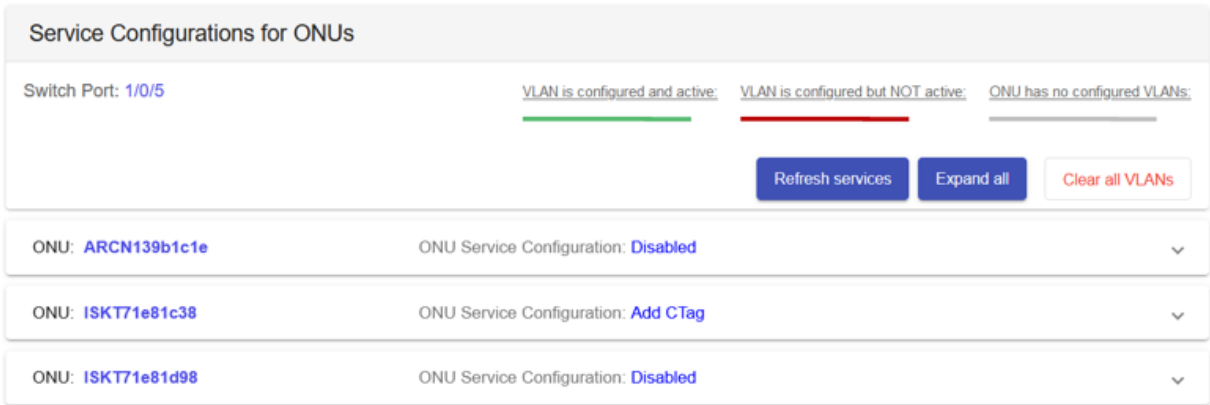


Expanded ONU panels show detailed service configurations, including a visual diagram. The diagram represents the OLT services with a switch, OLT, ONU, and CPE block. The switch block represents the connected switch or router. The OLT block displays service port number, name, and SLA configuration. The ONU block shows the corresponding UNI port number. The CPE block and the UNI VLANs adapt based on the configuration and the downstream QoS map. Green lines indicate matching config and state values, while red lines indicate mismatches.

PON automation supports ONU service configuration, parameters, name, enable, SLA, and VLANs fields.

The following figure describes the service configurations for ONUs.

Figure 72 Service Configurations for ONUs



OLT services

This section provides an overview of the edit mode for OLT services. Use OLT services to make and save changes to the OLT services configuration.

The following figure describes OLT services

Figure 73 OLT services

A maximum of eight OLT Services (0..7) can be configured per ONU and up to 16 VLANs can be configured per service. Deleting an OLT Service or VLAN configuration can also be performed on this tab.

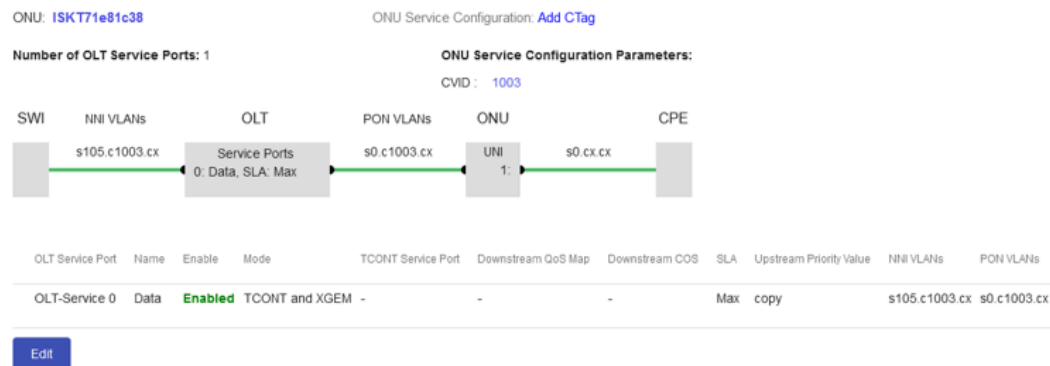


Table 29 OLT Services

Label	Description
1	ONU service configuration
2	Configure OLT service ports
3	SLA and CoS
4	Add OLT service ports
5	Remove OLT service ports
6	Add VLAN Tags
7	Remove VLAN Tags

ONU service configuration: Select a built-in service (Disabled, Add CTag, Unmodified) or a specific SRV-CFG file from the dropdown. Depending on the service, the user may then also edit the service values. Requirements for these inputs depend on the service configuration file selected.

Configure OLT service ports: Set the name, enable, mode and TCONT service port reference. An OLT service port with the mode set to XGEM only will require a TCONT service port reference. The TCONT service port reference must be an OLT service on the same ONU with the mode set to TCONT and XGEM.

SLA and CoS: Set SLA by selecting it from the dropdown.

Add OLT service ports: Add an OLT service to an ONU by clicking the Add Service button.

Remove OLT service ports: Click the red trash can icon to remove an OLT service from an ONU. This option is not available for the first service of a 10G EPON ONU as the primary link cannot be deleted.

Add VLAN Tags: Click filling in a blank row to add a VLAN. Enter X to match any, 0 for untagged/priority tagged or the VLAN ID values 1 - 4095.

Remove VLAN Tags: Click the red circular button to remove a VLAN.

Source MAC Verify

Source MAC verify is a security function implemented by the PON Controller to validate the legitimacy upstream CPE traffic received by the OLT.

When enabled, only CPE devices that have successfully completed 802.1X authentication or successfully acquired an IP address from an authorized DHCP server are permitted to forward traffic through the OLT.

The source MAC verify feature has a configurable limit to restrict the number of CPEs learned and allowed to forward traffic.

OLT ports tab

The OLT Ports tab has two sub-tabs: PON and NNI.

The PON sub-tab displays the OLT PON port configuration. The fields listed on this sub-tab depend on the OLT PON Mode setting. If the PON Mode is XGS-PON, XGS-PON configuration settings and state information are shown. If the PON Mode is 10G EPON, configuration and state specifics to 10G EPON display.

The following figure describes the OLT Ports tab

Figure 74 OLT Ports tab

PON

PON Mode:	XGS-PON
Supported PON Speeds:	10Gbps/10Gbps
PON Enable:	true
Discovery Period [ms]:	3000
Encryption:	Bidirectional
Encryption Key Time [s]:	600
Laser Shutdown:	Laser ON
Loss of Signal:	false
Max Frame Size [bytes]:	9600
Downstream FEC:	true
Guard Time [12.8ns]:	64
Error Det Max Ratio:	20%
Error Det Min Sample [bursts]:	100
Error Det Max HEC Ratio:	20%
Error Det Min HEC Sample [headers]:	100
PON ID:	1886397886 (Auto)
PON-TAG:	11071b17747474ff (Auto)
Fiber Reach:	Standard (0..20 km)
Shared Downstream Policer:	true
TOD Reference Clock:	PON Controller System

Upstream Burst Profile

Preamble Length [16 bytes]:	64
Preamble Pattern:	946102fc66ed2717 (Auto)
Upstream Delimiter:	4b63e1acaf916360 (Auto)
Upstream FEC:	true

Edit

When configuring a pre-provisioned OLT without state data, the interface will show the PON mode based on the global PON mode setting, rather than the OLT's state. If an OLT with state data is configured, it will not switch from the global PON mode to another mode. An indicator will display if the OLT is in the incorrect PON mode according to the global setting.

The NNI sub-tab contains the OLT's management VLAN, management TPID, and configuration for the NNI max frame size, LLDP transmit and receive toggles. The MAC address is the NNI port MAC address, which is equivalent to the ID of the OLT.

The following figure describes the NNI tab.

Figure 75 NNI tab

NNI	
Management TPID:	S-Tag (0x88A8)
Management VLAN:	4090
Supported Speeds:	10Gbps
Max Frame Size [bytes]:	9600
LLDP Transmit:	false
LLDP Receive:	true
DOCSIS Provisioning Gateway	
vCM TPID:	Disabled

Edit

OLT NNI networks tab

The NNI networks tab is used to configure and manage NNI VLANs, bridging, and networking for the OLT device. It comprises of two panes: MAC learning and NNI networks.

On the MAC learning pane, age limit, allow CPEs to move, and campus mode are all configurable.

On the NNI networks pane, network VLAN, learning limit, inventoried, PON flood type, etc are all configurable.

OLT config tab

The config tab is used to configure and manage OLT NNI networking, including MAC learning controls and NNI network inventory. The MAC learning controls configure the aging time for CPE MAC addresses and allow a CPE to move between ONUs.

The following figure describes the MAC Learning Configuration tab.

Figure 76 MAC Learning Configuration tab

MAC Learning

Age Limit [Seconds]: 3600

Allow CPEs To Move: false

Campus Mode: false

[Edit](#)

The NNI network inventory pane is used to configure VLANs and networks for Layer 2 switch domains (L2SD) on the OLT. Existing NNI networks may be added to the OLT's inventory and new networks may be created.

The following figure describes NNI Networks

Figure 77 NNI Networks

NNI Networks

Filter

Active	Inventoried	Network VLAN	Learning Limit	Learning Table	PON Flood Type	PON Flood ID	Downstream Flooding SLA	DHCPv6 Filter	DHCPv4 Filter	PPPoE Filter	EAPoL Filter
✓	✓	Remove s0.c0.c0	2046 0 - 2046 (Addresses)	✗	Auto	State: 2045	Max	host	host	pass	pass
✓	✓	Remove s0.c200.c0	2046 0 - 2046 (Addresses)	✗	Private	0	None	host	host	pass	pass
✓	✓	Remove s0.c1000.c0	2046 0 - 2046 (Addresses)	✗	Auto	State: 2046	None	host	host	pass	pass
✓	✓	Remove s0.c2000.c503	2046 0 - 2046 (Addresses)	✗	Auto	State: 1158	None	pass	host	host	pass
✗	✓	Remove s2.c111.c0	2046 0 - 2046 (Addresses)	✗	Auto		None	drop	host	drop	pass

Items per page: 10 1 - 5 of 5 < > >>

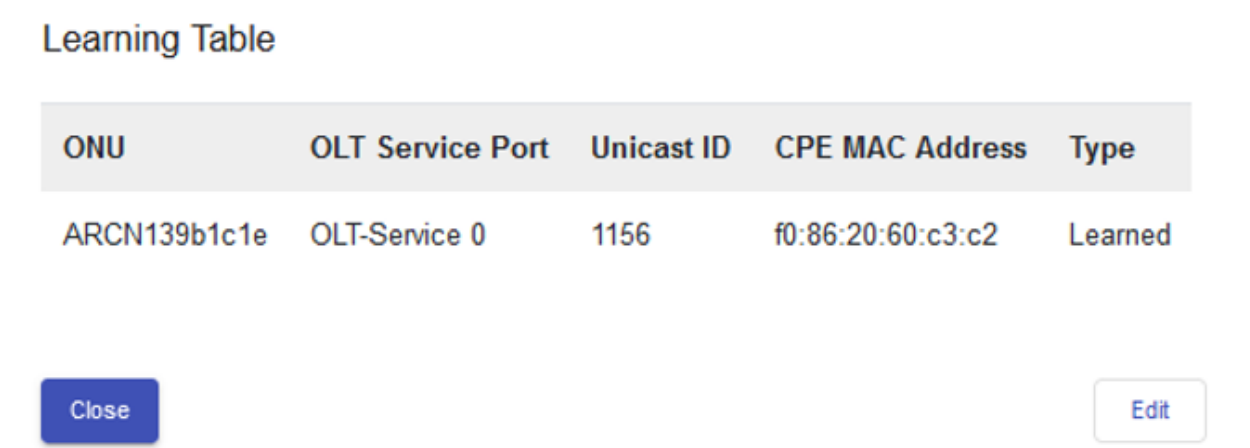
[Add new](#)
[Inventory all networks](#)

[Save](#)
[Cancel](#)

The learning table icon displays dynamically learned and statically configured CPE MAC addresses for the selected NNI network.

The following figure describes the Learning Table.

Figure 78 Learning Table



Note: The PON Manager does not support configuring EAPOL for NNI networks.

PON flood type

The PON flood type and ID are used to configure the destination for downstream broadcast, multicast, and unlearned frames which do not have a dynamically learned or static MAC address table entry.

This configuration determines the type of destination to forward flooding traffic. There are 4 PON flood type options: private, shared, auto, and all ONUs. The 'All ONUs' option is available only for EPON ONUs. Changing the PON flood type will affect the accepted range of values for PON flood IDs. Selecting private will set the downstream flooding SLA field to none. Selecting auto disables the configuration of the PON flood ID field.

The ranges of the PON flood IDs and meaning of the PON flood type depend on the type of PON used: EPON or GPON. The ranges and descriptions for each type are described in the table below.

Table 30 EPON Flooding

Type	Range	Description
Private	0	Specifies the LLID of the link which uses the network is used.
Shared	1919 to 2046	Specifies the number of frames that are flooded to one

Type	Range	Description
		or more ONUs on the specified multicast LLID.
Auto	-	The PON flooding ID is automatically set by the PON Controller to a unicast or multicast LLID depending on the number of ONUs attached to the NNI Network.
All ONUs	32766	Frames are flooded to all ONUs on the broadcast LLID defined by EPON.

Table 31 GPON Flooding

Type	Range	Description
Private	0	Private specifies the Alloc ID/ XGEM port of the link which uses the network is used.
Shared	1917 to 2046	Frames are flooded to one or more ONUs on the specified multicast (downstream only) XGem Port ID.
Auto	-	The PON flooding ID is automatically set by the PON Controller to a unicast or multicast XGem Port ID depending on the number of ONUs attached to the NNI network.

CPE tab

The CPEs tab displays a table showing all NNI networks on the OLT.

CPE MAC addresses are displayed with their associated service which maps to their Unicast ID (GPON: ALLOC ID/Gem Port ID, EPON: LLID), VLAN tags, ONU, OLT-Service and the type, being either learned or static. The DHCP state information is displayed in parentheses next to the IP addresses.

The following figure describes CPEs.

Figure 79 CPEs

OLT CPEs						
Filter						
ONU + OLT Service	Unicast ID	NBI Network	CPE MAC Address	IPv4 Address	IPv6 Address	Type
BFWS00118872, OLT-Service 0	1158	s0.c2000.c503	00:10:94:00:01:6b	-	-	Learned
BFWS00118872, OLT-Service 0	1158	s0.c2000.c503	00:10:94:00:01:6c	-	-	Learned
BFWS00118872, OLT-Service 0	1158	s0.c2000.c503	00:10:94:00:01:6f	-	-	Learned
BFWS00118872, OLT-Service 0	1158	s0.c2000.c503	00:10:94:00:01:70	-	-	Learned
BFWS00118872, OLT-Service 0	1158	s0.c2000.c503	00:10:94:00:01:71	-	-	Learned
BFWS00118872, OLT-Service 0	1158	s0.c2000.c503	00:10:94:00:01:72	-	-	Learned
BFWS00118872, OLT-Service 0	1158	s0.c2000.c503	00:10:94:00:01:73	-	-	Learned
BFWS00118872, OLT-Service 0	1158	s0.c2000.c503	00:10:94:00:01:74	-	-	Learned
BFWS00131375, OLT-Service 0	1154	s0.c1000.c0	2c:d1:41:88:bf:d	10.1.22.36 (ACK)	2100::100:100:9f (Bound)	Learned
BFWS00131388, OLT-Service 0	1155	s0.c1000.c0	2c:d1:41:88:bf:17	10.1.22.239 (ACK)	2100::100:100:86 (Solicit)	Learned
				Items per page: 10	1 - 10 of 13	< >

ONU inventory for OLT

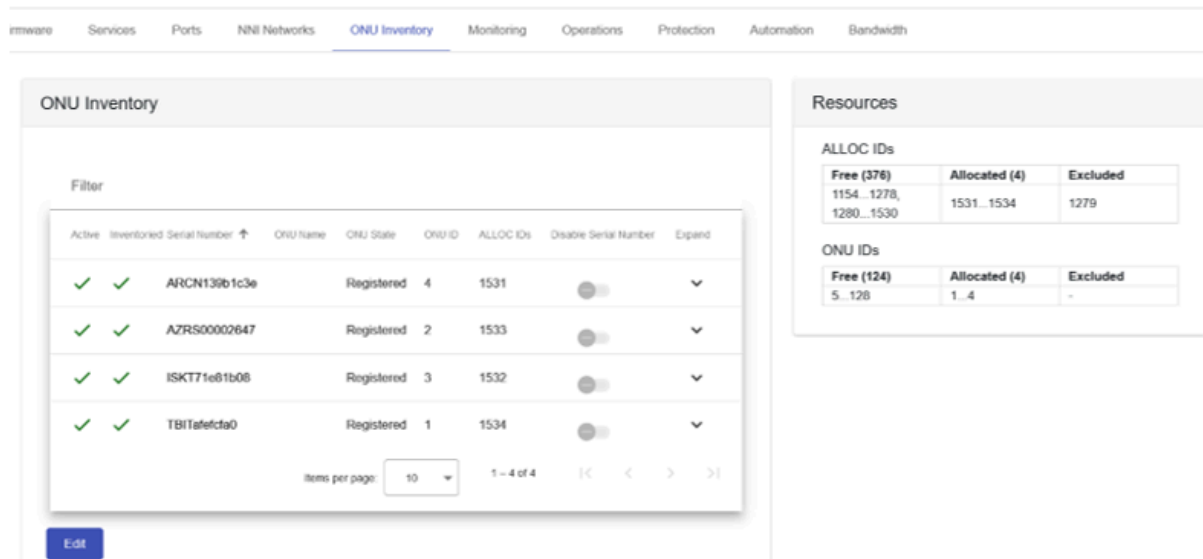
The ONU inventory tab allows for the viewing and configuration of the OLT's inventory of ONUs. The inventory allows the OLT to quickly re-add and reconfigure attached ONUs upon restart.

Note: Ciena recommends that all ONUs be inventoried on the OLT they are connected to. This is required for fast restart and to avoid transmit collisions from faulty ONUs using obsolete configurations after the system is rebooted.

If an ONU has more configuration information than can be displayed in the table, a chevron displays in the Expand column on the far right for displaying the additional information.

The ONU ID field is supported by the PON automation service. Refer to the PON automation documentation for more information on managing configuration for these fields.

The following figure describes the ONU Inventory,

Figure 80 ONU Inventory

The Resources card shows a summary of ALLOC IDs and ONU IDs that are free to use, already allocated, or excluded for the OLT. The resources vary depending on the type of OLT.

The following table displays ALLOC IDs for GPON and EPON.

Table 32 ALLOC IDs for GPON and EPON

PON	Available ALLOC IDs	Excluded ALLOC IDs
GPON	1154-1534	1279
EPON	5121-6013	5375, 5631, 5887

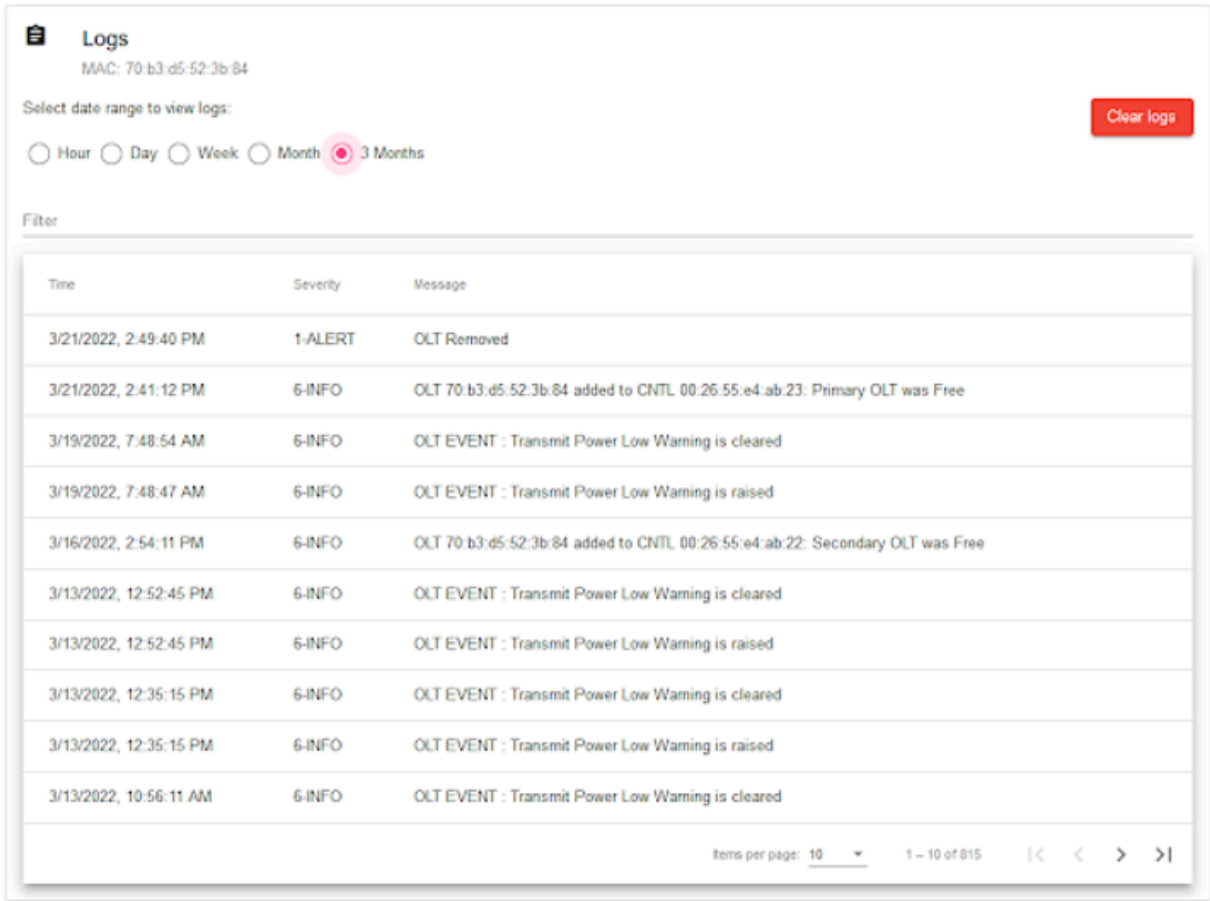
OLT monitoring tab

The OLT monitoring contains five sub-tabs:

- The stats sub-tab displays the statistics generated from the OLT's operation.
- The config sub-tab allows the user to view and edit the OLT's alarm profile and to enable real-time stats.
- The alarms sub-tab displays the same table seen on the summary tab for viewing the active alarms in detail.
- The logs sub-tab lists all log messages for the OLT that exist within a specified time range.

The following figure describes the Logs,

Figure 81 Logs



- The debug tab provides an option to configure the OLT Debug Logging Level, and generate and download a JSON formatted dump of the OLT debug information. The following figure describes the Debug configuration,

Figure 82 Debug configuration

Debug Configuration

ONU Diagnostic Data:

Generate debug information for this ONU, it's OLT, controller and switch/router.

GenerateDownload

Generate OLT Debug Dump

*Note: Generate OLT Debug Dump is disabled when parent controller is paused/offline.

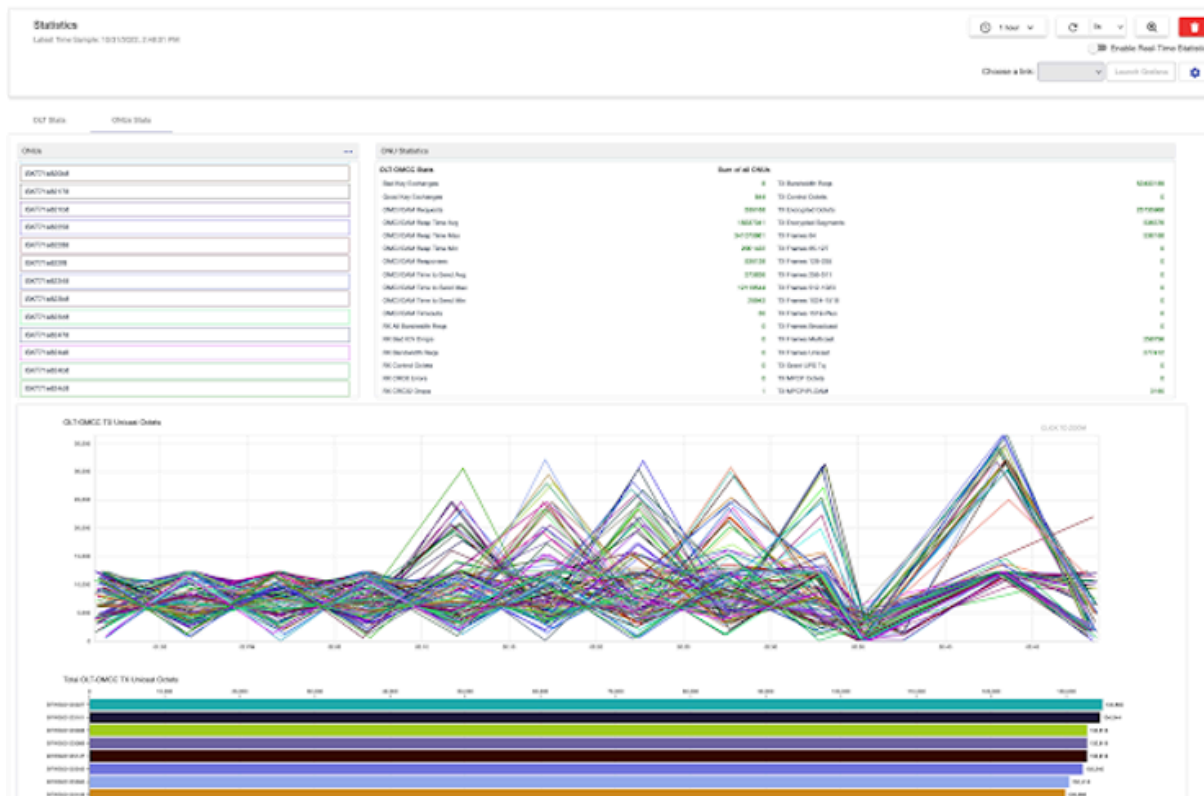
Last Debug Dump Time: 2024-04-05 21:10:13.812118

ONUs stats tab

The ONUs stats sub-tab, located on the OLT stats tab, displays statistics for all of the managed ONUs for the OLT. Line graphs and bar charts can be displayed at the bottom of the window by selecting a time frame in the Statistics pane, one or more ONUs in the ONUs pane, and one or more statistics from the ONU statistics pane.

When multiple ONUs are selected, each ONU is highlighted by a unique line color in the ONUs pane and the line and bar charts. Hovering over the line graph displays more information about the datapoint closest to the cursor. Zooming and panning across the graph is enabled by clicking and dragging on the graph and using the mouse wheel.

The following figure describes ONU Statistics.

Figure 83 ONU Statistics

OLT operations tab

There are several operations that can be performed on an OLT from this tab:

- Reset OLT
- Delete OLT Data
- Allow ONU Registration
- Enable ONU Serial Number

The following figure describes OLT Operations.

Figure 84 OLT Operations

Reset OLT

Reset this OLT

Reset

Delete OLT Data

Remove this OLT and it's records from the database

Delete

Allow ONU Registration

Clear an ONU(s) from the Disallowed Error state

Reg Allow ONU *

ALL

Allow ONUs

Enable ONU Serial Number

Send Enable Serial Number command to an inventoried ONU(s)

ONU Serial Number *

ALL

Enable ONUs

Enter an ONU Serial Number to enable a specific ONU or 'ALL' to send a broadcast enable message

OLT protection tab

The protection tab contains two panes: OLT protection and managed switchover.

The OLT protection pane offers the following configuration options:

- The OLT protection partner
- NNI RX LOS pulse settings
- ONU fault limit

The protection pane offers the following state information:

- Active OLT
- Standby OLT
- Automatic switchover status
- Last switchover time
- Last switchover type

Arm the PON protection auto detector or force an OLT switchover on the managed switchover pane.

OLT automation tab

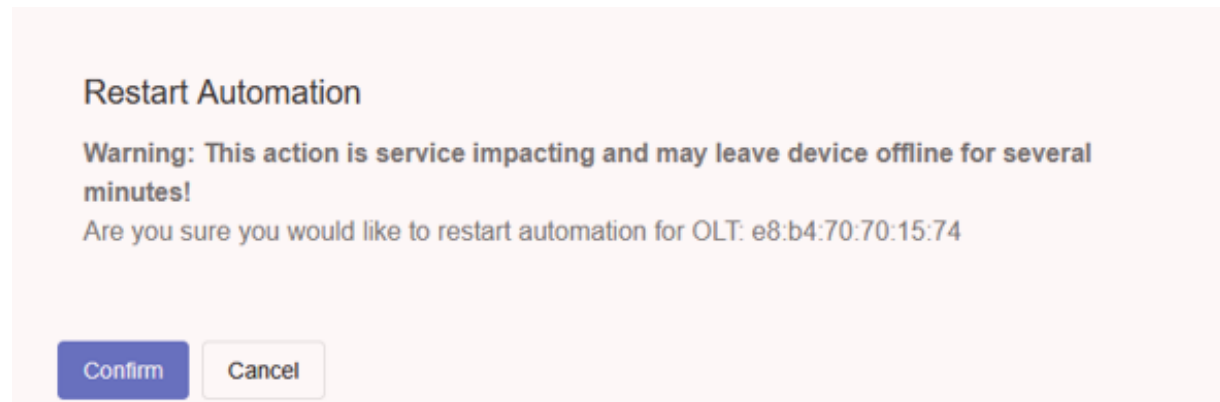
The automation tab contains a single tile displaying the PonAuto status and configuration for this OLT device. It is organized and functions similarly to the PON Controller automation tab.

See the PON Controller automation section for a detailed description of the tab organization, operation, and behavior for the UI elements on this tab.

An OLT has three manageable tasks: identify, firmware, and add ONU. Override an OLT's image from the ID task. Override the PON auto firmware banks and bank pointer through the firmware task. Configure the PON Auto settings for assigning the OLT's ONU inventory through the add ONU task. Click add ONU to add a new ONU the inventory. Click the delete overrides button to clear all overrides on the OLT.

If PON Automation is active on the current database, the button to restart PON auto is enabled. Click restart automation to update the device's automation configuration. When attempting to restart automation, a warning pop-up appears to notify users that restarting automation on devices may leave the device offline for several minutes. Either Confirm to continue and reset automation, or Cancel to return to the Pon Automation Screen.

The following figure describes the Restart Automation dialogue.

Figure 85 Restart Automation

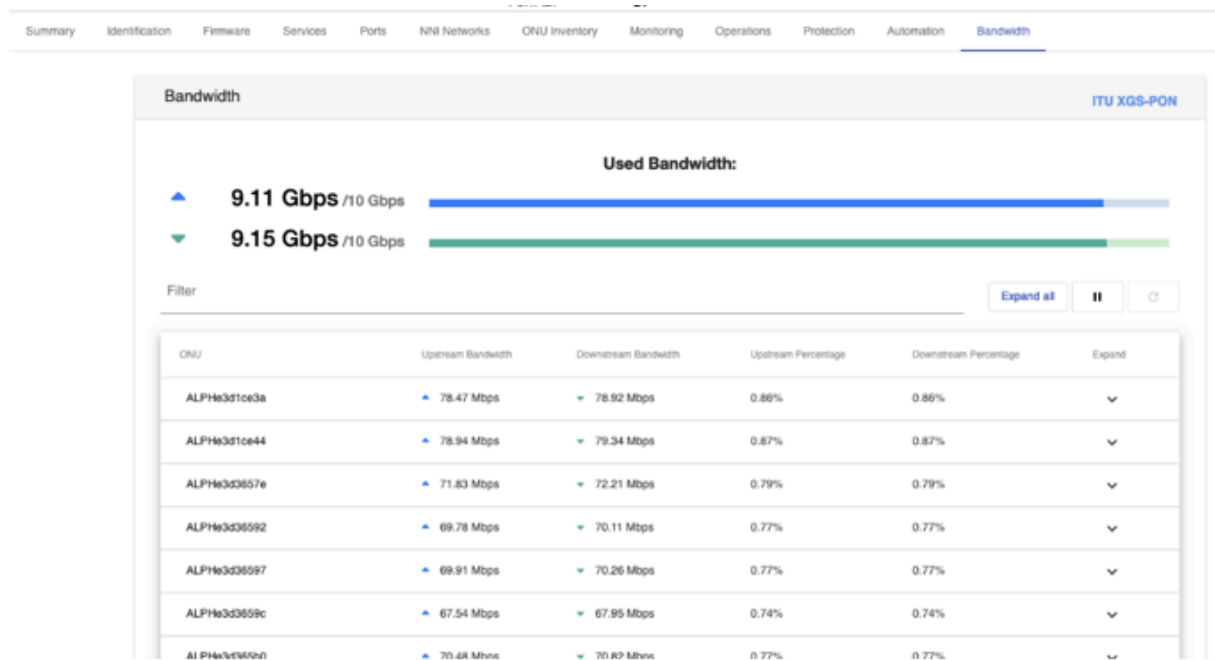
OLT Bandwidth tab

OLT Bandwidth tab is used to display PON aggregate upstream and downstream bandwidth utilization.

PON bandwidth utilization is displayed graphically using bar graphs and with numerical values in bits-per-second units. It displays overall bandwidth utilization summary for the whole PON network, the total available and currently used upstream and downstream bandwidth. Bandwidth utilization for each ONU is displayed in a table underneath the PON bandwidth summary.

The following figure describes the OLT bandwidth tab.

Figure 86 OLT bandwidth tab



- Bandwidth tab displays the following features:
- Displays PON aggregate bandwidth for both upstream and downstream.
 - Displays all ONUs for OLT with the following information:
 - upstream bandwidth
 - downstream bandwidth
 - upstream percentage for total allowed bandwidth on OLT
 - downstream percentage for total allowed bandwidth on OLT
 - an expand option to display upstream and downstream bandwidth per service
 - Expand and collapse all button for showing services for all ONUs.
 - Pause and play for stopping the automatic updates on the page.
 - Refresh button for showing the latest data when the page is paused.

List of procedures

- Procedures for OLT configuration are:
- Procedure 48, “Configuring an OLT protection partner”
 - Procedure 49, “Enabling automatic switchover for OLT active and standby”
 - Procedure 50, “Enabling automatic switchover with OLT toggle”
 - Procedure 51, “Disabling automatic switchover for OLT active and standby”
 - Procedure 52, “Forcing a switchover from active OLT to standby OLT”
 - Procedure 53, “Enabling OLT service ports on the ONU”
 - Procedure 54, “Enabling OLT service ports”

- Procedure 55, “Configuring the downstream QoS map on the ONU”
- Procedure 56, “Configuring an SLA for an OLT service on the ONU”
- Procedure 57, “Configuring VLAN tagging for an OLT service on an ONU”
- Procedure 58, “Configuring VLAN priority”
- Procedure 59, “Adding a VLAN tag”
- Procedure 60, “Removing a VLAN tag”
- Procedure 61, “Enabling DHCP relay”
- Procedure 62, “Adding an OLT to the switch inventory”
- Procedure 63, “Deleting switch or router data”
- Procedure 47, “Removing the ONU from the inventory”
- Procedure 65, “Synchronizing automatic assigned in the inventory”
- Procedure 66, “Assigning next free block of consecutive ALLOC IDs to a specified number of OLT service ports”
- Procedure 67, “Adding an OLT to an inventory”
- Procedure 68, “Removing an OLT from an inventory”
- Procedure 69, “Upgrading OLT firmware”
- Procedure 70, “Disabling OLT firmware upgrade”
- Procedure 71, “Adding an NNI network to an OLT”
- Procedure 72, “Adding a new NNI network to the inventory”
- Procedure 73, “Removing an NNI network from the inventory”
- Procedure 74, “Adding static MAC addresses to the network VLAN”
- Procedure 75, “Enabling source MAC verify”
- Procedure 76, “Disabling source MAC verify”
- Procedure 77, “Enabling PPPoE on NNI networks”
- Procedure 78, “Resetting the OLT”
- Procedure 79, “Deleting OLT data”
- Procedure 80, “Allowing ONU registration on the OLT”
- Procedure 81, “Enabling the ONU serial number to enable transmit laser”
- Procedure 82, “Configuring the OLT image”
- Procedure 83, “Configuring the OLT name”

Procedure 48 Configuring an OLT protection partner

Configure an OLT protection partner as required by the network plan.

Overview

PON protection is managed as a group of two OLTs providing redundancy. Type-B Protection utilizes an optical splitter between two OLTs and N ONUs. To utilize PON Protection, all ONUs must be inventoried on the OLT. Both OLTs must be managed and inventoried as primary by the same PON Controller. PON protection is supported for XGS-PON only. The following figure describes OLT Protection

Figure 87 OLT Protection

OLT Protection

Configuration

OLT Protection Partner:

e8:b4:70:70:15:76

NNI RX LOS Pulse [ms]:

1000

ONU Fail Limit:

8

State

Active OLT:

e8:b4:70:70:15:76

Standby OLT:

e8:b4:70:70:15:74

Automatic Switchover Status:

Disarmed

Last Switchover Time:

2024-04-17 17:29:43.983513

Last Switchover Type:

Management

Edit

Managed Switchover

Arm PON Protection auto detection or force OLT switchover

Arm

Force switch

Force switch + arm

PON Protection must be disarmed to perform a Forced Switch

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the protection menu.
- 5 Click edit in the OLT protection pane.
- 6 Enter the MAC address for the OLT partner in the configuration field.
- 7 Click Save.

Procedure 49 Enabling automatic switchover for OLT active and standby

Enable automatic switchover between active and standby OLTs as required by the network plan.

Requirements

This task assumes that a standby OLT is configured in the OLT protection partner field of the OLT protection pane.

Overview

PON protection is managed as a group of two OLTs providing redundancy. Type-B Protection utilizes an optical splitter between two OLTs and N ONUs. To utilize PON Protection, all ONUs must be inventoried on the OLT. Both OLTs must be managed and inventoried as primary by the same PON Controller. PON protection is supported for XGS-PON only.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the protection menu.
- 5 Click arm in the managed switchover pane.

Procedure 50 Enabling automatic switchover with OLT toggle

Enable automatic switchover with OLT toggle as required by the network plan.

Requirements

This task assumes that a standby OLT is configured in the OLT Protection Partner field of the Protection Partner pane. A Force Switchover operation can be performed when Automatic Switchover is armed.

Overview

PON protection is managed as a group of two OLTs providing redundancy. Type-B Protection utilizes an optical splitter between two OLTs and N ONUs. To utilize PON Protection, all ONUs must be inventoried on the OLT. Both OLTs must be managed and inventoried as primary by the same PON Controller. PON protection is supported for XGS-PON only.

- **Force Switch + Arm:** Performs both the functions of an immediate switchover and arms the automatic detection for switchover events. This button is not selectable if the toggle wait time is set to 65535 (disabled).

The Automatic Switchover Status displays the state of Protection and can be Disarmed, Arming, Armed, or Failed.

Once ONUs are registered on each OLT, triggers are armed by the PonCntl. If the toggle wait time is set to 65535 (disabled) no toggling happens as part of arming. Note that triggers can be armed immediately upon request.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the protection menu.
- 5 Click Force Switch + Arm in the managed switchover pane.

Note: This operation might take a few moments to complete.

Procedure 51 Disabling automatic switchover for OLT active and standby

Disable automatic switchover between active and standby OLTs as required by the network plan.

Overview

PON protection is managed as a group of two OLTs providing redundancy. Type-B Protection utilizes an optical splitter between two OLTs and N ONUs. To utilize PON Protection, all ONUs must be inventoried on the OLT. Both OLTs must be managed and inventoried as primary by the same PON Controller. PON protection is supported for XGS-PON only.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the protection menu.
- 5 Click disarm in the managed switchover pane.

Procedure 52 Forcing a switchover from active OLT to standby OLT

Force a switchover from the active OLT to the standby OLT as required by the network plan.

Requirements

This task assumes that a standby OLT is configured in the OLT protection partner field of the OLT protection pane. A Force Switchover can be executed regardless of Automatic Switchover status as long as both OLTs are running firmware R5.2.0 or higher, Fast Failover is enabled, and PON Controller version is R5.2.0 or higher.

Overview

PON protection is managed as a group of two OLTs providing redundancy. Type-B Protection utilizes an optical splitter between two OLTs and N ONUs. To utilize PON Protection, all ONUs must be inventoried on the OLT. Both OLTs must be managed and inventoried as primary by the same PON Controller. PON protection is supported for XGS-PON only.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the protection menu.
- 5 Click Force Switch in the managed switchover pane.

Note: This operation might take a few moments to complete.

Procedure 53 Enabling OLT service ports on the ONU

Enable OLT service ports on the ONU as required by the network plan.

Overview

This task is performed from the Services tab, accessible from the left navigation pane by selecting Network / Topology, then drilling down through the OLT to the ONU.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Services menu.
- 5 Select the desired ONU.
- 6 At the bottom of the pane, click Edit.
- 7 To enable an OLT service port, do the following:
 - Confirm that the person icon displays to the right of the service. If there is an earth icon instead, click it to switch it to a person icon.
 - From the drop-down list for the service, select True.
- 8 Click Save at the bottom of the pane.

Procedure 54 Enabling OLT service ports

Enable an OLT service port as required by the network plan.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Select the Ports tab.
- 5 Click the Edit button.
- 6 Select True to enable the PON.
- 7 Click Save.

Procedure 55 Configuring the downstream QoS map on the ONU

Configure the downstream QoS map on the ONU as required by the network plan.

Overview

The downstream QoS map selection only applies to XGS-PON ONUs where multiple XGEM ports are configured with a single TCONT. Furthermore, the selection is only configurable on an OLT service port that is operating as a T-CONT, where the Mode is set to TCONT and XGEM.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Services menu.
- 5 Select the desired ONU.
- 6 Click Edit.
- 7 Click the drop down arrow in the Downstream QoS Map.
- 8 Select the desired configuration.
- 9 Click Save.

The system might take a few moments to process the change.

Procedure 56 Configuring an SLA for an OLT service on the ONU

Configure an SLA for an OLT service on the ONU as required by the network plan.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Services menu.
- 5 Select the desired ONU.
- 6 Click Edit.
- 7 Use the drop-down list to select the desired SLA.
- 8 Click Save

Procedure 57 Configuring VLAN tagging for an OLT service on an ONU

Configure VLAN tagging for OLT services on an ONU as required by the network plan.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Services menu.
- 5 Select the desired ONU.
- 6 Click Edit.
- 7 Use the drop-down under Upstream Priority Value and select the priority.
- 8 Enter the desired values in the NNI VLANs and PON VLANs columns.
 - **Note:** When you begin to add values, a values are invalid message displays and remains until all values are added.
- 9 Click Save.

The new values display in their respective columns.

Procedure 58 Configuring VLAN priority

Configure VLAN priority as required by the network plan.

Overview

Configure VLAN tagging as either copy or as a specific priority value between 0 to 7.

- **Copy:** Specifies the priority bits from the inner C-Tag for OLT configurations that add an outer VLAN tag. Copy the priority bits from the original VLAN tag to the new VLAN tag for OLT configurations that translate an outer VLAN tag.
- **Priority:** Set the priority to a specific value between 0 and 7 in VLAN tags that are added or translated by the OLT, where 7 is the highest priority and 0 is the lowest.

Steps

- 1 Click the VLAN tagging tab.
- 2 Enter either copy or a priority value.

Procedure 59 Adding a VLAN tag

Add a VLAN tag to an ONU as required by the network plan.

Overview

The Services tab provides a detailed summary of the ONUs configured on the OLT and their corresponding services, including VLAN tags. The following figure describes adding a VLAN tag.

Figure 88 VLAN tag

OLT Services

OLT Service Ports	DHCP Relay	PPPoE	802.1x Authenticator	MAC Learning	VLAN Tagging
Service	Upstream Priority Value	NNI Networks	PON Networks		
OLT Service 0 ✓	Copy	5101 .C1001 .C0 x or 0-4094	50 .C1001 .C0 x or 0-4094		
OLT Service 1	Copy	S .C .C x or 0-4094	S .C .C x or 0-4094		
OLT Service 2	Copy	S .C .C x or 0-4094	S .C .C x or 0-4094		
OLT Service 3	Copy	S .C .C x or 0-4094	S .C .C x or 0-4094		
OLT Service 4	Copy	S .C .C x or 0-4094	S .C .C x or 0-4094		
OLT Service 5	Copy	S .C .C x or 0-4094	S .C .C x or 0-4094		
OLT Service 6	Copy	S .C .C x or 0-4094	S .C .C x or 0-4094		
OLT Service 7	Copy	S .C .C x or 0-4094	S .C .C x or 0-4094		

Save

Cancel

ONU: **CSC000185837**

ONU Service Configuration: [Add CTag](#)

Number of OLT Service Ports: 1

Add CTag

ONU Service Configuration Parameters:

CVID: 1001

SWI

NNI VLANs

OLT

PON VLANs

ONU

UNI VLANs

CPE

s101.c1001.c0

Service Ports

s0.c1001.c0

UNI

s0.cx.cx

0: SLA: Max

1:

OLT Service Port

Name

Enable

Mode

TCONT Service Port

Downstream QoS Map

SLA

Upstream Priority Value

NNI VLANs

PON VLANs

OLT Service 0

Name

True

TCONT and ...

None

Max

Copy

s101

.c1001

.c0

s0

.c1001

.c0

x or 0-4094

x or 0-4094

Add Service

Save

Cancel

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Services menu.
- 5 Select the desired ONU.
- 6 Click Edit.
- 7 In the row for the corresponding OLT service, enter the required values in each of the three NNI VLANs fields and each of the three PON VLANs fields.
- 8 Click Save.

Procedure 60 Removing a VLAN tag

Remove a VLAN tag from an ONU as required by the network plan.

Overview

The Services tab provides a detailed summary of the ONUs configured on the OLT and their corresponding services, including VLAN tags.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Services menu.
- 5 Select the desired ONU.
- 6 Click Edit.
- 7 Click the red circular button in the row for the corresponding OLT service.
- 8 Click Save.

Procedure 61 Enabling DHCP relay

Enable universal mobile telecommunications system (UMTS) encapsulation of the DHCP relay on an NNI network as required by the network plan.

Requirements

- Enable the DHCP host processing function in the PON Controller.
- Configure the DHCP relay for the ONU Service associated with this NNI network.

Overview

This task is performed from the NNI Networks tab, accessible from the left navigation pane by selecting Network / Topology, then drilling down to the OLT.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the NNI Networks menu.
- 5 Click Edit.
- 6 Locate the NNI Network.
- 7 Use the drop-down list to select a host in the DHCPv6 Filter column or the DHCPv4 Filter column or both.
- 8 Click Save.

*In the NNI Networks pane, the field(s) you set to host will display as **umt**, for UMT tunnel.*

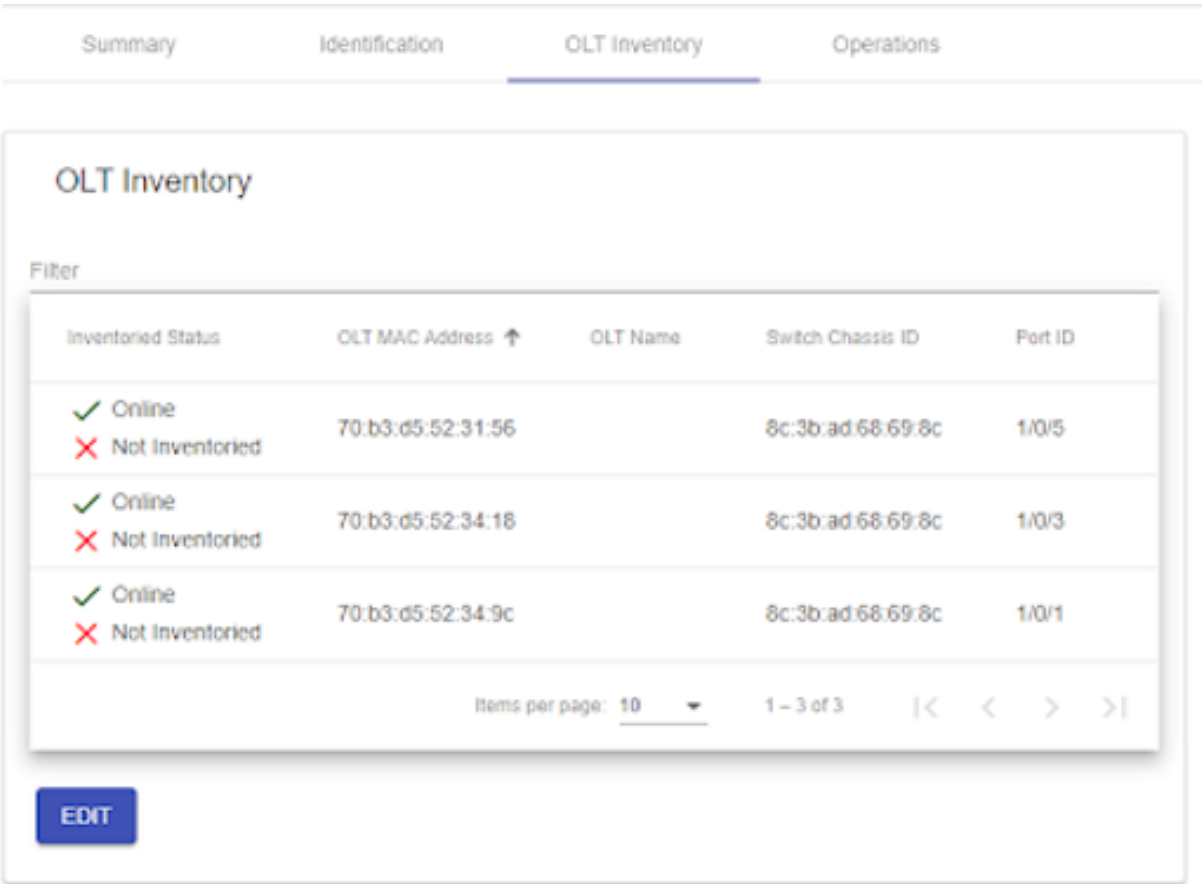
Procedure 62 Adding an OLT to the switch inventory

Add an OLT to the switch inventory as required by the network plan.

Overview

Each switch has its own OLT inventory. The OLT Inventory tab displays all OLTs managed by the selected switch with information such as statuses, MAC addresses, and names. The following figure describes an OLT Switch Inventory.

Figure 89 OLT Switch Inventory



Steps

- 1 Click Network on the left navigation pane.
- 2 Click MGMT LANs.
- 3 Navigate to the parent Controller of the desired OLT.
- 4 Click the OLT Inventory tab.

- 5** Click Edit.
- 6** From the Inventory Config drop down menu select one of the following options:
 - Primary Controller
 - Secondary
 - Controller
 - Excluded
- 7** Click Save.

Procedure 63 Deleting switch or router data

Delete switch or router data as required by the network plan.

Requirements

This task is performed from the Operations tab, accessible from the left navigation pane by selecting Network / Topology, then drilling down to the switch device.

Overview

The delete action removes configuration records for the specified switch. There is no need to save changes after the delete action is performed. The switch's records are immediately deleted. This action cannot be undone.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Operations menu.
- 5 Click Delete in the Delete OLT Data.
- 6 Click Delete again.

Procedure 64 Removing the ONU from the inventory

Remove the ONU from the inventory as required.

Requirements

Before provisioning the service configuration for an ONU, it must not be inventoried. Inventorying the ONU means that an AllocID will be pre-assigned to it, which can potentially cause out-of-sync issues when the ONU is provisioned for service later.

Steps

- 1 Navigate to **Network > select OLT > ONU Inventory**
- 2 Any ONUs that are inventoried will have a check under the Inventoried column and have an ONU State of **Registered**.
- 3 Click on the **Edit** button to inventory the ONUs
- 4 Click on **Remove** button for each ONU to be removed from the inventory
- 5 Click on the **Save** button and wait for the ONU removal process to complete

Procedure 65 Synchronizing automatic assigned in the inventory

Synchronize automatic assigned in the inventory when the configured settings do not match what is active in the OLT's state.

Overview

The sync automatic assigned function is only available when the configuration settings do not match what is active in the OLT's state.

Steps

- 1 From the ONU Inventory tab, select Edit to edit the inventory table.
- 2 Select the ONU from the inventory table.
- 3 Select the Sync automatically assigned button.

The system sets the values in each input field to match the active values in the OLTs state.

Procedure 66 Assigning next free block of consecutive ALLOC IDs to a specified number of OLT service ports

Assign the next free block of consecutive ALLOC IDs when you want the system to assign the next free block of consecutive ALLOC IDs to a specified number of OLT service ports.

Overview

The following table displays ALLOC IDs for GPON and EPON.

Table 33 ALLOC IDs for GPON and EPON

PON	Available ALLOC IDs	Excluded ALLOC IDs
GPON	1154-1534	1279
EPON	5121-6013	5375, 5631, 5887

Steps

- 1 From the ONU Inventory tab, select Edit to edit the inventory table.
- 2 Select the ONU from the inventory table.
- 3 From the ONU Inventory tab, enter the number of ALLOC IDs required in the Service port count box.

The system sets consecutive ALLOC IDs for each OLT service port.

Note: For example, if you enter 3, the system will designate the next available 3 ALLOC IDs to the first three OLT service ports with no ALLOC IDs.

Procedure 67 Adding an OLT to an inventory

Add an OLT to an inventory as required by the network plan.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Inventory menu.
- 5 Select the desired ONU.
- 6 Select one of the following: Primary Controller, Secondary Controller, Excluded.
- 7 Click save.

Procedure 68 Removing an OLT from an inventory

Remove an OLT from an inventory as required by the network plan.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the parent switch of the desired OLT.
- 4 Click the OLT Inventory tab.
- 5 Click Edit.
- 6 Select the OLT.
- 7 Select Remove
- 8 Click save.

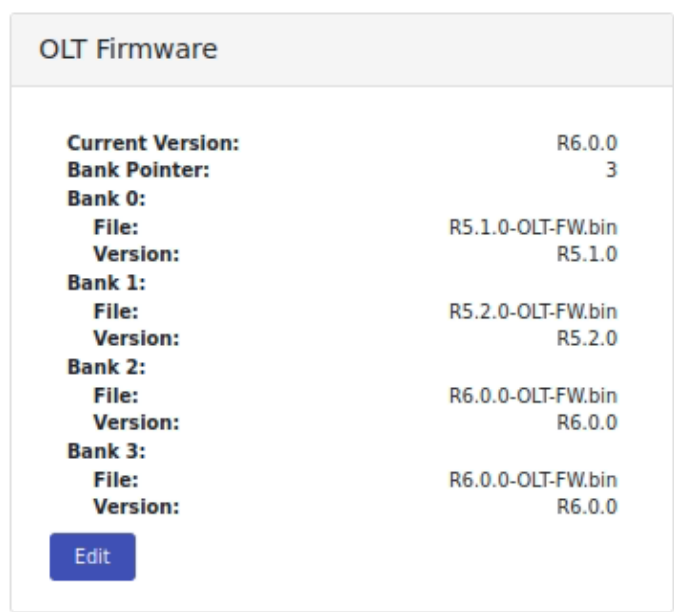
Procedure 69 Upgrading OLT firmware

Upgrade the OLT firmware as required by the network plan.

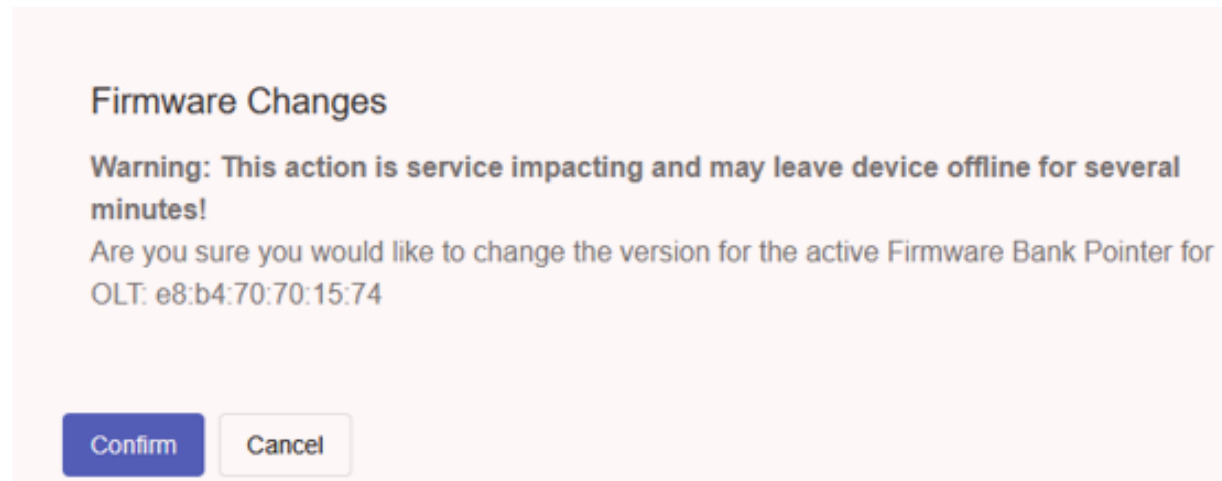
Overview

The Firmware tab contains two sub-tabs: OLT Firmware for managing the firmware on a given OLT, and ONU Firmware for monitoring the firmware status on subtended ONUs. This procedure is performed on the OLT Firmware sub-tab.
The following figure describes the OLT Firmware dialogue.

Figure 90 OLT Firmware



If the active bank pointer is being changed, a warning pop-up will display warning that this may leave the device offline for several minutes. Either click Confirm to continue to upgrade the OLT bank pointer or Cancel to go back to the OLT Firmware screen.
The following figure describes firmware changes.

Figure 91 Firmware changes

If firmware is being changed on the active bank pointer, a warning pop-up will display warning that this may leave the device offline for several minutes. Click either Confirm to continue to upgrade the OLT firmware or Cancel to go back to the OLT Firmware screen.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Firmware menu.
- 5 Click Edit.
- 6 Select a different bank in the bank pointer drop down menu to change the firmware.
- 7 Use the config version drop down menu for the desired firmware bank, to change the firmware in each bank.
- 8 Click Save.

Procedure 70 Disabling OLT firmware upgrade

Disable the OLT firmware upgrade as required by the network plan.

Overview

The Firmware tab contains two sub-tabs: OLT Firmware for managing the firmware on a given OLT, and ONU Firmware for monitoring the firmware status on subtended ONUs. This procedure is performed on the OLT Firmware sub-tab. Disabling firmware upgrade does not cancel a download that is already in-progress.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Firmware menu.
- 5 Click the OLT Firmware sub-menu.
- 6 Click Edit.
- 7 Click the Bank Pointer State arrow, and then select Upgrade Disabled.
- 8 Click Save.

Procedure 71 Adding an NNI network to an OLT

Add an NNI network to an OLT as required by the network plan.

Requirements

This task is performed from the NNI Networks tab, accessible from the left navigation pane by selecting Network / Topology, then drilling down to the OLT.

Overview

The NNI Network inventory is used to configure VLANs and networks for Layer2 Switch Domains (L2SD) on an OLT device. NNI network inventory configuration includes the VLAN stack, Learning Limit, PON Flood ID, Downstream Flooding SLA, DHCP filters, and PPPoE filter. Existing NNI networks may be added to the OLT's inventory and new networks may be created.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the NNI Networks menu.
- 5 Click Edit in the NNI Networks pane.
- 6 Select the Config sub-menu.
- 7 Click Edit in the NNI Networks pane.
- 8 Click Add New.

A new row is added at the bottom of the list for the new NNI network.

- 9 Configure the new NNI network as required.
- 10 Click Save.

The new row is arranged chronologically in the list by Network VLAN.

Procedure 72 Adding a new NNI network to the inventory

Add a new NNI network to the inventory as required by the network plan.

Requirements

This task is performed from the NNI Networks tab, accessible from the left navigation pane by selecting Network / Topology, then drilling down to the OLT.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the NNI Networks menu.
- 5 Select the Config sub-menu.
- 6 Click Edit in the NNI Networks pane.
- 7 Select the Add button to active NNI Network rows that are not inventoried.
A new configurable row is added to the table.
- 8 Configure the Network VLAN value and the other displayed settings for the NNI network as required.
- 9 Click Save.

The new NNI network displays as the last entry in the table.

Procedure 73 Removing an NNI network from the inventory

Remove an NNI network from the inventory as required by the network plan.

Requirements

An NNI network must be inventoried before it can be removed. A green tick mark in the **Inventoried** column indicates that the network is inventoried.

Overview

This task is performed from the NNI Networks tab, accessible from the left navigation pane by selecting Network / Topology, then drilling down to the OLT.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the NNI Networks menu.
- 5 Select the Config sub-menu.
- 6 Click Edit in the NNI Networks pane.
- 7 Locate the NNI network.
- 8 Click Remove in the Inventoried column.
- 9 Click Save.

The NNI network is removed from the inventory.

Procedure 74 Adding static MAC addresses to the network VLAN

Add static MAC addresses to a network VLAN as required by the network plan.

Requirements

The network VLAN must be both active and inventoried in order for MAC addresses to be added.

Overview

This task is performed from the NNI Networks tab, accessible from the left navigation pane by selecting Network / Topology, then drilling down to the OLT.

Steps

- 1 Click Network on the left navigation pane.
 - 2 Click Topology.
 - 3 Navigate to the desired OLT.
 - 4 Click the NNI Networks menu.
 - 5 Select the Config sub-menu.
 - 6 Click Edit in the NNI Networks pane.
 - 7 In the NNI Networks pane, locate the network VLAN.
 - 8 Click the pink icon in the Learning Table column.
- 9 Click Edit.
 - 10 Select the desired ONU from the ONU drop-down list.
 - 11 Select the desired OLT Service Port from the OLT Service Port drop-down list.
 - 12 Enter the MAC Address in the CPE MAC Address field.
 - 13 Click Add.

The Learning Table window displays.

The CPE MAC address displays in the table below the CPE MAC Addresses field.

- 14 Click Save, and then click Close.

The CPE MAC address does not display in the main NNI Networks table, but it now displays in the Learning Table window when you click the pink icon for that network VLAN.

Procedure 75 Enabling source MAC verify

Enable source MAC verify to set a security function implemented by the PON Controller to validate the legitimacy upstream CPE traffic received by the OLT.

Requirements

Do the following before enabling source MAC verify.

- Set the Learning Limit to 0 and Drop Unknown Source Mac to true to disable MAC table dynamic learning.
- Enable either authentication or DHCP Host Processing, or both functions on the PON Controller.

Overview

Disabling dynamic learning allows the PON Controller to program the MAC table with CPEs learned through the source MAC verify function.

Setting the Learning Limit to 0 configures the dynamic MAC learning table to a size of zero.

Setting Drop Unknown Source Mac to true configures the OLT discard upstream frames from CPE MAC addresses that have not been learned.

OLT service ports can be grouped together through referencing another OLT service port. When an OLT service port references another service port, the source MAC verify configuration is shared with the referenced service port.

An OLT service port source MAC verify parameter cannot be configured to reference itself. The following figure describes enabling Source MAC verify.

Figure 92 Source MAC verify

OLT Services					
OLT Service Ports		DHCP Relay	PPPoE	802.1x Authenticator	MAC Learning
Service	Learning Limit	Drop Unknown Source Mac		CPE Limit	Source MAC Verify
OLT Service 0	0	true		3	DHCPv4
OLT Service 1	0	true		3	OLT-Service 0
OLT Service 2	2046	false		1	Disabled
OLT Service 3	2046	false		1	Disabled
OLT Service 4	0	true		5	OLT-Service 7
OLT Service 5	2046	false		1	Disabled
OLT Service 6	2046	false		1	Disabled
OLT Service 7	0	true		5	EAPOL

[Edit](#)

*Note: Current values for a field in ONU State are shown in red, if different than configured value.

Steps

- 1 From the OLT Services MAC Learning tab, use the pull down menu to select EAPOL, DHCP, DHCPv4, or DHCPv6.
- 2 Set the CPE Limit to restrict the number of CPEs allowed to transmit on an OLT Service port.

Only CPE devices that have successfully completed 802.1X authentication or successfully acquired an IP address from an authorized DHCP server will be permitted to forward traffic through the OLT.

Procedure 76 Disabling source MAC verify

Disable source MAC verify to remove the security function implemented by the PON Controller to validate the legitimacy upstream CPE traffic received by the OLT.

Steps

- 1 From the OLT Services MAC Learning tab, use the pull down menu to select Disabled.

Procedure 77 Enabling PPPoE on NNI networks

Enable point-to-point protocol over Ethernet (PPPoE) on an NNI network as required by the network plan.

Requirements

- Enable the PPPoE intermediate agent host processing function on the PON Controller.
- Configure PPPoE for the ONU service associated with the NNI network.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the NNI Networks menu.
- 5 Select the Config sub-menu.
- 6 Click Edit in the NNI Networks pane.
- 7 Locate the NNI Network.
- 8 Select host in the PPPoE Filter column.
- 9 Click Save.

In the NNI Networks pane, the field you set to host will display as umt, for UMT tunnel.

Procedure 78 Resetting the OLT

Reset the OLT as required by the network plan.

Overview

This task is performed from the Operations tab, accessible from the left navigation pane by selecting Network / Topology, then drilling down to the OLT.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Operations menu.
- 5 Click Reset in the Reset OLT page.
- 6 Click Reset.
- 7 Click Rest.

Procedure 79 Deleting OLT data

Delete the data for an OLT as required by the network plan.

Overview

This action removes all configuration, state, statistics, and logging data for this OLT from the database. It does not remove the OLT from any PON Controller or switch OLT inventories. After the delete is confirmed, it cannot be undone.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Operations menu.
- 5 Click Delete in the Delete OLT Data pane.
- 6 Click Delete.

Procedure 80 Allowing ONU registration on the OLT

Allow ONU registration on the OLT as required by the network plan.

Overview

This action clears an ONU from the Disallowed Error state and allows it to register on the PON.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Operations menu.
- 5 Use the drop-down to select an ONU to register or select All in the Allow ONU Registration pane.
- 6 Click Allow ONUs.
 - **Note:** If the OLT is in the process of ONU registration, a message to this effect displays and the Allow ONUs button is disabled. Wait for the OLT to complete the pending registration operation before attempting another operation.

Procedure 81 Enabling the ONU serial number to enable transmit laser

Enable an ONU serial number from the OLT inventory in order to enable the ONU's transmit laser as required by the network plan.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Operations menu.
- 5 Use the drop-down list to select an ONU to enable or select All in the Enable ONU Serial Number pane.
- 6 Click Enable ONUs.

Allow a few moments for this action to complete.

Procedure 82 Configuring the OLT image

Configure an image for the OLT as required by the network plan.

Overview

The Identification tab contains two tiles. The upper tile displays identifying information about the OLT, such as its name, ID, picture, and more. Several of these items, including the picture, are configurable.

If you try to upload an image and receive the message “The selected file must have a unique name,” the image is already being used with a different Device Type. Create a copy of the image with a different file name. You’ll be instructed to select the corresponding Device Type for this new image in the steps below.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Identification menu.
- 5 Click the Edit button.
- 6 Click the Picture drop down list under Configuration.
- 7 Select the desired system.
- 8 Click Save.

Procedure 83 Configuring the OLT name

Configure the name for the OLT as required by the network plan.

Overview

The Identification tab contains two tiles. The upper tile displays identifying information about the OLT, such as its name, ID, picture, and more. Several of these items, including the name, are configurable. There are no restrictions on creating the name for the OLT.

Steps

- 1 Click Network on the left navigation pane.
- 2 Click Topology.
- 3 Navigate to the desired OLT.
- 4 Click the Identification menu.
- 5 Click the Edit button.
- 6 Enter a name for the ONU in the name field.
- 7 Click the Save button.

The new name displays in the Name field and in the navigation panel.

CHAPTER 12

Accounts

Create, edit, view, and manage user profiles and roles in the accounts area of the MCMS PON Manager user interface.

All users can access their profiles to update their names and passwords. Users who are assigned the administrators role can view and edit the information of other users.

Personal

The personal tab is the default view of the accounts area.

Currently logged in users can view and edit their own user profiles, including passwords, in the user profile window. They can also review and sort their own actions for the last hour, day, week, month, or three months in the your logs window.

The following figure describes User profiles.

Figure 93 User profiles

PersonalAdministration

User Profile

Email:

tibit@tibitcom.com

First Name:

Tibit

Last Name:

User

Last Login:

6/15/2023, 11:24:00 AM

Edit

Your Logs

Displaying logs from the last hour

Hour

Day

Week

Month

3 Months

Refresh logs

Download all logs

Filter

Time ↓	Severity	IP Address	URL	Method	Status	Message
6/15/2023, 11:24:46 AM	INFO	192.168.33.1	/user/password /requirements /unauthenticated/	GET	200 OK	-
6/15/2023, 11:24:45 AM	INFO	10.2.10.222	/v2/onus/configs /ISK71e81c38/	GET	200 OK	-
6/15/2023, 11:24:45 AM	INFO	10.2.10.222	/v2/onus /automation /states /ISK71e81c38/	GET	200 OK	-
6/15/2023, 11:24:45 AM	INFO	10.2.10.222	/onu/summary /ISK71e81c38/	GET	200 OK	-
6/15/2023, 11:24:45 AM	INFO	10.2.10.222	/v2/onus/alarm- histories /ISK71e81c38/	GET	200 OK	-

Items per page: 5

1 – 5 of 13921

<<

<

>

>>

MicroClimate Management System
MCMS 6.2
Copyright© 2024 - 2026 Ciena® Corporation

PON Manager User Guide
323-1961-302 Standard Revision A
March 2026

Administration

The Administration tab helps you manage all user profiles, roles, logs, user session timeout, display preferences, and user configuration. It is only visible and available to users assigned to an administration role. The all users window displays by default.

Users

An active user count is displayed at the top of the card with the number of users currently active and the number of users total. Users are displayed in a table sorted alphabetically by email.

Each user's email, first and last names, assigned roles, and session expiry age are listed as well as the creation date of the account and the last login time for the account. The table may be sorted by any column except for assigned roles. Each row is expandable by clicking to see the full list of the user's roles as a comma separated list. Administrators are able to edit any user's account details, assigned roles, view their assigned roles, or delete the user. However, Administrators do not have the ability to remove themselves from the Administrators role from their own account. If an administrator user needs to be removed from this role it must be done from a different administrator's account. The session expiry age is based on what roles the user is in. If a user is in multiple roles with different expiry ages, they will have the highest age from their roles.

The following figure describes All users.

Figure 94 All users

Local Users							
Local active users count: 1 of 3 Radius active users count: 0							
Filter							
Email ↑	Last Name	First Name	Assigned Roles	Session Expiry Age (Minutes)	Date Created	Last Login	Active
john_smith@ciena.com	Smith	John	Administrators	20	2/13/2026, 5:39:00 PM	2/13/2026, 5:41:29 PM	True
read_only@ciena.com	Only	Read	Read Only	20	2/13/2026, 5:40:15 PM	2/13/2026, 5:41:07 PM	False

Roles

Upon switching to the Roles tab the following screen is shown.

The table lists all system roles sorted alphabetically by name. For each role the user count, permission count, and session expiry age are displayed. The far right column, Edit, contains a menu to edit the users assigned to the role, permissions the role has, timeout for the role, or to delete the role.

Note: The built-in 'Administrators' and 'Read Only' roles cannot have their permissions changed or be deleted.

The following figure describes All user roles.

Figure 95 All user roles

Name ↑	User Count	Permission Count	Session Expiry Age (Minutes)	Edit
Administrators	2	81	20 (global)	⋮
Read Only	1	31	20 (global)	⋮

Items per page: 10 1 - 2 of 2

Create

Users
Permissions
Timeout
Delete

View Permissions

Note: View permissions only control what is displayed in the UI and DOES NOT restrict API access to users.

View permissions are used to show or hide sections of the UI from a group of users. Disabling view permissions will hide the tabs and reroute users back to login if they navigate to the pages. View permissions other than Admin, are enabled by default and can only be disabled for the Global Config.

Modify an Existing Role's Permissions

When the permissions menu item is selected, a dialog containing all assignable permissions as checkboxes is displayed. All permissions that a role is currently assigned have that checkbox selected.

Read permissions are not editable for any permission type except for Accounts Admin. View permissions are only editable for Accounts Admin and Global Config. Upon saving, all permissions with their checkboxes selected are given to the role.

The following figure describes how to edit technician's permissions.

Figure 96 Edit Technicians' permissions

The screenshot shows the 'All User Roles' interface. At the top is a 'Filter' input field. Below it is a table with the following columns: Name (with an upward arrow), User Count, Permission Count, Session Expiry Age (Minutes), and Edit (with a vertical ellipsis). The table contains three rows: Administrators (2 users, 81 permissions, 20 (global) expiry), Read Only (1 user, 31 permissions, 20 (global) expiry), and Technicians (0 users, 22 permissions, 20 (global) expiry). Below the table is a pagination section with 'Items per page: 10' (dropdown), '1 - 3 of 3', and navigation arrows. A green 'Create' button is at the bottom left. A context menu is open for the 'Technicians' role, showing options: Users, Permissions (highlighted with a red box), Timeout, and Delete.

Name ↑	User Count	Permission Count	Session Expiry Age (Minutes)	Edit
Administrators	2	81	20 (global)	⋮
Read Only	1	31	20 (global)	⋮
Technicians	0	22	20 (global)	⋮

Items per page: 10 1 - 3 of 3

Create

- Users
- Permissions
- Timeout
- Delete

Edit 'Technicians' permissions

Permission Type	View (UI)	Read (API)	Update (API)	Create (API)	Delete (API)	All
Dashboard						
Dashboard	☒	☒	☒	☒	☒	☒
Network						
Controllers	☒	☒	☒	☒	☒	☒
Olts	☒	☒	☒	☒	☒	☒
Onus	☒	☒	☒	☒	☒	☒
Switches/Routers	☒	☒	☒	☒	☒	☒
Cascading	☒	☒	☒	☒	☒	☒
Global Config						
Alarms	☐	☒	☐	☐	☐	☐
Slas	☐	☒	☐	☐	☐	☐
Services	☐	☒	☐	☐	☐	☐
Files	☐	☒	☐	☐	☐	☐
Databases	☐	☒	☐	☐	☐	☐
Automation	☐	☒	☐	☐	☐	☐
Devices	☐					☐

Save Cancel

Modify an Existing Role's Session Expiry Age

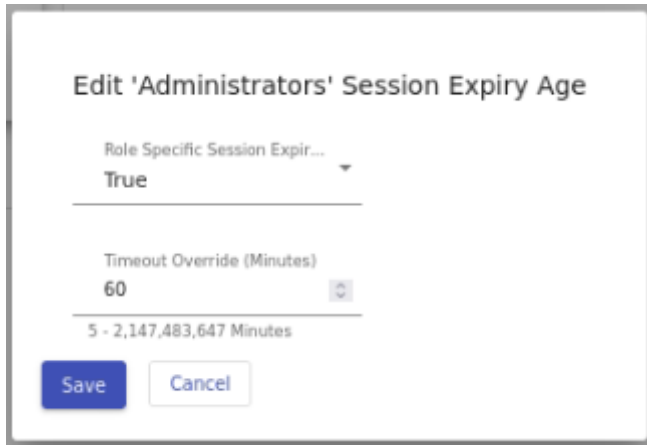
To edit a role's session expiry age, select the Timeout option from the edit menu.

To use the global session expiry age, set the role Specific Session Expiry Age to false.

To override the global and set a Role Specific Session Expiry Age, set this value to True and specify the desired age.

The following figure describes Session expiry age.

Figure 97 Session expiry age



Edit 'Administrators' Session Expiry Age

Role Specific Session Expir...
True

Timeout Override (Minutes)
60

5 - 2,147,483,647 Minutes

Save Cancel

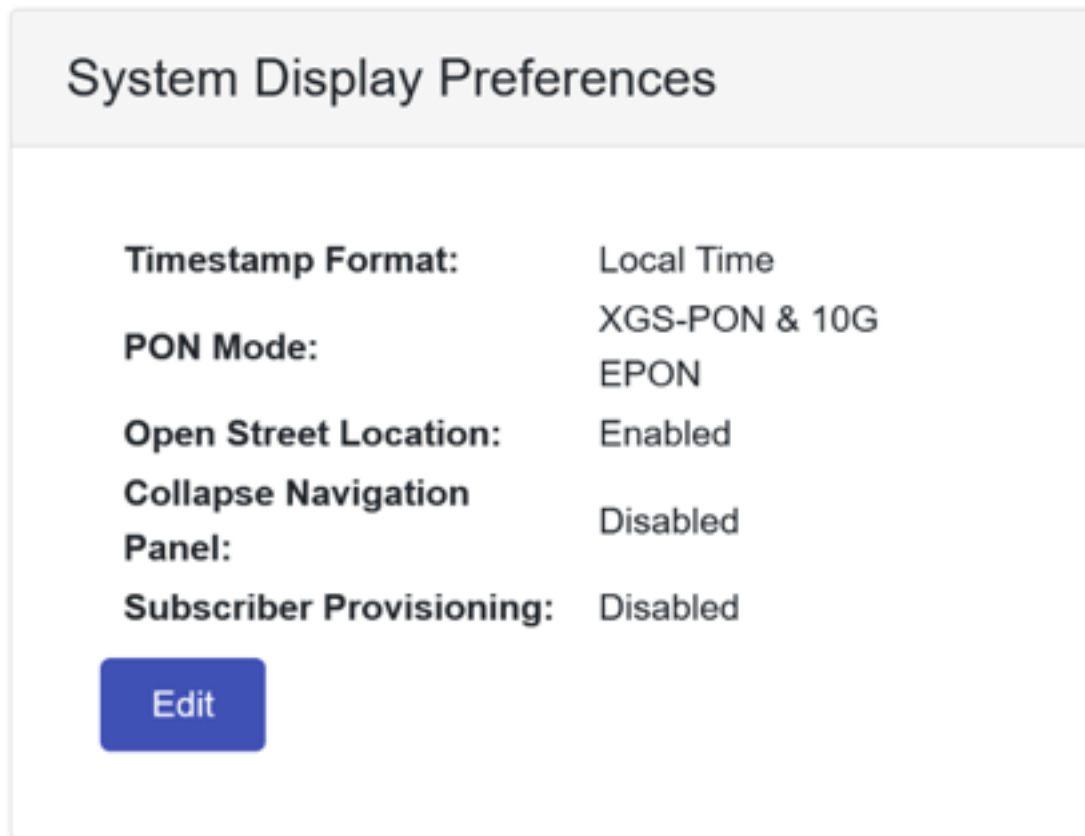
Display preferences

The display preferences tab enables the user to configure the timestamp format and the PON mode for the MCMS PON Manager. This configuration applies system-wide for all users.

The following display preferences are supported:

- Timestamp Format
- PON Mode
- Open Street Location
- Collapse Navigation Panel
- Subscriber Provisioning

The following figure describes the System Display Preferences

Figure 98 System Display PreferencesA screenshot of a web form titled "System Display Preferences". The form contains several settings, each with a label and a value. The settings are: "Timestamp Format:" with value "Local Time", "PON Mode:" with value "XGS-PON & 10G EPON", "Open Street Location:" with value "Enabled", "Collapse Navigation Panel:" with value "Disabled", and "Subscriber Provisioning:" with value "Disabled". At the bottom left of the form is a blue button labeled "Edit".

Timestamp Format:	Local Time
PON Mode:	XGS-PON & 10G EPON
Open Street Location:	Enabled
Collapse Navigation Panel:	Disabled
Subscriber Provisioning:	Disabled

Edit

Logs

The Logs tab contains a card to display all logs, and a card to control Traceback Logging.

An administrator may select a custom time range or display the most recent logs going back by selecting a pre-determined time range. Logs can then be sorted by time or severity, as well as filtered by time, severity, and message. Each log message includes a timestamp, severity level, the email of the user, the IP address the request came from, the relative PON Manager REST API URL that was accessed, the HTTP method used, the HTTP status code, and a message describing the request/event if applicable.

The **Download all logs** option will save the logs to the user's computer in JSON format. The **Refresh logs** will get the latest logs from the database. To delete all logs, click on the **Clear Logs** button. A prompt appears to confirm the action. After this is performed it cannot be undone.

The following figure describes All logs.

Figure 99 All logs

All Logs

Displaying logs from the last hour

☒ Hour
 ☐ Day
 ☐ Week
 ☐ Month
 ☐ 3 Months

Refresh logs Download all logs

Filter

Time ↓	Severity	User	IP Address	URL	Method	Status	Message
8/9/2024, 2:27:27 PM	INFO	tibit@tibitcom.com	10.32.6.201	/v3/onus/states/ISK771e81c38/	GET	200 OK	-
8/9/2024, 2:27:27 PM	INFO	tibit@tibitcom.com	10.32.6.201	/v3/databases/selection/	GET	200 OK	-
8/9/2024, 2:27:27 PM	INFO	tibit@tibitcom.com	10.32.6.201	/v3/databases/status/	GET	200 OK	-
8/9/2024, 2:27:26 PM	INFO	tibit@tibitcom.com	10.32.6.201	/switch/tree/Unassigned/Unassigned /	GET	200 OK	-
8/9/2024, 2:27:26 PM	INFO	tibit@tibitcom.com	10.32.6.201	/v3/onus/stats/ISK771e81c38/?start-time=2024-08-09%20%27:14	GET	200 OK	-

Items per page: 5 1 – 5 of 372

The Trace Logging card contains options to enable and configure more verbose logging for the REST API. Trace Logs are stored in a separate local file and contain significantly more information than the standard logs, including detailed HTTP request and response message headers and payloads. Trace logging can be used to help analyze and debug issues between API client applications and the PON Manager server.

The following figure describes Trace logging.

Figure 100 Trace logging

Trace Logging

Enable: true

HTTP Methods: GET, PUT

Status Codes: 500 504 503

URL Filter: None

Client IPs: 10.32.6.201

Users: tibit@tibitcom.com

[Edit](#)

Trace Log configuration includes controls for filtering on specific API message contents to help reduce the debug logging output and focus the debugging effort.

Filters configure the following API message and protocol elements:

- HTTP Methods
 - including GET, PUT, POST, PATCH and DELETE.
- Status Codes in an HTTP response message.
- URL Filter
 - matches any string contained in the request URL.
- Client IPs
 - matches IP addresses of the Client API applications.
- Users
 - matches usernames of the users sending API requests

Note: Trace logging with no filters is not recommended. Unfiltered trace logging can generate a large amount of log data. This can quickly filling up storage and impact performance of the PON Manager and REST API.

Sessions

The Sessions tab contains a list of active user sessions, as well as a card to display and edit the active session expiry time.

The Active Sessions table displays all the active web sessions for users that are currently logged in. Each row of the table shows the username, authentication type, client IP address, client operating system, client browser information, session create date/time, and session

expiration date/time. The **Auth Type** column displays Local for local PON Manager users stored in MongoDB, or Radius for users authenticated through an external Radius server. Editing the table allows the user to delete any active sessions other than their own. When a user session is deleted, the user is logged out and must re-authenticate.

The following figure describes Active sessions.

Figure 101 Active sessions

Active Sessions

Active Sessions Count: 3

Filter

User ↑	Auth Type	IP Address	OS	Browser	Date Created	Expire Date
radius@ciena.com	Radius	10.100.124	Windows 10	Firefox 122.0	1/24/2024, 10:20:33 AM	1/24/2024, 12:21:58 PM
user@tibitcom.com	Local	10.0.0.104	Unknown OS	Unknown Browser	1/17/2024, 1:37:36 PM	1/24/2024, 12:21:13 PM
user@tibitcom.com	Local	10.100.124	Windows 10	Chrome 120.0.0.0	1/24/2024, 10:21:33 AM	1/24/2024, 12:22:00 PM

Items per page: 10 1 – 3 of 3

Edit

The Sessions Expiry Age card contains a single option to set the length of time in minutes for how long a user should remain logged in without activity. If a user is logged in and there is no activity from them within the time limit defined here, then they are automatically logged out and their session is invalidated.

Timestamp Format

There are two options for Timestamp Format; Local Time, and UTC. All timestamps within the PON Manager UI will be formatted based on this choice. When changed, the timestamp display format will be updated for all users in the current database after they logout and login again or refresh the page. Note that changing this option does not change the format of timezones in the PON Controller database, only the display format within the PON Manager.

PON Mode

There are three options for PON Mode; XGS-PON, 10G EPON, and XGS-PON & 10G EPON. This setting controls what PON Mode specific configurations will be available to modify within the UI. When a PON Mode is selected, all configurations in the interface that do not apply to the given PON Mode will be removed.

For demonstration and lab systems that have both XGS PON and 10G EPON OLTs and ONUs, select 'XGS-PON & 10G EPON' to have the ability to properly configure and provision both types of devices.

Authentication

The Authentication tab provides the ability to configure the password requirements for new and existing users, and to configure external RADIUS user authentication.

Radius authentication

The Radius Authentication card provides the needed configuration options to enable Radius authentication for PON Manager.

The NAS Identifier field is a string included with Radius authentication access requests from PON Manager. The Retries field is how many access request messages will be attempted per Radius server before the authentication fails and returns an error to the user. The Timeout field is how many seconds the PON Manager will wait for an access accept from the Radius server before failing the authentication attempt. Up to two Radius servers can be configured, each containing a host, port, and secret key. The priority field on each server determines which Radius server will be attempted first. If two Radius servers are configured and retries is greater than 0, then the servers will be attempted in priority order 1, 2, 1, 2, and so on.

The following figure describes Radius authentication

Figure 102 Radius authentication

Radius Authentication

Enable:

true

NAS Identifier:

MCMS

Retries:

0

Timeout:

60

Priority	IP	Port	Secret
1	127.0.0.1	1812	

Edit

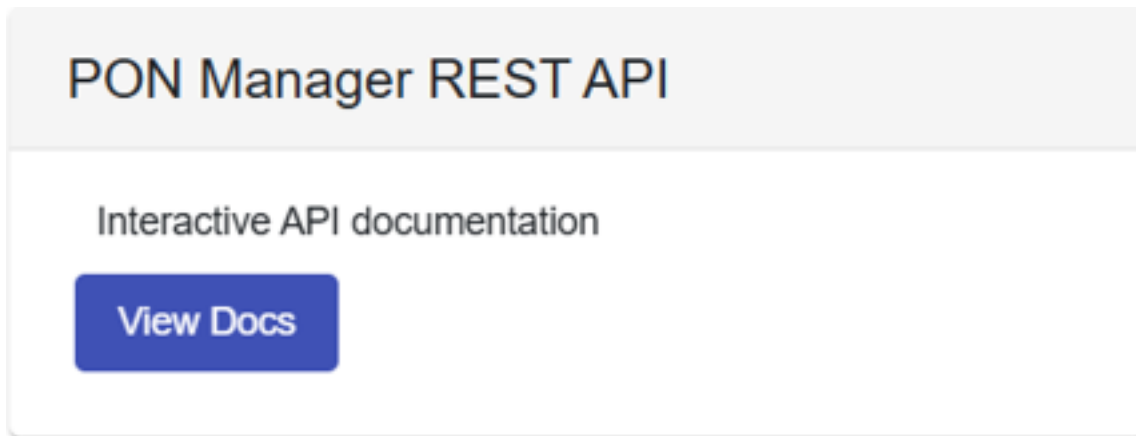
API Documentation

The API Documentation tab provides a link to the Swagger API documentation service.

Clicking on this link navigates to a separate web page outlining all API endpoints and valid requests.

The following figure describes the PON Manager REST API

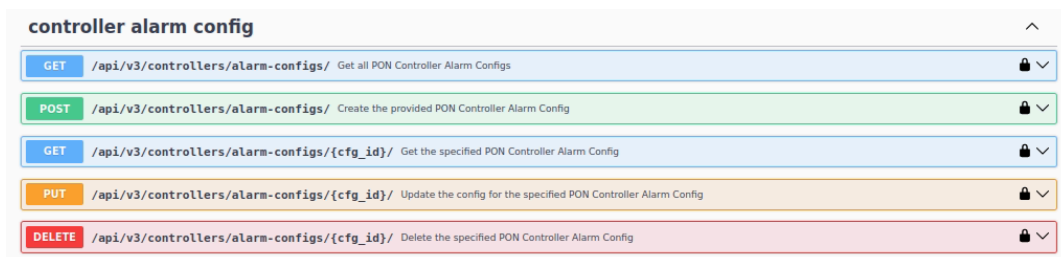
Figure 103 PON Manager REST API



When expanding a tag for an API endpoint, each HTTP method supported by that endpoint is displayed along with the valid extension format and a brief description.

The following figure describes the Controller alarm configuration

Figure 104 Controller alarm configuration



Expanding an extension drop-down provides a sample request that is able to be customized. Requests that include parameters provide an input field in which to enter a custom value. An input field for a custom request body is available, along with an example schema to follow.

The following figure describes an example schema.

Figure 105 Example schema

PUT /api/v3/cascading/{casc_id}/ Update the provided Cascading Config

Parameters Cancel Reset

Name	Description
casc_id * required string (path)	casc_id

Request body application/json

```
{
  "id": "string",
  "CNTL": {
    "CFG Version": "string"
  },
  "CASC": {
    "Max Rate": 10000000,
    "Max Burst": 256000,
    "VLAN": {
      "TPID": 0,
      "COS": 7,
      "VID": 4094
    },
    "Multicast MAC Address": "a1:9f:3e:c4:05:26",
    "Response Timeout": 50000,
    "Request Period": 1000000,
    "Inactivity Timeout": 384000,
    "Create Date": "string"
  }
}
```

Execute

Responses

Code	Description	Links
201	Created	No links

Media type: application/json

Controls Accept header.

Example Value | Schema

```
{
  "id": "string",
  "CNTL": {
    "CFG Version": "string"
  },
  "CASC": {
    "Max Rate": 10000000,
    "Max Burst": 256000,
    "VLAN": {
      "TPID": 0,
      "COS": 7,
      "VID": 4094
    },
    "Multicast MAC Address": "46:83:5e:1d:95:72",
    "Response Timeout": 50000,
    "Request Period": 1000000,
    "Inactivity Timeout": 384000,
    "Create Date": "string"
  }
}
```

When pressing 'Execute', a sample request is sent to the API. This action does not affect any existing data in MongoDB. The API tag drop-down further expands to provide the curl implementation, the request URL, response headers, and the response body. The response body can be copied to the clipboard or downloaded. Using valid parameters is need for execution to be successful.

The following figure describes the Response body.

Figure 106 Response body

Responses

Curl

```
curl -X 'PUT' \
  'https://127.0.0.1/api/v3/cascading/1/' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -H 'X-CSRFToken: weZcwZUBER571vDclTanhs4TKH0ZUyucuc00050bJlygsNFq4jex3qQuHIA5d51' \
  -d '{
    "id": "string",
    "CNTL": {
      "CFG Version": "string"
    },
    "CASC": {
      "Max Rate": 10000000,
      "Max Burst": 250000,
      "VLAN": {
        "TPID": 0,
        "COS": 7,
        "VID": 4094
      },
      "Multicast MAC Address": "01:9f:3e:c4:05:26",
      "Response Timeout": 50000,
      "Request Period": 1000000,
      "Inactivity Timeout": 304000,
      "Create Date": "string"
    }
  }'
```

Request URL

https://127.0.0.1/api/v3/cascading/1/

Server response

Code	Details
201	Response body <pre>{ "status": "success" }</pre> Response headers <pre>cache-control: no-store,max-age=0 content-length: 20 content-security-policy: default-src 'none'; script-src 'self'; connect-src 'self'; img-src 'self' data: https: blob:; style-src 'self' 'unsafe-inline'; font-src 'self'; frame-ancestors 'none'; content-type: application/json cross-origin-opener-policy: same-origin date: Mon, 16 Feb 2026 16:40:40 GMT referrer-policy: same-origin server: Apache/2.4.41 (Ubuntu) strict-transport-security: max-age=63072000; includeSubdomains; vary: origin, Cookie x-content-type-options: nosniff x-firefox-spydy: h2 x-frame-options: DENY</pre>

Responses

Code	Description	Links
201	Created	No links

Media type:

Controls Accept header.

Example Value | Schema

```
{
  "id": "string",
  "CNTL": {
    "CFG Version": "string"
  },
  "CASC": {
    "Max Rate": 10000000,
    "Max Burst": 250000,
    "VLAN": {
      "TPID": 0,
      "COS": 7,
      "VID": 4094
    },
    "Multicast MAC Address": "05:30:8e:5d:df:92",
    "Response Timeout": 50000,
    "Request Period": 1000000,
    "Inactivity Timeout": 304000,
    "Create Date": "string"
  }
}
```

Open Street Location

There are two options for open street location: enabled and disabled. This setting controls the use of Subscriber Provisioning throughout the UI.

When it is enabled, any device can access a hyperlink that displays a map with the device's coordinates. By default, this setting is disabled upon account creation. To enable open street location, change the ponmgr-web.conf file prior to starting PON Manager.

Collapse navigation panel

There are two options for collapse navigation panel: enabled and disabled. This setting allows the web application to start with the left side navigation panel collapsed on login or refreshed.

When it is enabled, the side navigation panel will begin collapsed upon login or page refresh.

Note: This setting is disabled by default.

CHAPTER 13

Global configuration

Global configuration tabs are used to configure the PON network.

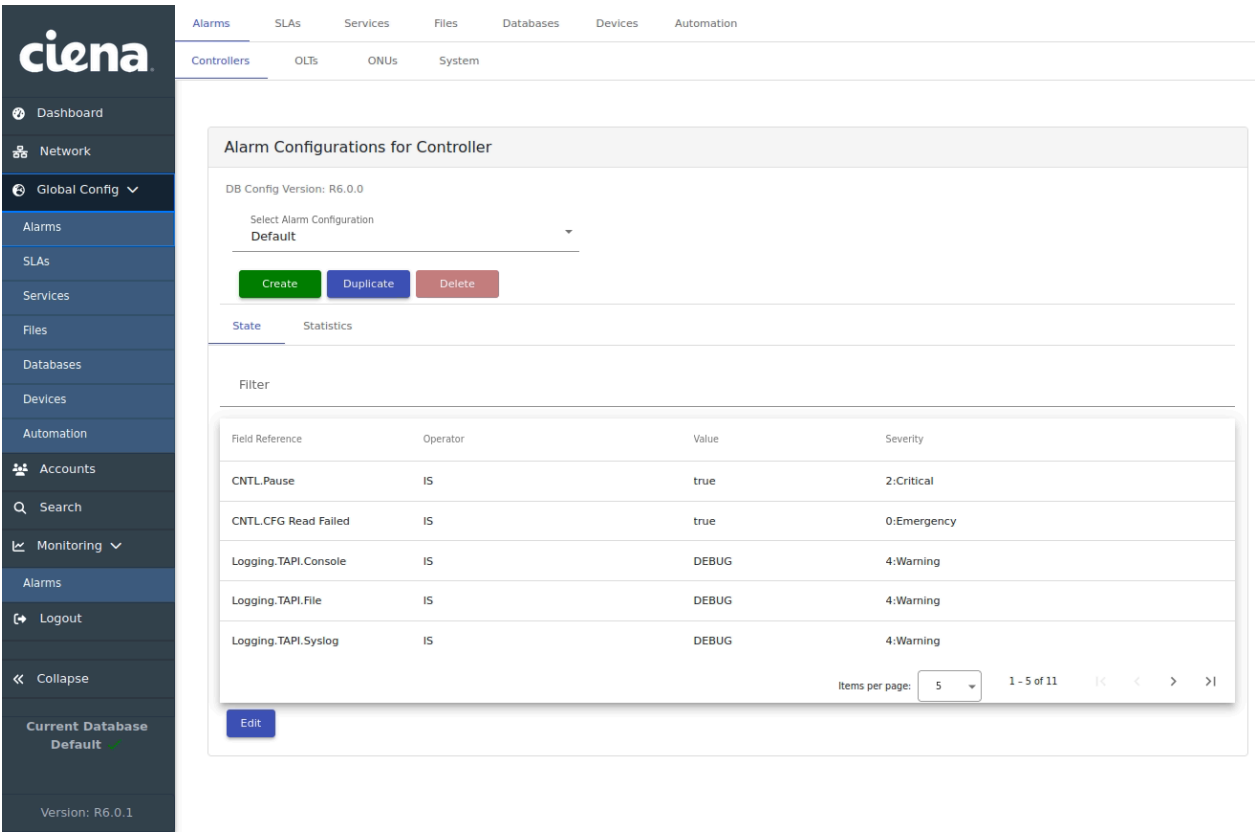
Alarms

The Alarms tab has three sub-tabs: Controllers, OLTs, and ONUs.

Create, edit, delete, and duplicate alarms on all three sub-tab.

The following figure describes Global Configuration Alarms

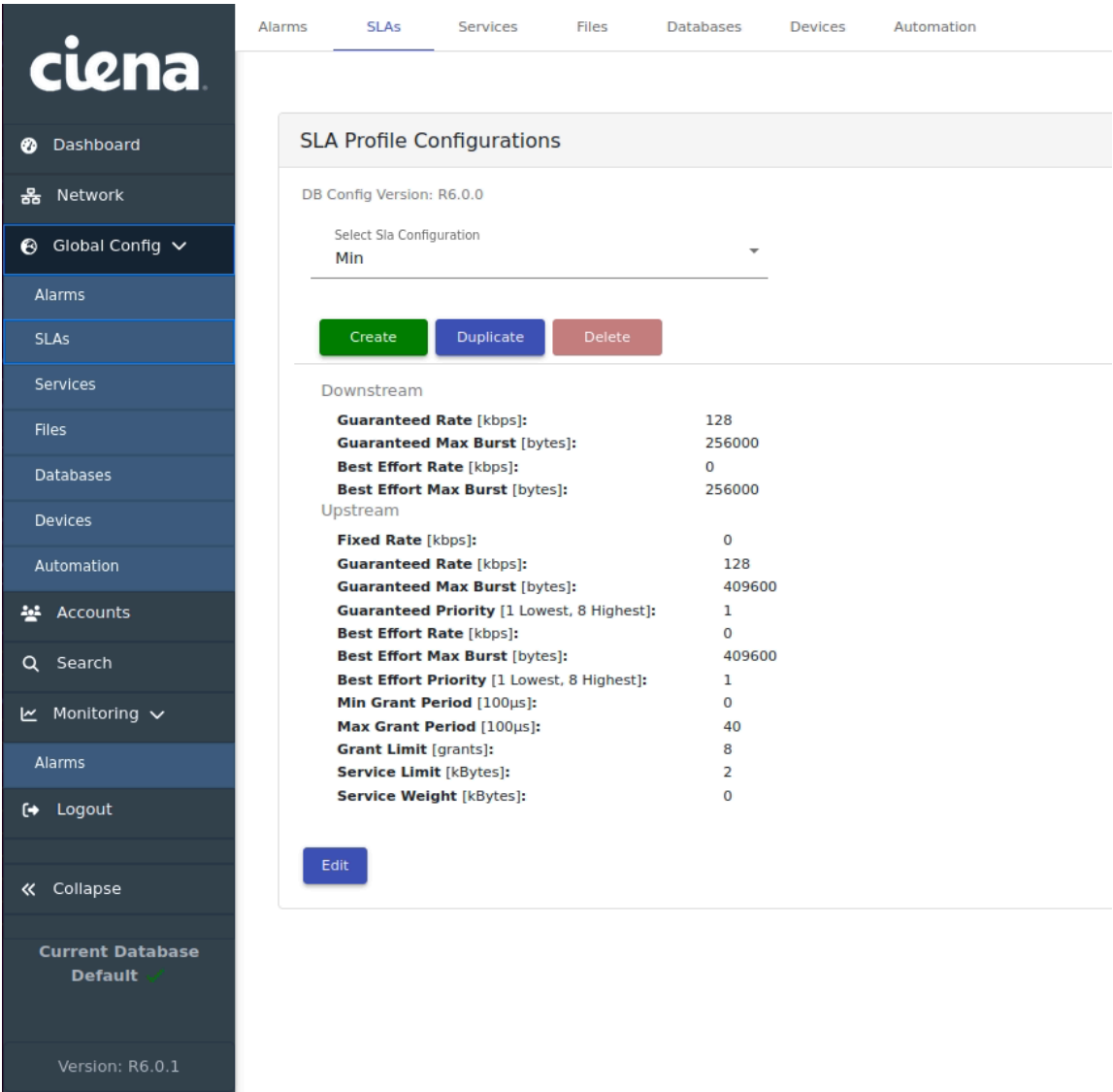
Figure 107 Global Configuration Alarms



SLAs tab

Use the SLAs tab for viewing, creating, editing, duplicating, and deleting device, SLA profiles. The following figure describes the SLAs tab.

Figure 108 SLAs tab



Services tab

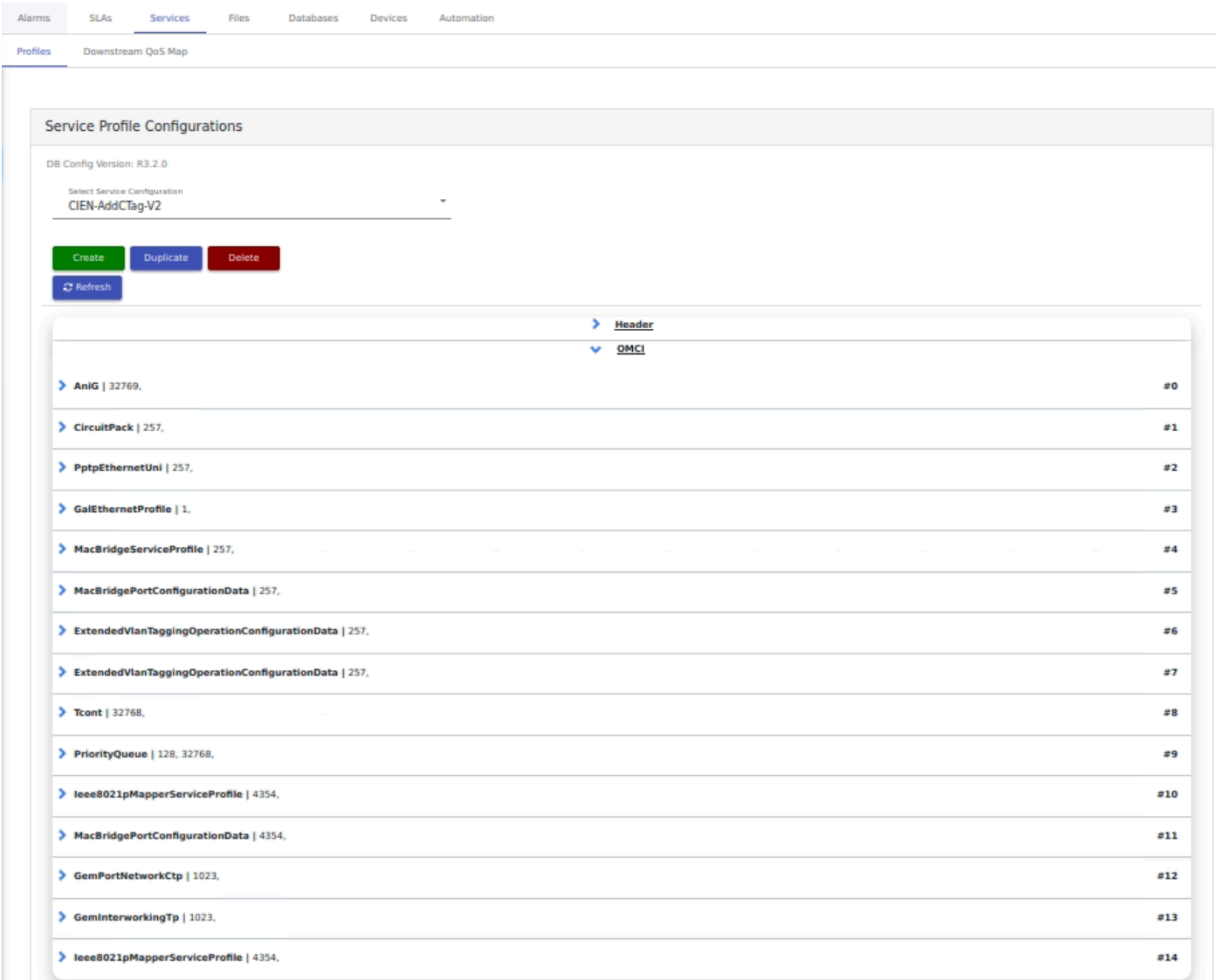
The Services tab has two sub-tabs: Profiles and Downstream QoS Map.

Profiles tab

Create, edit, and view ONU service profile configurations on the Profiles tab.

The following figure describes the ONU service profile configurations in the Profile tab.

Figure 109 ONU service profile configurations on the Profiles tab



Downstream QoS Map tab

The downstream QoS map tab creates, edits, and displays QoS mappings for downstream traffic received by the OLT on the NNI port.

These profiles are referenced by GPON ONU multi-XGem configurations and map priority bits in the VLAN tag to OLT service XGem ports.

The following figure describes Downstream QoS map configurations.

Figure 110 Downstream QoS map configurations

Downstream QoS Map Configurations

DB Config Version: R6.0.0

Select Downstream QoS Map Configuration
Default

Create Duplicate Delete

VLAN Priority Bit Value	OLT-Service Offset
COS: 0	0
COS: 1	1
COS: 2	2
COS: 3	3
COS: 4	4
COS: 5	5
COS: 6	6
COS: 7	7

Edit

The mapping associates VLAN priority bit (CoS) values 0 to 7 with OLT service offsets 0 to 7. Each OLT service represents a T-CONT and a group of associated XGem ports. The OLT service offset indicates that the position of the OLT service port within the T-CONT and XGem port group. This configuration enables downstream traffic to be distributed across different XGem ports based on the CoS values. The ONU service configuration on the OLT service port in T-CONT and XGEM mode refers to the downstream QoS map.

Downstream QoS map service restrictions:

- The alloc-IDs assigned to the OLT services referenced by the downstream QoS map must be consecutive.

- If an OLT service's service offsets refer to XGEM-only services that are not present on the ONU, a downstream QoS map cannot be assigned to that OLT service.
- To disable an OLT service that is referenced by a downstream QoS map, it is necessary to first clear the downstream QoS map reference from the T-CONT and XGEM OLT service.
- A maximum of three unique downstream QoS maps can be assigned to a single OLT, while the same downstream QoS map can be used across different OLTs.
- An OLT service cannot be assigned a downstream QoS map where all OLT service offset values are set to zero. This configuration is equivalent to having no downstream CoS mapping.

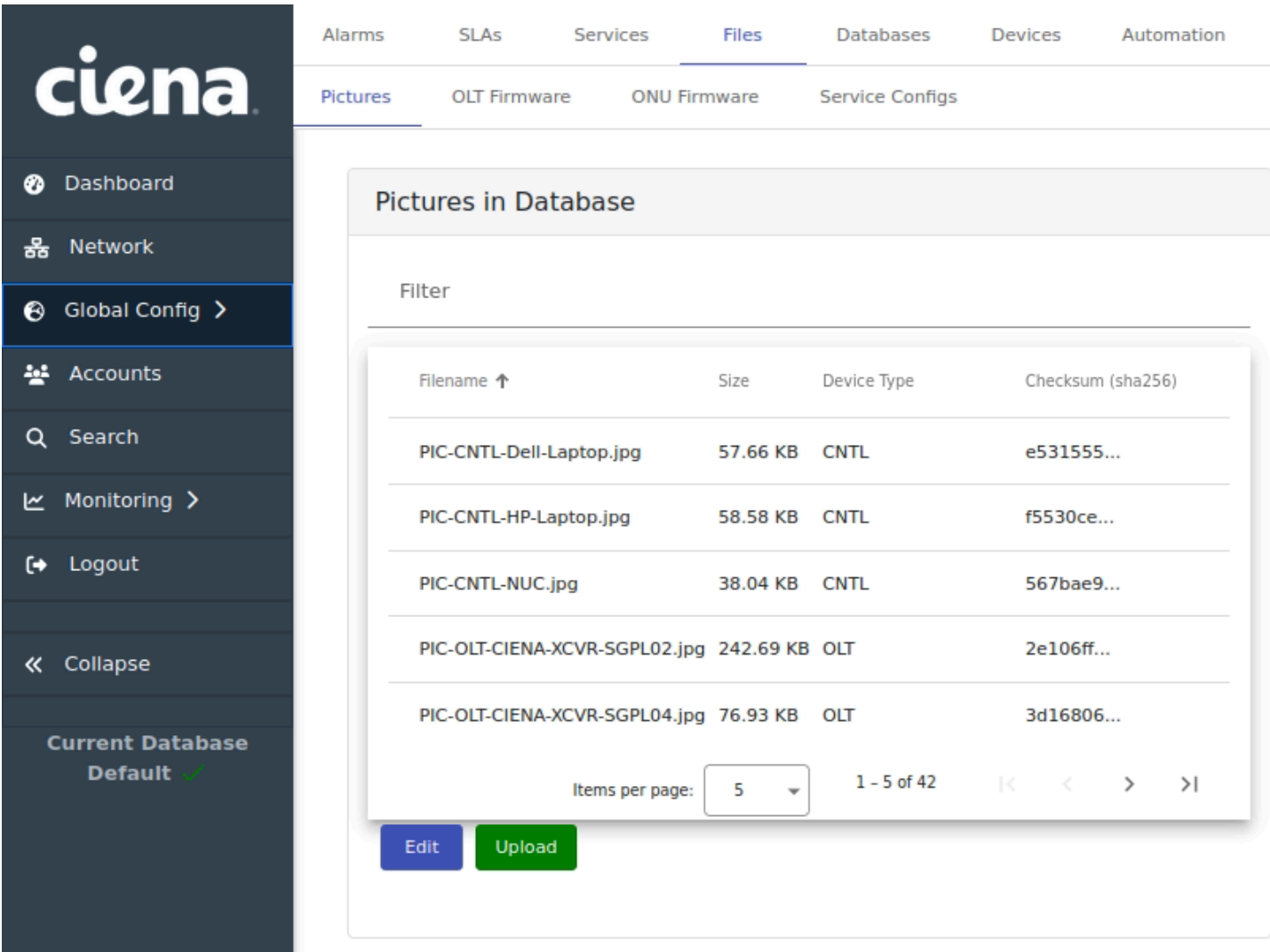
Files tab

The Files tab is used for uploading and deleting files, and editing the metadata of firmware and pictures. The tab includes four sub-tabs:

- Pictures
- OLT Firmware
- ONU Firmware
- Service Configs

The following figure describes Pictures.

Figure 111 Pictures



Service configuration file

The service configuration file contains a list of OMCI messages for provisioning service for an ONU. The PON Controller uses the service configuration file to send all the defined OMCI messages needed when setting up services. It will contain the following information

- number of T-CONTs, XGEMs and UNI ports
- ONU priority queue configuration
- CVID/SVID tag(s)
- traffic flows between XGEM and UNI ports
- upstream Priority
- enabling performance monitoring statistics

Deploying the service configuration file has the following advantages:

- Defines all the necessary OMCI MEs needed for ONU service provisioning and can be applied to multiple ONUs of the same brand/model
- OMCI messages are easily customizable to be configured for different types of services and work through potential interoperability issues such as change of order for OMCI messages.
- The OMCI specifications allow the current service configuration file to be modified with a text editor or the MCMS PON Manager user interface which simplifies the editing of the service configuration files.
- The service configuration file is stored in the database in the SRV-CFG collection.

The MCMS PON Manager uses the service configuration file for sending all the defined OMCI MEs needed for provisioning services for the ONU. After selecting the service configuration for an ONU, specific parameters are entered before saving the configurations. Once the configuration completes, the ONU configurations are updated in the database in the ONU-CFG configuration file.

The following table describes the contents of the service configuration file.

Table 34 Contents of the service configuration file

Section	Contents
Header	• Documentation of title, PON Controller Version compatibility, and ONU compatibility • Inputs lists the ONU configuration file (for per-device config) and ONU State file (for currently assigned values) reference • Ports documents the UNI ports used in the config file
OMCI	List of OMCI Management Elements (MEs) to configure based on the order they are listed in the configuration file Note: This is important due to MEs possibly having a dependency of upon other MEs being created beforehand. • Each ME specified can have one or more ME identifiers (ME IDs) specified • Attributes of all or a subset of the ME IDs can be configured • If ME ID does not exist, the ME ID will be created on the ONU with the provided value set in the config file • If ME ID exists, the values will be checked. • Values can be constants or references to the ONU-CFG or ONU-STATE file.

Databases tab

The Databases tab has three sub-tabs: Initialize, Update, and manage. is used for adding, removing, modifying, initializing, and updating databases for MCMS PON Manager.

The MCMS PON Manager enables a database with default configurations, pictures, and firmware images. This includes an SLA, service, PON Controller, switch, OLT, ONU, PON auto default configuration documents, and default device pictures and firmware images that come with the installation package. After initialization, the inserted documents and files can be edited.

Initialize

Databases in the MCMS PON Manager can be initialized with default configurations, pictures, and firmware images.

The user may select any of the configuration documents, device pictures, and firmware images that are included with the install package. The user may then choose a database from the list of configured databases.

The following figure describes Initializing a database.

Figure 112 Initialize a database

Database to initialize

Select database

☒ Toggle all configurations and files

Collection	Document ID
☒	AUTO-ALARM-CFG
☒	CASC-CFG
☒	CNTL-ALARM-CFG
☒	CNTL-CFG
☒	DS-MAP-CFG
☒	OLT-ALARM-CFG
☒	OLT-CFG
☒	ONU-ALARM-CFG

Collection	Document ID
☒	SRV-CFG
☒	SRV-CFG
☒	SRV-CFG
☒	SRV-CFG
☒	SRV-CFG
☒	SRV-CFG
☒	SRV-CFG
☒	SRV-CFG

Collection	Document ID
☒	AUTO-TASK-CFG
☒	CNTL-AUTO-CFG
☒	CNTL-AUTO-CFG
☒	OLT-AUTO-CFG
☒	OLT-AUTO-CFG
☒	ONU-AUTO-CFG
☒	ONU-AUTO-CFG

Filename	Vendor	Models	Version
☒	R6.0.0-OLT-FW.bin	TIBITCOM	Models: 1807... Version: R6.0.0

Filename	Device Type
☒	PIC-CNTL-Dell-Laptop.jpg
☒	PIC-CNTL-HP-Laptop.jpg

Note that pictures, firmware, and other large files might require several minutes to upload.

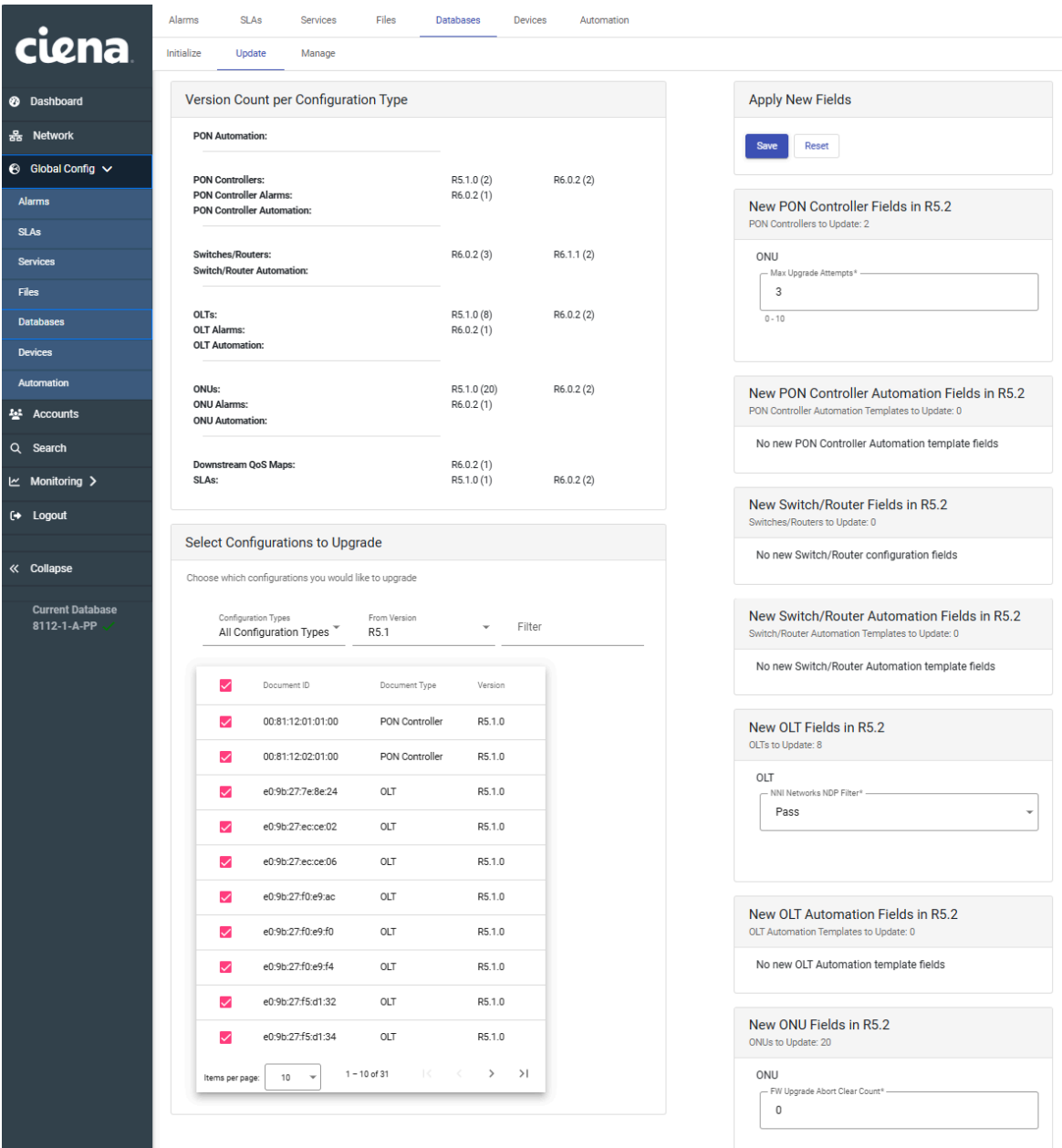
After initialization, the inserted documents and files may be edited or modified as normal.

Update tab

The databases update tab has three panes: Version Count per Configuration Type, and Select Configurations to Upgrade.

The following figure describes the Update tab.

Figure 113 Update tab



Use the Version Count per Configuration Type pane to view information such as PON Automation, PON Controllers, Switches and Routers, OLTs, ONUs, and Downstream QoS maps.

Use the Select Configurations to Upgrade pane to select which configurations to upgrade.

Manage tab

The databases manage tab supports adding, modifying, cloning, and deleting database connections from the MCMS PON Manager.

To view the data for a database connection, select the ID from the drop-down list at the top of the tab. If the MongoDB server is offline or cannot be reached, the status shows offline and the heartbeat failure warning panel displays. If a server is online but is not initialized, the not populated warning panel displays.

The following figure describes Manage Database Connections

Figure 114 Manage Database Connections

The screenshot displays the 'Manage Database Connections' interface in the Ciena MCMS PON Manager. The interface is divided into a sidebar and a main content area. The sidebar contains navigation links: Dashboard, Network, Global Config (selected), Accounts, Search, Monitoring, and Logout. The main content area has a top navigation bar with tabs: Alarms, SLAs, Services, Files, Databases (selected), Devices, and Automation. Below this, there are sub-tabs: Initialize, Update, and Manage (selected). The 'Manage Database Connections' section includes a dropdown menu to select a database (currently 'Default'). Below the dropdown, the 'Connection Details' are listed: Status (Online), Connection Type (Direct), Database Name (tibit_pon_controller), MongoDB Version (4.4.29), Host (127.0.0.1), and Port (27017). The 'Authentication' section shows 'Auth Enabled' as false. The 'Encryption' section shows 'TLS Enabled' as false. At the bottom of the connection details are buttons for Edit, Create, Clone, and Delete. To the right of the connection details is the 'Database Connection Statistics' section, which shows: Current Count: 11, Max Count: 11, and Average Count: 10. Below the statistics is a table for Servers with columns: Host, Status, Type, Latency (ms), and Heartbeat Failure Count. The table contains one entry: Host 127.0.0.1:27017, Status Online, Type RSPPrimary, Latency 1, and Heartbeat Failure Count 0. Below the servers table is a table for Commands with columns: Command, Average Latency (ms), Min Latency (ms), Max Latency (ms), Failure Count, and Success Count. The table contains eight entries: Build Info, List Collections, Aggregate, Find, Distinct, Find and Modify, Delete, and Get More. At the bottom right of the commands table is a 'Clear Statistics' button.

Note that PON Manager user names and PON Manager user profiles are stored in the users database. The users database connection settings cannot be modified using the web app. Refer to the user_database.json configuration file.

Device tab

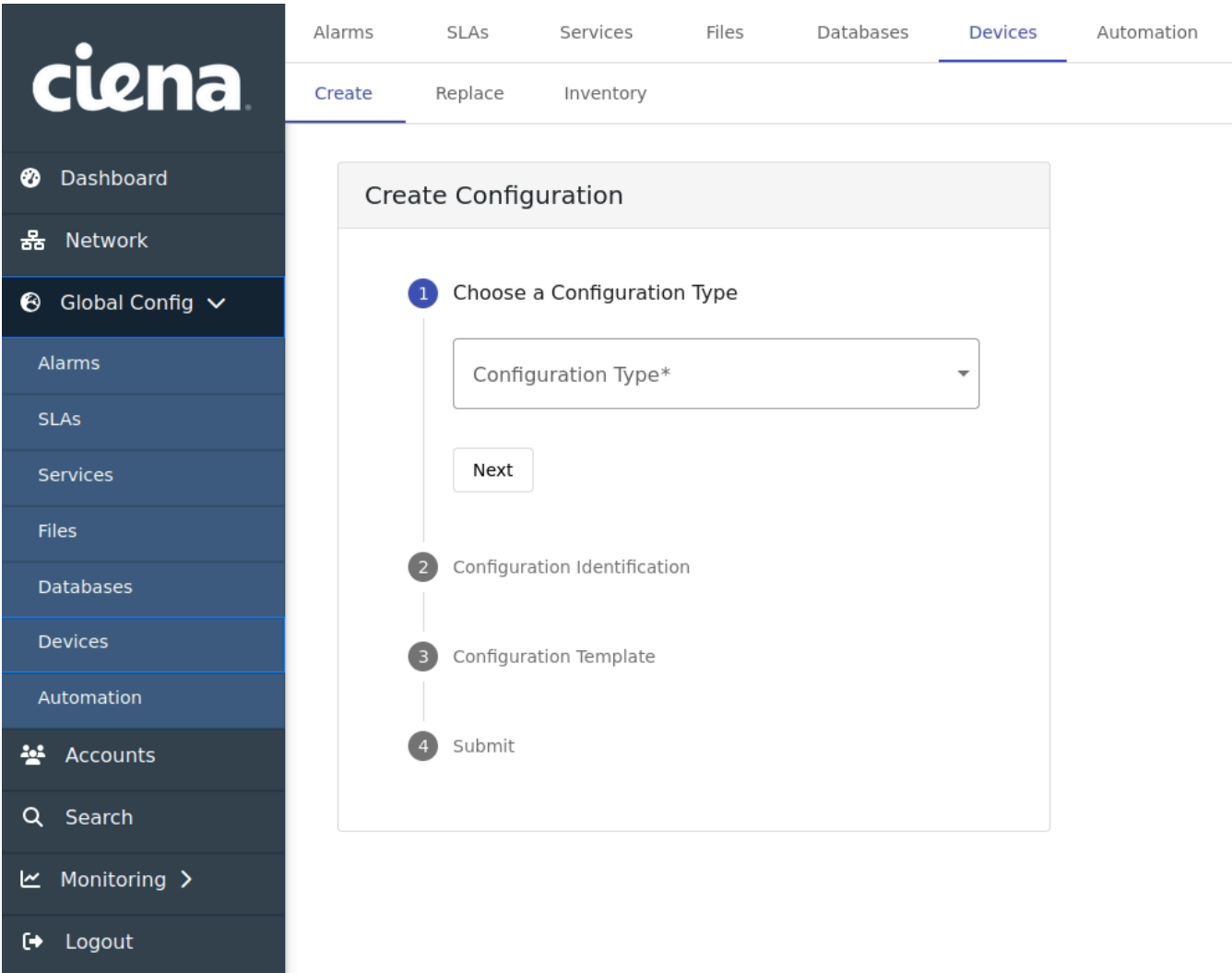
Use the device create tab to pre-provision PON controllers, switches, OLTs, and ONUs.

Also, use device create to pre-provision subscribers when subscriber-based provisioning is enabled on the PON manager.

A base configuration template is selected when configuring a new configuration. This new configuration uses the base configuration template.

The following figure describes Create Configuration

Figure 115 Create Configuration



A new OLT and ONU configuration may be inventoried under a PON Controller and Switch or OLT, respectively, but is not required.

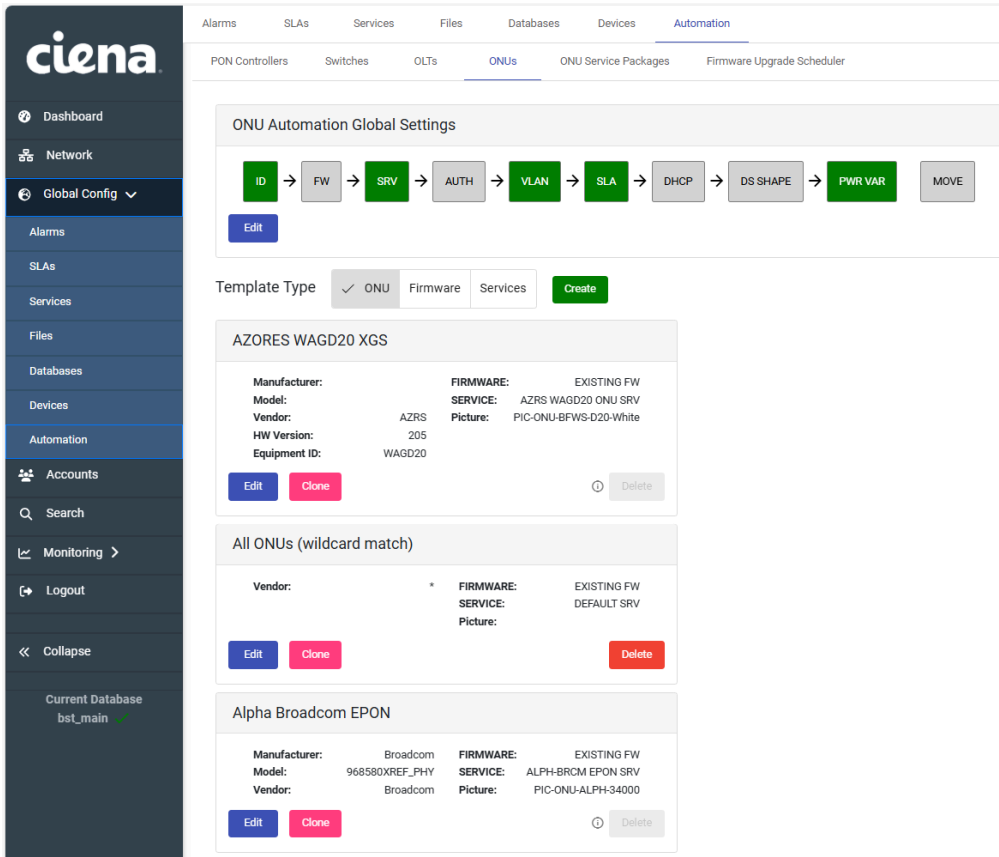
Global configuration automation tab

The global configuration automation tab provides a user interface for managing automation templates for each type of device.

It contains five sub-tabs for PON Controllers, Switches, OLTs, ONUs, and ONU Service Packages. Each sub-tab manages the automation templates for that device type, allowing the creation, editing, and deletion of the templates.

The following figure describes the Global configuration automation tab,

Figure 116 Global configuration automation tab



There are four input types in the Automation tabs. They have different behaviors and are listed in the table below.

Table 35 Automation tab input types

Input mode	Description
Exact value	Specifies the exact value entered.
Database reference	Specifies a database field to reference, such as ONU ID.
Ignore	Do not include this field in the PonAuto configuration.
Stop for input	Stops automation and waits for manual input

PON Auto switches and routers

There are three tasks that PON auto executes before a Switch is active: Identify, Add OLTs, and Port. PON auto can be configured to skip any of these tasks except for Identify.

ONU Service Packages

ONUs are unique in PON Auto in that they require an additional configuration called a Service Package in order to automatically configure an ONU to support data service. The Service Packages define the number of links the ONU will be configured for and the configuration for items that are link-specific. This includes, but is not limited to, Service Names, SLAs, SRV-CFGs, and VLANs.

The following figure describes ONU service packages.

Figure 117 ONU service packages

ONU Automation Service Packages

Create

Default

Name	SLA	ONU VLAN ID Offset
Edit	Clone	Delete

Data Only

	Name	SLA	ONU VLAN ID Offset
Service 0	Data	Max	1000
Edit	Clone		Delete

Triple Play

	Name	SLA	ONU VLAN ID Offset
Service 0	Data	Max	1000
Service 1	Video	Max	2000
Service 2	Voice	Max	3000
Edit	Clone		Delete

To create a service package, click the CREATE button. From here, provide a name for the service package. By default, one OLT-Service is available to edit. To add more, click the ADD

SERVICE button. This will add more OLT-Services up to the allowed eight. Unwanted OLT-Services may be removed using the delete icon to the right of the drop down for that service. Each service allows for the input of a service name, SLA, OLT and ONU VLAN, authentication, and DHCP configuration. The service package will not be able to be saved until all required fields have been filled out. Input options will vary depending on other selections for the OLT VLAN, ONU VLAN, authentication, and DHCP steps. Make sure all required fields are provided for each step. Once complete, click SAVE to finish creating the service package.

Editing a service package is very similar to creating one. Click EDIT on the service package to be updated. All fields will be the same as during creation, however the service package name may not be changed. Once all required fields are completed and all desired updates are done, click SAVE to update the service package.

To delete a service package click the DELETE button on the service package to be deleted. The user will be prompted to confirm this deletion. Once confirmed, the chosen service package will be removed from the list of available packages.

OLTs

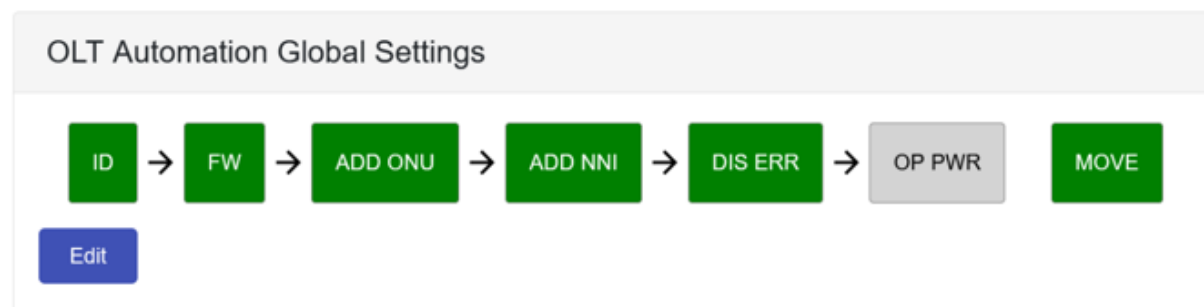
There are several tasks that PON auto may execute before a PON OLTs is active: Identify, Firmware, Add ONUs, Add NNI Networks, Disallowed Error, and Optical Power.

Note: The Optical Power task is skipped in the default PON automation configuration.

There is also the MOVE task which indicates that the OLT has been moved to another port.

The following figure describes OLT automation global settings.

Figure 118 OLT automation global settings



Each task is configurable except for Identify. To modify configuration for a task, click **Edit** on the OLT automation global settings. Select the task to update and edit the desired fields. All configurable tasks have the Skip field. If Skip is True, PON auto will not execute this task for any OLT it attempts to configure. Disallowed Error and Optical Power have additional configuration parameters for Rogue ONU controls. The Move task has a Stop option. If Stop is True, PON auto halts automation for an OLT that enters the Move task. At this point, automation is halted for this device and operator intervention is required to recover and resume automation for this device.

Each OLT template for PON auto is shown below the global settings. These templates define the state information that PON auto should match on to identify an OLT, and what fields to configure for that OLT.

To create a new template, click **Create**, provide the unique ID of the new template, and input any desired fields. To update a template, click the **Edit** button. This will allow for the adjustment of any field in the template except for the ID. The **Clone** button begins creating a new template just like **Create**, but pre-fills all fields except for the template ID from the original template. Use the **Delete** button to remove a template. A popup will ask for confirmation. Once confirmed, that template will be deleted. This cannot be undone.

OLTs also have an extra layer of templates for firmware settings. To view the firmware templates select the Firmware option for template type. These are managed the same as OLT templates, but store the firmware configuration for an OLT. Each OLT template refers to one firmware template to configure an OLT's firmware banks.

ONUs

There are several tasks that PON auto executes before it considers an ONU to be Active: Identify, Firmware, Service, Authentication, VLAN, SLA, and DHCP.

Note: The Authentication, DHCP, and Power Variation tasks are skipped in the default PON Automation configuration.

For details refer to the MCMS PON Automation document. PON auto can be configured to skip any of these tasks except for Identify. To do so, click **Edit** on the first tile of the tab labeled ONU automation global settings. Navigate to the desired task to update and change the value for Skip to True or False. If True, PON auto will not execute this task for any ONU it attempts to configure.

The following figure describes ONU automation global settings.

Figure 119 ONU automation global settings



Each task is configurable except for Identify. To modify configuration for a task, click **Edit** on the ONU automation global settings. Select the task to update and edit the desired fields. All configurable tasks have the Skip field. If Skip is True, PON auto will not execute this task for any ONU it attempts to configure. Power Variation has additional configuration parameters for Rogue ONU controls. The Move task has a Stop option. If Stop is True, PON auto halts automation for an ONU that enters the Move task. At this point, automation is halted for this device and operator intervention is required to recover and resume automation for this device.

Each ONU template for PON auto is shown below the global settings. These templates define the state information that PON auto should match on to identify an ONU, and what fields to configure for that ONU. To create a new template, click **Create**, provide the unique ID of the new template, and input any desired fields. To update a template, click the **Edit** button. This will allow for the adjustment of any field in the template except for the ID. The **Clone** button begins creating a new template just like **Create**, but pre-fills all fields except for the template

ID from the original template. Use the **Delete** button to remove a template. A popup will ask for confirmation. Once confirmed, that template will be deleted. This cannot be undone.

ONUs also have an extra layer of templates for firmware settings and service configuration. To view the firmware or service templates, select the Firmware or Service option for Template Type. These are managed the same as ONU templates, but store the firmware or service configuration for an ONU. Each ONU template refers to one firmware template to configure an ONU's firmware banks and one service template to configure an ONU's service links.

Firmware Upgrade Scheduler

The firmware upgrade scheduler tab is used to create or manage jobs for bulk upgrades of ONUs or OLTs in specified time blocks.

Once a job reaches its start time, PON Automation begins setting the bank pointer and the bank versions in the device configuration for the first device. Once a PON Controller has performed the firmware upgrade, PON Automation moves on to the next device and the process repeats for every device in the job. The length of this process varies depending on how the devices are spread across controllers. The PON Controller performs ONU upgrades in parallel based on the controller and the OLT configurations.

The following figure describes the Firmware Upgrade Scheduler.

Figure 120 Firmware Upgrade Scheduler

The screenshot displays the 'Firmware Upgrade Scheduler' interface. At the top, there is a 'Create' button and status filters for 'Scheduled', 'Running', and 'Complete'. The main section shows a job card for 'ONU Upgrade Job'. The job card is divided into three columns: 'Job Info', 'Firmware', and 'Device Summary'. The 'Job Info' column contains details like Description, Create Date, Create User, Scheduled Start Time, Scheduled End Time, Status, Time Remaining, and Job Details. The 'Firmware' column shows the 'FW Bank Ptr' and a table of 'Bank' and 'Version'. The 'Device Summary' column shows a table of 'Status' and 'Count'.

Job Info		Firmware		Device Summary	
Description:	Upgrade for TBIT ONUs	FW Bank Ptr:	0	Status	Count
Create Date:	4/21/2025, 10:09:30 AM	Bank	Version	Pending	2
Create User:	tibit@tibitcom.com	0	R5.0.0	Not Ready	0
Scheduled Start Time:	4/4/2025, 9:01:00 AM	1	R5.0.0	In Progress	0
Scheduled End Time:	-			Paused	0
Status:	Running (33%)			Failure	0
Time Remaining:	0:03:40			Success	1
Job Details:	-			Offline	0

The header portion of the job card contains the job name, status, estimated time to complete, and operation buttons. When the status of a job changes, so will its available operations.

Table 36 Available operations for job card

Input mode	Description
Edit	Modifies the configuration of the selected job

Input mode	Description
Clone	Creates a new job based off the selected job
Pause	Temporarily suspends the selected job from running
Resume	Continue running the selected job
Cancel	Stops the selected job from running permanently
Delete	Removes the selected job from the database

The Configuration section of the card gives an overview of configured job settings. Create Date reports the time and day when a job was created. The Last user displays the username of the user that most recently modified the job. The Firmware section displays the selected firmware bank pointer and the firmware bank versions configured for this job. The Device Summary section displays a quick reference with a count of devices and their status. A user can filter jobs by status using the three check boxes – “Scheduled”, “Running”, or “Complete” – in the top right. A job remains in the Completed status until a user deletes it.

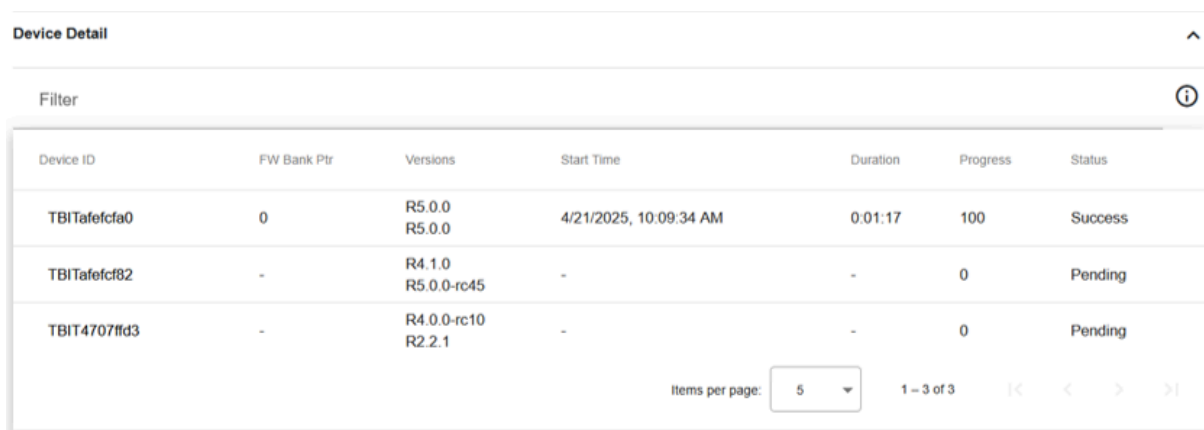
Device Details

Expand the Device Details section of the job card to view a detailed status of each device included in the job.

To view additional information about a device, click the Device ID. The FW Bank Pointer and Versions columns display the firmware settings applied for the current job. The start time column shows the actual time that a device began its upgrades. Duration is a measure of how long the upgrade took for a specific device. Progress is an estimate of a device's upgrade completion out of 100. Status explains which point of the upgrade process the device is in, or the outcome of the upgrade.

The following figure describes device details.

Figure 121 Device Details



The screenshot shows a 'Device Detail' section with a table of device upgrade details. The table has columns for Device ID, FW Bank Ptr, Versions, Start Time, Duration, Progress, and Status. There are three rows of data. Below the table, there is a pagination control showing 'Items per page: 5' and '1 - 3 of 3'.

Device ID	FW Bank Ptr	Versions	Start Time	Duration	Progress	Status
TBITafefca0	0	R5.0.0 R5.0.0	4/21/2025, 10:09:34 AM	0:01:17	100	Success
TBITafefcf82	-	R4.1.0 R5.0.0-rc45	-	-	0	Pending
TBIT4707ffid3	-	R4.0.0-rc10 R2.2.1	-	-	0	Pending

Items per page: 5 1 - 3 of 3

Search tab

The search tab is a user’s view into the database. Users can query the database by device type to discover devices on their network that match a specified attribute for a requested value. The menu items that are listed are retrieved directly from the database and may show small changes when using different databases.

The following figure describes the Search Devices on the Network option.

Figure 122 Search Devices on the Network

Search Devices on the Network

ONU

✓ OLT

Controller

Switch/Router

CPEs

Filter Criteria

Collection*
OLT Configurations

Attribute*
OLT.PON Enable

Operator*
=

Value*
true

Add search criteria

Search

Clear filters

Filter

	Device	OLT Configurations OLT.PON Enable	Change Status
☐			
☐	70:b3:d5:52:3b:52	true	-
☐	e8:b4:70:70:15:74	true	-
☐	e8:b4:70:70:15:76	true	-
☐	e8:b4:70:70:08:9c	true	-
☐	e8:b4:70:70:25:bb	true	-

NOTE: To avoid conflicts, only 1 bulk change can be made at a time.

Download Results

Delete devices

Items per page: 5

1 – 5 of 9

Values that are returned from the database are displayed in a table with the MAC address of the device matching the query. By clicking on the device ID in the table row, users can navigate to the device in the network tab.

There are eight choices of operations for querying a database. “All” searches for all values while “Containing” looks for partial matches. The others are used for values that contain numbers with the exception of “=” which looks for an exact match.

Collections of search queries can be saved to eliminate repetitive filtering. multiple criteria can be added to each search. The saved searches can be edited or deleted.

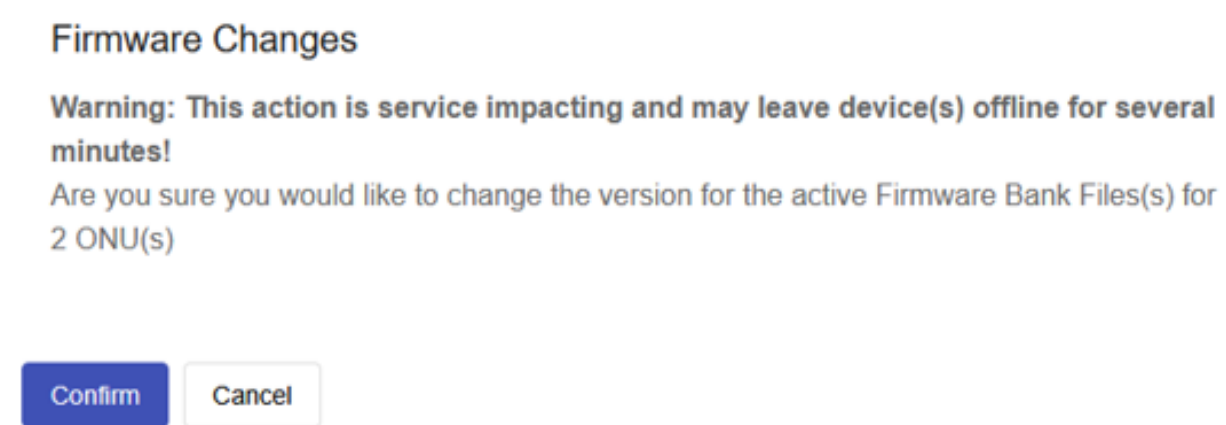
Bulk updating

The Search page also has another function, bulk updating. Most configurable fields can be bulk updated by first searching on that attribute name. If a field is available to be safely bulk updated, the row beneath the header row in the table of results will display an input field. Users can then select the devices they want to update, make their desired change on the input field and save by clicking the save icon. A response from the database will change the 'Change Status' column to indicate if the change was successful, pending or failed to save.

When updating either ONU or OLT configurations for FW bank files, FW bank versions, or FW bank pointers on multiple devices, users will be given a warning pop-up when a change will be made to its current configurations. This notifies users that these services will leave devices offline for several minutes, making it service impacting. Users can then either confirm to continue to save and make changes, or cancel to go back to the Search page.

The following figure describes firmware changes.

Figure 123 Firmware Changes



Note: Only one attribute can be updated at a time.

Bulk deleting

Users can efficiently manage multiple OLT and ONU records by using the bulk delete feature of the search page.

CPE records can be managed using the bulk delete feature. When searching for CPEs, some records can have a status of "CPE Pending Delete". The records selected that have this status are not included when clicking the "Delete devices" button since the UMT Relay is in the process of removing the CPE.

After performing a search based on their preferred criteria, users can select the OLTs they want to remove by checking the corresponding boxes next to each device.

Once the desired records are selected, users can click the Delete devices button located at the bottom of the table to permanently delete the chosen OLTs or ONUs records from the database.

Monitoring tab

The Monitoring tab provides a global, system-wide view of operational data across all devices in the PON network.

Alarms

The Alarms page gathers and displays alarms across all devices on the system. Alarm information such as state, severity, raised, cleared, and acknowledged details is displayed. Purging, acknowledging, and commenting on alarms are operations available from this page from the edit view.

Alarms are categorized by device type and ordered first by severity, then by time. Retrieval of ONU alarms is limited to 20,000 with highest severity prioritized. The content of the table can be filtered by alarm state, alarm severity, device type, and by keyword. All alarm severities and device types are selected by default. All alarm state is set to raised and unacknowledged by default to prioritize display of alarms that may require attention.

The following figure describes the Alarm state.

Figure 124 Alarm state



Alarm count graphics

The alarm count graphics at the top of the table give an overview of alarm counts for each device type.

The following figure describes OLT alarms.

Figure 125 OLT alarms



The bar chart items can be selected and used to quickly apply a filter to the table.

The following figure describes the Alarms table.

Figure 126 Alarms table

Alarm State	Alarm Severity	Device Type	Filter	
All	1:Alert	OLTs		
Device Type	Device ID	Time	State	Severity
OLT	e8:b4:70:70:15:76	4/16/2024, 3:28:10 PM	Cleared	1-ALERT
OLT	e8:b4:70:70:15:76	4/12/2024, 8:17:56 PM	Cleared	1-ALERT
OLT	e8:b4:70:70:15:74	4/2/2024, 6:37:32 PM	Cleared	1-ALERT

List of procedures

Procedures for Global configuration are:

- Procedure 84, "Creating an alarm configuration"
- Procedure 85, "Deleting an alarm configuration"
- Procedure 86, "Editing an SLA profile configuration"
- Procedure 87, "Creating an SLA profile configuration"
- Procedure 88, "Deleting an SLA profile configuration"
- Procedure 89, "Viewing a service profile configuration"
- Procedure 90, "Creating a service profile configuration"
- Procedure 91, "Deleting a service profile configuration"
- Procedure 92, "Creating a downstream QoS mapping"
- Procedure 93, "Creating subscriber provisioning"
- Procedure 94, "Viewing a downstream QoS mapping"
- Procedure 95, "Uploading a picture to the database"
- Procedure 96, "Uploading an OLT firmware image to the database"
- Procedure 97, "Uploading an ONU firmware image to the database"
- Procedure 98, "Uploading the ONU firmware onto the PON Manager"
- Procedure 99, "Uploading a service configuration to the database"
- Procedure 100, "Editing a picture type in the database"
- Procedure 101, "Deleting a picture from the database"
- Procedure 102, "Editing service configuration details in the database"
- Procedure 103, "Deleting a service configuration from the database"
- Procedure 104, "Creating a database connection"
- Procedure 105, "Editing a database connection"
- Procedure 106, "Clearing statistics for a database connection"
- Procedure 107, "Cloning a database connection"

- Procedure 108, “Deleting a database connection”
- Procedure 109, “Replacing an OLT”
- Procedure 110, “Replacing an ONU”
- Procedure 111, “Configuring PON auto switches and routers to skip tasks”
- Procedure 112, “Creating a new template”
- Procedure 113, “Editing a template”
- Procedure 114, “Creating a user”
- Procedure 115, “Editing user information”
- Procedure 116, “Deleting a user”
- Procedure 117, “Creating a user role”
- Procedure 118, “Editing user role assignments”
- Procedure 119, “Deleting a user role”
- Procedure 120, “Editing user password requirements”
- Procedure 121, “Creating an upgrade job”
- Procedure 122, “Editing an existing upgrade job”
- Procedure 123, “Cloning an upgrade job”
- Procedure 124, “Pausing an upgrade job”
- Procedure 125, “Canceling an upgrade job”
- Procedure 126, “Deleting an upgrade job”
- Procedure 127, “Exporting the alarms table”

Procedure 84 Creating an alarm configuration

Create an alarm configuration as required by the network plan.

Overview

This task is performed from the Global Config tab and the Alarms sub-tab, accessible from the left navigation pane. Note that the alarm configurations created with this task are accessed for OLTs and ONUs from the left navigation pane by selecting Network / Topology, then drilling down to the OLT or the ONU and clicking the Monitoring tab and then the Config sub-tab. The following figure describes Alarm Configurations for OLT

Figure 127 Alarm Configuration for OLT

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Alarms.
- 3 Click the desired tab for your device type from the top sub-menu selection.
- 4 Click Create in the Alarm Configurations for Controller pane.
A new empty alarm configuration row displays further down the page.
- 5 Enter a New Configuration ID.
- 6 Use the drop-down lists in each column to populate all fields. Manually enter a value in the Value field.
- 7 Click Save.
The ID displays in the Select Alarm Configuration field above the Create button, and the new configuration row displays above the Edit button.

Procedure 85 Deleting an alarm configuration

Delete an alarm configuration as required by the network plan.

Overview

This task is performed from the Global Config tab and the Alarms sub-tab, accessible from the left navigation pane.

The following figure describes the Alarm Configuration for Controller.

Figure 128 Alarm Configuration for Controller

Alarm Configurations for Controller

DB Config Version: RS.2.0

Edit Configuration ID
Default

Create Duplicate Delete

State Statistics

Filter

Delete	Field Reference	Operator	Value	Severity
☐	Field Reference* CNTL.Pause	Operator* IS	True True	2:Critical* 2:Critical
☐	Field Reference* CNTL.CFG Read Failed	Operator* IS	True True	0:Emergency* 0:Emergency
☐	Field Reference* Logging.TAPI.Console	Operator* IS	DEBUG DEBUG	4:Warning* 4:Warning
☐	Field Reference* Logging.TAPI.File	Operator* IS	DEBUG DEBUG	4:Warning* 4:Warning
☐	Field Reference* Logging.TAPI.Syslog	Operator* IS	DEBUG DEBUG	4:Warning* 4:Warning

Items per page: 5 1 - 5 of 11

Save Cancel Add alarm

Steps

- 1 In the second menu row from the top, click the tab for your device type: **Controllers**, **OLTs**, or **ONUs**.
- 2 In the **Alarm Configurations for Controller** pane, in the **Select Alarm Configuration** field, use the drop-down list to select the configuration to be deleted.
- 3 Click **Delete**, then **Delete** again .

*The configuration is removed from the list, and the **Default** configuration displays in the **Select Alarm Configuration** field.*

Procedure 86 Editing an SLA profile configuration

Edit an SLA profile configuration as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click SLAs.
- 3 Use the drop-down list to select a configuration in the SLA Profile Configurations pane, in the Select Sla Configuration field.
- 4 Click Edit at the bottom of the pane.
A collection of editable fields displays further down the page.
- 5 Use the arrows or drop-down lists in each field to edit the fields as required.
- 6 Click Save.

The ID still displays in the Select Sla Configuration field above the Create button, and the values from each field display above the Edit button.

Procedure 87 Creating an SLA profile configuration

Create an SLA profile configuration as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click SLAs.
- 3 Click Create in the SLA Profile Configurations pane.
A collection of editable fields displays further down the page.
- 4 Use the arrows or drop-down lists in each field to populate the fields.
- 5 Enter the ID above the Create button in the New Configuration ID field.
- 6 Click Save below the new SLA profile configuration fields.

The ID displays in the Select Sla Configuration field above the Create button, and the values from each field in the new configuration display above the Edit button.

Procedure 88 Deleting an SLA profile configuration

Delete an SLA profile configuration as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click SLAs.
- 3 Use the drop-down list to select the configuration to be deleted in the SLA Profile Configurations pane, in the Select Sla Configuration field.
- 4 Click Delete and then Delete again.

The configuration is removed from the list, and the Min configuration displays in the Select Sla Configuration field.

Procedure 89 Viewing a service profile configuration

View a service profile configuration to see its diagram and text-based details as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Services.
- 3 Use the drop-down list to select the configuration to be viewed in the Service Profile Configurations pane, in the Select Service Configuration field.
- 4 To view a diagram of the data flow path for the selected configuration (if the data flow path has been created):
 - Scroll to the bottom of the page.
 - To adjust the view, use the tools in the left side of the window, or click to drag the image and use the mouse wheel to zoom.
 - To view the behavior of a specific ONU with the selected configuration, click in the Search ONU field, make a selection from the drop-down list that displays, and click the blue arrow to the right of the field. The display might take a moment to refresh.
- 5 To view more details about the management entities (MEs):
 - Click the chevron to the left of OMCI to display the list.

To the right of each ME in the list are the associated IDs, which can be clicked for viewing and editing.
 - Click an ME from the list.

The OMCI Specification pane displays on the right.
 - Scroll through the pane to read more, and click the chevron next to any item in the Attributes list for a description of the attribute.
- 6 To change the arrangement of the MEs:
 - Click Edit.

To the left of the ME's chevron, toggle arrows display for the up and down directions.
 - Click a toggle arrow to move the ME up or down, one row at a time.
 - Click Save to save the new arrangement or Cancel to return to the previous arrangement.

Procedure 90 Creating a service profile configuration

Create a service profile configuration as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Services and then click the Profiles sub-tab.
- 3 Click Create in the Service Profile Configurations pane.
- 4 Enter the ID above the Create button in the New Configuration ID field.
- 5 Click the chevron to the left of Header to display the configuration fields.
- 6 Enter the Title and Version for the new configuration in their respective fields.
- 7 Click the ellipsis to the right and then select Add input for Inputs (below the Version field).
- 8 Click Add.
- 9 Repeat the previous two steps for Ports and Compatibility.
- 10 Click the chevron to the left of OMCI to display the configuration fields.
- 11 Edit the fields as needed.
- 12 To add a management entity:
 - Click Add management entity to display the window.
 - Use the drop-down list to make a selection in the Select Management Entity section. Refer to the Attributes descriptions further down the page.
 - Enter an ID in the Enter ME ID(s) section.
 - Click Add.
- 13 Click Save in the Service Profile Configurations pane.

The new service configuration ID displays in the Select Service Configuration field above the Create button.

Procedure 91 Deleting a service profile configuration

Delete a service profile configuration as required by the network plan.

Overview

This task is performed from the Profiles tab, accessible from the left navigation pane by selecting the Global Config tab and the Services sub-tab.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Services and then click the Profiles sub-tab.
- 3 Use the drop-down list to select the configuration to be deleted in the Service Profile Configurations pane.
- 4 Click Delete and then click Delete again.

The configuration is removed from the list.

Procedure 92 Creating a downstream QoS mapping

Create a downstream QoS mapping as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Services and then click the Downstream QoS Map sub-tab.
- 3 Click Create in the Downstream QoS Map Configurations pane.
- 4 Enter the ID above the Create button in the New Configuration ID field.
- 5 Use the drop-down lists to set the offset values as needed in the OLT-Service Offset column.
- 6 Click Save.

Procedure 93 Creating subscriber provisioning

Create subscriber provisioning as required by the network plan.

Overview

The following figure describes creating subscriber provisioning.

Figure 129 Creating subscriber provisioning

ciena

Dashboard

Network

Global Config

Alarms

SLAs

Services

Files

Databases

Devices

Automation

Accounts

Search

Monitoring

Logout

Collapse

Current Database

Version: R6.0.1

Alarms

SLAs

Services

Files

Databases

Devices

Automation

Create

Replace

Inventory

Create Configuration

1 Choose a Configuration Type

2 Configuration Identification

3 Configuration Template

4 Service Package

5 Submit

Subscriber Name*

Subscriber 09AL4Y

Serial Number

Registration ID

Back

Next

MicroClimate Management System
MCMS 6.2
Copyright© 2024 - 2026 Ciena® Corporation

PON Manager User Guide
323-1961-302 Standard Revision A
March 2026

Note: Entering a device ID (Serial Number, MAC Address, or Reg ID) is optional. Provision a subscriber with just a name if required.

Steps

- 1 Select Subscriber.
- 2 Select the PON type: XGS-PON or 10G EPON
- 3 Enter a name, vendor and serial number, or EPON MAC address.
- 4 Click Submit.

Procedure 94 Viewing a downstream QoS mapping

View a downstream QoS mapping as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Services and then click the Downstream QoS Map sub-tab.
- 3 Use the drop-down list to select the configuration to view in the Downstream QoS Map Configurations pane, in the Select Downstream QoS Map Configuration field.

The table below the field displays the VLAN Priority Bit Values (CoS values) and their corresponding OLT-Service Offset values.

Procedure 95 Uploading a picture to the database

Upload a picture to the database as required by the network plan.

Requirements

The system supports all MIME types.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Files and then click the Pictures sub-tab.
- 3 Click Upload.
- 4 Choose file.
- 5 Navigate to and then select the required image.
- 6 Click Open.
- 7 Use the drop-down list to select the type in the Device Type field.
- 8 Click Save.

The image displays in the table. Use the arrow keys at the bottom of the table to locate the image if needed.

Procedure 96 Uploading an OLT firmware image to the database

Upload an OLT firmware image to the database as required by the network plan.

Requirements

The system supports only *.bin files.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Files and then click the OLT Firmware sub-tab.
- 3 Click Upload.
- 4 Choose file.
- 5 Navigate to and then select the required image.
- 6 Click Open.
- 7 Use the drop-down list to select the model.
- 8 Enter the version.
- 9 Click Save.

The image displays in the table. Use the arrow keys at the bottom of the table to locate the image if needed.

Procedure 97 Uploading an ONU firmware image to the database

Upload an ONU firmware image to the database as required by the network plan.

Requirements

Ensure that the file type of the firmware image is .bin or .img.

Obtain the version as captured in the version field embedded in the firmware.



CAUTION
Risk of upload failure

If the version is not entered correctly the PON Controller continues to attempt an upgrade in a continuous loop.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Files and then click the ONU Firmware sub-tab.
- 3 Click Upload.
- 4 Click Choose file.
- 5 Navigate to the required image and then select it.
- 6 Click Open.
- 7 Use the drop-down menu to select the vendor.

If	Then
The drop down menu does not have the desired value.	Enter the vendor name in the Custom Vendor field.

- 8 Use the drop-down menu to select the model.

If	Then
The drop down menu does not have the desired value.	Enter the model name in the Custom Model field.

- 9 Enter the version.
- 10 Click Save.

The image displays in the table.

Procedure 98 Uploading the ONU firmware onto the PON Manager

Upload the ONU firmware onto the PON Manager as required.

Requirements

Before upgrading the ONU firmware by means of OMCI, the ONU firmware needs to first be uploaded onto MCMS PON Manager.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click the Files tab then click the ONU Firmware sub-tab.
- 3 Choose the location of where the ONU firmware is located.
- 4 Enter the vendor, model and version of the ONU firmware.
- 5 Click on the **Save** button when done.

Procedure 99 Uploading a service configuration to the database

Upload a service configuration to the database as required by the network plan.

Requirements

Ensure that ONUs are upgraded to the latest firmware.

The service configuration must have a .json extension.

When naming the new ONU service config file, the prefix “SRV-“and the suffix “-CFG” must be removed from the file name. Otherwise, the MCMS PON Manager cannot upload the files.

The database only recognizes the first 14 characters of the service config file name. The service config file name can be longer, but it is ignored and not stored in the database.

Overview

When developing a new ONU service configuration file, it is typical to use an existing service config file and then make the necessary modifications. The base service config files starts with “SRV-“and ends with “-CFG”.

This task is performed from the Service Configs tab, accessible from the left navigation pane by selecting the Global Config tab and the Files sub-tab.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Files and then click the Service Configs sub-tab.
- 3 Click Upload.
- 4 Click Choose file.
- 5 Navigate to and then select the desired file.
- 6 Click Open.
- 7 Enter the ID in the Service ID field.
- 8 Click Save.

The file displays in the table. Use the arrow keys at the bottom of the table to locate the file if needed.

Procedure 100 Editing a picture type in the database

Edit a picture type in the database as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Files and then click the Pictures sub-tab.
- 3 Click Edit.
- 4 Click the drop-down list and then select the Device Type in the Device Type column.
- 5 Click Save.

The new device type for the image displays in the table. Use the arrow keys at the bottom of the table to locate the image if needed.

Procedure 101 Deleting a picture from the database

Delete a picture from the database as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Files and then click the Pictures sub-tab.
- 3 Click Edit.
- 4 Select the check box in the Delete column for the desired picture. If the file is currently saved to a device's configuration, an info icon displays instead of a check box.
- 5 Click Save, and then click Delete.

The picture is deleted from the table.

Procedure 102 Editing service configuration details in the database

Edit service configuration details in the database as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Files and then click the Service Configs sub-tab.
- 3 Click Edit.
- 4 Enter the version, if needed.
 - **Note:** All configurations must have a value in the Version column before the Save button is activated.
- 5 Enter the title, if needed.
 - **Note:** All configurations must have a value in the Title column before the Save button is activated.
- 6 Click Save.

The new details for the configuration display in the table. Use the arrow keys at the bottom of the table to locate the configuration if needed.

Procedure 103 Deleting a service configuration from the database

Delete a service configuration from the database as required by the network plan.

Requirements

This task is performed by selecting the check box to the left of the configuration's ID. If the ID is currently saved to a device's configuration, an info icon displays instead of a check box. Clicking this icon displays a list of up to ten devices which have the configuration file saved to their configurations. The file must be removed from all device configurations before it can be deleted.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Files and then click the Service Configs sub-tab.
- 3 Click Edit.
- 4 Select the desired check box in the Delete column.
- 5 Click Save and then click Delete.

The ID is deleted from the table.

Procedure 104 Creating a database connection

Create a database connection as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Databases and then click the Manage sub-tab.
- 3 Click Create at the bottom of the Manage Database Connections pane.
The Create Database pane displays.
- 4 Enter an ID in the Database ID field.
 - **Note:** The ID in the Database ID field becomes the name of the database as it will appear in MCMS PON Manager.
- 5 Use the drop-down lists or enter text for the remaining fields in the pane.
- 6 Click Save.

The Manage Database Connections pane displays. The details of the new database can be viewed by clicking the drop-down list in the Select database field at the top of the pane and selecting the database ID.

Procedure 105 Editing a database connection

Edit a database connection as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Databases and then click the Manage sub-tab.
- 3 Click the drop-down list to select the desired database to edit at the top of the Manage Database Connections pane, in the Select database field.
- 4 Click Edit at the bottom of the Manage Database Connections pane.
- 5 Use the drop-down lists or enter text to edit the fields as needed.
- 6 Click Save.

The Manage Database Connections pane displays. The new details can be viewed by clicking the drop-down list in the Select database field at the top of the pane and selecting the database ID.

Procedure 106 Clearing statistics for a database connection

Clear statistics for a database connection as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Databases and then click the Manage sub-tab.
- 3 Click the drop-down list to select the desired database at the top of the Manage Database Connections pane, in the Select database field.
- 4 Click Clear Statistics at the bottom of the Manage Database Connections pane.

All statistics for the selected database connection clear.

Procedure 107 Cloning a database connection

Clone a database connection as required by the network plan.

Overview

This task is performed from the Manage tab, accessible from the left navigation pane by selecting the Global Config tab and the Databases sub-tab.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Databases and then click the Manage sub-tab.
- 3 Click the drop-down list to select the database to clone at the top of the Manage Database Connections pane, in the Select database field.
- 4 Click Clone.
The Create Database pane displays.
- 5 Enter an ID in the Database ID field.
 - **Note:** The ID in the Database ID field becomes the name of the database as it will appear in MCMS PON Manager.
- 6 Use the drop-down lists or enter text to change the values in the remaining fields in the pane, as needed.
- 7 Click Save.

The Manage Database Connections pane displays. The details of the new database can be viewed by clicking the drop-down list in the Select database field at the top of the pane and selecting the database ID.

Procedure 108 Deleting a database connection

Delete a database connection as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Databases and then click the Manage sub-tab.
- 3 Click the drop-down list to select the database to delete at the top of the Manage Database Connections pane, in the Select database field.
- 4 Click Delete, and then click Delete again.

The database connection is deleted, and the ID no longer displays from the drop-down list in the Select database field at the top of the pane.

Procedure 109 Replacing an OLT

Replace an OLT as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Devices and then click the Replace sub-tab.
- 3 Select the Device Type, and then click Next.
- 4 Select the Old Device, and then click Next.
- 5 Enter the MAC Address for the new device
- 6 Enter a name for the device in the New Name field.
- 7 Click Next.
- 8 Click Save.

Procedure 110 Replacing an ONU

Replace an ONU as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Devices and then click the Replace sub-tab.
- 3 Select the Device Type, and then click Next.
- 4 Select the Old Device, and then click Next.
- 5 Enter the MAC Address for the new device
- 6 Enter a name for the device in the New Name field.
- 7 Click Next.
- 8 Click Save.

Procedure 111 Configuring PON auto switches and routers to skip tasks

Configure PON automation switches and routers to skip tasks as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Automation and then click the desired sub-tab.
- 3 Click Edit in the desired Global Settings pane.
- 4 Set the desired task to skip to either true, to not execute that task, or false, to execute that task. If true, PON auto will not execute this task for any Switch or router it attempts to configure.
- 5 Click Save.

Procedure 112 Creating a new template

Create a new template as required by the network plan

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Automation and then click the desired sub-tab.
- 3 Click Create.
- 4 Enter a Template ID for the template.
- 5 Complete the remaining fields as required.

Procedure 113 Editing a template

Edit a template as required by the network plan.

Steps

- 1 Click Global Config from the left navigation pane.
- 2 Click Automation and then click the desired sub-tab.
- 3 Click the Edit button under the desired template.
- 4 Edit the desired fields.
- 5 Click Save.

Procedure 114 Creating a user

Create a user as required by the network plan.

Requirements

Perform this task as administrator.

Steps

- 1 Click Accounts from the left navigation pane.
- 2 Click Administration and then click the Users sub-tab.
- 3 Click Create.
- 4 Enter the email address for the new user.
- 5 Enter the first name and the last name for the new user.
- 6 Enter the password for the new user.
- 7 Confirm the password for the new user.
- 8 Choose the role or roles of the new user from the drop-down list.
- 9 Click Save.

*The new user (minus the password) appears in the **All Users** window.*

Procedure 115 Editing user information

Edit user information as required by the network plan.

Requirements

Perform this task as administrator.

Steps

- 1 Click Accounts from the left navigation pane.
- 2 Click Administration and then click the Users sub-tab.
- 3 Click Edit.
- 4 Edit the information related to one or more users.
Note: To remove an Administrators role for yourself, you must use a different administrator's account.
- 5 Click Save.

The changes (minus the password) appear in the All Users window.

Procedure 116 Deleting a user

Delete a user as required by the network plan.

Requirements

Perform this task as administrator.

Steps

- 1 Click Accounts from the left navigation pane.
- 2 Click Administration and then click the Users sub-tab.
- 3 Click Edit.
The Edit window opens.
- 4 Select the checkbox in the left-most column for one or more users to delete.
The checkbox turns red and the inputs for the selected users become disabled.
- 5 Click Save.
The checked users are permanently deleted.

Procedure 117 Creating a user role

Create a user role as required by the network plan.

Requirements

Perform this task as administrator.

The following figure describes Creating a new user role.

Figure 130 Create a new user role

Create new role

Name*

Role name is required

Users

Permission Type	View (UI)	Read (API)	Update (API)	Create (API)	Delete (API)	All
Dashboard						
Dashboard	☒	☒	☐	☐	☐	☐
Network						
Controllers	☒	☒	☐	☐	☐	☐
Olts	☒	☒	☐	☐	☐	☐
Onus	☒	☒	☐	☐	☐	☐
Switches/Routers	☒	☒	☐	☐	☐	☐
Cascading	☒	☒	☐	☐	☐	☐
Global Config						
Alarms	☒	☒	☐	☐	☐	☐

Save

Cancel

Steps

- 1 Click Accounts from the left navigation pane.
- 2 Click Administration and then click the Roles sub-tab.
- 3 Click Create.
- 4 Enter the unique name for the new role.
- 5 Optionally, assign users to the role using the drop-down list in the Users field.
- 6 Enable and disable permissions for the role as needed in the Permission Type table.

Note: All View permissions are enabled by default (except for Accounts Admin) and cannot be disabled except for Accounts Admin, Search and the Global Config settings. All Read permissions are enabled by default (except for Accounts Admin) and cannot be disabled except for Accounts Admin.

- 7 Click Save.

Procedure 118 Editing user role assignments

Edit user role assignment as required by the network plan.

Requirements

Perform this task as administrator.

Steps

- 1 Click Accounts from the left navigation pane.
- 2 Click Administration and then click the Users sub-tab.
- 3 Click the three vertical dots in the Edit column for the user role you wish to edit.
- 4 Click Users.
- 5 Select a user on the left, and then click the green arrow to assign the role to that user.
The selected user moves to the right of the window.
- 6 Select a user on the right and click the red arrow to unassign the role from that user.
The selected user moves to the left of the window.
- 7 Click Save.

Procedure 119 Deleting a user role

Delete a user role as required by the network plan.

Requirements

Perform this task as administrator.

Overview

The Delete option on the Edit menu only appears when the role contains no users. To delete a role that contains users, you must first remove the users from the role.

Note: The built-in Administrators and Read Only roles can never be deleted.

Steps

- 1 Click Accounts from the left navigation pane.
- 2 Click Administration and then click the Users sub-tab.
- 3 Click the three vertical dots in the Edit column for the user role you wish to delete.
*The **Edit** menu opens.*
- 4 Click Delete and then click Delete again.

Procedure 120 Editing user password requirements

Edit user password requirements as required by the network plan.

Requirements

Perform this task as administrator.

Overview

Changes you make here affect creating editing user profiles.

Steps

- 1 Click Accounts from the left navigation pane.
- 2 Click Administration and then click the Authentication sub-tab.
- 3 Click Edit.
- 4 Edit the requirements.
- 5 Click Save.

The system displays a message stating the updated password requirements are saved. Verify your changes in the Minimum Password Requirements window on the Administration tab.

Procedure 121 Creating an upgrade job

Create an upgrade job as required by the network plan.

Requirements

Perform this task as administrator.

Overview

If ONU is selected for upgrade type and the global PON Mode for PON manager is set to XGS-PON & 10G EPON, a PON mode selection is required.

Steps

- 1 Select the device type (either OLT or ONU) and click Create.
The upgrade type can only be set when creating a job. This field cannot be changed when editing after the job has already been created.
- 2 Configure the job settings.
 - a. Specify a unique name for the job and provide an optional description if desired.
 - b. Set the firmware bank and versions to apply during the upgrade.
 - c. Select a start time for the job.
Note: The device upgrades might not start exactly at the start time provided. Factors like the number of devices in the job, and PON Controller processing availability impacts the true start time. End time is an optional field used to stop upgrades at a set time.
- 3 Search for devices to upgrade.

Figure 131 Job Info

 Upgrade Type
2  Configure

Job Info

Name*

ONU firmware upgrade, April 21, 2025, 10:18:07

Description

Firmware

Bank Pointer*

1 

Bank 0 Version*

R5.0.0 [vendor: TBIT] [models: HBG7100A] 

Bank 1 Version*

R5.5.5 [vendor: TBIT] [models: TBITafefcfa0] 

Schedule

[Use current time](#)

Start Time

04/21/2025, 10:18 AM 

End Time

mm/dd/yyyy, --:-- -- 

Note: Like the Search page, a user can find devices by field values using filter criteria. Saved filters are shared with the Search page and a user can apply them to complete the frequently used criteria. For upgrade jobs, it is useful to know the bank pointer and bank versions of a device. If the configuration of the active bank is changing, it might impact a service. Equipment ID and Vendor also provide useful information as they must be compatible with the selected firmware for ONU jobs. Select any device to include it in the upgrade job. To continue, select at least one device.

- 4 To review the configuration and check for any warnings or errors, enter the validation step. If changes are made to the firmware configuration or device selection, the user must re-enter the validation step before saving.

Figure 132 Filter Criteria

Filter Criteria

Collection* ONU States Attribute* ONU.Vendor Operator* All Value test

Collection* ONU States Attribute* ONU.Equipment ID Operator* All Value X

Collection* ONU States Attribute* ONU.FW Bank Ptr Operator* All Value X

Collection* ONU States Attribute* ONU.FW Bank Versions Operator* All Value X

Add search criteria Search Q Clear filters

Device	ONU States ONU.Vendor	ONU States ONU.Equipment ID	ONU States ONU.FW Bank Ptr	ONU States ONU.FW Bank Versions
☐ AZRS00002710	AZRS	ONT150A 1.2 06/2021	0	3.2.36 3.2.36
☐ BFWS00131415	BFWS	ONT150A 1.0 04/2020	0	3.2.30 3.2.30
☒ TBITafefcfa0	TBIT		0	R5.0.0 R5.0.0
☒ TBITafefcf82	TBIT		0	R4.1.0 R5.0.0-rc45
☒ TBIT4707ffd3	TBIT		0	R4.0.0-rc10 R2.2.1

Items per page: 5 1 - 5 of 8

Note 1: A warning message is displayed for OLT or ONU jobs if the active bank is changed or if the firmware in the active bank is changed for any devices included in the job. Warnings are shown in yellow and will not prevent the job from being saved. To resolve warnings, either remove the affected devices from the job, or configure the job in such a way that the active bank is not altered on any devices included in the job.

Note 2: An error message is displayed for ONU jobs if an ONU's vendor or model does not match the vendor or model of any of the firmware versions selected for

the job. Errors are shown in red and must be fixed before saving is allowed. To fix an error either remove affected ONUs from the job or chose firmware options that are compatible with all selected ONUs. The following figure describes the Review dialogue.

Figure 133 Review

Review

Configuration

Name:

ONU firmware upgrade, April 21, 2025, 10:18:07

Description:

-

Scheduled Start Time:

4/21/2025, 10:18:00 AM

Scheduled End Time:

-

Devices to Upgrade:

3

Firmware

FW Bank Ptr:

1

Bank	Version
0	R5.0.0-ONU-FW.bin
1	R5.0.0-rc45-ONU-FW.bin

Warning: The job will be service affecting. Active banks will be modified for the following ONUs:

TBIT4707ff3

Active bank is changing from 0 to 1, Firmware version in the active bank is changing from R2.2.1 to R5.5.5

TBITafcf82

Active bank is changing from 0 to 1, Firmware version in the active bank is changing from R5.0.0-rc45 to R5.5.5

TBITafcf90

Active bank is changing from 0 to 1, Firmware version in the active bank is changing from R5.0.0 to R5.5.5

Procedure 122 Editing an existing upgrade job

Edit an existing upgrade job as required by the network plan.

Overview

A user can edit a job before it begins, while its status is listed as Scheduled. A user can modify any value apart from the job name.

Steps

- 1 Click the dark blue Edit icon at the top right of the job card.

Procedure 123 Cloning an upgrade job

Clone an upgrade job as required by the network plan.

Overview

A user can clone a job at any stage of progression. This operation allows a user to quickly create a new job based off another job.

Steps

- 1 To clone a job, click the pink Clone icon at the top right of the job card.

Procedure 124 Pausing an upgrade job

Pause an upgrade job as required by the network plan.

Overview

A user can pause a job while it is running. While a job is paused, it temporarily stops processing upgrades.

Steps

- 1 To pause a job, click the blue Pause button at the top right of the job card.
- 2 To resume a job, click the blue Resume button at the top right of the card.

Procedure 125 Canceling an upgrade job

Cancel an upgrade job as required by the network plan.

Overview

A user can cancel a job while it is in the Scheduled or Running state. Canceling a job sends a signal to stop processing upgrades. Once the job has been successfully canceled, it moves to Complete.

Steps

- 1 To cancel a job, click the red Cancel icon at the top right of the job card.

Procedure 126 Deleting an upgrade job

Delete an upgrade job as required by the network plan.

Overview

A user can delete a job once it is completed. Deleting a job removes all the records and detailed device task states associated with that job.

Steps

- 1 To delete a job, click the red Delete icon at the top right of the job card.

Procedure 127 Exporting the alarms table

Export the alarms table as required by the network plan.

Overview

Export the Alarms Table to a spreadsheet in Microsoft Excel and Comma-separated values format.

Steps

- 1 Click the Download Table button.
- 2 Select either the csv or xlsx format.

MicroClimate Management System

PON Manager User Guide

Copyright© 2024 - 2026 Ciena® Corporation. All rights reserved.

MCMS 6.2

Publication: 323-1961-302

Document Status: Standard

Revision A

Document release date: March 2026

CONTACT CIENA

For additional information, office locations, and phone numbers, please visit the Ciena web site at **www.ciena.com**

