Cisco Routed PON Manager

User Guide

© 2024 Cisco and/or its affiliates. All rights reserved.

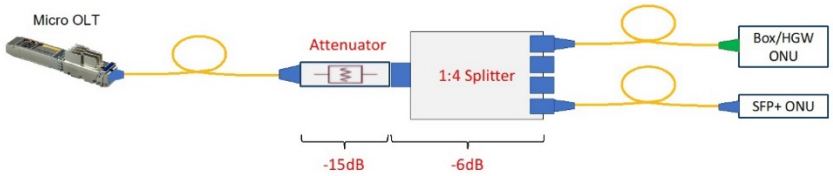
CAUTION

Refer to the Install Guide before Installation

Warranty Notice: Device Attenuation Required

Do not connect OLT directly to ONUs without proper attenuation. PON transceivers will be **permanently damaged** unless connected with **minimum** 16dB attenuation (20dB recommended). **Damage from optical overload will void warranty.**

Combination of attenuator and splitters can provide required attenuation. Refer to the example:



523682

© 2024 Cisco and/or its affiliates. All rights reserved.

Table of Contents

Table of Contents 3
References 11
Document Purpose 12
Introduction 13
  Routed PON Manager 13
  Routed PON REST API 14
  MongoDB Datastore 15
Architecture Overview 15
  Routed PON Manager Web Application 16
  Routed PON Manager Web Server and API 17
    Private APIs 17
  MongoDB 17
Installation 18
  Requirements and Dependencies 18
    Supported Browsers 18
    Supported Operating Systems 18
    Required Packages 19
    Python Package Dependencies (pip3) 20
  Package Contents 21
  Installation Methods 22
    Debian Package 23
      Prerequisites: 23
      Installation Steps: 23
      Configuration steps: 25
        Using Alternate Certificates: 28
      Validation Steps after Installation: 28
      Installation Notes: 28
      uninstall 30
MongoDB Installation 31

© 2024 Cisco and/or its affiliates. All rights reserved.

Security 32
TCP/IP Ports and Network Services 32
Role Based Access Control 32
HTTPS 33
Authentication 33
Session Expiration 34
Session Purging 34
System Diagrams 34
User Authentication and Session Establishment 34
Authentication for Existing Session 35
Authentication Failure 36
Django Key 38
Web Interface 39
Logging In for the first time 39
Creating and Managing Accounts 39
Password Requirements 40
Logging Out 41
Version 41
Site Customization 42
Site Navigation 43
Auto Refresh 43
PON Controller Database Compatibility 44
Dashboard 45
Alarms Summary 46
Network 47
Devices 47
Device Navigation Tree 48
ONU Device States 50
Hierarchy View 51
PON Controller 52
Summary 52

© 2024 Cisco and/or its affiliates. All rights reserved.

Identification 53
Configure Controller Name 53
Configure Controller Picture 53
Configure Location Coordinates 54
Firmware 54
Authentication 55
OLT Inventory 57
Add OLT to Inventory 57
Remove OLT from Inventory 58
Monitoring 58
Alarms 58
Logs 58
Operations 59
Pause a Controller 59
Shutdown a Controller 60
Delete a Controller 60
Switch/Router 60
Summary 60
Identification 60
Configure Switch/Router Name 61
Configure Switch/Router Picture 61
Configure Location Coordinates 61
OLT Inventory 62
Add OLT to Inventory 63
Remove OLT from Inventory 63
Operations 63
Delete a Switch/Router 64
OLT 65
Summary 65
Provisioned Bandwidth Summary 66
Identification 67

© 2024 Cisco and/or its affiliates. All rights reserved.

Configure OLT Name 67
Configure OLT Picture 67
Configure Location Coordinates 67
Firmware 68
OLT Firmware 68
Upgrade OLT Firmware 68
Disable OLT Firmware Upgrade 68
ONU Firmware 69
Services 69
Edit Mode 71
Ports 72
NNI Networks 73
Config 73
PON Flood Type 75
EPON Flooding 75
GPON Flooding 76
Add An Existing NNI Network To Inventory 76
Add a new NNI Network to Inventory 76
Remove an NNI Network from Inventory 76
Enable DHCP Relay 76
Enable PPPoE 77
Add Static MAC Addresses 77
MAC Addresses 77
ONU Inventory 78
Add ONU to Inventory 79
Remove ONU from Inventory 80
Disable Serial Number 80
Update ONU IDs, Alloc ID, and LLIDs in Inventory 81
Monitoring 81
ONUs Stats 82
Operations 84

© 2024 Cisco and/or its affiliates. All rights reserved.

Reset the OLT 85
Delete the OLT 85
Allow ONU Registration 86
Enable ONU Serial Number/Upstream Laser 86
Rogue ONU 86
Identification 87
Configure ONU Name 88
Configure ONU Picture 88
Configure Location Coordinates 88
Firmware 89
Upgrade ONU Firmware 89
Disable ONU Firmware Upgrade 90
CPEs 90
Services 91
OLT Services 92
Enable OLT Service Ports 92
Service Configuration Mismatches 93
Set the Downstream QoS Map 93
Set the SLA 93
Configure VLAN Tagging 94
Configure VLAN Priority 94
Add a VLAN 94
Remove a VLAN 95
Enable DHCP Relay 95
Enable PPPoE 96
ONU Services 96
Set the ONU Service Configuration 97
Provisioned Bandwidth Summary 98
MIB Current/Reset 98
MIB Config 98
Ports 99

© 2024 Cisco and/or its affiliates. All rights reserved.

Monitoring 101
Operations 102
Reset the ONU 103
Allow ONU registration 103
Disable ONU Laser 104
Delete the ONU 104
Statistics 105
Displaying Graphs 107
Real-Time Statistics 108
ONUs under OLT stats 108
Grafana 109
Prerequisites 109
Grafana Dashboard Links 109
Upgrading Routed PON Manager 111
Alarms 111
Logs 112
Global Config 112
Alarms 112
View and Edit Alarm Configurations 113
Create an Alarm Configuration 114
Delete an Alarm Configuration 115
SLAs 115
View and Edit SLA Configurations 116
Create an SLA Configuration 116
Delete an existing configuration 117
Services 117
Profiles 117
View and Edit Service Profile Configurations 118
Create a Service Profile Configuration 120
Delete an existing Service Profile Configuration 120
View and Edit Downstream QoS Mappings 122

© 2024 Cisco and/or its affiliates. All rights reserved.

Create a Downstream QoS Mapping 122
Delete an existing Downstream QoS Mapping 122
Files 122
Uploading 123
Firmware 124
Services 124
Editing and Deleting 124
Pictures 125
Firmware 125
Services 126
Databases 126
Initialize 127
Update 128
Manage 129
Add a New Database Connection 130
Modify an Existing Database Connection 130
Clone an Existing Database Connection 130
Delete an Existing Database Connection 130
Configurable Fields 130
Devices 132
Create 132
Inventory 133
Search 133
Bulk Updating 134
Accounts 135
Personal 135
Change Password 136
Administration 136
Users 136
Create a New User 137
Modify an Existing User 138

© 2024 Cisco and/or its affiliates. All rights reserved.

Delete a User 139
Roles 139
Create a New Role 141
View Permissions 142
Modify an Existing Role’s Users 142
Modify an Existing Role’s Permissions 143
Modify an Existing Role’s Session Expiry Age 144
Delete a Role 144
Logs 144
Sessions 145
Display Preferences 146
Timestamp Format 146
PON Mode 147
User Configuration 147

© 2024 Cisco and/or its affiliates. All rights reserved.

References

ID	Document Description
Django	Django Documentation <https://docs.djangoproject.com/en/>.
Cisco Routed PON Installation Guide	Cisco Routed PON Installation Guide
Cisco Routed PON Manager User Guide	Cisco Routed PON Manager User Guide
Cisco Routed PON REST API	Cisco Routed PON REST API Developer Guide
TR-383	TR-383 Common YANG Modules for Access Networks, Issue 1, Amendment 3, October 2020, <https://www.broadband-forum.org/technical/download/TR-383_Amendment-3.pdf>.
TR-385	TR-385 ITU-T PON YANG Modules, Issue 2, October 2020, <https://www.broadband-forum.org/technical/download/TR-385_Issue-2.pdf.pdf>.

© 2024 Cisco and/or its affiliates. All rights reserved.

Document Purpose

This document serves as the User Guide for the Routed PON Manager software. It describes the architecture, installation, setup, security features, and usage information for the PON Manager. This document is intended for users of the PON Manager who are responsible for configuring Controller, OLT, and ONU devices and subscriber services on the PON Network. The document is also intended for system administrators for the purpose of installation and maintenance for the Routed PON Manager Web Server.

Although the open-source MongoDB is shown as part of the Routed PON architecture, MongoDB is not provided as part of the Routed PON Manager package. MongoDB is a dependency of the PON Manager. Installation, maintenance, and operation of MongoDB is considered out of scope.

© 2024 Cisco and/or its affiliates. All rights reserved.

Introduction

The Cisco Routed PON Manager is the management solution for PON Networks. The Routed PON architecture is shown in Figure 1 and consists of the Routed PON Manager graphical user interface, Routed PON Netconf Server, and Routed PON Controller. Together these components provide a complete network management solution for provisioning and monitoring Cisco Routed PON OLT devices, as well as the subtended ONUs compliant with the XGS-PON and 10G-EPON standards.

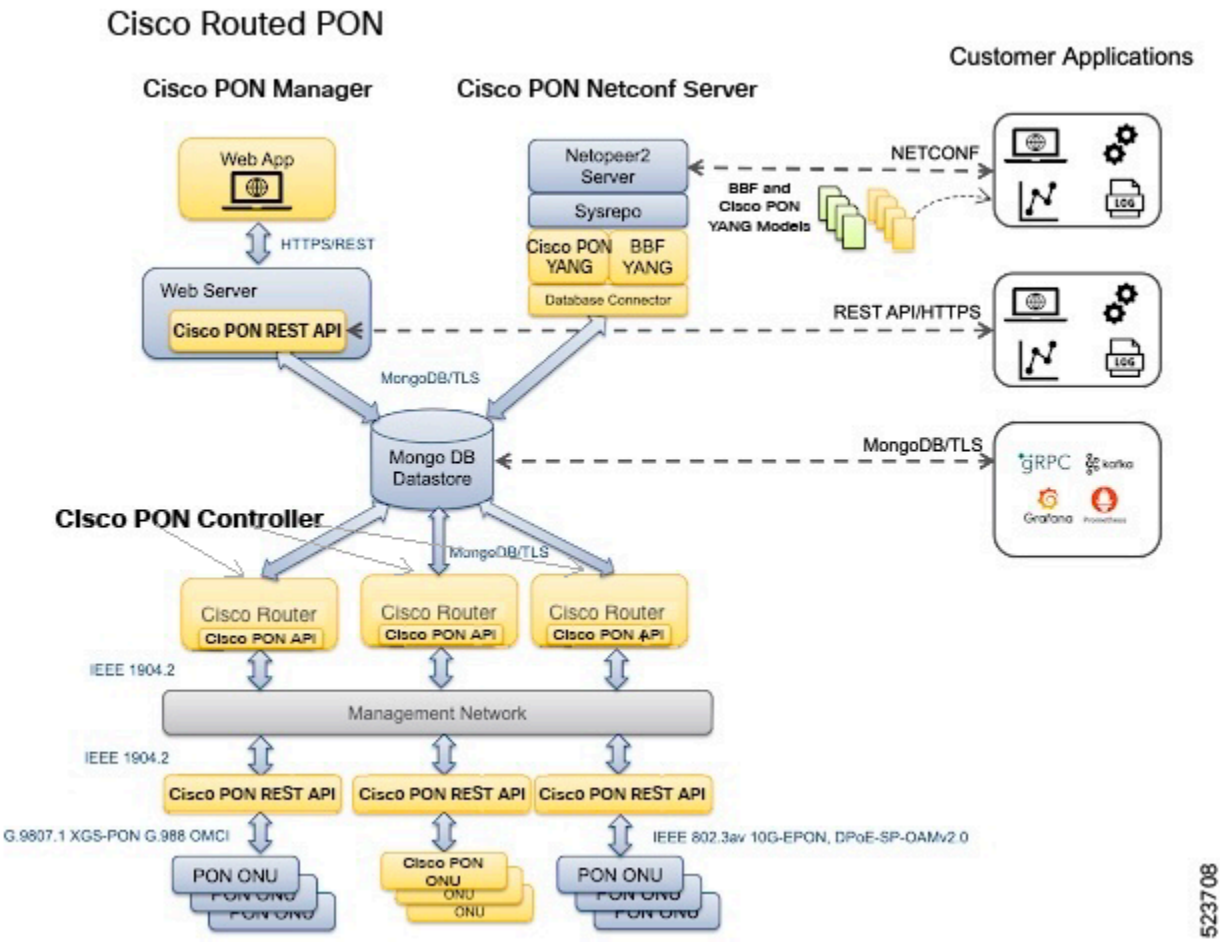


Figure 1 - Cisco Routed PON Architecture

Routed PON Manager

The Routed 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

© 2024 Cisco and/or its affiliates. All rights reserved.

front-end user interface. The REST API accompanies the Web App for the purposes of providing access to MongoDB for managing Routed PON Manager users and the PON Network.

The Routed 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.
- Polyglot graphical OMCI (and future 10G EPON OAM) service configuration tool.
- Routed PON Controller database management.
- Routed PON Manager user management.

Routed PON REST API

The Routed PON REST API is a component of the PON Manager that provides an application programming interface over HTTPS for managing PON devices for the Cisco solution. Customers 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 utilizes 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 Routed PON REST API implements endpoints for managing the following:

- Device configuration and status for PON Controllers, OLTs, ONUs, and Switches/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.

© 2024 Cisco and/or its affiliates. All rights reserved.

MongoDB Datastore

The Mongo database (MongoDB) provides the datastore for the Cisco Routed PON. 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 Routed PON Manager and customer applications interface with MongoDB to provision and retrieve monitoring information for devices in the PON network. MongoDB serves as the interface between the PON Manager 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 write device configuration 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.

Architecture Overview

The Routed PON Manager software is composed of a graphical user front-end web application (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 as shown in Figure 2.

© 2024 Cisco and/or its affiliates. All rights reserved.

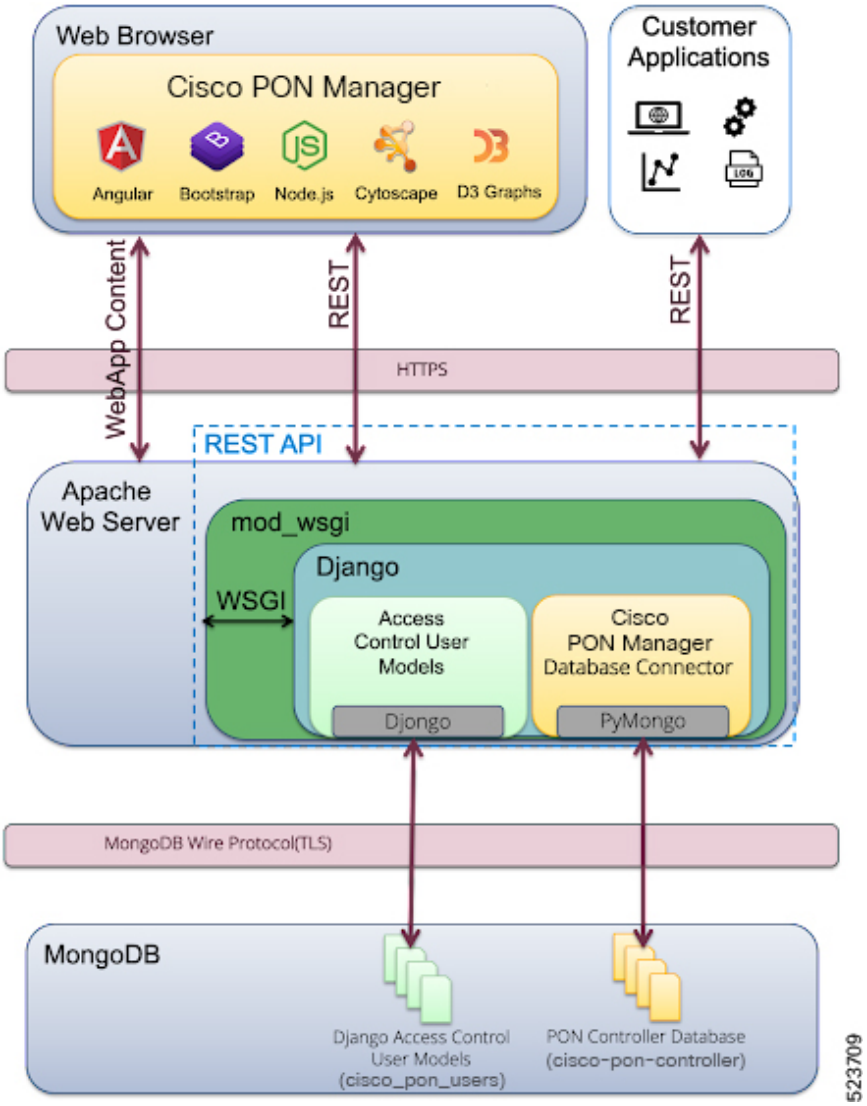


Figure 2 - Routed PON Manager Architecture

Routed PON Manager Web Application

The core of the Routed PON Manager Web App is built on the Angular 13 framework and Bootstrap web front-end toolkit, along with libraries that support specific elements of the user interface. The Cytoscape library provides network visualization utilities 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. See Section Web Interface for information on using the Web App.

© 2024 Cisco and/or its affiliates. All rights reserved.

Routed PON Manager Web Server and API

The Routed 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 Cisco-created interface to the Routed 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 security and account management features.

By default, Django does not support integration with non-relational databases. The djongo library is used in parallel with a custom module to communicate with MongoDB. As HTTP requests are received, they are handled by Django accordingly, but are mapped to the custom module 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 subject to change from release to release.

MongoDB

The Mongo database provides the datastore for the Cisco Routed PON, and is used to store PON device provisioning and monitoring information collected by the PON Controller. MongoDB is an open source, secure database (www.mongodb.com) which employs a NoSQL architecture. See section MongoDB Installation for information on installation and configuration for use in Cisco management solutions.

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.

© 2024 Cisco and/or its affiliates. All rights reserved.

Installation

There are two primary ways of installing and configuring the PON Manager: Debian Package installation and Docker container. This setup guide assumes that you have already set up a MongoDB server as described in the Cisco Routed PON Installation Guide.

NOTE: 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

Supported Browsers

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

Supported Operating Systems

Operating System	Version
Ubuntu	20.04

© 2024 Cisco and/or its affiliates. All rights reserved.

Required Packages

The following Ubuntu Linux apt packages are installed by the Debian package. See Section Installation Methods for installation instructions.

NOTE: MongoDB is not installed by the Debian package. See Cisco Routed PON Installation Guide for information on MongoDB installation, setup, and operation.

Package	**Ubuntu 20.04**
Apache2	2.4.41
Libapache2-mod-wsgi-py3	4.6.8
Libjpeg8-dev	8.0.0
Lsb-release	11.1.0
Mongo	4.4.0
openssl	1.1.1
Pip3	20.0.2
Python	3.8.2
Python3-dev	3.8.2
Python3-venv	3.8.2
Systemd	245.4
Zlib1g-dev	1.2.11

© 2024 Cisco and/or its affiliates. All rights reserved.

Python Package Dependencies (pip3)

The following Python 3 packages are installed with pip3 by the Debian package within a Routed PON Manager specific Python virtual environment. See Section Installation Methods for installation instructions.

Package	Version
dataclasses	0.6
Django	2.2.28
django-cors-headers	3.4.0
django-rest-swagger	2.2.0
djangorestframework	3.11.2
djongo	1.2.30
drf-spectacular	0.17.2
jsondiff	1.3.0
jsonschema	3.2.0
Pillow	Ubuntu 18.04 == 8.4.0, Ubuntu 20.04 == 9.2.0
pymongo	Ubuntu 18.04 == 4.1.1, Ubuntu 20.04 == 4.3.3
python-resize-image	1.1.19
simplejson	3.16.0
sqlparse	0.2.4
zxcvbn	4.4.28

© 2024 Cisco and/or its affiliates. All rights reserved.

Package Contents

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

File/Directory	Description
tibit-ponmgr_R4.0.0_all.deb	Debian Package based Routed PON Manager application
docker/	Directory containing docker container and configuration files
docker/databases.json	Docker container based Routed PON Manager configuration file. See Docker
docker/docker-compose.yml	Contains VM install parameters to be utilized by docker compose
docker/Dockerfile	Responsible for building docker image
docker/README.txt	Quick startup guide for installing and configuring PON Manager Docker container
docker/recovery_email_configuration.json	Docker container based Routed PON Manager configuration file. See Docker
docker/tibitdev-api.conf	Docker container based Routed PON Manager configuration file. See Docker
docker/tibitdev-web.conf	Docker container based Routed PON Manager configuration file. See Docker
docker/user_database.json	Docker container based Routed PON Manager configuration file. See Docker
examples/	Directory containing example REST API query requests
legacy_uninstall.py	Uninstallation script for Routed PON Manager versions R1.2.0 and below
LICENSES.txt	Lists the licensing information for third party software used
mongodb_install.sh	Installs mongoDB

© 2024 Cisco and/or its affiliates. All rights reserved.

mongodb_start.sh	Starts forked mongod instance
mongodb_uninstall.sh	Removes mongodb application, logs, configuration, and databases
README.txt	Quick startup guide for installing and configuring 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 Routed PON Manager
tools/generate_django_key.py	Python 3 script to generate a randomized Django key
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/db_import/	Directory containing database import utility
tools/db_import/db_import.py	Database import Python 3 script. Imports device firmware, pictures, and ONU Service Configuration files into MongoDB.
tools/branding/	Contains script and files for creating a custom branded PON Manager.
version.txt	Version information

Installation Methods

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

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

© 2024 Cisco and/or its affiliates. All rights reserved.

Debian Package

The tibit-ponmgr_R4.0.0_all.deb package handles installation of all dependencies except for Python.

Prerequisites:

- Ensure that you have an active internet connection.
- Install/upgrade existing python3 package to be equal to or greater than version 3.6.7.
- Install/upgrade existing pip3 package to be equal to or greater than version 9.0.0.
- Ensure that you have your MongoDB Server running that will manage user authentication and serve as your default database.
- Ensure you have the latest ubuntu updates.

Installation Steps:

NOTE: By default, Routed PON Manager will deploy over HTTPS utilizing a self-signed certificate created during installation. THIS IS NOT SAFE FOR A PRODUCTION ENVIRONMENT. If installing Routed PON Manager for any use other than evaluation, you should use legitimate certificates. See Using Alternate Certificates for how to configure alternate certificates.

1. Open a shell and change to the root directory of Routed PON Manager application.

2. *Optional* | If desired, 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:
    - [req_distinguished_name]

countryName	Country code. | Ex: 'US' (United States), etc
ST	State or Province
localityName	City or Locality
organizationName	Name of organization
organizationalUnitName	Name of group/unit within organization
CN	Fully Qualified Domain Name of system

© 2024 Cisco and/or its affiliates. All rights reserved.

- [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. Use apt to install the package.
   - Use the following command to install PON Manager with the default self-signed certificate:

     ```
     sudo apt install ./tibit-ponmgr_R4.0.0_all.deb
     ```

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

     ```
     sudo TIBIT_PONMGR_CERT_REQ=/path/to/file.conf apt \
     install ./tibit-ponmgr_R4.0.0_all.deb
     ```


© 2024 Cisco and/or its affiliates. All rights reserved.

Configuration steps:

Ensure that you have root/sudo access to modify files.

1. Navigate to the directory: '/etc/tibit/ponmgr/'
   - Within this directory, there are several PON Manager configuration files that will need to be edited with a text editor of your choice.

   - user_database.json
     - Stores configuration for database to be used for user authentication.

Key	Description
host	Hostname/IP Address of the MongoDB server hosting your user database.
name	Name of your user database. Default user database name is 'tibit_users'. *(If it doesn't exist, it will be created)*
port	MongoDB port number.
auth_enable	Boolean value determining if the MongoDB server at *host:port* is using authentication.
auth_db	Name of your MongoDB authentication database. *(Used when auth_enabled = true)*
username	The username of the MongoDB user to authenticate with. *(Used when auth_enabled = true)*
password	The password of the specified MongoDB user. *(Used when auth_enabled = true)*
tls_enable	Boolean value specifying whether the MongoDB server at *host:port* is using encryption.
ca_cert_path	The local path to the encryption certificate.
compression	Boolean value specifiything whether to enable snapy compression for MongoDB connections.

© 2024 Cisco and/or its affiliates. All rights reserved.

dns_srv	Boolean value specifying whether the MongoDB server is using a DNS seed list.
db_uri	Raw MongoDB connection URI. All Other fields are ignored if this is used.
replica_set_enable	Boolean value specifying if the MongoDB server is running as a replica set.
replica_set_name	The name of the MongoDB replica set. *(Used when replica_set_enabled = true)*
replica_set_hosts	List of hosts to be used as the MongoDB replica set. *(Used when replica_set_enabled = true)*
django_key	Cryptographic key used by django. The format of the field is a freeform string, however, Django recommends it be minimum 50 characters with minimum 5 unique characters. See section Django Key for more information on the Django Key. (Note: that a randomized key will be generated during installation if the 'django_key' field is not present.)

- databases.json
    - Stores list of all available PON databases in PON Manager.

Key	Description
host	Hostname/IP Address of your mongoDB server hosting your PON Controller database
name	Name of your PON Controller database. Default PON Controller database name is 'tibit_pon_controller'. *(If it doesn't exist, it will be created)*
port	MongoDB server port number.
auth_enable	Boolean value determining if the MongoDB server at *host:port* is using authentication.
auth_db	Name of your MongoDB authentication database.

© 2024 Cisco and/or its affiliates. All rights reserved.

	(Used when auth_enabled = true)
username	The username of the MongoDB user to authenticate with. *(Used when auth_enabled = true)*
password	The password of the specified MongoDB user. *(Used when auth_enabled = true)*
tls_enable	Boolean value specifying whether the MongoDB server at *host:port* is using encryption.
ca_cert_path	The local path to the encryption certificate.
dns_srv	Boolean value specifying whether the MongoDB server is using a DNS seed list.
db_uri	Raw MongoDB connection URI. All Other fields are ignored if this is used.
replica_set_enable	Boolean value specifying if the MongoDB server is running as a replica set.
replica_set_name	The name of the MongoDB replica set. *(Used when replica_set_enabled = true)*
replica_set_hosts	List of hosts to be used as the MongoDB replica set. *(Used when replica_set_enabled = true)*

- recovery_email_configuration.json
    - Configures SMTP email server for sending user password recovery emails.

Key	Description
host	Host to use for sending email
port	Port to use for the SMTP server defined above *Type: String*
use_tls	Use TLS connection *'true' or 'false'* *Type: String*
user	Username for the SMTP server

© 2024 Cisco and/or its affiliates. All rights reserved.

password	Password for user

2. Restart Apache
   - ‘sudo systemctl restart apache2.service’

Using Alternate Certificates:

This section describes the steps to replace the default self-signed certificate and key with alternates.

Prerequisites:
- You will need a valid certificate and private key

To change the certificate and keys, these configuration files will need to be modified (located in /etc/tibit/ponmgr/):

1. tibitdev-api.conf
   a. Within this configuration file, there is a section titled; ‘HTTPS Options’. There will be two directives; SSLCertificateFile and SSLCertificateKeyFile
   b. Replace the existing values of each of these directives with the path to a valid certificate and private key, respectively.

2. tibitdev-web.conf
   a. Within this configuration file, there is a section titled; ‘HTTPS Virtualhost’. There will be two directives; SSLCertificateFile and SSLCertificateKeyFile
   b. Replace the existing values of each of these directives with the path to a valid certificate and private key, respectively.

3. Restart Apache

Validation Steps after Installation:

In a browser, navigate to “http://*IPofServerGoesHere*”
- Ex. “http://10.1.10.255”

Installation Notes:

- If you run into issues after updating the configuration files and restarting apache, try clearing your browser’s cache.

© 2024 Cisco and/or its affiliates. All rights reserved.

- It is recommended that 127.0.0.1 be used for the mongoDB server if you have it running locally
- Web pages are served from the default port 443. Any request over non-secure port 80 is redirected to port 443.
- Location of install: /opt/tibit/ponmgr, /etc/tibit/ponmgr, /var/www/html (Symbolic links)

© 2024 Cisco and/or its affiliates. All rights reserved.

uninstall

To Remove (keep config files):
- Run: "sudo apt remove tibit-ponmgr"
This will remove the PON Manager, but will leave configuration files behind

To Remove (remove config files):
- Run: "sudo apt remove tibit-ponmgr --purge"
This will remove the PON Manager, and will also remove configuration files

Legacy Uninstall:
- Run: "sudo ./legacy_uninstall.py"
This will remove PON Manager versions R1.3.0 and prior

© 2024 Cisco and/or its affiliates. All rights reserved.

MongoDB Installation

NOTE: MongoDB is not provided as part of the PON Manager package.

MongoDB serves the purpose of being the datastore for the Cisco Routed PON. This includes all PON-specific information as well as user models. See Cisco Routed PON Installation Guide for information on MongoDB installation, setup, and operation.

© 2024 Cisco and/or its affiliates. All rights reserved.

Security

TCP/IP Ports and Network Services

Routed 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:

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 Routed PON Manager REST API.

In addition to providing network services, the Routed PON Manager Server requires network services from external systems to operate. PON Manager requires client access to the following network services:

Network Service	TCP Port	Description
MongoDB	27017	Default TCP port of the MongoDB server that the PON Manager connects to.
Open Layers (*Open Street Maps*)	443	Open Layers/OpenStreetMap render server that generates all geographic maps for PON Manager. *DNS Names:* - *https://openlayers.org* - *https://a.tile.openstreetmap.org* - *https://b.tile.openstreetmap.org* - *https://c.tile.openstreetmap.org*

Role Based Access Control

Routed PON Manager utilizes user roles and permissions to control what actions each user may perform. Every user may be 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

© 2024 Cisco and/or its affiliates. All rights reserved.

permission has an access type associated with it based on the Create, Read, Update, 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's 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 here. See Authentication 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 Accounts for more information on configuring users, roles, and permissions using the Web Client.

HTTPS

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

Authentication

The PON Manager utilizes the session authentication mechanism from the Django framework. This mechanism associates a given HTTP request with a user.

Authentication relies on the following session state and data:

- **Session Identifier** is represented as a cookie with the key: '__host-sessionid', which is a token that associates an HTTP request to a user. This token maps directly to the primary key of a Session Object stored in MongoDB.
- **CSRF Token** (Cross Site Request Forgery protection token) is sent to the requester in the form of a set-cookie header. This token is required to be sent on all unsafe HTTP verb (Post, Put, Delete, etc.)] requests as a header with the key; 'X-CSRFToken'

© 2024 Cisco and/or its affiliates. All rights reserved.

- **Session Object** stores encoded data for the session, including the associated user, as a document in MongoDB in the PON Manager User Database (tibit_users). A unique Session identifier identifies the session object.

The following describes the process of authenticating a user session:

1. Before a successful request can be made, the user must authenticate via email/password and retrieve a valid session token. (POST /user/authenticate/)
2. Upon successful authentication, the requester must send the '__host-sessionid' cookie and X-CSRFToken header (if required, for unsafe HTTP verbs) on every request.
3. If an HTTP request lacks a valid Session Token, a 403 (Forbidden) response will be returned.

Session Expiration

A user session will expire after a period of inactivity. The session expiration timeout is configured in the PON Manager User Database in units of minutes. The session expiration timeout can be 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 response of 403 will be returned. The user will have to re-login and authenticate with PON Manager when their session expires.

Session Purging

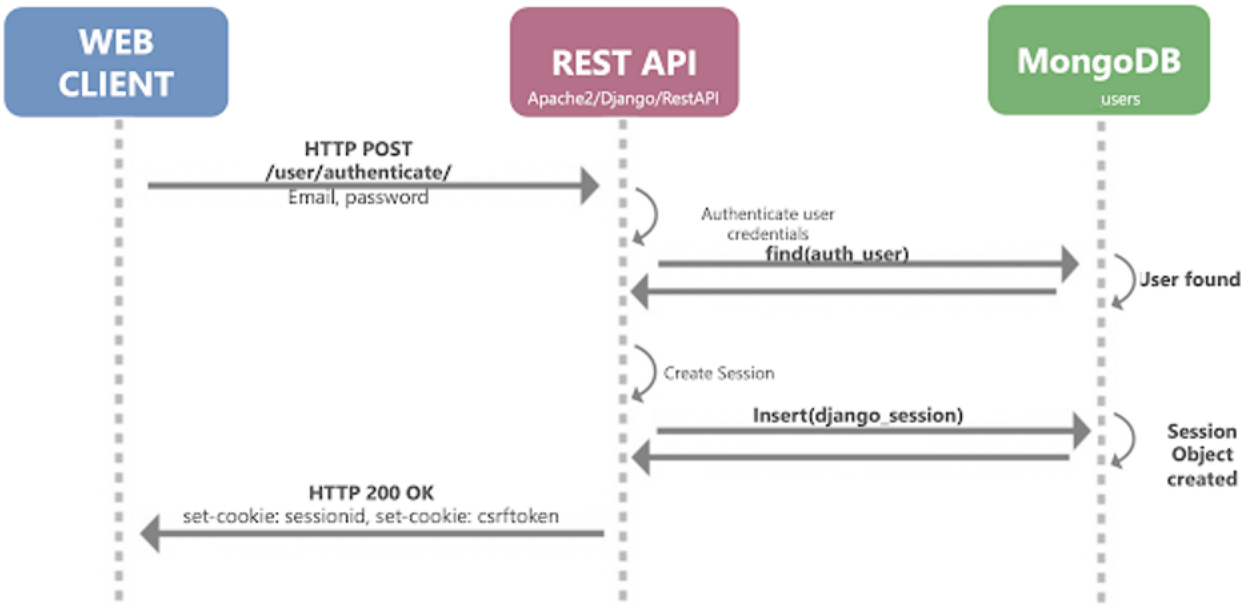
A new Session Object is created and stored in MongoDB upon successful authentication. This is the case even if the user already has a previous Session Object(s) stored. Expired Session Objects are purged from MongoDB every 24 hours.

System Diagrams

User Authentication and Session Establishment

The following diagram displays the sequence of creating a user session.

© 2024 Cisco and/or its affiliates. All rights reserved.

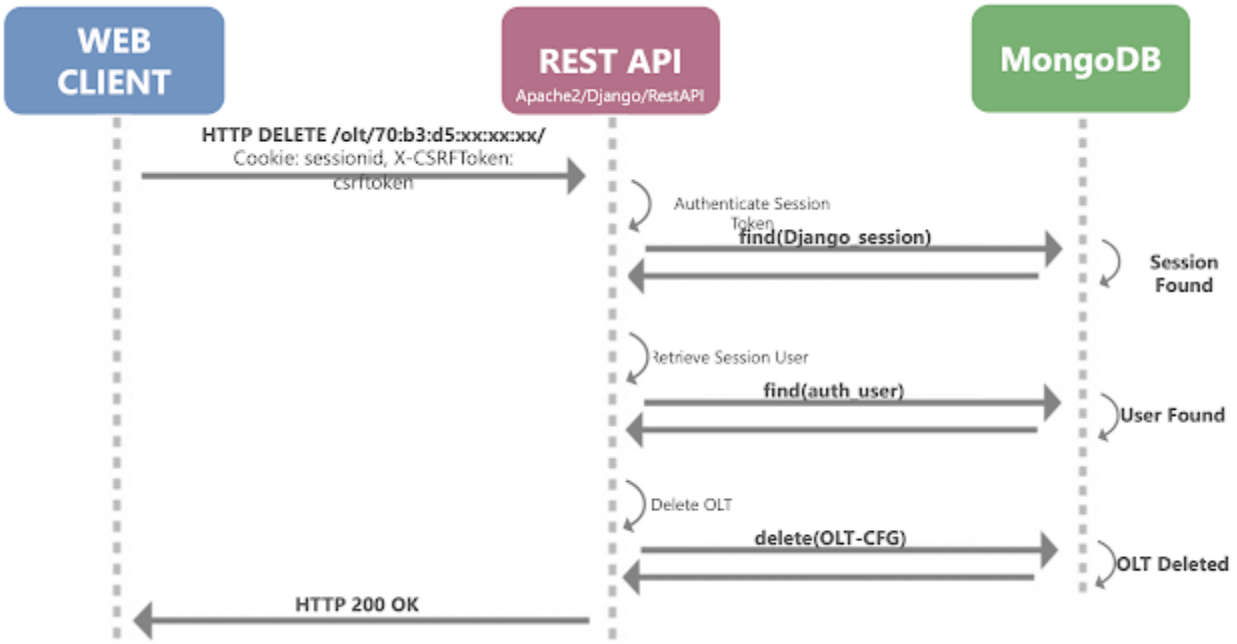


1. **HTTP POST -** a user makes an HTTP request with a valid email and password combination to the REST API to authenticate.
2. **find(auth_user) -** the REST API queries the user collection tibit_users in MongoDB to find and return the user profile matching the email password combo provided.
3. **Insert(django_session) -** the REST API creates a session associated with the authenticating user and inserts the session object into MongoDB.
4. **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 displays the sequence of successfully authenticating with a valid user session.

© 2024 Cisco and/or its affiliates. All rights reserved.

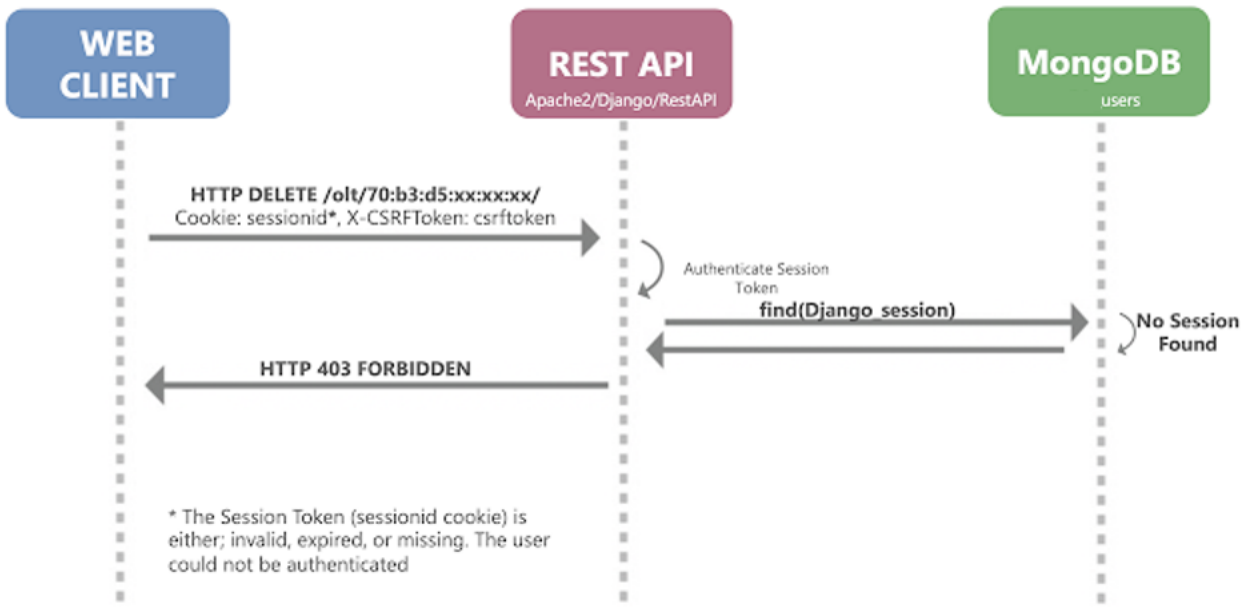


1. **HTTP DELETE -** a user makes an HTTP request containing a valid sessionid and csrftoken cookie
2. **find(Django_sesson) -** the REST API queries the session collection in MongoDB to find and return the session object with a matching sessionid.
3. **find(auth_user) - t**he REST API queries the user collection tibit_users in MongoDB to find and return the user profile associated with the session object.
4. **delete(OLT-CFG) -** the authenticated request is performed
5. **HTTP 200 OK -** a successful response is returned to the user

Authentication Failure

The following diagram displays the sequence of failed authentication

© 2024 Cisco and/or its affiliates. All rights reserved.



1. **HTTP DELETE -** a user makes an HTTP request containing an invalid, expired, or missing sessionid cookie.
2. **find(Django_sesson) -** 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.
3. **HTTP 403 FORBIDDEN -** an unsuccessful forbidden response is returned to the user.

© 2024 Cisco and/or its affiliates. All rights reserved.

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 minimum 50 characters with minimum 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 reauthenticate.

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

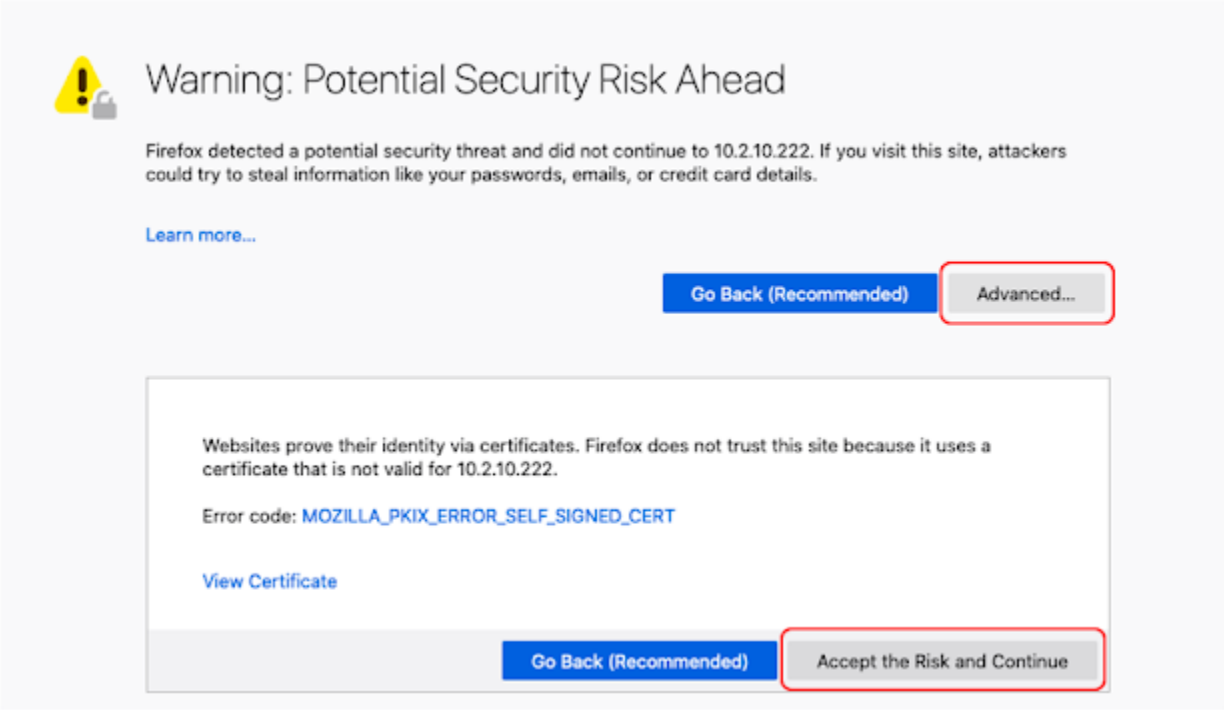
© 2024 Cisco and/or its affiliates. All rights reserved.

Web Interface

Logging In for the first time

If using a configured user database that has no users, the user is prompted to create the first administrative user. Otherwise, the user is directed to enter their credentials to access the Web App.

If 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 REST API. To do so, connect to the IP address for the Web App. The browser displays a warning similar to the following:



Even with the security exception, HTTPS traffic is still encrypted. Click the button labeled “Advanced” and then click the button labeled “Accept the Risk and Continue”.

Creating and Managing Accounts

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

© 2024 Cisco and/or its affiliates. All rights reserved.

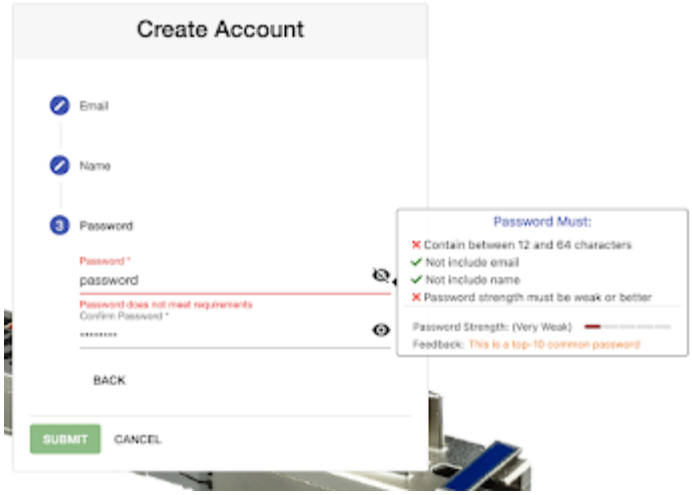
Administrators are responsible for creating additional user accounts. This can be done from the Accounts tab.

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 via the User Configuration tab. By default, user account passwords require;

- 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



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

If the password does not adhere to the configured requirements, a label below the field will appear 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

© 2024 Cisco and/or its affiliates. All rights reserved.

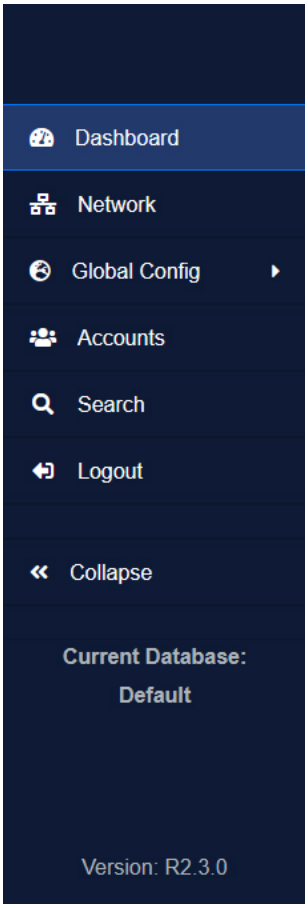
to save a non-compliant password. In this case, a label below the password field will appear in orange to indicate that the password is invalid but can still be saved.

Logging Out

The option to logout is accessible from the Site Navigation menu on the left of the PON Manager user interface. When 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.

Version



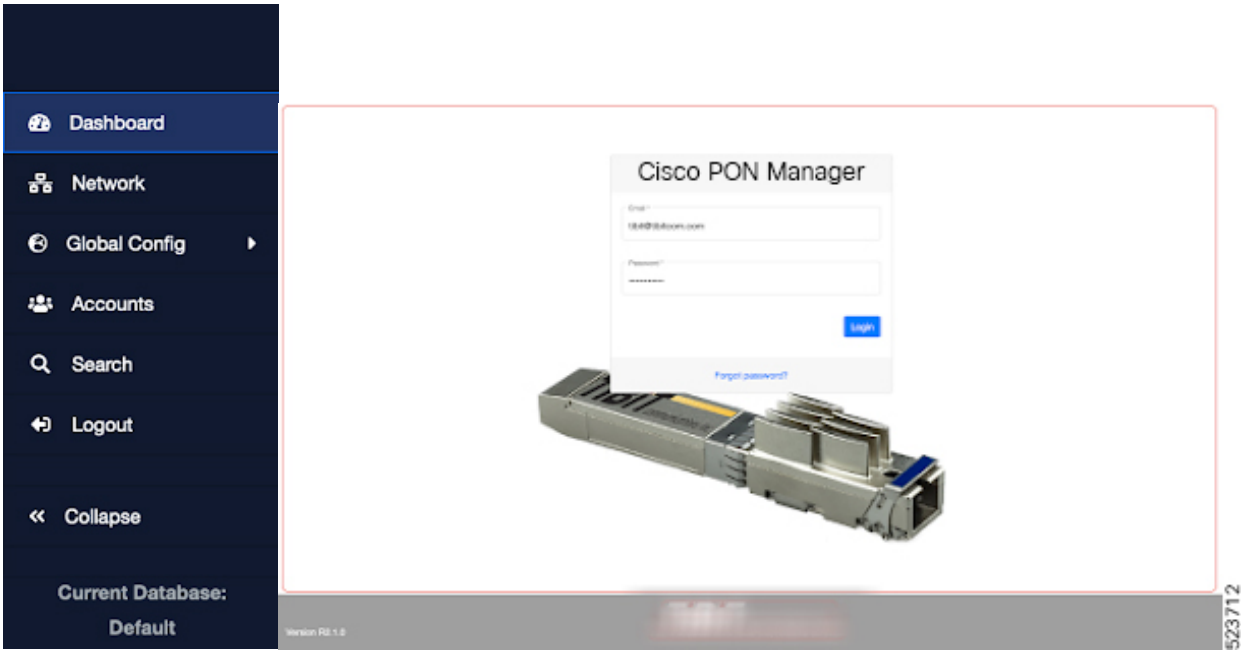
A user can see more about the version of the Routed PON Manager by clicking on the “Version” label on the bottom of the Site Navigation menu. This button displays a popup that gives details on the current build being used as well as any third party software used in the creation of the Routed PON Manager.

© 2024 Cisco and/or its affiliates. All rights reserved.

Site Customization

To customize the look and feel of the PON manager user interface, you have two options:

1. Option 1: 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.
2. Option 2: If the PON Manager is already installed, you can make changes directly to the user interface after installation. The Routed 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 and logo of the login screen and 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 Cisco 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.



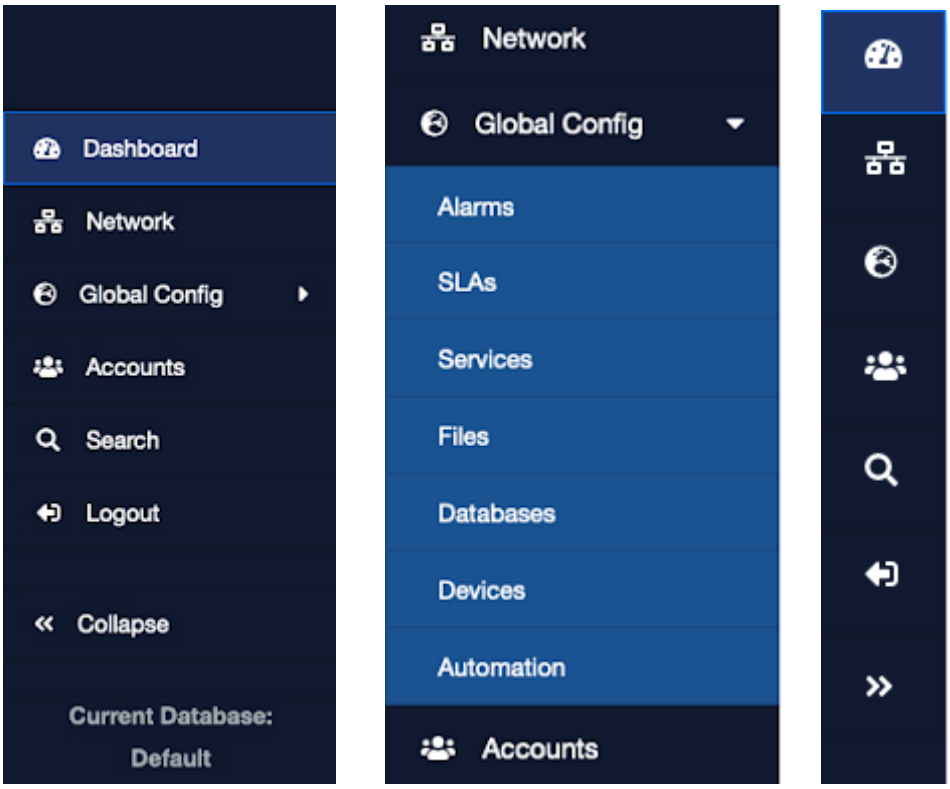
These two methods give you flexibility in customizing the PON Manager according to your preference.

© 2024 Cisco and/or its affiliates. All rights reserved.

Note: Images uploaded larger than the recommended size will not be displayed.

Site Navigation

After having logged into the PON Manager, site navigation is visible on the left-hand side of the window. The current page that is selected is marked by the highlighted section of this navigation menu. The first view a user sees after logging in is the Dashboard page. From anywhere on the site it is possible to transition between the Dashboard, Network, Global Config, Search, and Accounts pages as well as logout of the application. The Global Config section expands to its own menu for navigation to the Alarms, SLAs, Services, Files, Databases, and Devices pages. This menu may be collapsed to allow for more horizontal screen space. The ID of the current database in use is shown at the bottom of the menu. The following images show the navigation menu with Network selected, the expanded Global Config menu, and the view when collapsed.



Auto Refresh

Most pages of PON Manager will automatically refresh their data. This occurs every 5 seconds on most pages. Some pages that require retrieval of larger amounts of data may use a longer timer such as 10-15 seconds. Those pages that require the most data will not update

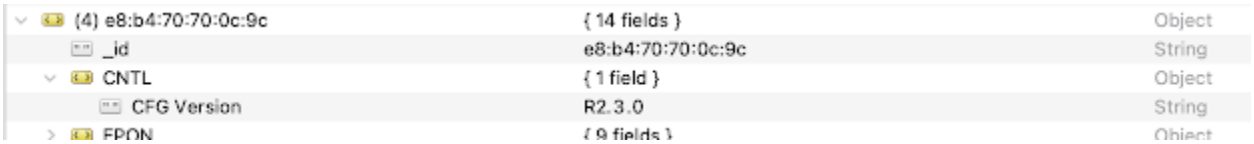
© 2024 Cisco and/or its affiliates. All rights reserved.

automatically, but will have a refresh button to update the page's data manually. It is not required to refresh the browser to retrieve the updated data for a tab.

PON Controller Database Compatibility

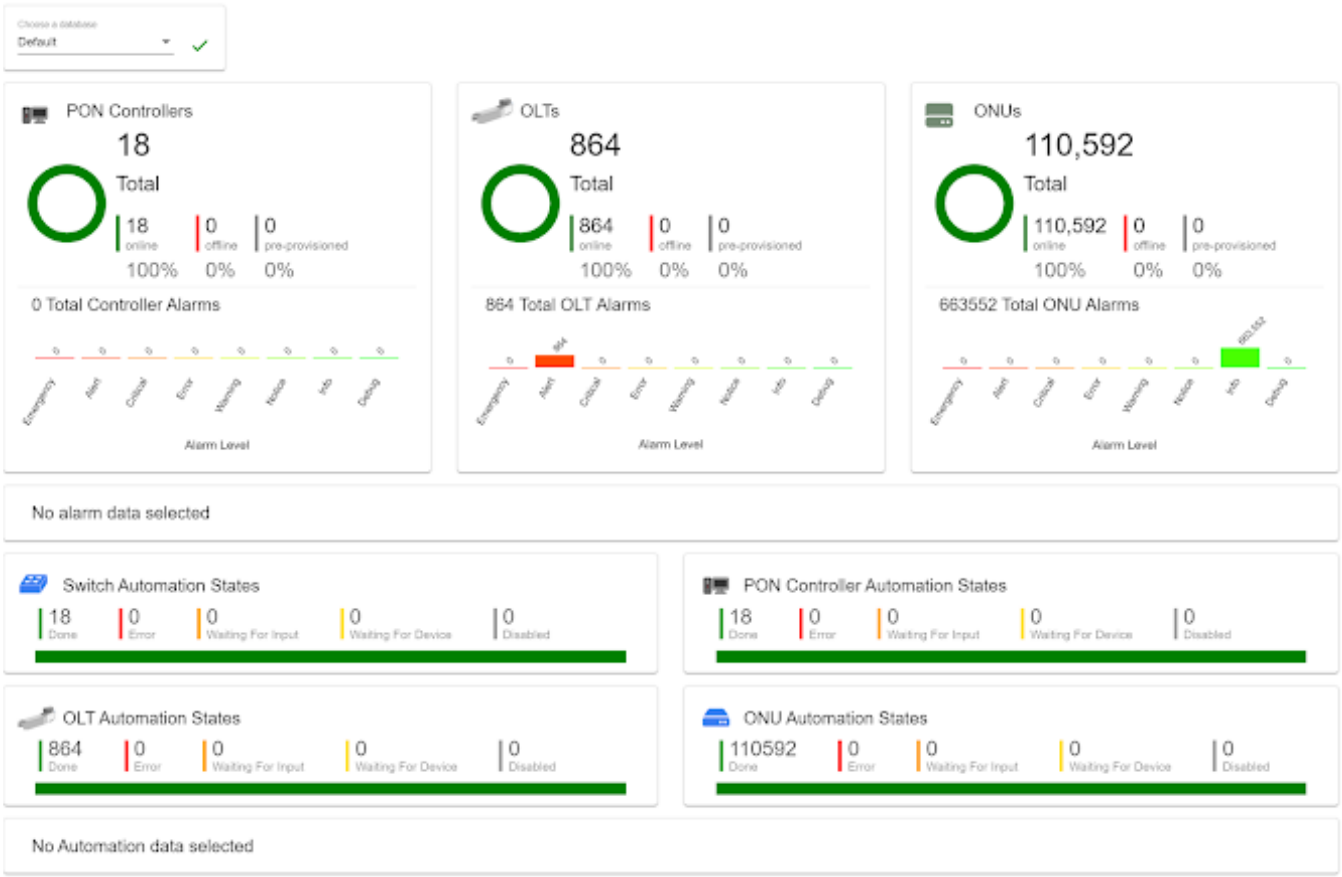
The PON Manager is designed to be backwards compatible supporting PON Controller database revisions R2.0.4 and greater. The Web App only displays configuration parameters that are applicable and available for the version specified in the device configuration document stored in the database. When using older, previous releases of the database or device configuration files, only configuration and state attributes for that version will be displayed in the UI. Meaning 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 most often seen on the Network portion of the web interface and pertains to all devices.

The PON Manager uses the field 'CNTL.CFG Version' in the device's configuration document to determine what fields are shown in the UI. This field as well as the entire device configuration file can be updated from the PON Manager by navigating to the page Global Config → Databases → Update.



© 2024 Cisco and/or its affiliates. All rights reserved.

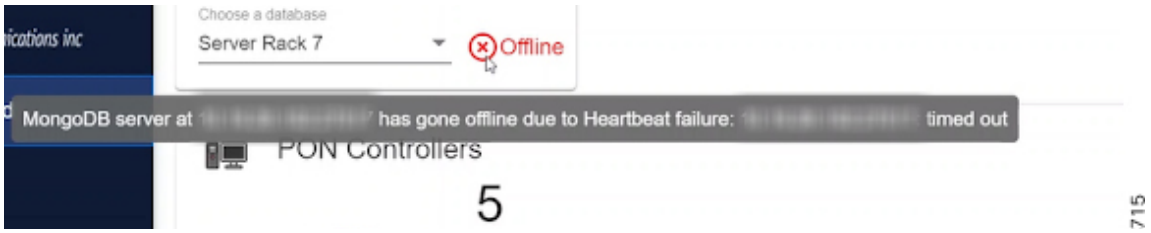
Dashboard



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, and counts of Automation States for each device type. Clicking an alarm level for a device will display those alarms 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. The Automation tiles are only displayed if PON Auto has run on the database.

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. When selecting, if the database is accessible the green checkmark will show as a button to choose the database. If the database is offline however, a red “X” will be shown indicating the database cannot be chosen.

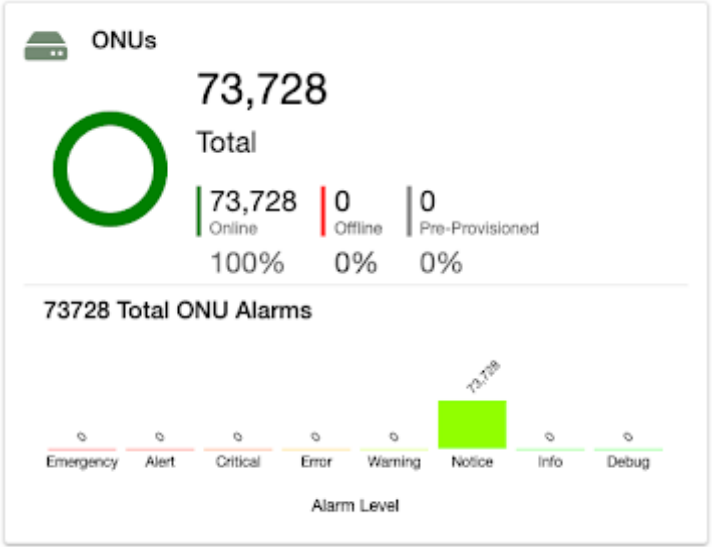
© 2024 Cisco and/or its affiliates. All rights reserved.



Devices are categorized into three different states: Online, Offline, and Pre-Provisioned. These counts are reflected in pie charts and percentages. Beneath the device counts are bar charts displaying the total number of Raised and Unacknowledged alarms of each type for each device type. If a database becomes unreachable during its use the following message is displayed to the user to notify them of the problem.

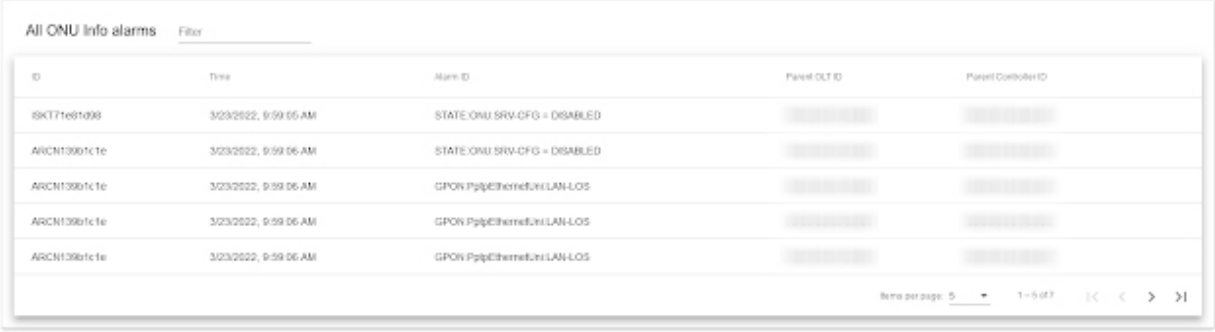
Alarms Summary

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 on the "Info" bar, a table of all Information level alarms populates below the device summary tiles.



© 2024 Cisco and/or its affiliates. All rights reserved.

The Alarms table displays the ID of the device the alarm is for, followed by the time the alarm was reported, the Alarm ID, and the IDs of the parent OLT and PON Controller (where applicable).



Network

The Network page allows the user to view/edit the states and configurations of the devices (PON Controllers, Switches/Routers, OLTs, and ONUs) in the selected database. The user is shown the hierarchy of devices they are viewing, and may monitor device states, alarms, logs, and statistics, and configure settings.

Devices

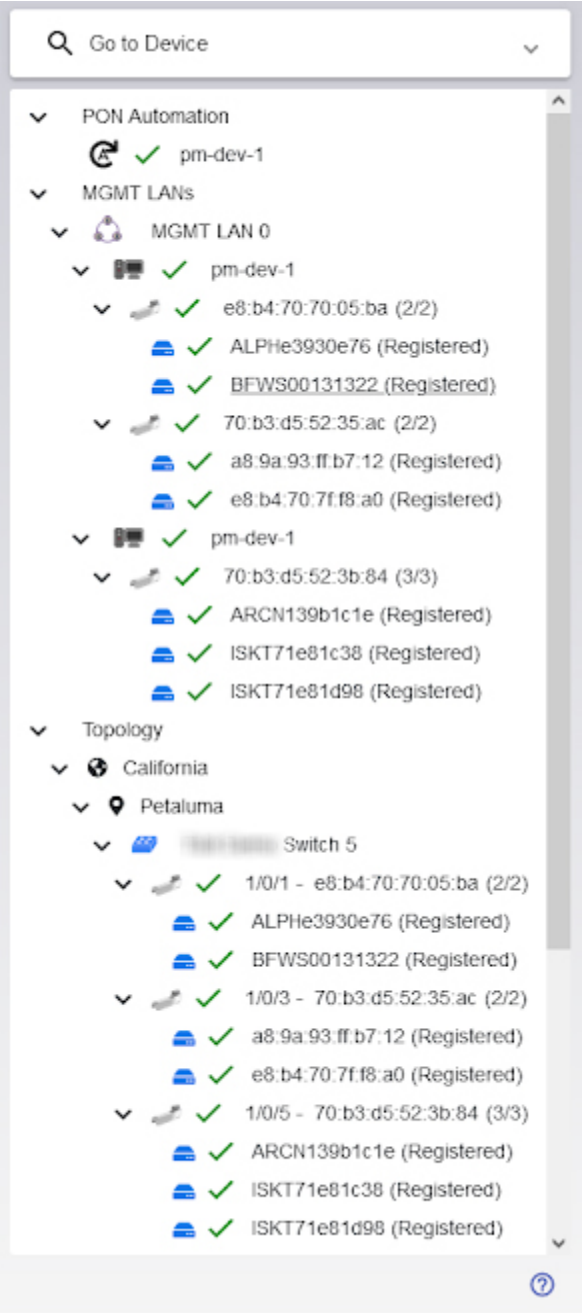
Cisco defines several device types listed in the table below which are top-level management entities within the PON Manager. Each device is represented in the Device Navigation Tree and is identified in the tree by the icon shown in the table below.

Device	Icon	Description
Switch/Router[1]		Network switch with respect to switch properties associated with PON. Switches are discovered by OLT devices through LLDP.
PON Controller		Cisco PON Controller with respect to management of the application service, not the system hosting the Controller.
OLT		Cisco MicroPlug OLT device.
ONU		ONUs compliant with the XGS-PON or 10G EPON standards.

[1] The term “switch” is used generically throughout this document to reference a switching or routing device.

© 2024 Cisco and/or its affiliates. All rights reserved.

Device Navigation Tree



On the left side of the network page there is a navigation tree that displays the manageable devices available from the selected database. The tree has four root-level branches: MGMT LANs, Topology, and Unattached Devices. By default, there is one branch under the MGMT LANs branch, “Unnamed”. This name may change and others will 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.

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 which can also be found under the MGMT LAN hierarchy described above. 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” will appear if there are OLTs without LLDP information.

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

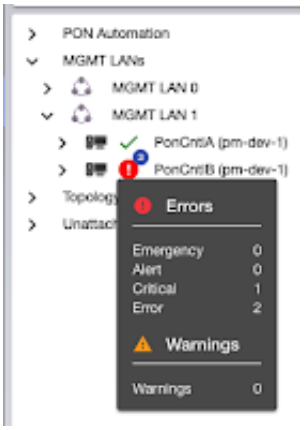
Each device type is marked by their unique icon to help quickly identify the device type. All PON Controller, Switch/Router, OLT, and ONU branches also have a secondary icon indicating device status and alarms. This device tree will

© 2024 Cisco and/or its affiliates. All rights reserved.

automatically update any open nodes. Each of these device branches list the device's ID (Name if available) as clickable text to navigate to that device. **Note:** it 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 popup to explain the various icons and levels of the tree.

Active warnings and alarms for devices will be displayed as icons on the tree nav next to their respective device. When hovering over the icon, a panel will be displayed showing what type of alarm it is and how many there are. Clicking on the icon will navigate users to the device's alarm page and clicking on the alarm type in the panel will pre-filter the page's alarm table showing only that type of alarm.



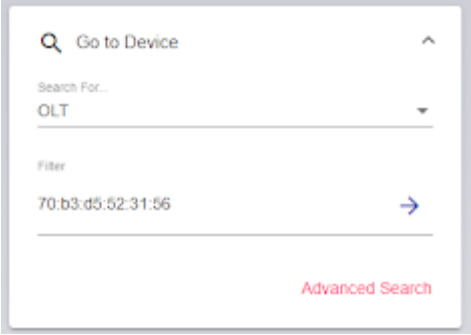
Different statuses of devices in the tree can be identified by the icons in the table below:

Status	Icon	Description
No alarms	✓	Device is online with no active warnings or errors.
Offline	⊗	Device is offline. This icon will display as priority over errors or warnings.
Errors	! 3	Device has active errors. The sum of errors are shown within its badge. This icon takes priority over warnings on the same device.
Warnings	⚠ 1	Device has active warnings. The sum of warnings are shown within its badge.

At the top of the navigation tree there is the "Go to Device" section. By expanding this section, the user may select a criteria to search on, enter the search text to find a specific device, and

© 2024 Cisco and/or its affiliates. All rights reserved.

then select the arrow to navigate to that device. Selecting the advanced search button takes the user to the Search page of the application.



ONU Device States

In the network device tree, device state is displayed to the right of the ONU in parentheses. These ONU device states display the current state of the ONU in relation to its parent OLT. The device states will not appear for ONUs within the “Unattached Devices” section of the tree as these ONUs are not associated with any OLT.

State	Description
Deregistered	The ONU is deregistered and inventoried in the OLT configuration file. This indicates a Loss-of-signal (LOS) condition for this 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.

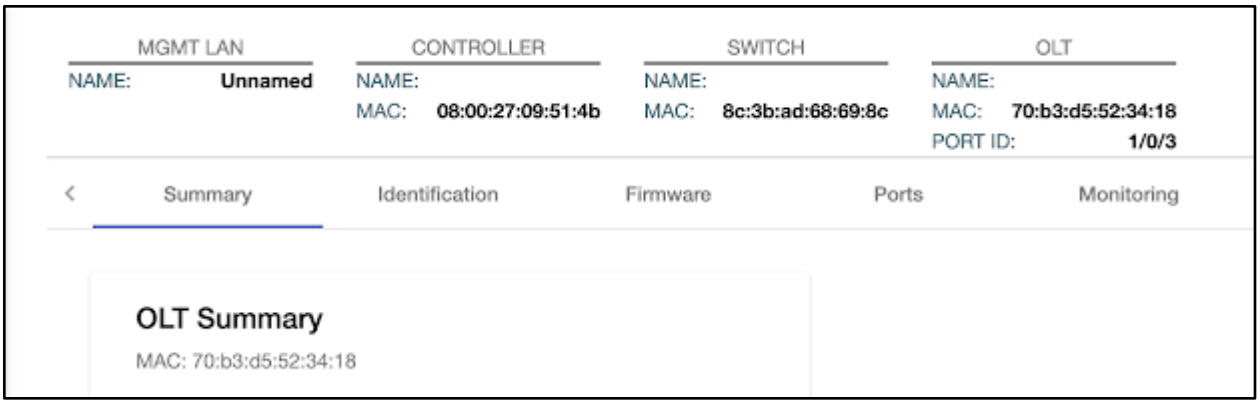
© 2024 Cisco and/or its affiliates. All rights reserved.

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

Displayed at the top of the Network page, the Hierarchy View bar displays the current hierarchy of devices that are being viewed. Starting on the left with the Management LAN, the selected PON Controller and/or Switch/Router, OLT and ONU are displayed. The Name, ID/MAC Address, Switch Port (for OLTs), and State (for ONUs) of the current hierarchy devices are all displayed here. Each device listed, excluding the MGMT LAN, is clickable to quickly navigate to any device in the hierarchy. Only those devices that have already been selected are shown here. For example, if a user selects a PON Controller to view, and then selects an OLT under that Controller, they would see the following (Note that the ONU portion of the hierarchy is not displayed in this example):

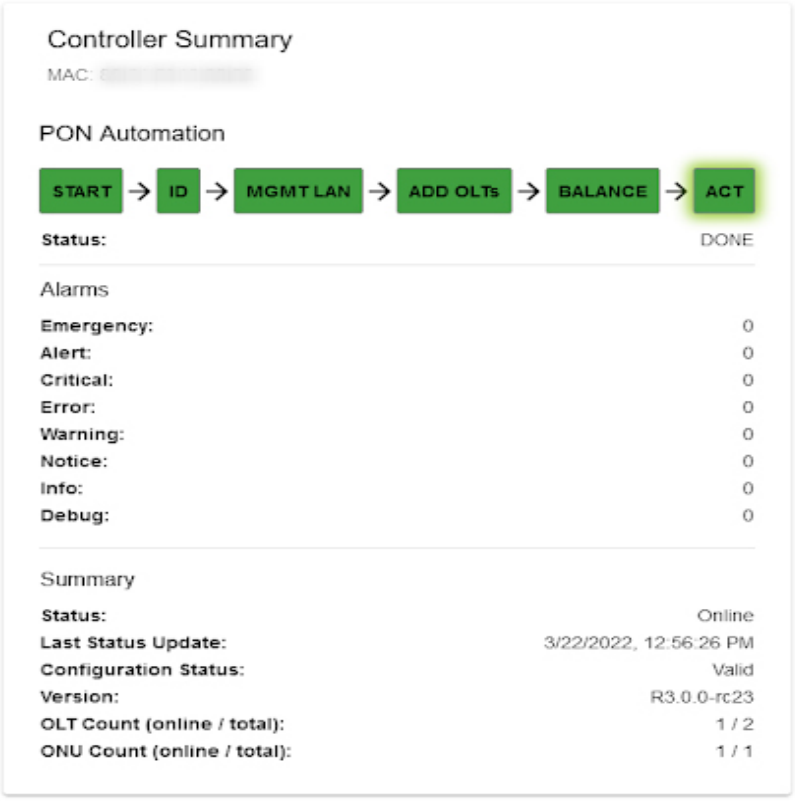
© 2024 Cisco and/or its affiliates. All rights reserved.



PON Controller

Summary

The Summary tab displays information relevant to the device's current state and status. Values such as the total alarm count, MAC Address, version, OLT and ONU counts, and status are displayed as well as the time stamp when the PON Controller's state was updated. A table is also shown to display 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.



© 2024 Cisco and/or its affiliates. All rights reserved.

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 on the Edit button at the bottom of the tile. The second tile shows a table of all network interfaces on the PON Controller device.

Configure Controller Name

At the top of the card above the Controller picture there will be an input box which you can type in any name with no restrictions for the new Controller name. Click SAVE to save your changes.

Configure Controller Picture

Where the “Picture” label was before you will see a dropdown list of all of the Controller pictures in your database. Select the one you want to see a preview of. (If you do not see the picture you want, you can add pictures by going to: Global Config, Files, Pictures tab). Click SAVE to save your changes.

Note: Differences between what is in the state file from what is in the configuration file of devices will be shown in red next to the field of the mismatched value like so:

© 2024 Cisco and/or its affiliates. All rights reserved.

Configure Location Coordinates

The *Location Coordinates* field accepts Decimal Degrees(excluding direction designation and degree symbol) formatted as *latitude,longitude* with latitude first followed by longitude separated with a comma. *e.g. 38.24,-122.64*

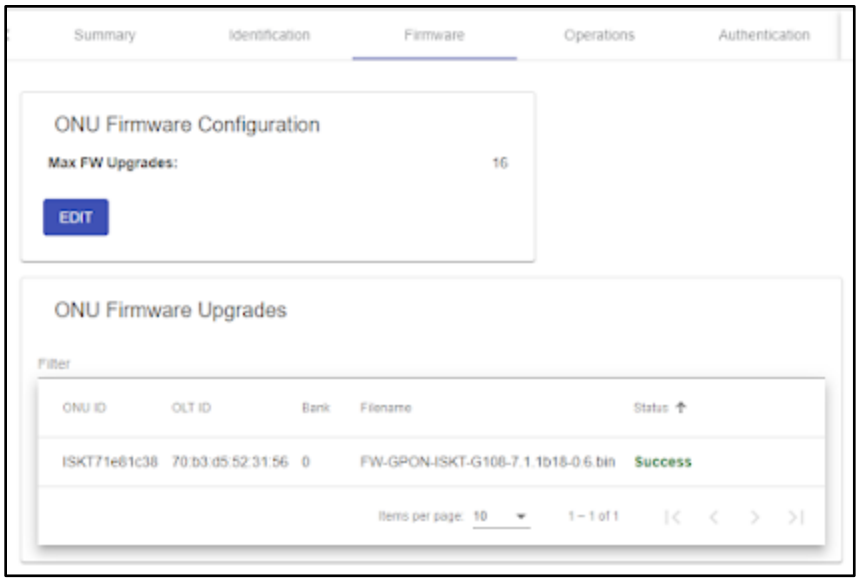
To view the device's position on a map, click the blue link icon to the right of the field *Location Coordinates.* If no coordinates are defined, then there will be no device marker on the map.

NOTE: The device accessing Routed PON Manager must have external access to the internet for mapping capability.

Firmware

The PON Controller Firmware tab has two tiles. The first displays the configured maximum allowed parallel ONU firmware upgrades on this Controller. This attribute can be changed by clicking Edit. The second tile lists all ONU firmware upgrades reported by the PON Controller. The table displays the ONU that was/is being upgraded, its parent OLT’s ID, the firmware bank, filename, and the last available upgrade status. This status updates automatically and shows the progress of an active upgrade.

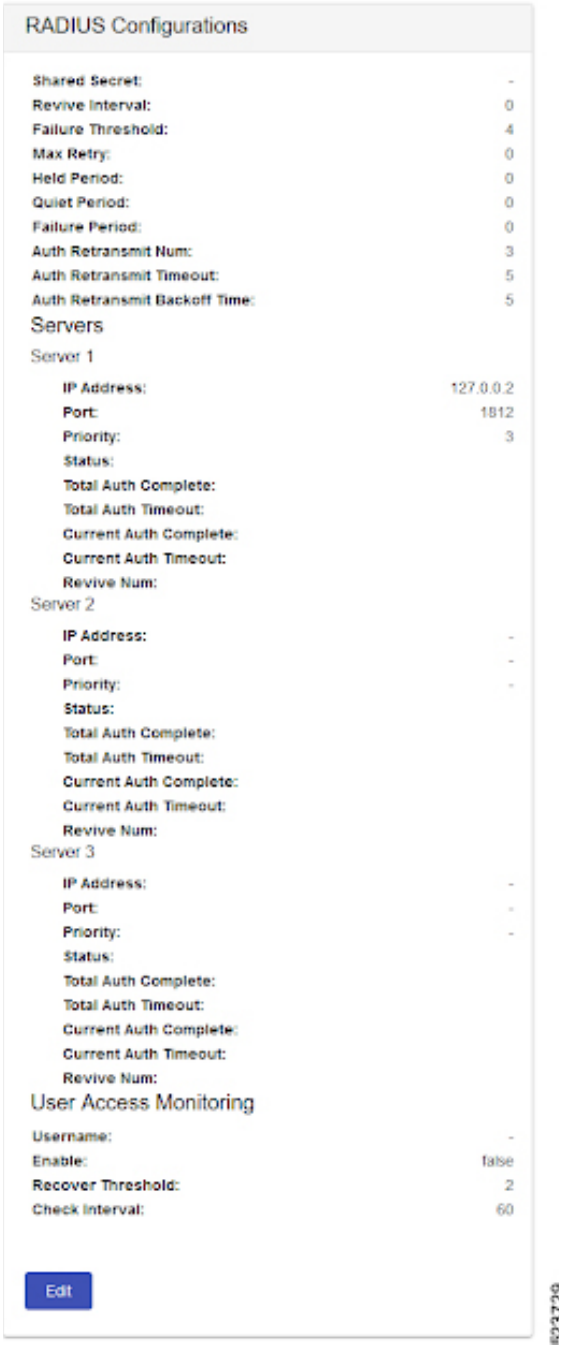
© 2024 Cisco and/or its affiliates. All rights reserved.



Authentication

This tab allows for the configuration of RADIUS settings on this PON Controller. The Shared Secret, Revive Interval, and Failure Threshold are configured here along with the RADIUS servers and User Access Monitoring settings.

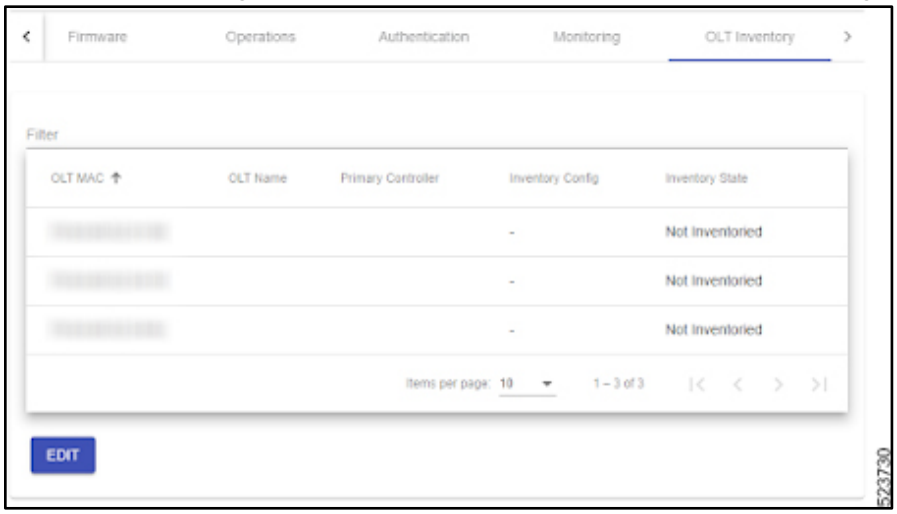
© 2024 Cisco and/or its affiliates. All rights reserved.



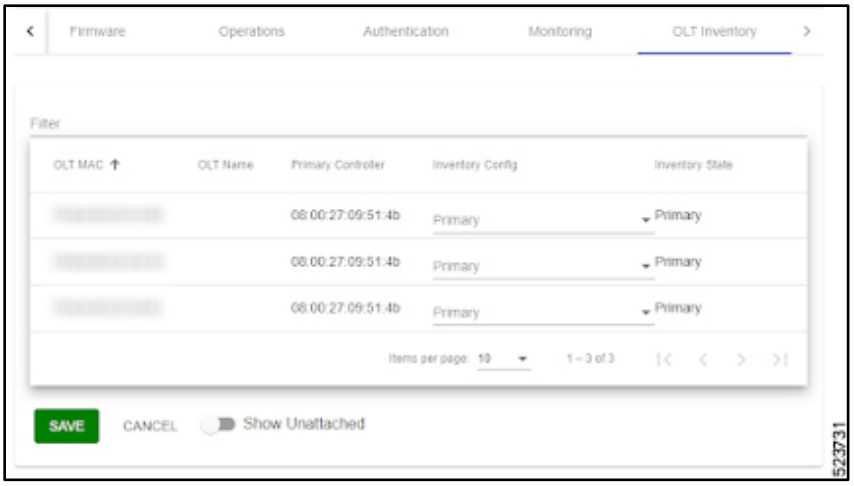
© 2024 Cisco and/or its affiliates. All rights reserved.

OLT Inventory

Each PON Controller has its own OLT Inventory. When navigating to this tab the user sees all of the OLTs managed by this Controller. OLT IDs, Names, Primary Controllers, and Inventory information are shown. The image below shows a Controller's OLTs before being inventoried.



In the Edit view, a user has the ability to set each OLT to be saved in this Controller's inventory as Primary, Secondary, Excluded, or Not Inventoried. OLTs that do not have a Controller (common case for Pre-Provisioned OLTs) can be added by toggling "Show Unattached" while editing. The example below shows the Edit view of the same Controller after its OLTs were all set to Primary.



Add OLT to Inventory

Select the dropdown in the Inventory Config column of the OLT you wish to configure. Choose if you would like to make this Controller its "Primary" Controller, "Secondary" Controller in case its primary fails, or "Excluded" from being controlled by this Controller. Click SAVE to save the

© 2024 Cisco and/or its affiliates. All rights reserved.

changes. Note that text will appear red for Inventory Config and State while the controller cycles through before recognizing the changes.

Remove OLT from Inventory

Select from the Inventory Config column the dropdown of the OLT you wish to configure. Choose “Not Inventoried” and click SAVE to save your changes.

Monitoring

A PON Controller has four sub-tabs beneath Monitoring. 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.

Alarms

See Alarms section for information about the alarms page.

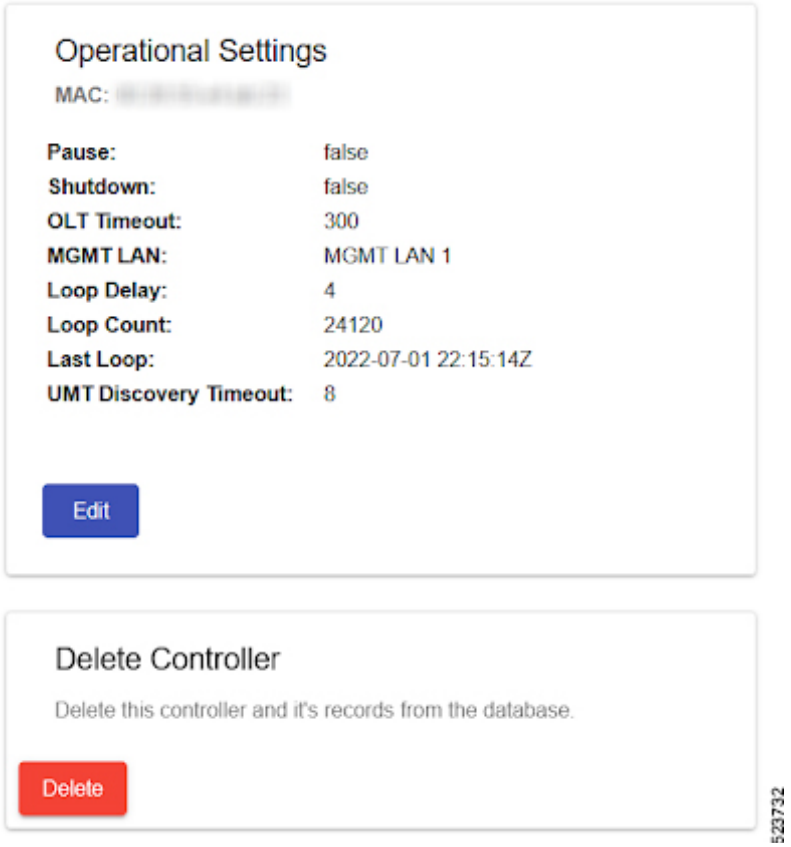
Logs

See Logs section for information about the logs page.

© 2024 Cisco and/or its affiliates. All rights reserved.

Operations

There are several fields describing a PON Controller's behavior. From this tab, the PON Controller can be Paused or Shutdown, and the OLT Timeout, Management LAN Name, and Loop Delay can be configured. All data belonging to this Controller may also be deleted. The delete action prompts for a confirmation and cannot be undone if confirmed.



Pause a Controller

To pause a controller, click EDIT to modify the configuration. Select "True" from the Pause dropdown menu. When the PON Controller is paused, the Controller continues to run, but skips processing configuration changes and gathering monitoring data for OLTs and ONUs. Click SAVE to apply your changes.

© 2024 Cisco and/or its affiliates. All rights reserved.

Shutdown a Controller

To shutdown a controller, click EDIT to modify the configuration. Select “True” from the Shutdown dropdown menu. When PON Controller Shutdown is set to 'true', the PON Controller application completes outstanding processing for OLTs and ONUs and cleanly exits. Click SAVE to apply your changes.

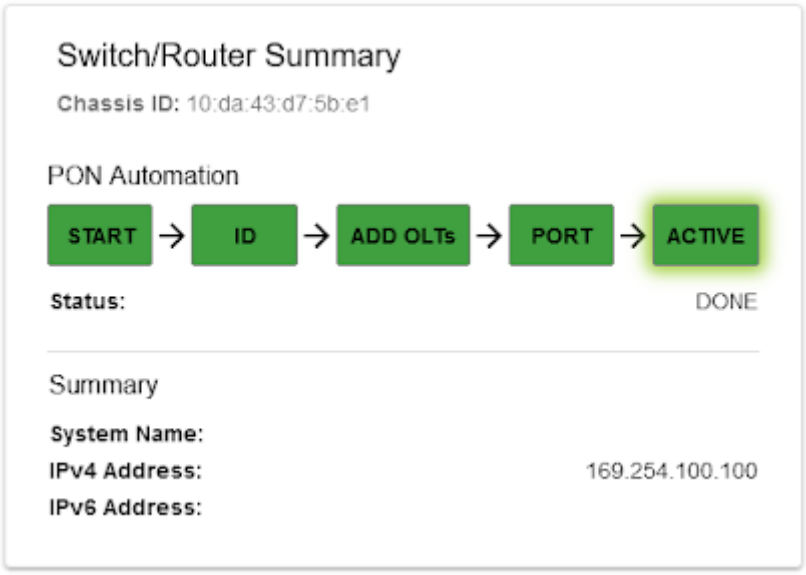
Delete a Controller

Click DELETE and confirm you wish to delete all configuration records from the database in the popup. After confirming the popup, the Controller’s records will be immediately deleted.

Switch/Router

Summary

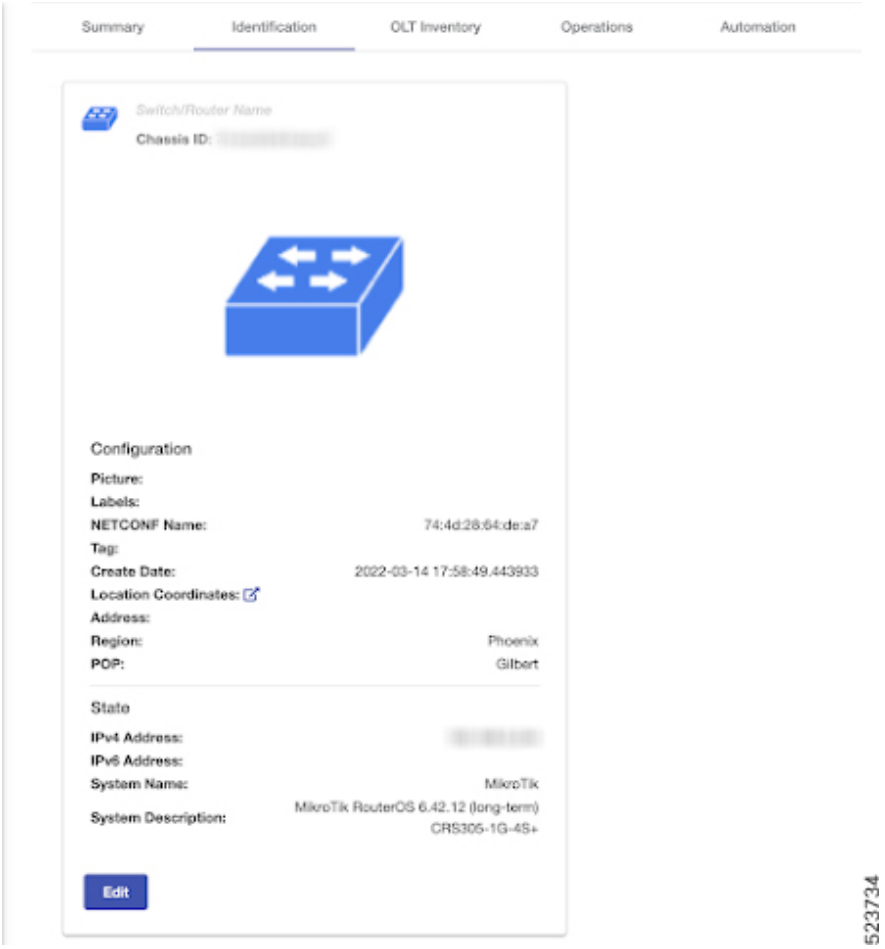
A Switch/Router’s Summary tab shows the Switch’s ID, System Name, IPv4 and IPv6 Addresses for quick reference.



Identification

Similar to the Identification tab of a Controller, this tab for a Switch allows the viewing and configuration of a Switch’s Name, Tag, Location, and more. The configurable fields are listed under the “Configuration” heading, while informational read-only fields are listed under “State”. If a Switch’s picture configuration is set to an image in the database, it displays that image in place of the default blue icon.

© 2024 Cisco and/or its affiliates. All rights reserved.



Configure Switch/Router Name

At the top of the card above the switch picture, there will be an input box where you can type in any name with no restrictions for the new switch name. Click SAVE to save your changes.

Configure Switch/Router Picture

Where the “Picture” label was before, you will see a dropdown list of all of the switch pictures in your database. Select the one you want to see a preview of. (If you do not see the picture you want, you can add pictures by going to: Global Config, Files, Pictures tab). Click SAVE to save your changes.

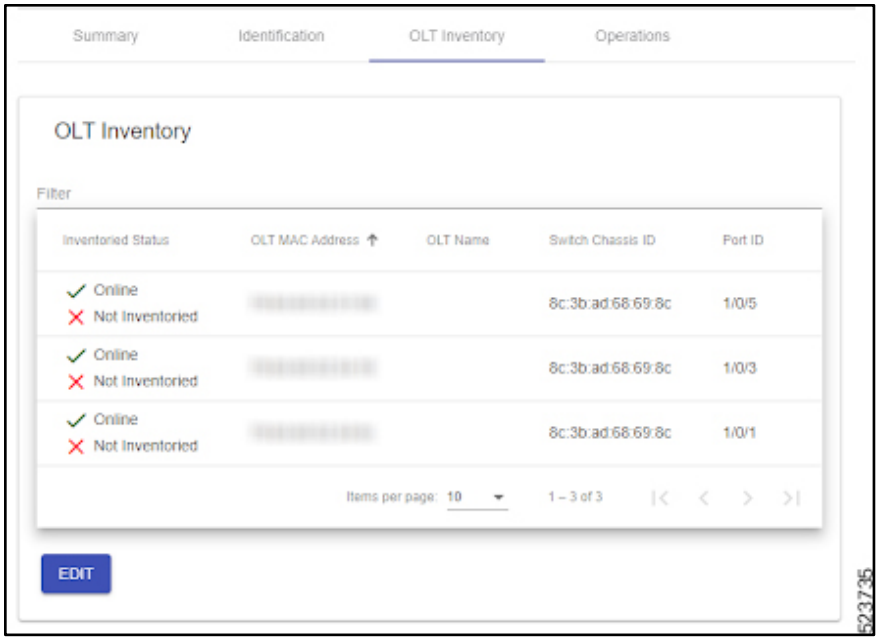
Configure Location Coordinates

See Configure Location Coordinates

© 2024 Cisco and/or its affiliates. All rights reserved.

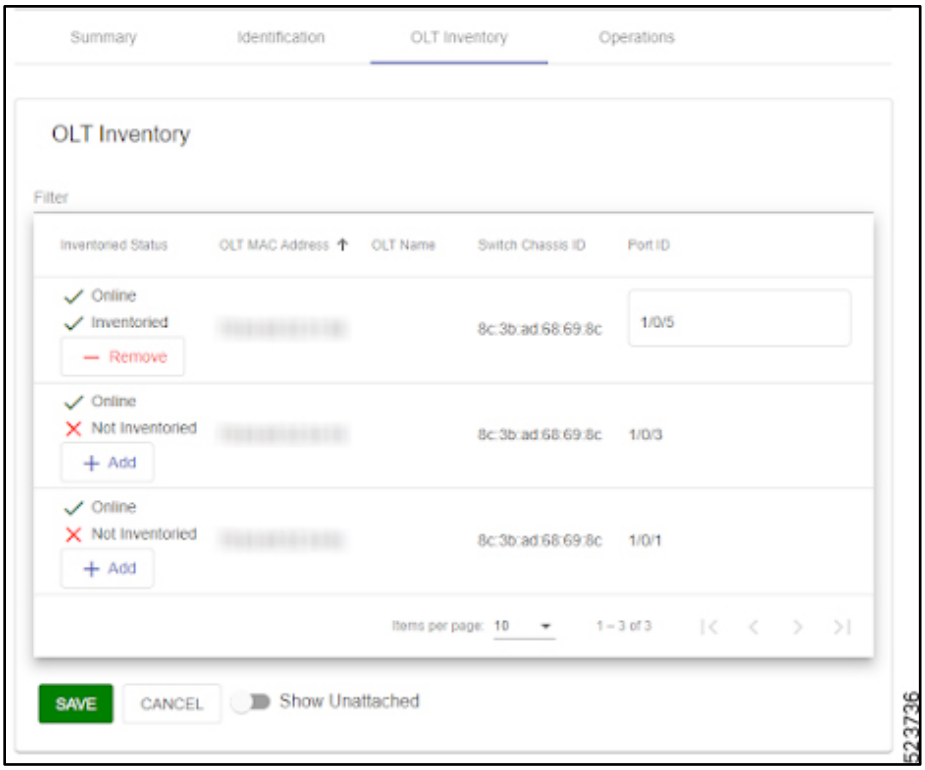
OLT Inventory

Much like the PON Controller's OLT Inventory, the Switch OLT Inventory lists all of the OLTs plugged into the Switch. The main view displays each OLT's status, MAC Address, and Name, alongside the Switch ID, and each OLT's Port ID. The image below shows a Switch with three OLTs that are active but not inventoried.



The next example shows the edit view of the same Switch's OLT Inventory after one OLT has been added. After adding the OLT to the inventory, the Port ID becomes editable. One case where a user may want to edit the Port ID is so the PON Manager will show when the actual port the OLT is in does not match the configured/desired port, indicating the OLT was moved. To show and edit Unattached OLTs (OLTs that do not belong to a Switch), toggle the "Show Unattached" option.

© 2024 Cisco and/or its affiliates. All rights reserved.



Add OLT to Inventory

Click the Add button on the OLT which you would like inventoried. This will then inventory the OLT in the Switch's configuration and will allow you to edit the Port ID. Click the SAVE button on the bottom of the card in order to save your changes.

Remove OLT from Inventory

After clicking EDIT, click the Remove button. Click the SAVE button to save your changes. The OLT reports online or offline status, but the user is no longer able to make changes to the Port ID.

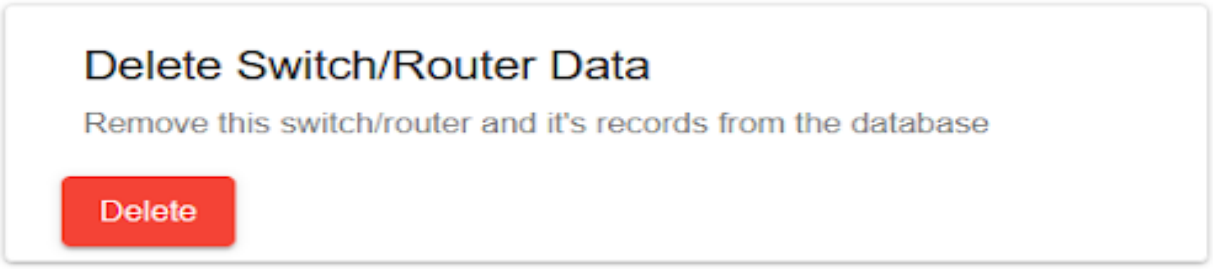
Operations

The Operations tab contains actions that apply to a Switch.

© 2024 Cisco and/or its affiliates. All rights reserved.

Delete a Switch/Router

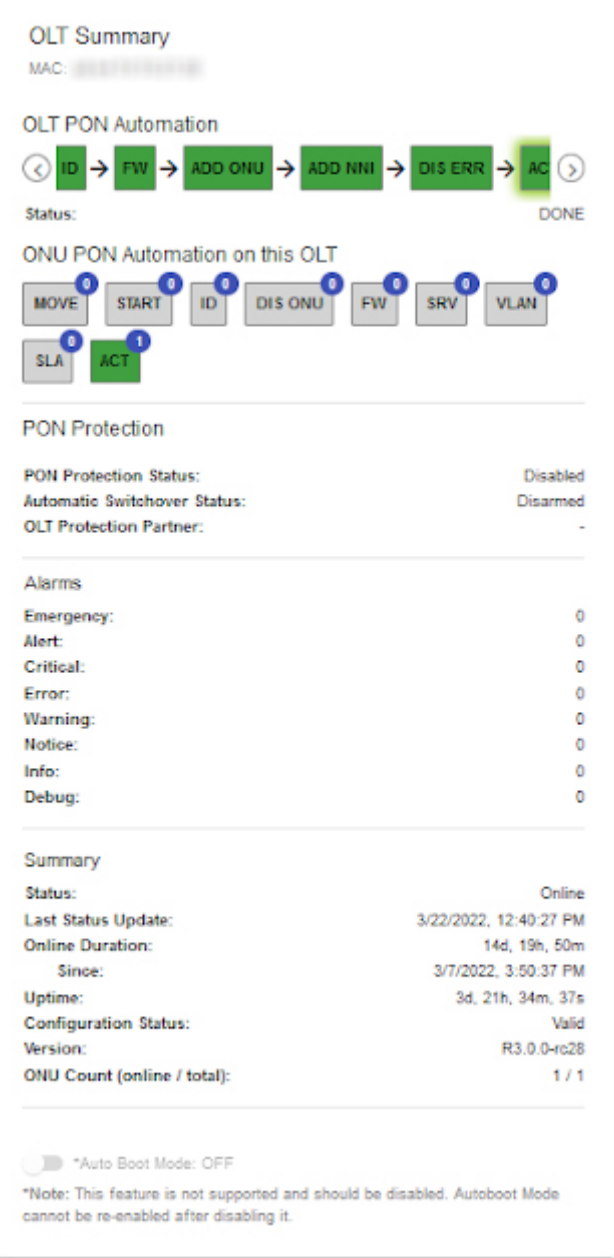
Click DELETE to remove configuration records for this switch from the database and confirm the operation in the popup. There is no need to save changes after you confirm the popup. The Switch's records will be immediately deleted. This action cannot be undone.



© 2024 Cisco and/or its affiliates. All rights reserved.

OLT

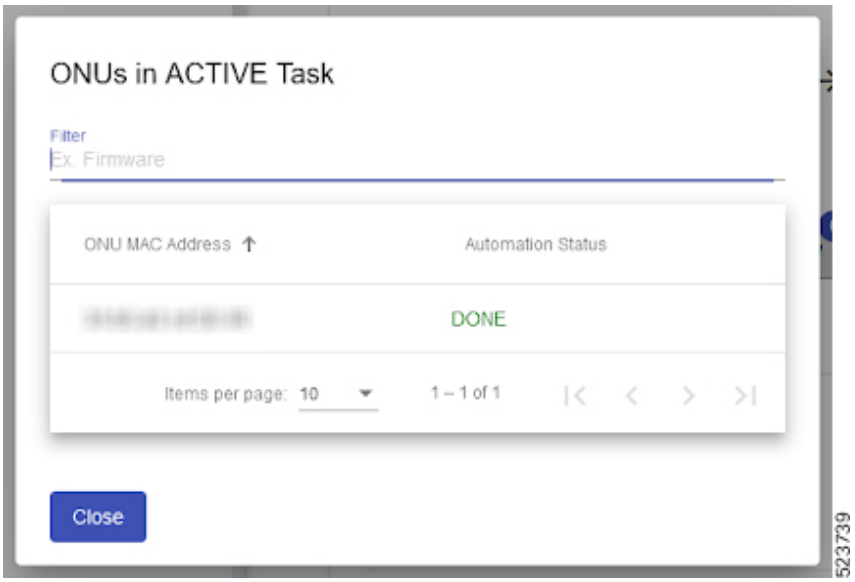
Summary



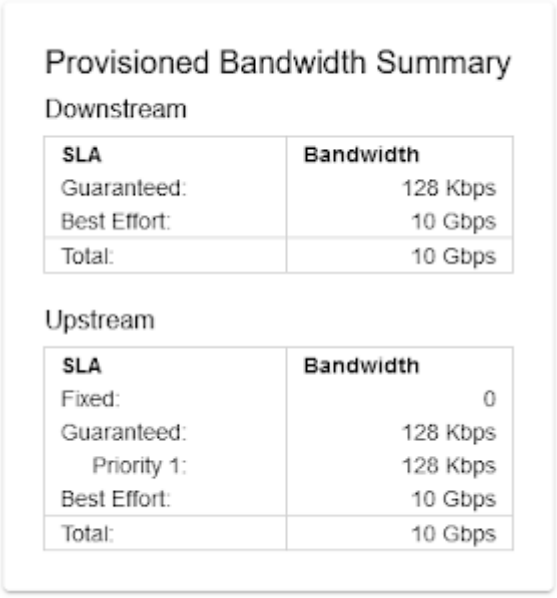
The OLT Summary tab contains three tiles with information about that OLT. The first tile has the total Raised and Unacknowledged alarm counts and device status details. The second tile displays the provisioned bandwidth of the OLT. Finally, the third tile is a detailed list of Raised and Unacknowledged alarms on this OLT.

Several details about the OLT can be found on the first tile. The ‘Online Duration’ field is displayed for an online OLT and 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.

© 2024 Cisco and/or its affiliates. All rights reserved.



Provisioned Bandwidth Summary



Provisioned Bandwidth Summary

Downstream

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

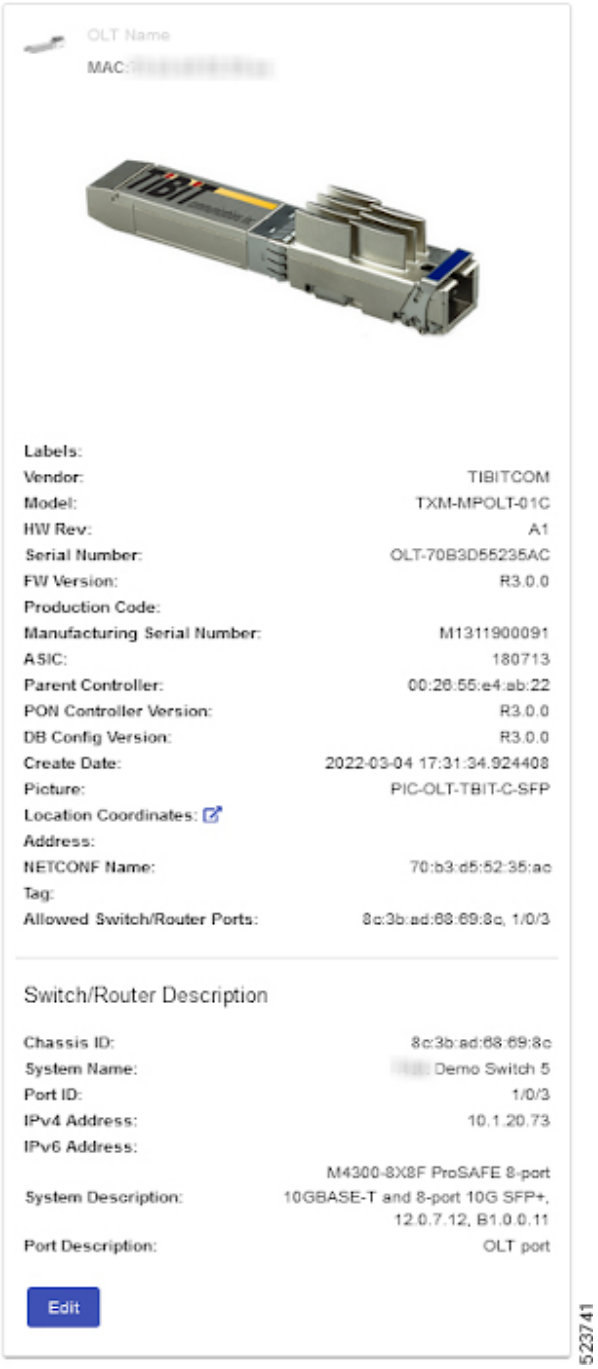
Upstream

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

The OLT Summary's provisioned bandwidth tile provides a quick view of the OLT's configured guaranteed and best effort rates for both upstream and downstream bandwidth based on its ONUs' SLAs. The guaranteed row is a summation of the priority # rows below it. The priority # comes from the configured priorities of each of the ONUs' SLAs and are ordered 1-8. Each priority row is a summation of all ONUs on that OLT whose SLA has that priority.

© 2024 Cisco and/or its affiliates. All rights reserved.

Identification



The OLT Identification tab contains various fields that help to describe and identify the OLT. The single tile lists details about the OLT hardware, firmware and a few configurable items. There is also a Switch Description at the bottom that provides the OLT's parent Switch information as well.

Several values are configurable from this tab including the OLT's Name, Picture, and Tags.

Configure OLT Name

Click EDIT. At the top of the card above the OLT picture, there will be an input box where you can type in any name with no restrictions for the new OLT name. Click SAVE to save your changes.

Configure OLT Picture

Click EDIT. Where the "Picture" label was before, you will see a dropdown list of all of the OLT pictures in your database. Select the one you want to see a preview of. (If you do not see the picture you want, you can add pictures by going to: Global Config, Files, Pictures tab). Click SAVE to save your changes.

Configure Location Coordinates

See Configure Location Coordinates

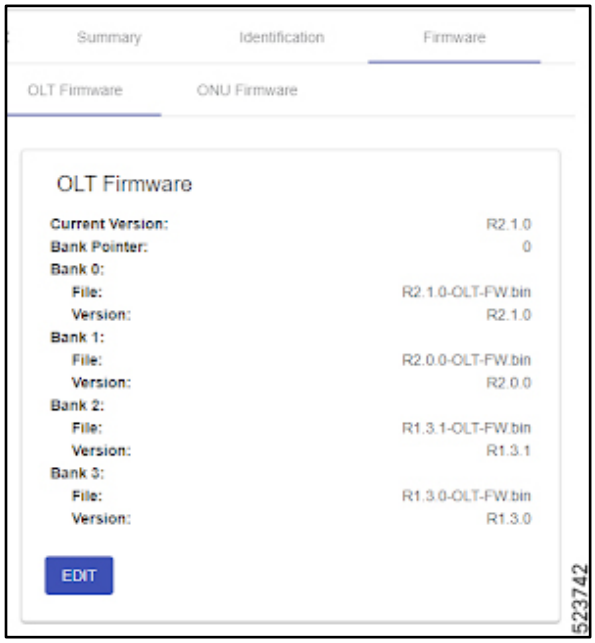
© 2024 Cisco and/or its affiliates. All rights reserved.

Firmware

The Firmware tab contains two sub-tabs that allow for managing the Firmware on a given OLT and monitoring the firmware status on subtended ONUs, respectively; OLT Firmware and ONU Firmware.

OLT Firmware

The OLT Firmware sub-tab shows the configured and active settings for the OLT's firmware. The tile displays the firmware versions in each firmware bank and the current version that is running. When editing, the firmware banks allow for the selection of any version of OLT firmware found in the database.



Upgrade OLT Firmware

To upgrade the OLT firmware, click EDIT. Set the Bank Pointer by selecting the bank from the dropdown with the desired Firmware Image to be used. Ensure that this dropdown is not set to 'Upgrade Disabled'. For Banks 0-3, use the dropdowns to select the desired firmware image for each bank. Click SAVE.

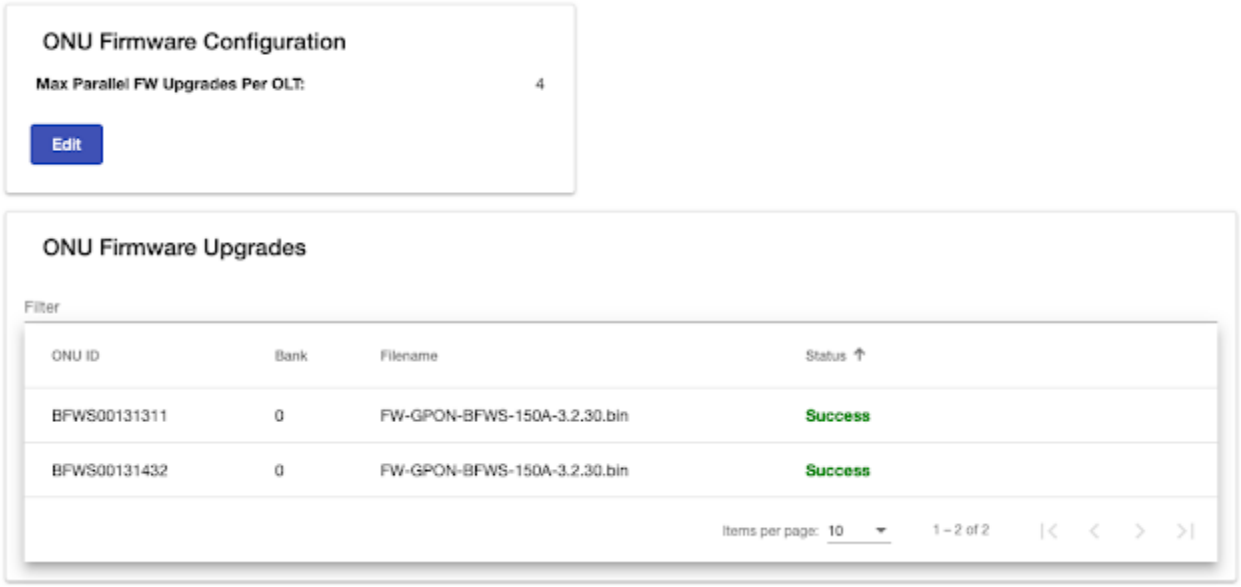
Disable OLT Firmware Upgrade

To disable firmware upgrade for an OLT, click EDIT. Set the Bank Pointer dropdown to 'Upgrade Disabled'. Click SAVE. Note: disabling firmware upgrade does not cancel a download that is already in-progress.

© 2024 Cisco and/or its affiliates. All rights reserved.

ONU Firmware

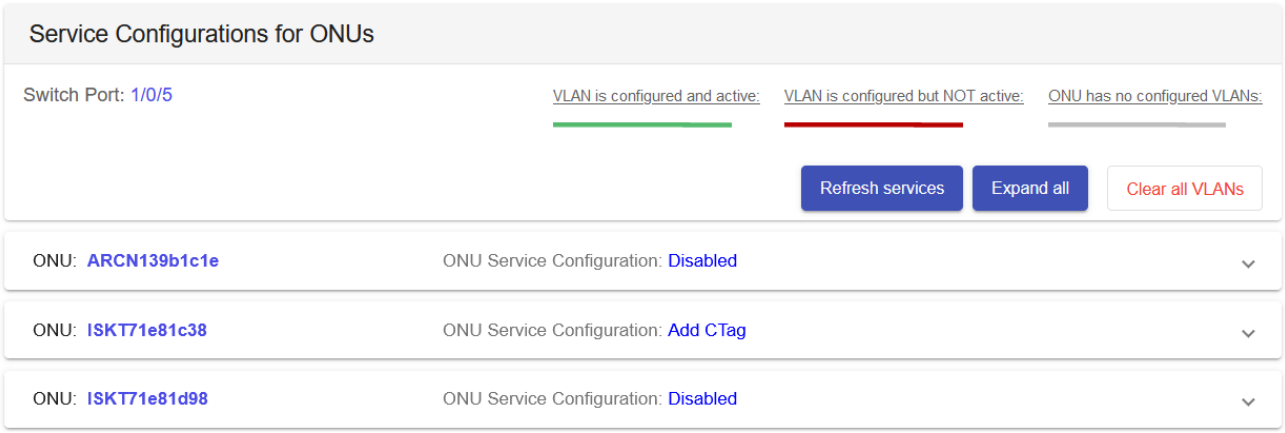
The ONU Firmware sub-tab is similar to the PON Controller ONU Firmware tab, displaying the maximum allowed parallel upgrades on this OLT and the firmware upgrade status for all ONUs connected to this OLT. The first tile allows for the viewing and configuration of the maximum parallel ONU upgrades on this OLT. The second tile displays the ONU firmware upgrade status, which lists the ID of the ONU, the firmware bank the file was saved to, the filename, and the status. The status column displays the last reported status for the firmware upgrade: “Success”, “Downloading” with percent complete, or “Failed”.



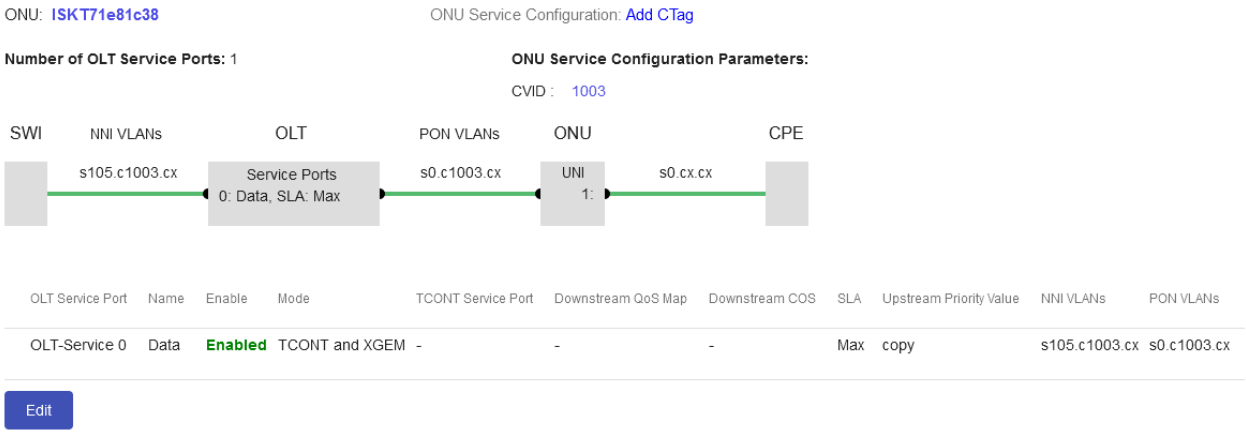
Services

The Services tab provides a detailed summary of the services configured on this OLT. This tab displays a list of ONUs attached to this OLT with dropdown panels, which the user can expand to see the detailed service configuration for each ONU.

© 2024 Cisco and/or its affiliates. All rights reserved.



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.

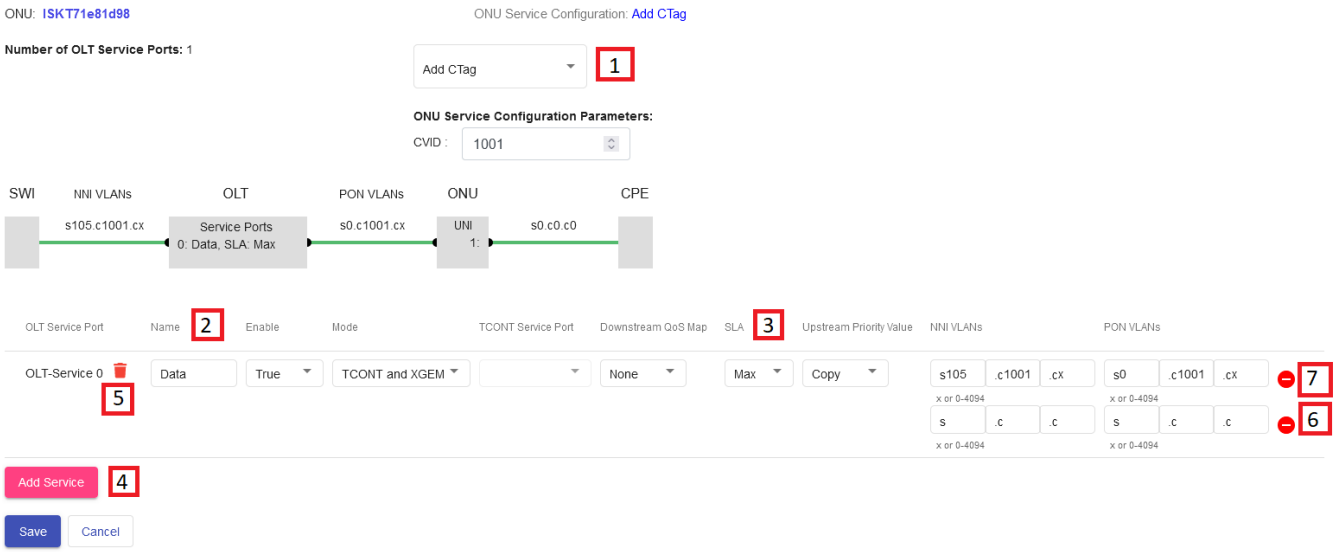


The diagram is a visual representation of the OLT services configured on the selected ONU. Each configured OLT service will appear in the diagram as a single row containing a Switch, OLT, ONU, and CPE block. The SWI block represents the switch or router the OLT is inserted into. The OLT block has text displaying OLT Service port number, name, and SLA configuration. The ONU block has text representing which UNI port number correlates to this OLT Service. The CPE block and UNI VLANs connection adapt to the diagram depending on the selected Service Configuration, Service Values, and selected Downstream QoS Map. The NNI, PON, and UNI VLAN lines will appear green if the config values are matching the state values. Alternatively, the lines will appear red if the config values do not match the state values.

© 2024 Cisco and/or its affiliates. All rights reserved.

Edit Mode

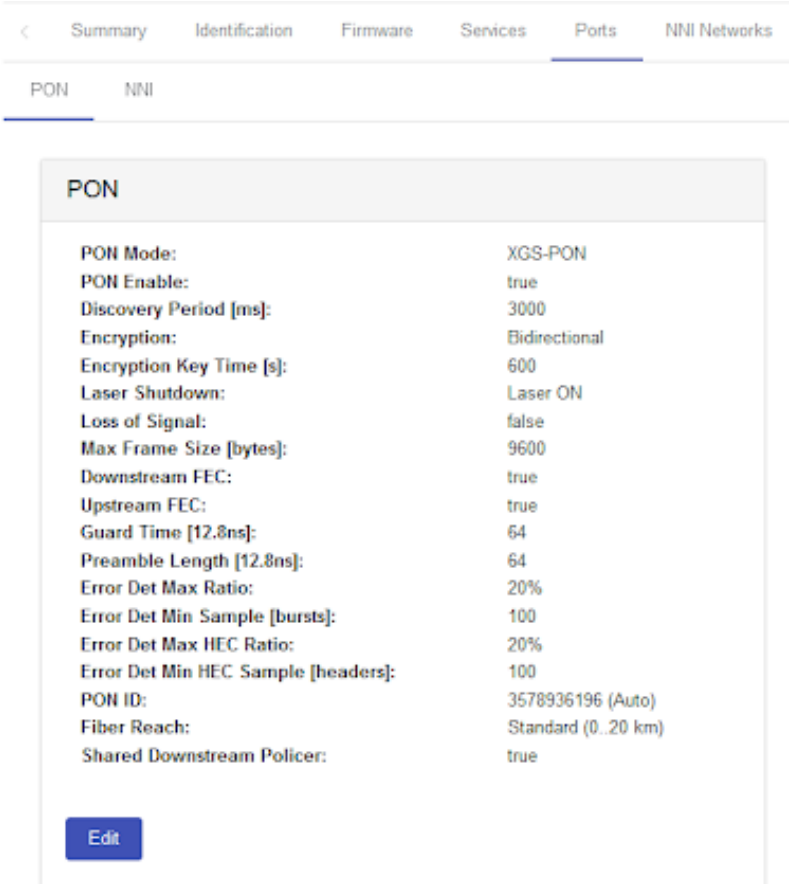
This section provides an overview of the edit mode for OLT Services. Here, the user can make and save changes to the OLT Services configuration. To begin, click the Edit button.



1. **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.
2. **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”. See OLT Services for more information.
3. **SLA and CoS** - Set SLA by selecting it from the dropdown. See OLT Services for information about the Mode, Downstream QoS Map and Upstream Priority Values.
4. **Add OLT Service Ports** – Add an OLT Service to an ONU by clicking the “Add Service” button.
5. **Remove OLT Service Ports** – Remove an OLT Service from an ONU by clicking the red trash can icon. This option is not available for the first service of a 10G EPON ONU as the primary link cannot be deleted.
6. **Add VLAN Tags** - Add a VLAN by clicking filling in the next available blank row. Users may enter ‘X’ to match any, 0 for untagged/priority tagged or the VLAN ID values 1 - 4095.
7. **Remove VLAN Tags** - Remove VLAN by clicking the red circular button to at the end of the row.

© 2024 Cisco and/or its affiliates. All rights reserved.

Ports



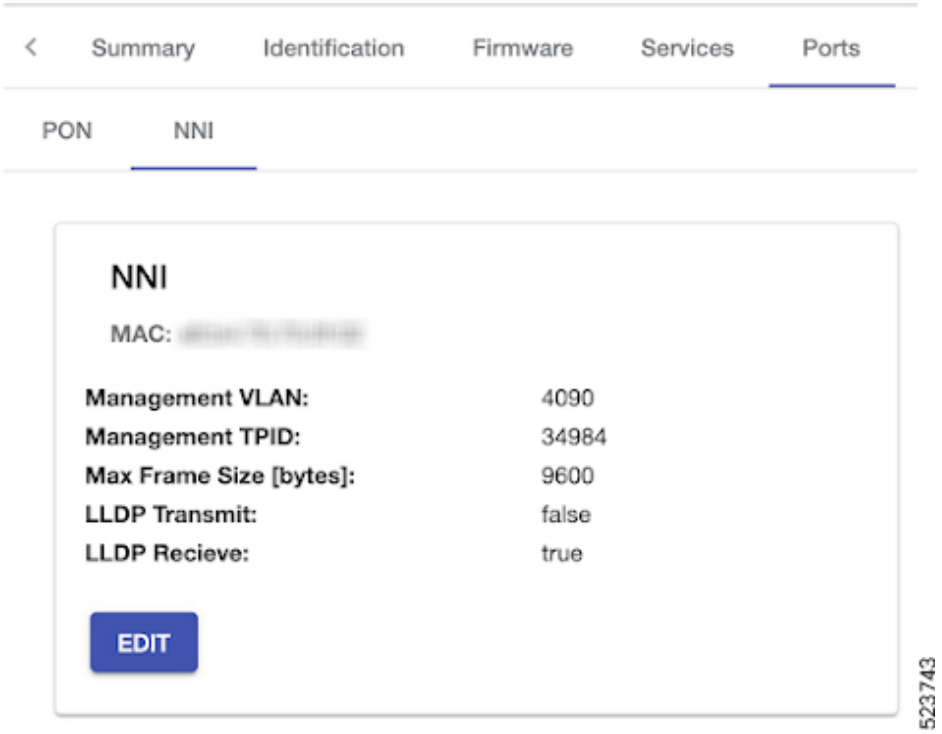
The OLT Ports tab has two sub-tabs. The PON sub-tab has a single tile with the OLT PON port configuration. Note that fields listed on this sub-tab depend on the OLT PON Mode setting. If the PON Mode is set to 'XGS-PON', this tab lists XGS-PON configuration settings and state information. If the PON Mode is set to '10G EPON', this tab shows configuration and state specific to 10G EPON. (The PON mode is set to 'XGS-PON' in the example shown).

Note: the MAC Address shown at the top of this tile is the PON Port MAC Address, not the ID of the OLT.

When configuring a pre-provisioned OLT, the device will have no state data. Because of this the interface will display the PON Mode defined not by the OLT's state, but by the global PON Mode setting. When configuring an OLT that does have state data, the OLT will not be allowed to change from the global PON Mode to the other (unless the global PON Mode is set to both XGS-PON and 10G EPON). There will also be an indicator shown if the OLT is in the wrong PON Mode based on the global PON Mode setting.

© 2024 Cisco and/or its affiliates. All rights reserved.

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 shown at the top of this tile is the NNI Port MAC Address, which is equivalent to the ID of the OLT.



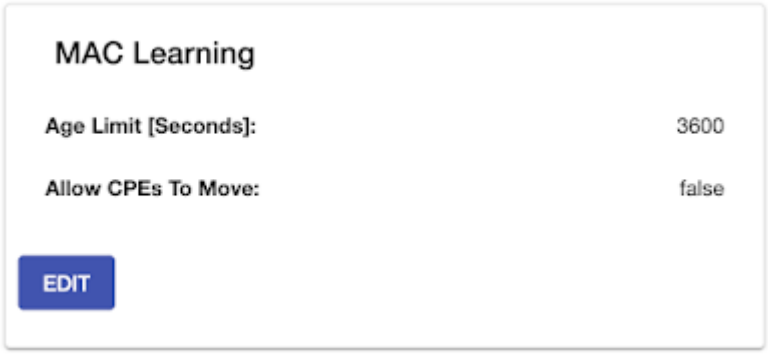
NNI Networks

The NNI Networks tab is used to configure and manage NNI VLANs, bridging, and networking for the OLT device.

Config

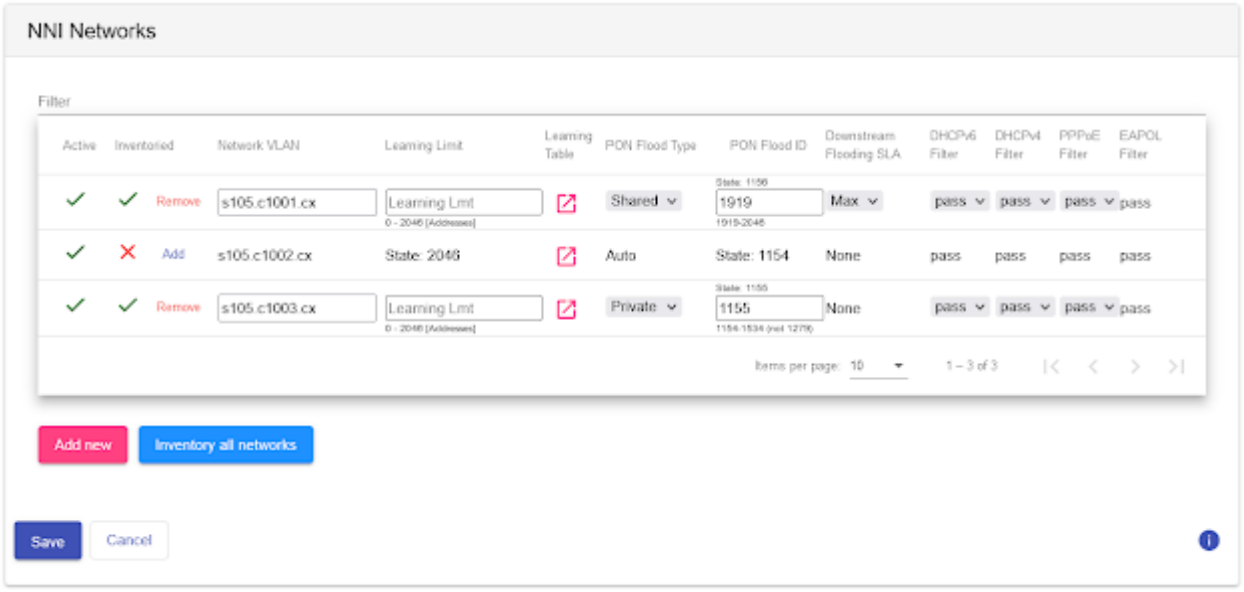
The Config tab is used to configure and manage OLT NNI Networking, including MAC learning controls and NNI Network inventory. The MAC learning controls configure the aging time for CPE MAC addresses and allow a CPE to move between ONUs.

© 2024 Cisco and/or its affiliates. All rights reserved.



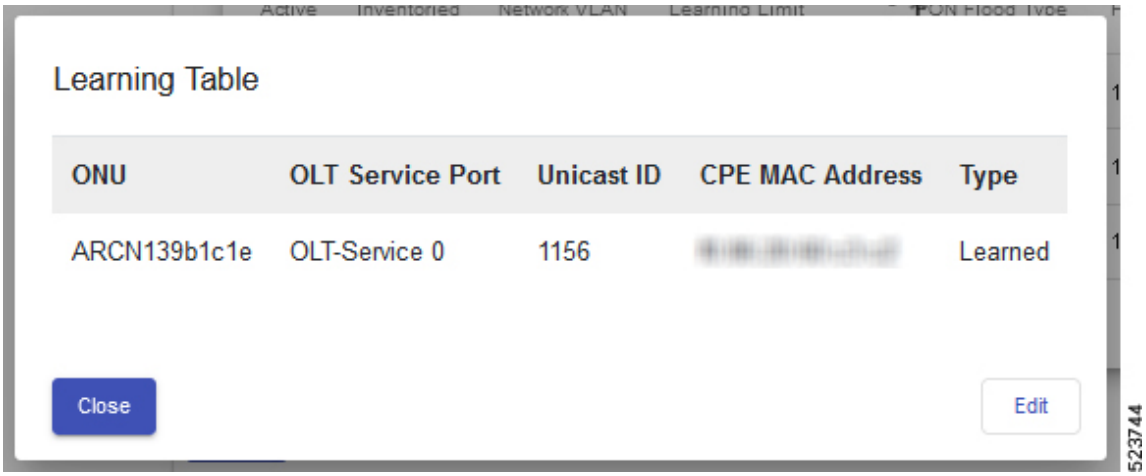
The NNI Network inventory is used to configure VLANs and Networks for Layer2 Switch Domains (L2SD) on an OLT device. NNI network inventory configuration includes the VLAN stack, DHCP Relay Protocol Filters, PPPoE filter, Learning Limit, along with the PON Flood ID and the associated Downstream Flooding SLA. Existing NNI networks may be added to the OLT's inventory and new networks may be created as well.

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



The Learning Table displays dynamically learned and statically configured CPE MAC addresses for an NNI Network. Click the Learning Table column to view the list of CPE devices learned on a network. The following fields are displayed in the learning table: ONUs, OLT Service Ports, CPE MAC Addresses and Unicast IDs.

© 2024 Cisco and/or its affiliates. All rights reserved.



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, or 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" will disable 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 being used: EPON or GPON. The ranges and descriptions for each type are described in the table below.

EPON Flooding

Type	Range	Description
Private	5121 - 6013 (not 5375, 5631, 5887)	Frames are flooded to a single ONU on the specified unicast LLID.
Shared	6014 - 6141	Frames are flooded to one or more ONUs on the specified multicast LLID.
Auto	-	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.

© 2024 Cisco and/or its affiliates. All rights reserved.

GPON Flooding

Type	Range	Description
Private	1154 - 1534 (not 1279)	Frames are flooded to a single ONU on the specified unicast (bidirectional) XGem Port ID.
Shared	1919 - 2046	Frames are flooded to one or more ONUs on the specified multicast (downstream only) XGem Port ID.
Auto	-	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.

Add An Existing NNI Network To Inventory

To add an existing NNI Network to inventory, first click the ‘Edit’ button on the desired OLT NNI Network table. Following this, select the ‘Add’ button in the ‘Inventoried’ column of the NNI Network to be added. An NNI Network can be added to inventory if it is Active and Not Inventoried, as indicated by their respective columns.

Add a new NNI Network to Inventory

To add a new NNI Network to inventory, first click the ‘Edit’ button on the desired OLT NNI Network table. Following this, select the ‘Add New’ button on the bottom of the panel. This inserts a new row to be configured. The new NNI Network can be found as the last entry in the table. The Network VLAN needs to be configured before the table can be saved. The PON Flood ID, Learning Limit, Static MAC Addresses, Downstream Flooding SLA, PPPoE filter, and DHCP relay can be configured as well.

Remove an NNI Network from Inventory

To remove an NNI Network from inventory, first click the ‘Edit’ button on the desired OLT NNI Network table. Following this, select the ‘Remove’ button in the ‘Inventoried’ column of the NNI Network to be removed. An NNI Network that exists and can be removed from inventory has the state; Inventoried.

Enable DHCP Relay

Note: DHCP Relay requires the DHCP Host Processing function to be enabled in the PON Controller.

To enable UMT encapsulation of the DHCP Relay on an NNI network, first click the ‘Edit’ button on the desired OLT NNI Network table. Set DHCPv4 and/or DHCPv6 in the Enable Filters column to ‘umt’, which programs the OLT to forward DHCP messages over a UMT tunnel to the

© 2024 Cisco and/or its affiliates. All rights reserved.

DHCP Relay Agent Host Processing function in the PON Controller. When enabled, the DHCP Relay Agent inserts Option 82 in DHCP messages received from the client. Set the DHCPv4(v6) dropdown to ‘pass’ to disable this feature.

DHCP Relay must also be configured for the ONU Service associated with this NNI Network. See Enable DHCP Relay in ONU Service for more information.

Enable PPPoE

Note: PPPoE requires the PPPoE Intermediate Agent Host Processing function to be enabled in the PON Controller.

To enable PPPoE on an NNI network, first click the ‘Edit’ button on the desired OLT NNI Network table. Set PPPoE in the Enable Filters column to ‘umt’.

PPPoE must also be configured for the ONU Service associated with this NNI Network. See Enable PPPoE in ONU Service for more information.

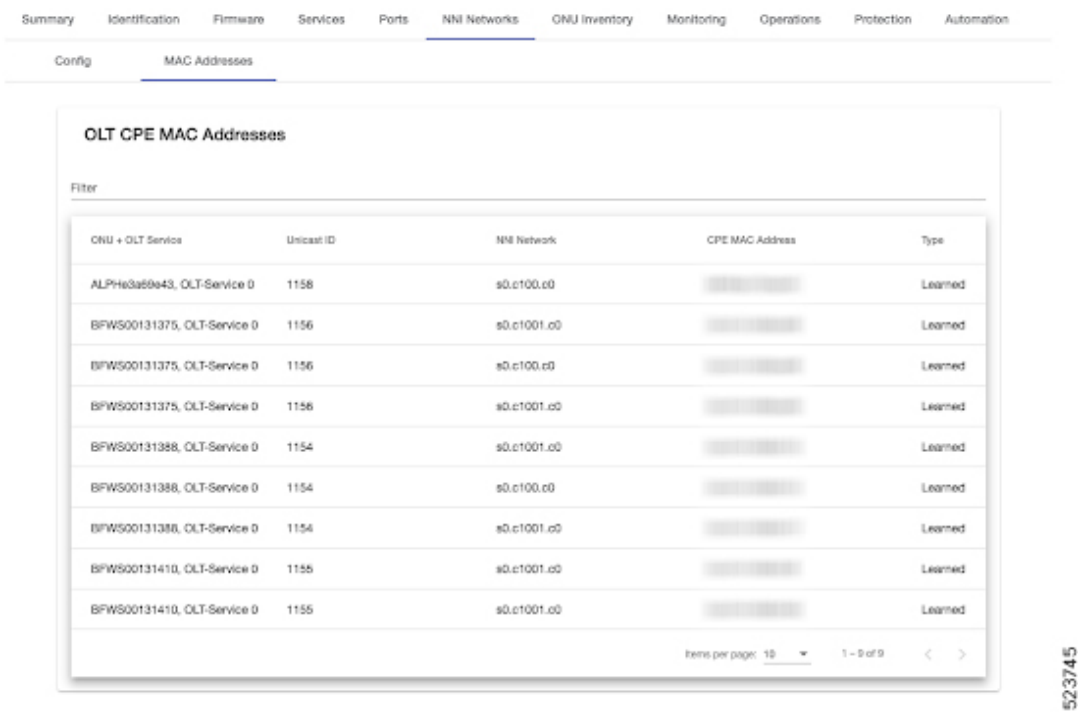
Add Static MAC Addresses

Click the icon in the column ‘Learning Table’ for the network VLAN you wish to add to. After clicking ‘Edit’ in the popup you can start adding CPE MAC addresses. Start by selecting the ONU and the OLT service port you would like to add to and then type in a properly formatted MAC address. The ‘ADD’ button will then allow you to add to the table. Save to the database by clicking the ‘SAVE’ button before closing the popup or your edits will be lost.

MAC Addresses

The MAC Addresses 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”.

© 2024 Cisco and/or its affiliates. All rights reserved.

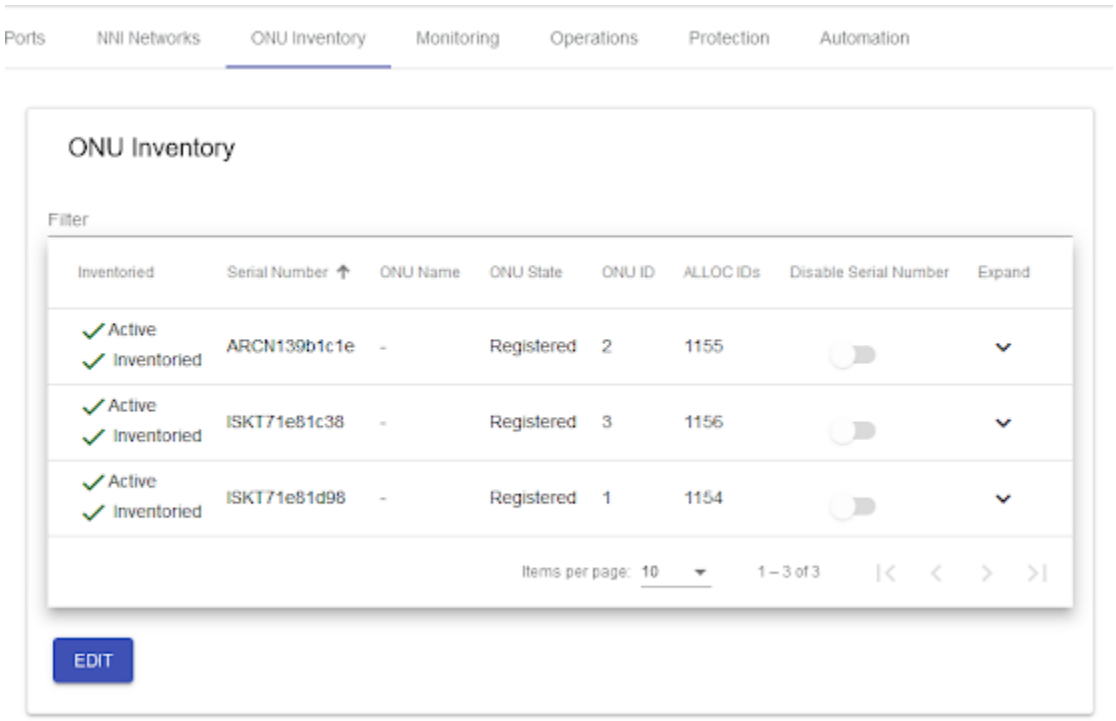


ONU Inventory

The ONU Inventory tab allows for the viewing and configuration of this OLT's inventory of ONUs. The inventory allows the OLT to quickly re-add and reconfigure attached ONUs upon restart. The table shown on this tab displays the ONU IDs, Serial Number/MAC Address, Name, State, ONU Inventory ID, and ALLOC IDs/LLIDs, and the disable Serial Number/Upstream Laser state. An ONU that has more information than what can be displayed has a chevron in the far right Expand column. Clicking on the row acts like an accordion. When expanded, the configured ALLOC IDs/LLIDs for the OLT Services are shown. The first image below shows this table with the second row expanded in view mode.

Note: Cisco strongly recommends that all ONUs be inventoried on the OLT they are connected to. This is required to permit fast restart and avoid transmit collisions from faulty ONUs that continue to use stale configuration after system reboots.

© 2024 Cisco and/or its affiliates. All rights reserved.

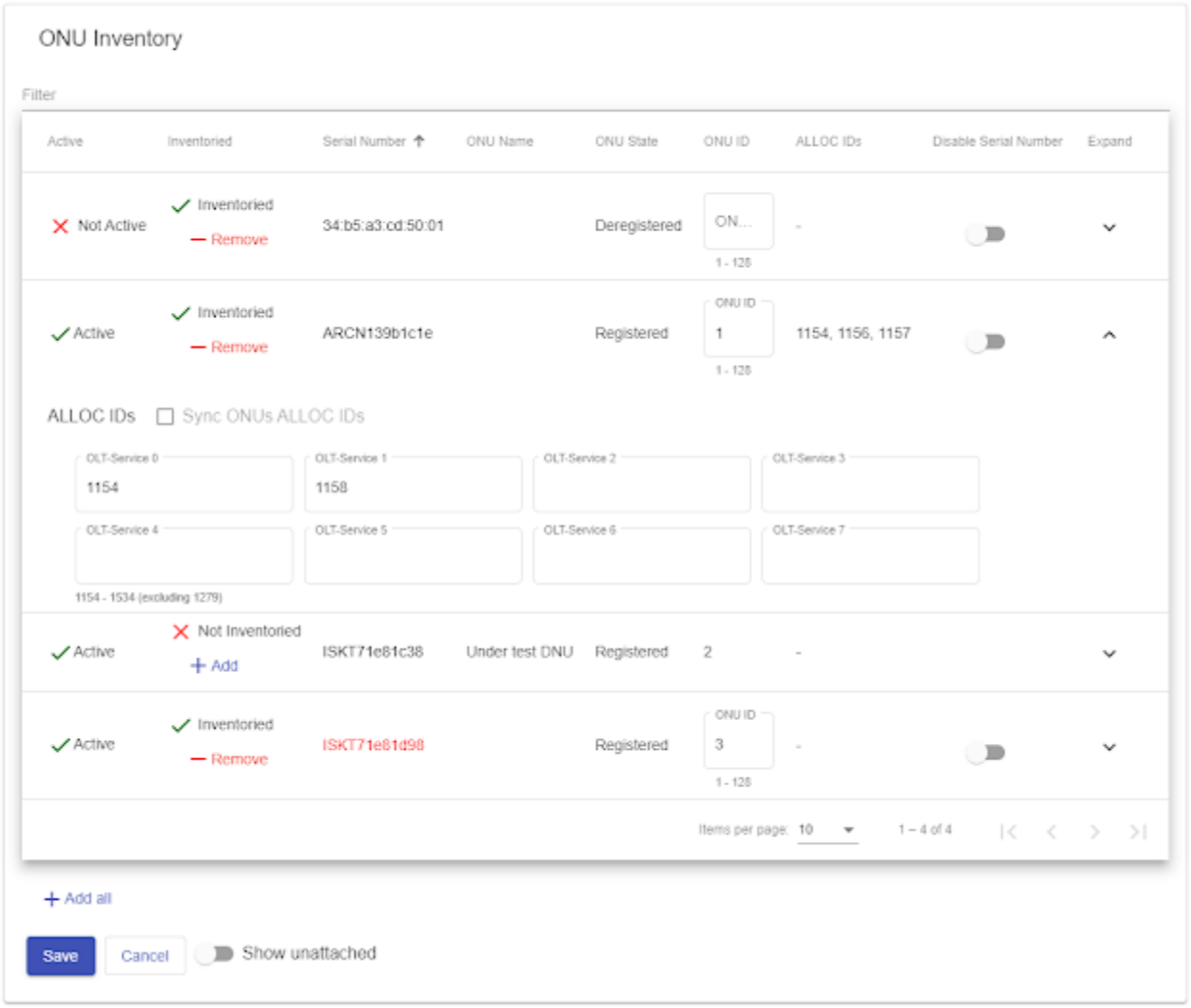


Add ONU to Inventory

Click EDIT to modify the OLT's inventory. If an ONU is not inventoried, the row displays an Add button. This sets the ONU to be saved in the OLT's inventory and allows for the inventory values to be edited. The "Add all" button has the same functionality, but for all ONUs that aren't inventoried. The ALLOC ID/LLID inputs provide the acceptable ranges and display warnings for disallowed values as they are filled in. The ONU ID is also settable from here. All ONU IDs must

© 2024 Cisco and/or its affiliates. All rights reserved.

be unique per OLT, as well as all ALLOC IDs/LLIDs. Once the desired ONUs are added and their values updated, click SAVE.



Remove ONU from Inventory

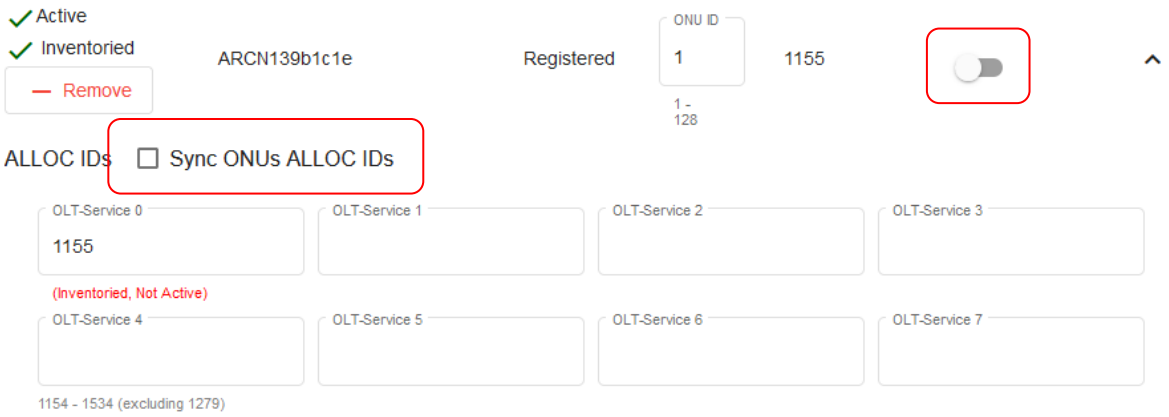
Click EDIT to modify the inventory. If the Remove button is selected, this sets the ONU to be removed from the OLT's inventory. This action does not remove the ONU from the OLT, only the inventory configuration data.

Disable Serial Number

When the ONU is added to the inventory, several operations are available to the user. There is an action to use the Disable and Enable Serial Number features of the OLT Inventory. The

© 2024 Cisco and/or its affiliates. All rights reserved.

Disable toggle action disables the ONU's transmit laser so it can no longer send messages to the OLT. To trigger this action enable the toggle and click SAVE.



Update ONU IDs, Alloc ID, and LLIDs in Inventory

A SYNC checkbox appears if the configured settings do not match what is active in the OLT's state. Clicking SYNC disables the input fields and will set them each 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.

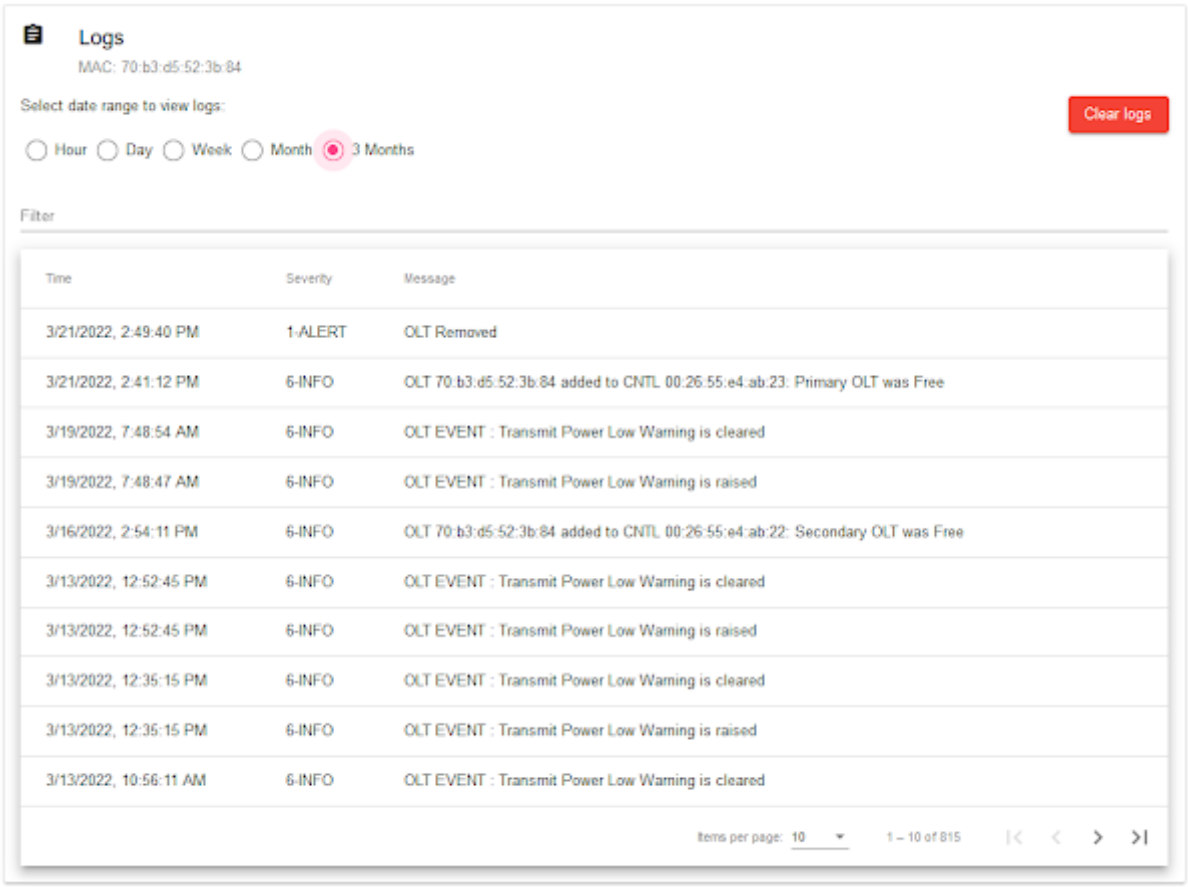
Monitoring

OLT Monitoring contains five sub-tabs: Stats, Config, Alarms, Logs, and Debug. The Config 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 to see the active alarms in detail. See the Alarms section of this document for more information on Alarms. See the Logs section of this document for more information on Logs.

The Logs sub-tab lists all log messages for this OLT that exist within the selected time range of one Hour, Day, Week, Month, or three Months. There is also an option to clear all existing logs for this OLT. Upon clicking this, the user is prompted to confirm the deletion. If confirmed, all logs for this OLT are removed from the database. This cannot be undone.

© 2024 Cisco and/or its affiliates. All rights reserved.

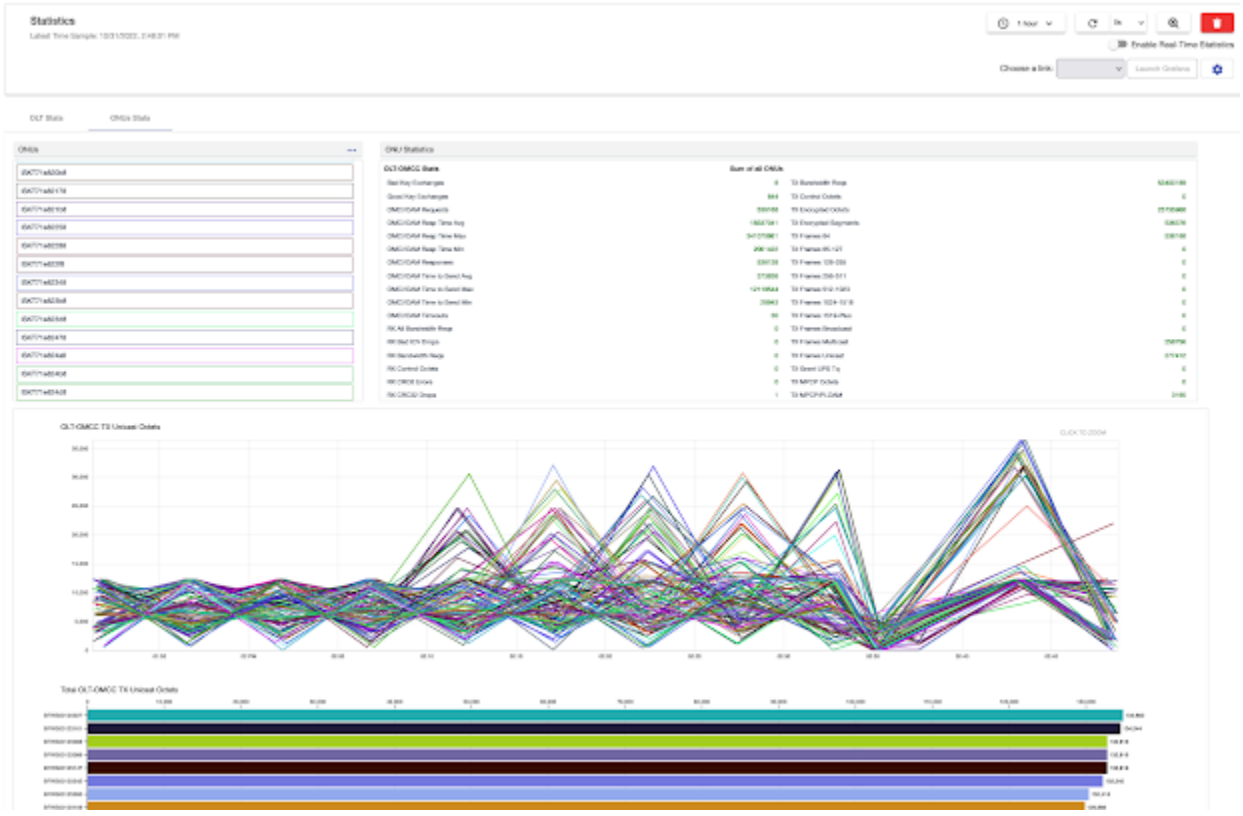


The next sub-tab under Monitoring for an OLT is the Stats tab, which presents a view of the statistics generated about the OLT's operation. See Statistics for more details on using this tab to select and display statistics counters and graphs for this device.

ONUs Stats

The OLT statistics tab also allows you to see the statistics for all of the managed ONUs for that respective OLT. The ONUs Statistics tab will display all of the subtended ONUs on one line graph per selected statistic. Users can see all of the ONUs or just a selected few. The color of the line on the graph will correspond to the outline color on the ONU after the desired stats have been selected. Hovering over the graph will show more information about the datapoint closest to the cursor. Under each line graph will be a bar chart that shows the accumulated total of each ONU over the selected time period. Zooming and panning can be done by clicking on the graph first.

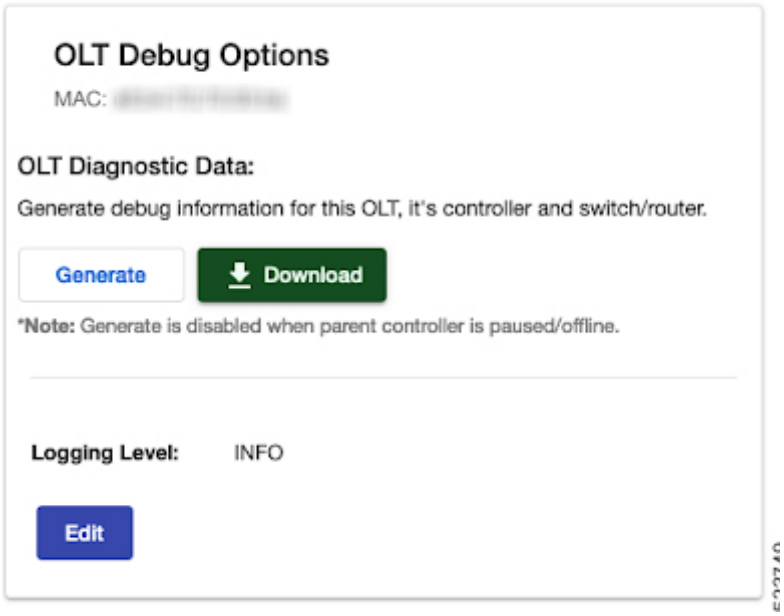
© 2024 Cisco and/or its affiliates. All rights reserved.



The Debug sub-tab contains a single tile that allows the user to configure OLT Debug Logging Level, as well as generate and download a JSON formatted dump of the OLT debug information.

Generating and downloading OLT Diagnostic data is a multi-stage process. First, click ‘Generate’ to trigger the PON Controller to collect diagnostic information from the OLT device. The ‘Download’ button remains disabled until the data collection is complete. Once the PON Controller completes the data collection, PON Manager detects that the process is complete and the ‘Download’ button is enabled, allowing the user to download the diagnostic data to the local PC.

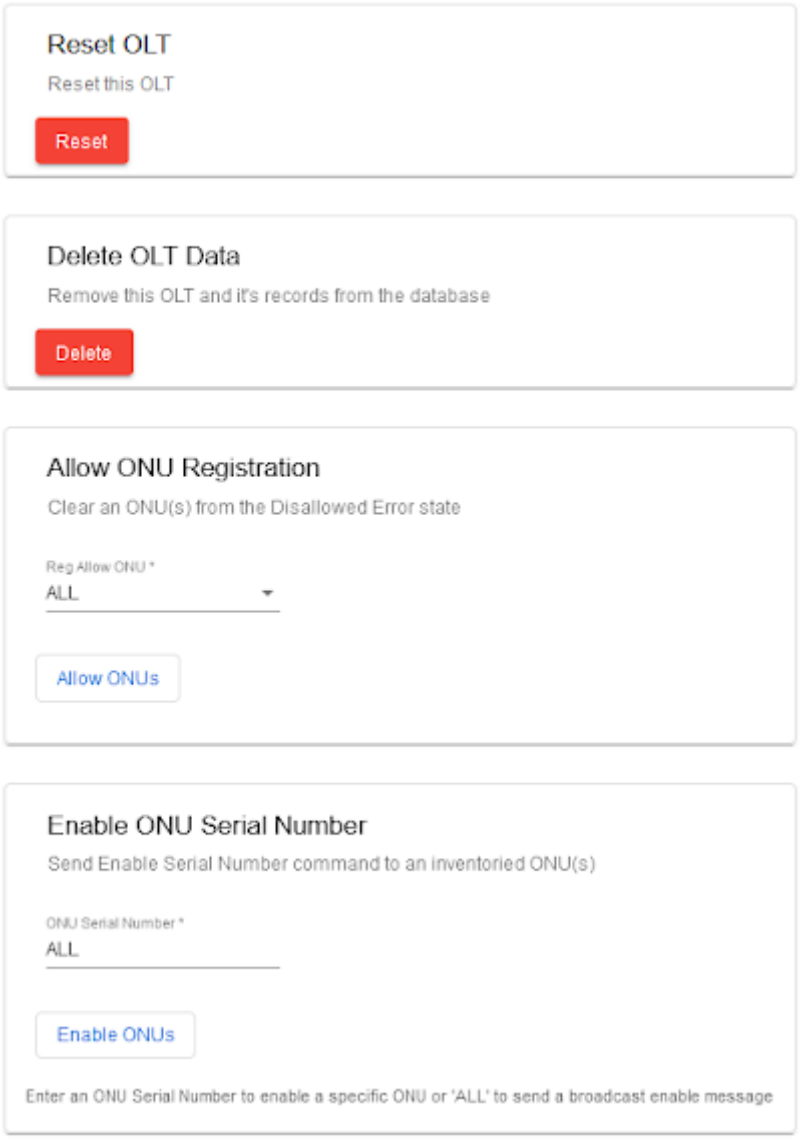
© 2024 Cisco and/or its affiliates. All rights reserved.



Operations

There are several operations that may be performed on an OLT from this tab.

© 2024 Cisco and/or its affiliates. All rights reserved.



Reset the OLT

When clicked, the user is prompted to confirm the action. Once confirmed, the OLT is sent a signal to restart. This process may take a few minutes.

Delete the OLT

The Delete action removes all configuration, state, statistics, and logging data for this OLT from the database. (However, Delete does not remove the OLT from any PON Controller or Switch OLT Inventories). After the delete is confirmed, it cannot be undone.

© 2024 Cisco and/or its affiliates. All rights reserved.

Allow ONU Registration

When an OLT detects a faulty ONU on the PON (e.g., ONU transmitting over other ONUs), the OLT restricts the ONU's access to the PON and transitions the ONU to the Disallowed Error state. The Allow ONU Registration operation clears the Disallowed Error State condition for a specific ONU or all ONUs in the Disallowed Error State.

To clear the Disallowed Error for an ONU, select the desired ONU or ALL from the dropdown field 'Reg Allow ONU'. Next, click the 'ALLOW ONUs' button to trigger the OLT to allow the ONU(s) to register.

If the OLT is busy in the process of allowing an ONU(s) to register, the message 'Allow ONU Registration operation is in progress . . .' is displayed and the 'ALLOW ONUs' button is disabled. Wait for the OLT to complete the pending Allow ONU Registration operation before attempting another Allow ONU operation.

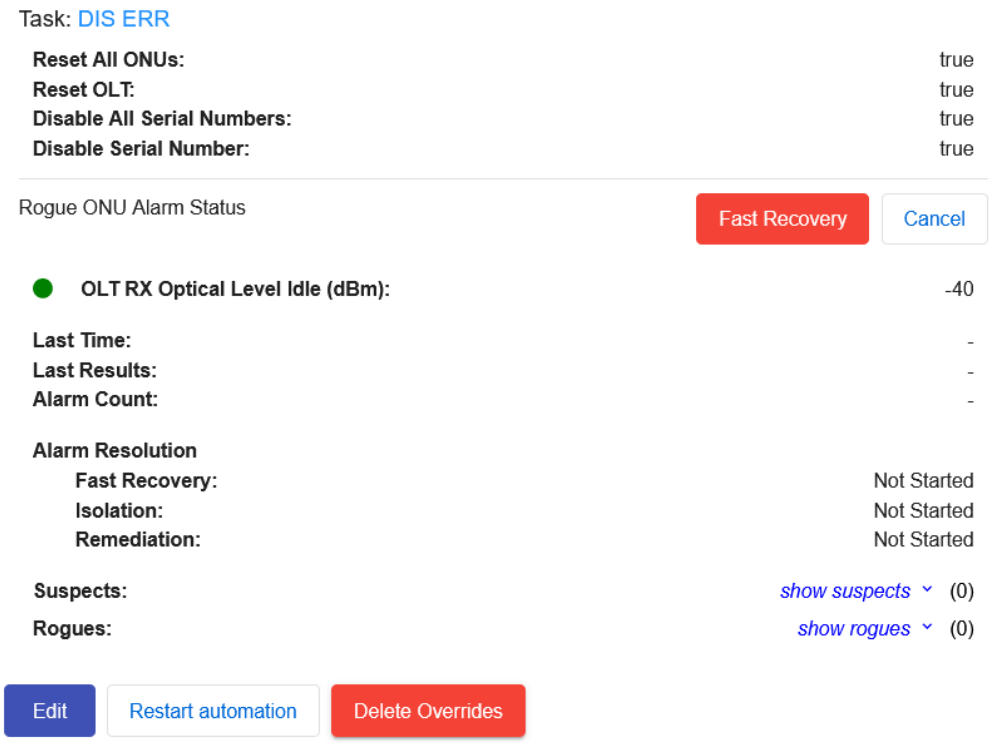
Enable ONU Serial Number/Upstream Laser

The Enable Serial Number action is an operation that enables an ONU's transmit laser such that it can communicate to the OLT. A specific ONU MAC/SN can be entered to enable a specific device or 'ALL' can be entered to send a broadcast enable message to all ONUs on the PON.

Rogue ONU

Disallowed Error and Idle Optical Power are Rogue ONU tasks for OLT automation. If issues occur during these tasks, the user will have the ability to start Fast Recovery, Isolation, or Remediation by clicking the button under Rogue ONU Alarm Status. Status of the operation is displayed under the Alarm resolution section. An operation can be canceled at any time by clicking the Cancel button.

© 2024 Cisco and/or its affiliates. All rights reserved.



Identification

The Identification tab hosts the configurations for the ONU's Name, Picture, Location, Address, NETCONF Name, Tag, Create Date, Allowed OLTs, and Expected Registration ID (XGS-PON only). This ID may be any String or 'ANY' to allow any registration ID value. Beneath the configurable items, there is a section of state details. Included here is data about the ONU's Model, Vendor, Firmware, and more. If the ONU has its picture configured, then the image is displayed in place of the default blue icon.

© 2024 Cisco and/or its affiliates. All rights reserved.

Configure ONU Name

Click EDIT. At the top of the card above the ONU picture, there will be an input box where you can type in any name with no restrictions for the new ONU name. Click SAVE to apply your changes.

Configure ONU Picture

Click EDIT. Where the “Picture” label was before you will see a dropdown list of all of the ONU pictures in your database. Select the one you want to see a preview of. (If you do not see the picture you want, you can add pictures by going to: Global Config, Files, Pictures tab). Click SAVE to apply your changes.

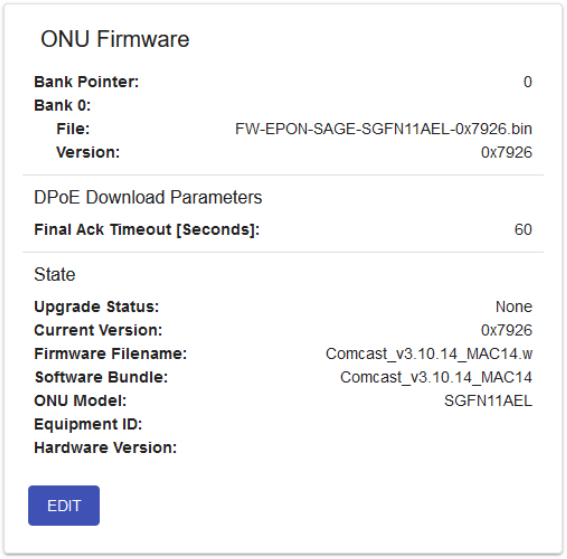
Configure Location Coordinates

See Configure Location Coordinates

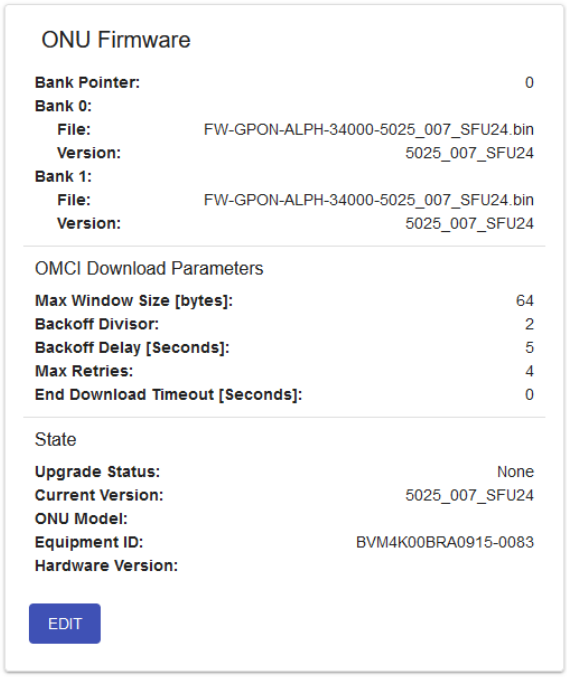
© 2024 Cisco and/or its affiliates. All rights reserved.

Firmware

The ONU Firmware tab provides information about the installed firmware on this ONU. The Upgrade Status field refreshes during a firmware upgrade to reflect the progress/status. The currently running version is shown along with some identifying information about the ONU, such as its model number. The interface differs for XGS-PON and 10G EPON ONUs. XGS-PON ONUs show the OMCI Download Parameters, while 10G EPON ONUs display the DPoE Download Parameters.



10G EPON ONU



XGS-PON ONU

Upgrade ONU Firmware

Click EDIT to update the firmware options. The user can select the active firmware bank and what firmware version to assign to each bank. **Note:** only Bank 0 is available in 10G EPON Mode. Use the “Bank Pointer” drop-down to select which firmware bank should be active and used. All compatible firmware images within the database, and the firmware currently installed (if not found in the database) are presented as options for each file bank. The options are listed by the compatible ONU model then version. After selecting the desired ONU firmware versions for each bank, click SAVE. This updates the ONU configuration and triggers a download of the new firmware(s) if needed.

© 2024 Cisco and/or its affiliates. All rights reserved.

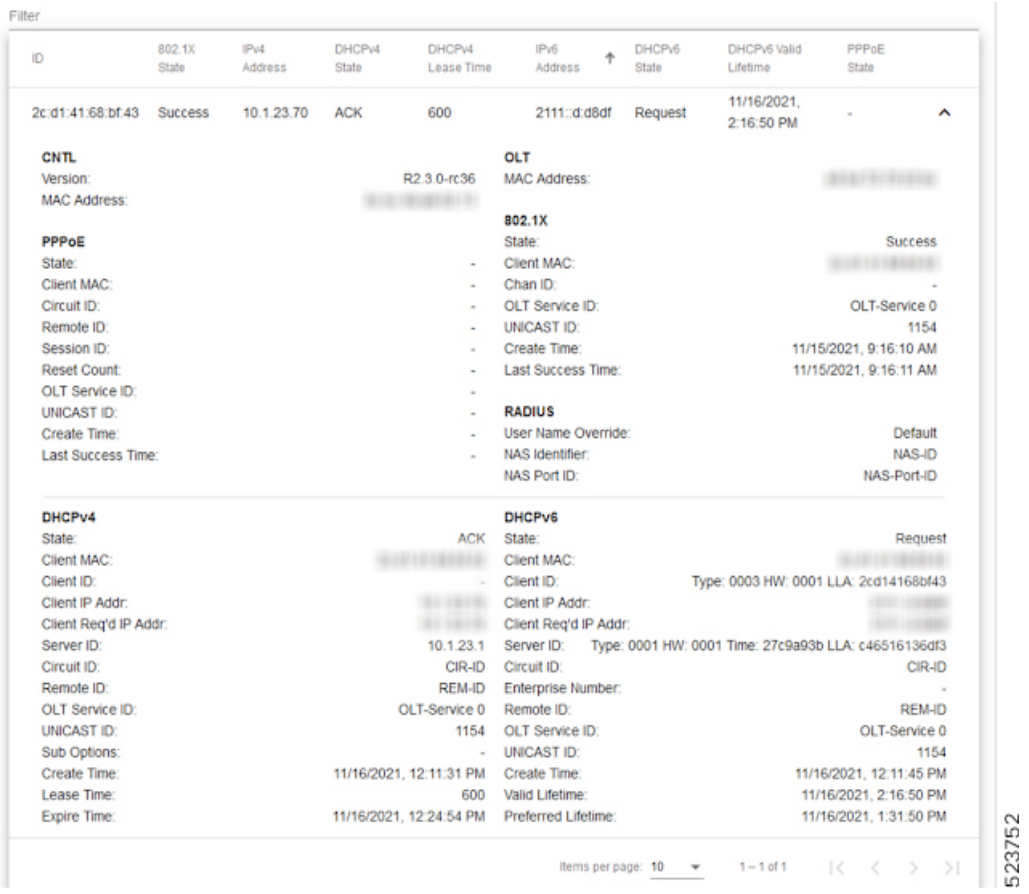
Disable ONU Firmware Upgrade

To disable firmware upgrade on an ONU, click EDIT. Select the “Upgrade Disabled” option from the “Bank Pointer” selection. For each Bank, set the “Config Version” field to ‘None’. Click SAVE. **Note: this action does not cancel a firmware upgrade if it is already in-progress.**

CPEs

Note: Displaying CPE information requires the Authentication, DHCP, and/or PPPoE Host Processing function to be enabled in the PON Controller.

The CPEs tab lists CPEs attached to the ONU which have been learned through 802.1X authentication and DHCP Relay. For each learned CPE, the table includes the CPE ID (MAC Address), 802.1X State, IPv4 Address, DHCPv4 State, DHCPv4 Lease Time, IPv6 Address, DHCPv6 State, and DHCPv6 Valid Lifetime. Each row of the table can be expanded to display all available state information for a specific CPE. The CPE’s PPPoE information can also be viewed here if applicable. **Note:** the table filter only applies to the values listed in the main columns, not the data within the expandable rows.



© 2024 Cisco and/or its affiliates. All rights reserved.

CPEs may also be deleted from this tab. After clicking ‘Edit’ the user sees three delete buttons: Delete Selected, Delete Expired, and Delete All. To manually select CPE entries for deletion, mark each CPE to be deleted by clicking the checkbox for that CPE in the ‘Delete’ column. Once all CPEs to be deleted are checked, click on the Delete Selected button. This removes all of the marked CPEs from the database. The Delete Expired button deletes all CPEs whose DHCPv4 and DHCPv6 State is “EXPIRED”. If only DHCPv4 or DHCPv6 is enabled, then the Delete Expired button will remove all CPEs whose respective DHCP State is “EXPIRED”. Finally, the Delete All button removes all CPEs for this ONU from the database. These actions cannot be undone after completion.

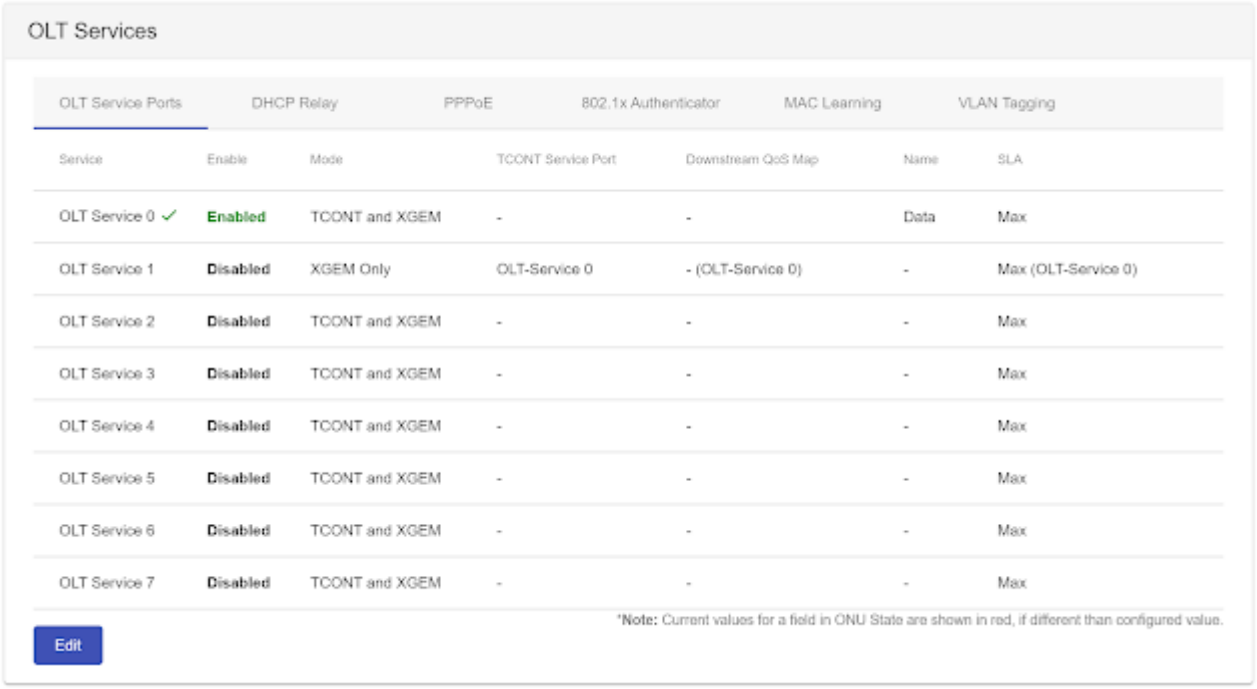
Services

The Services tab contains all subscriber service-related configuration that applies to this ONU. This includes selection of the GPON OMCI or EPON DPoE service configuration to be 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. ONU Services contains four sub-tabs: Config, MIB Reset, MIB Config, and MIB Current. The Services Config sub-tab has multiple sections.

© 2024 Cisco and/or its affiliates. All rights reserved.

OLT Services

In the “OLT Services” tile, there’s a table with a row for each OLT Service Port (0..7). The table has tabs that when selected, will change the columns of the table to display different categories of configuration (DHCP Relay, PPPoE) for each of the OLT Service Ports.



For XGS-PON ONUs, the OLT Service Port has two modes: ‘TCONT and XGEM’ or ‘XGEM Only’. Setting the mode to ‘TCONT and XGEM’ mode configures the OLT Service Port to operate as both a TCONT and associated XGEM. With ‘XGEM Only’ mode, the Service Port operates as an XGem Port only and must reference a Service Port that operates as a TCONT. This allows for multiple XGEM ports per TCONT.

Enable OLT Service Ports

To enable an OLT Service, click the “OLT Service Ports” tab. Click the Edit button. The “Enable” column contains options “True” and “False”. Set the selection to “True” for the desired OLT Service Port. Setting “Enable” to “False” disables the OLT Service. This may take a few minutes to take full effect.

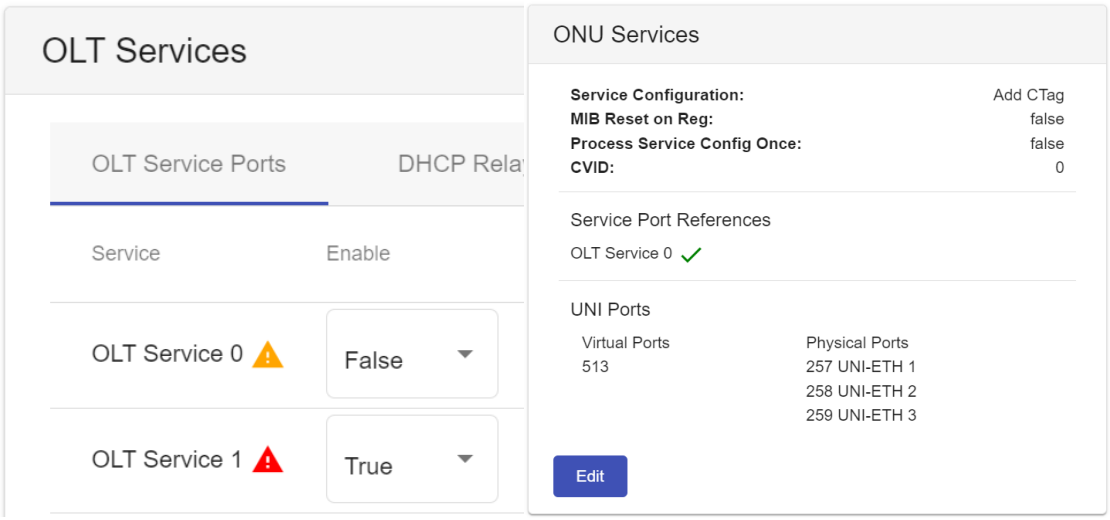
Note: Service 0 cannot be disabled for 10G EPON ONUs.

© 2024 Cisco and/or its affiliates. All rights reserved.

Service Configuration Mismatches

If an OLT Service is enabled that is not configured in the selected ONU Service Configuration (SRV-CFG), then a red warning icon will appear. If the selected ONU Service Configuration (SRV-CFG) references an OLT Service that is not enabled, then an orange warning icon will appear. Hovering over either of the icons will show a tooltip explaining what's wrong.

Note: Mismatch warnings currently only available with XGS-PON ONUs



Set the Downstream QoS Map

To configure the Downstream QoS Map for an OLT Service, click the "OLT Service Ports" tab. Click the Edit button and locate the column for "Downstream QoS Map". For a specific OLT Service, choose the desired Downstream QoS Map configuration from the options. Once the desired Downstream QoS map is selected, click Save. This may take a few minutes to take full effect.

The Downstream QoS Map selection only applies to XGS-PON ONUs using a configuration where multiple XGem Ports are configured with a single T-CONT. Furthermore, the Downstream QoS Map selection is only configured on the OLT Service Port that is operating as a T-CONT, where the Mode is set to "TCONT and XGEM".

Set the SLA

To configure the SLAs for an OLT Service, click the "OLT Service Ports" tab. Click the Edit button. Locate the column for "SLA". For any of your OLT Service Ports, choose the desired

© 2024 Cisco and/or its affiliates. All rights reserved.

SLA configuration from the options. Once the desired SLA is selected, click Save. This may take a few minutes to take full effect.

Configure VLAN Tagging

To configure the VLANs of an OLT Service click the “VLAN Tagging” tab. Tagging is organized by NNI-side and PON-side tag formats. The NNI-side tags define the tag stack format for egress frames and match format for ingress frames on the OLT’s NNI port. Likewise, the PON-side tags define the tag stack format for frames transmitted and received on the OLT’s PON port. If the NNI-side tags are not equal to the PON-side tags, the OLT performs VLAN tag translation, push, or pop operations to produce the configured tag format.

Configure VLAN Priority

To configure the VLAN Upstream Priority Value (VLAN CoS bits) for an OLT Service click the “VLAN Tagging” tab. The Upstream Priority Value can be configured as either ‘Copy’ or a specific priority value from 0 to 7.

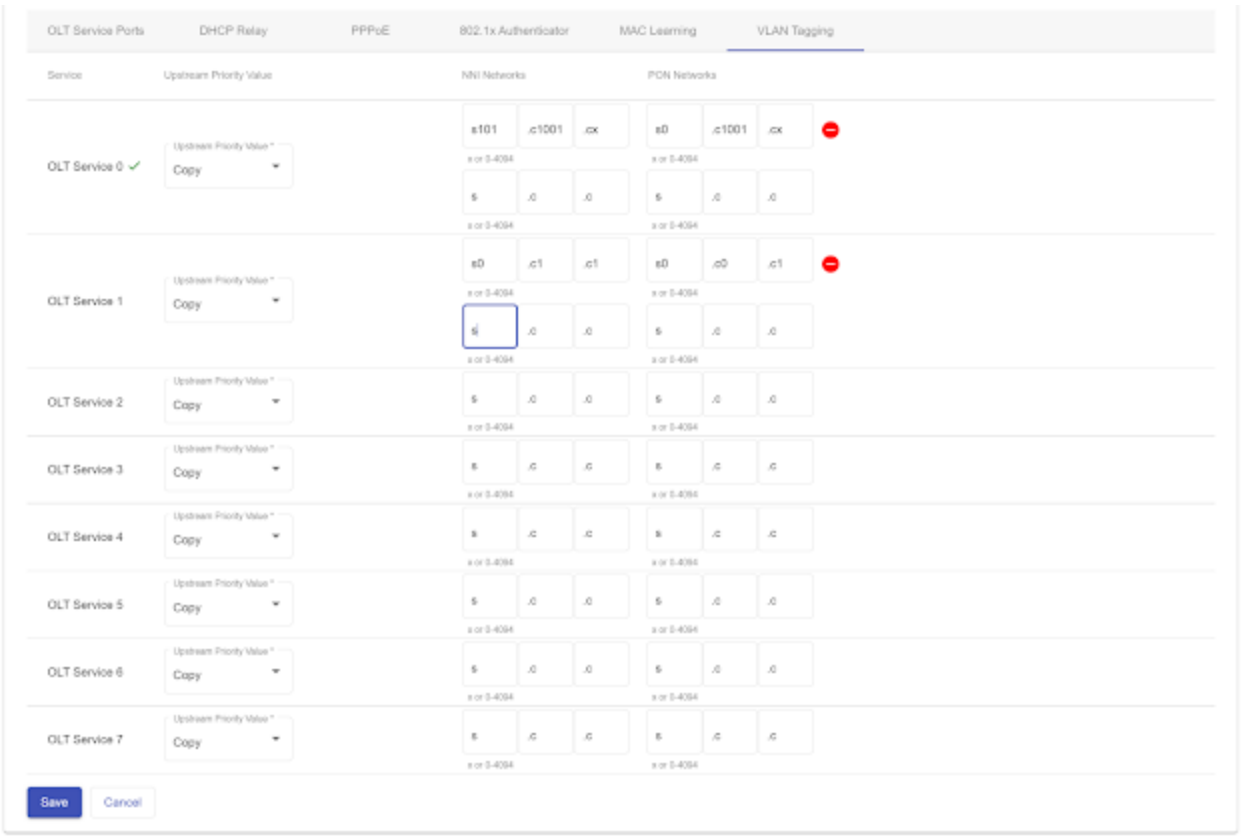
- ***Copy*** : Copy the priority bits from the inner C-Tag for OLT configurations that add an outer VLAN tag. Copy the priority bits from the original VLAN tag to the new VLAN tag for OLT configurations that translate an outer VLAN tag.

- ***Priority 0..7*** : 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.

Add a VLAN

To add a VLAN tag to an OLT Service click the “VLAN Tagging” tab. Click the Edit button. Enter the VLAN tag stack S-Tag, outer C-Tag, and inner C-Tag values. Illegal tag and conflicting tag formats are flagged and highlighted to the user when adding or modifying VLAN tags. The user is allowed to save changes only when all inputs are valid. If the changes are not desired and should not be saved, click the CANCEL button to exit the edit view and discard the changes.

© 2024 Cisco and/or its affiliates. All rights reserved.



Remove a VLAN

To remove a VLAN of an OLT Service click the “VLAN Tagging” tab. Click on the red minus circle and click the Save button.

Enable DHCP Relay

Note: DHCP Relay requires the DHCP Host Processing function to be enabled in the PON Controller.

UMT encapsulation can be enabled for both DHCPv4 and DHCPv6.

To enable UMT encapsulation of the DHCP Relay for an OLT Service Port, click the “DHCP Relay” tab. Click the Edit button. Set the Enable dropdown to either; DHCPv4 Only, DHCPv6 Only, or DHCPv4 and DHCPv6. These selections program the OLT to forward the selected DHCP messages over a UMT tunnel to the DHCP Relay Agent Host Processing function in the PON Controller. Enter values for Circuit ID, Remote ID, and Enterprise Number and click ‘Save’. When DHCPv4 Relay is enabled, the DHCP Relay Agent inserts Option 82 in DHCP messages received from the client. When DHCPv6 Relay is enabled, the DHCP Relay Agent sets the Circuit ID value as the DHCPv6 Interface-Id (Option 18), and combines the Enterprise Number

© 2024 Cisco and/or its affiliates. All rights reserved.

value with Remote ID to set OPTION_REMOTE_ID (37) in relay forward messages. Set the Enable dropdown to ‘None’ to disable this feature.

DHCP Relay must also be configured for the NNI Network configured for this service. See Enable DHCP Relay in NNI Network for more information.

Enable PPPoE

Note: PPPoE requires the PPPoE Intermediate Agent Host Processing function to be enabled in the PON Controller.

To enable PPPoE on an ONU’s OLT-Service Port click the “PPPoE” tab. Click the Edit button. Change the Enable dropdown to True and enter the desired Circuit and Remote IDs. Click the Save button when complete to submit the changes to the database for configuration.

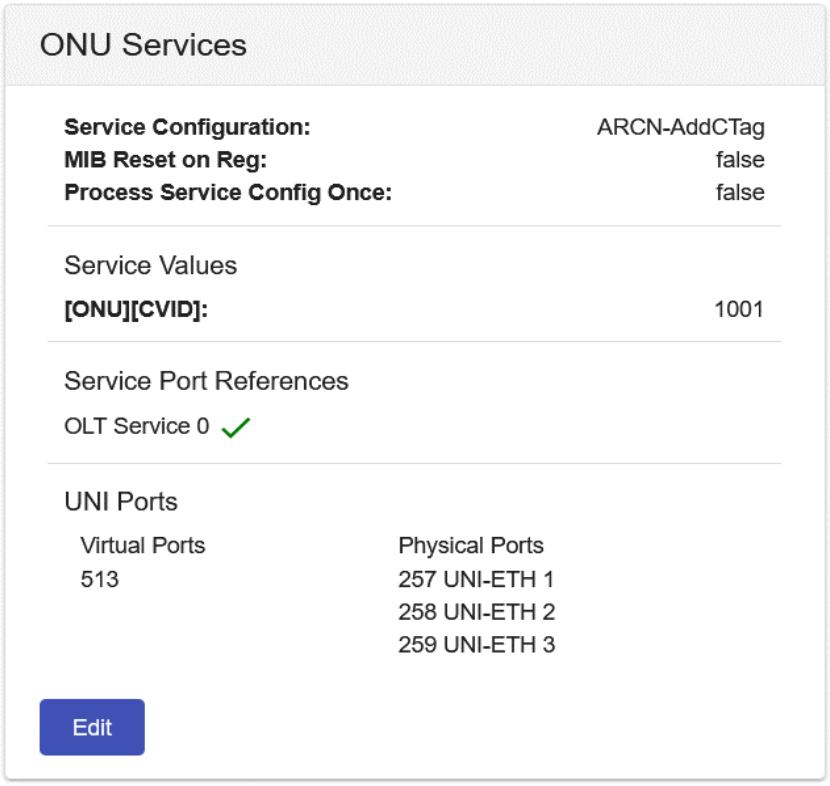
PPPoE must also be configured for the NNI Network configured for this service. See Enable PPPoE in NNI Network for more information.

ONU Services

The “ONU Services” tile displays information about the service configuration programmed on the ONU device itself. The selected Service Configuration is displayed here along with the input values and ports referenced within it. The “UNI Ports” subsection is used to configure and enable service for specific ports on the ONU. This configuration only applies 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 may 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” are available for configuration on GPON devices.

© 2024 Cisco and/or its affiliates. All rights reserved.

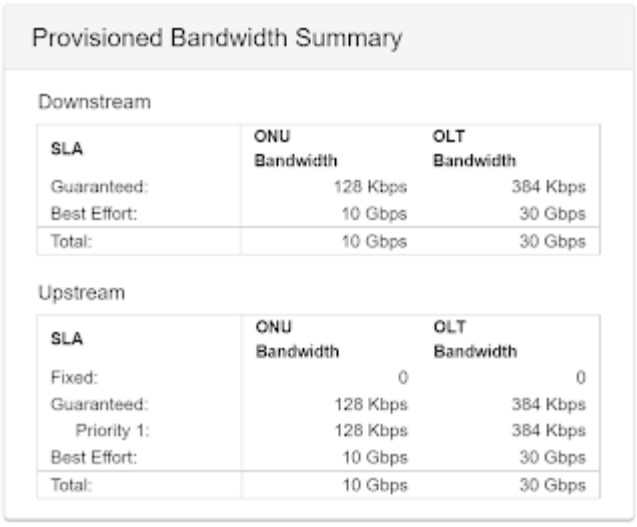


Set the ONU Service Configuration

To edit an ONU's service configuration, use the 'ONU Services' tile on the Config sub-tab. There are three steps to configuring the ONU Service Configuration (SRV-CFG).

1. Select the Service Configuration ID for this ONU. There are several options to select from:
    a. 'Disabled' - Disables service for this ONU.
    b. 'Unmodified' - Configures the ONU with a service that forwards customer traffic applying no VLAN tag modifications.
    c. 'Add CTag' - Configures the ONU to push/pop a C-Tag. If this service is selected, a CVID must be specified in Step (2).
    d. <SRV-CFG file> - All other values not listed above in a..care SRV-CFG files stored in MongoDB. Depending on the file selected, additional Service Values may need to be configured in Step (2).
2. Set the Service Values for the selected configuration. These are typically VLAN IDs or credentials that need to be configured for the specific service.
3. Set the UNI Ports for the service. This step applies when using the built-in 'Unmodified' and 'Add CTag' services only.

© 2024 Cisco and/or its affiliates. All rights reserved.

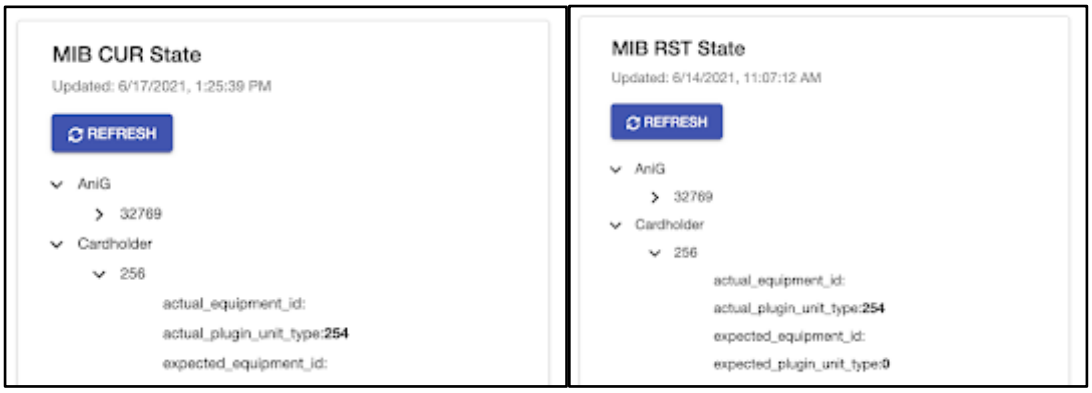


Provisioned Bandwidth Summary

The Services Config sub-tab provisioned bandwidth tile provides a quick view of the ONU's 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 # comes from the configured priorities of each of the ONUs 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.

MIB Current/Reset

The MIB Reset and MIB Current sub-tabs display the MIB Reset State and MIB Current State respectively, as expansion trees. All keys at each level of the tree are sorted alphabetically for viewing.



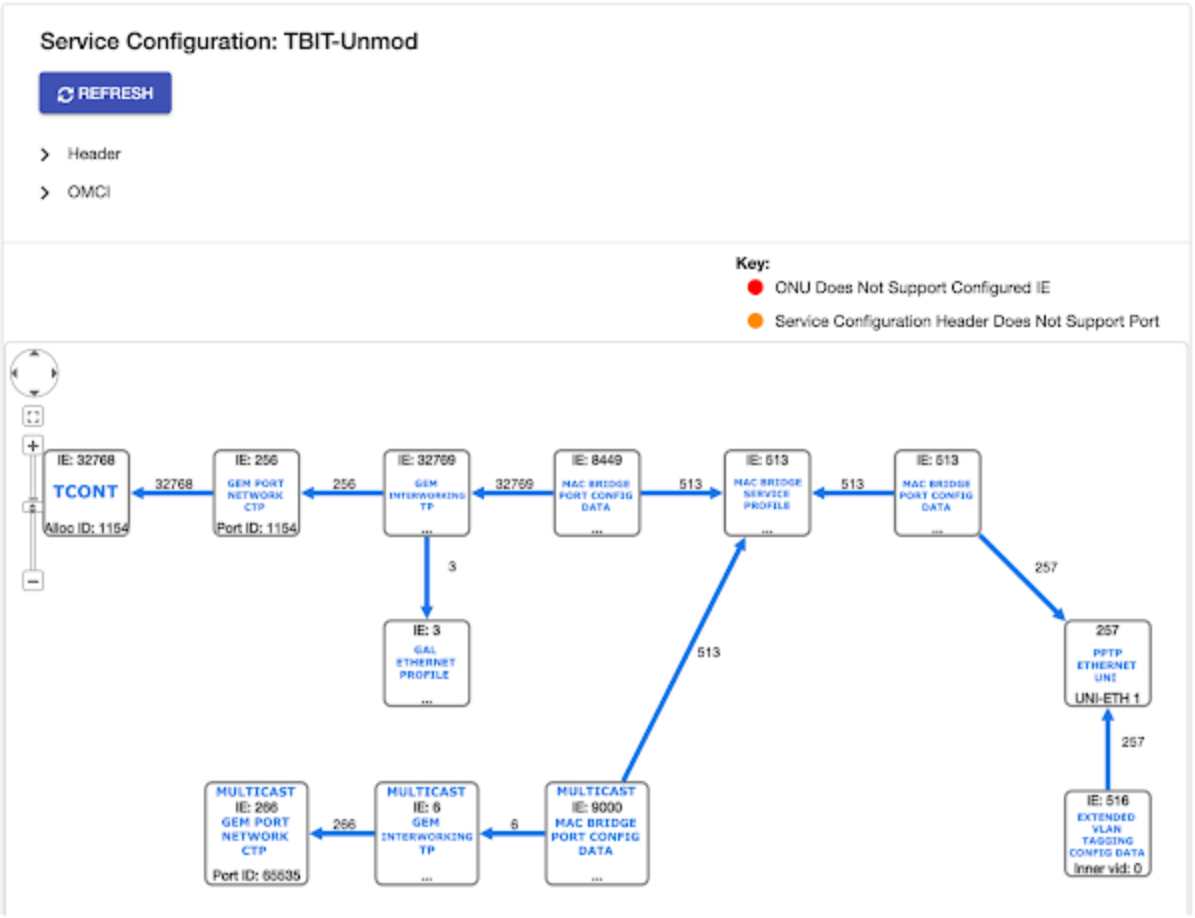
MIB Config

The MIB Config sub-tab displays detailed information about the ONU's service configuration. If the ONU is assigned a SRV-CFG file, this tab displays the configuration using the same expandable tree structure as the MIB Reset and MIB Current sub-tabs. The MIB configuration is

© 2024 Cisco and/or its affiliates. All rights reserved.

not available to 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 is displayed under the MIB configuration tree tile.

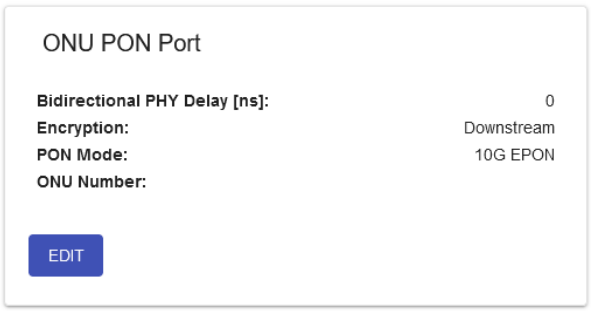
Note that the MIB Reset and MIB Config sub-tabs only apply to GPON ONUs, and do not have content for 10G EPON ONUs.



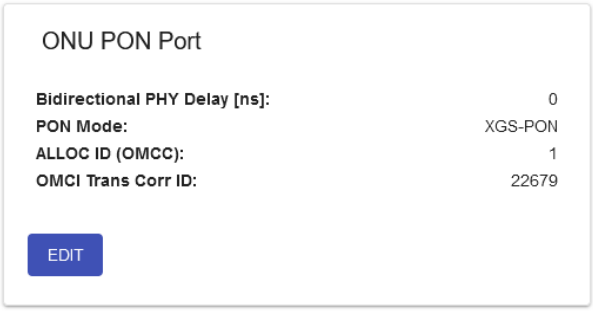
Ports

The ONU Ports tab contains 3 sub-tabs: PON, UNI and Voice. The PON sub-tab lists the values for Bidirectional PHY Delay and PON Mode, as well as ALLOC ID (OMCC) and OMCI Trans Corr ID in XGS-PON, and ONU Encryption and ONU Number in 10G EPON.

© 2024 Cisco and/or its affiliates. All rights reserved.

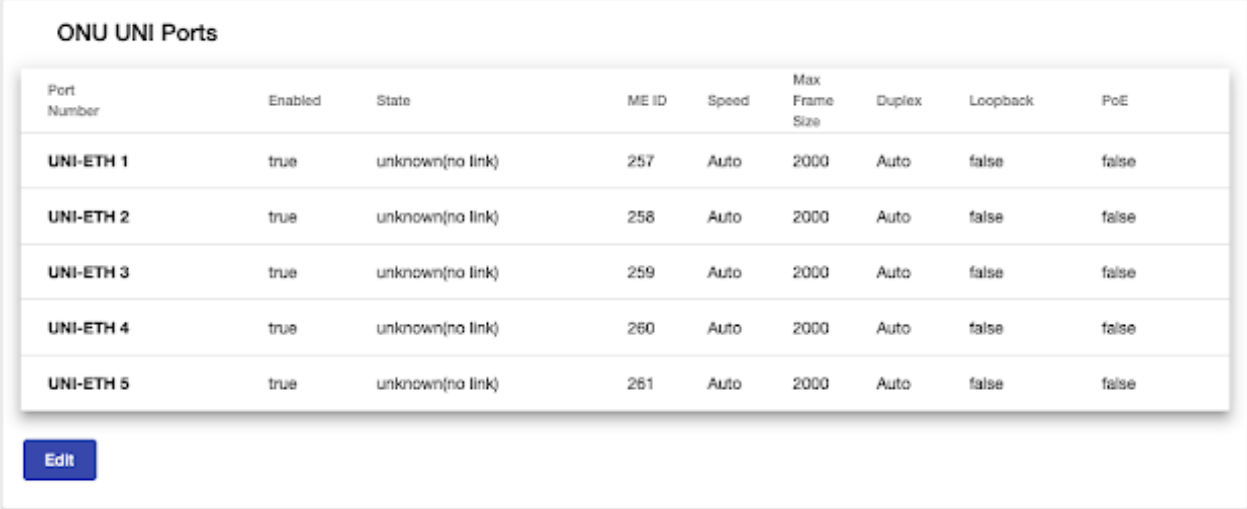


10G EPON ONU



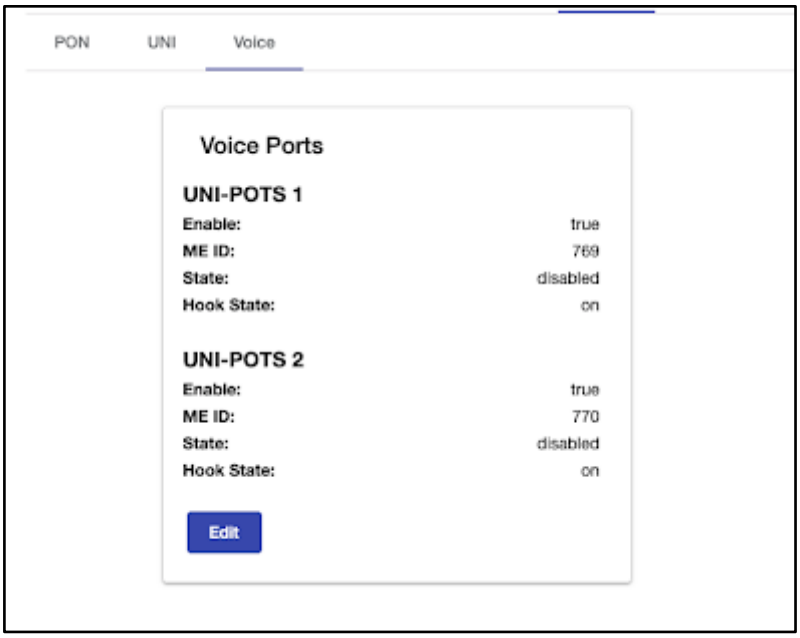
XGS-PON ONU

The UNI sub-tab shows a table with five rows, each representing a UNI port. The image shown below is for an ONU which has three UNI ports. Listed in the table are the Enabled, State, ME ID, Speed, Max Frame Size, Duplex, Loopback and Power over Ethernet (PoE) values for each UNI port. DPoE Broadcast Rate Limit and ONU MAC Learning configuration is also supported on 10G EPON ONUs. All of these values except for State and ME ID are editable for each UNI port. The State and ME ID columns are hidden while editing.



The Voice sub-tab appears only for XGS-PON ONUs. This page displays two UNI-POTS and lets the user configure if the ports are enabled or not. The page also displays state information such as the ME ID, State and Hook State.

© 2024 Cisco and/or its affiliates. All rights reserved.



Monitoring

ONU Monitoring contains five sub-tabs: Config, Alarms, Logs, Stats, and Debug. The Config tab allows the user to view and edit the ONU's alarm profile.

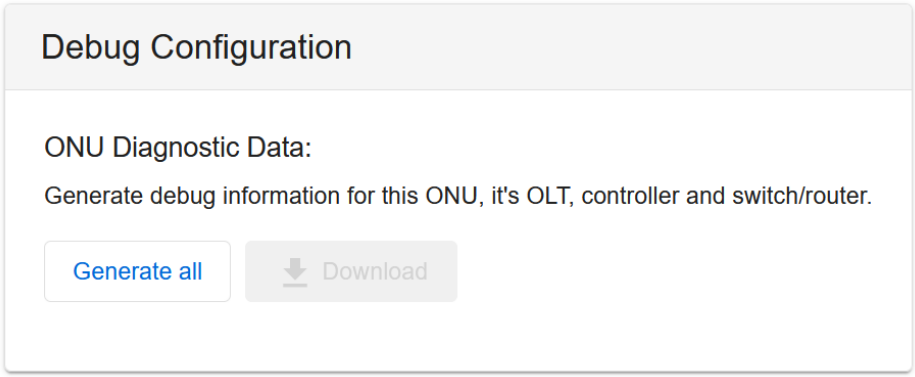
The Alarms sub-tab displays the same table seen on the Summary tab to see the active alarms in detail. See the Alarms section of this document for more information on Alarms. See the Logs section of this document for more information on Logs.

The Logs tab provides the user with all logs for this ONU that exist within the selected time range of one Hour, Day, Week, Month, or three Months. There is also an option to clear all existing logs for this ONU. Upon clicking this, the user is prompted to confirm the deletion. If confirmed, all logs for this ONU are removed from the database. This cannot be undone.

© 2024 Cisco and/or its affiliates. All rights reserved.

The next sub-tab under Monitoring for an ONU is the Stats tab, which presents a view of the statistics generated about the ONU's operation. See Statistics for more details on using this tab to select and display statistics counters and graphs for this device.

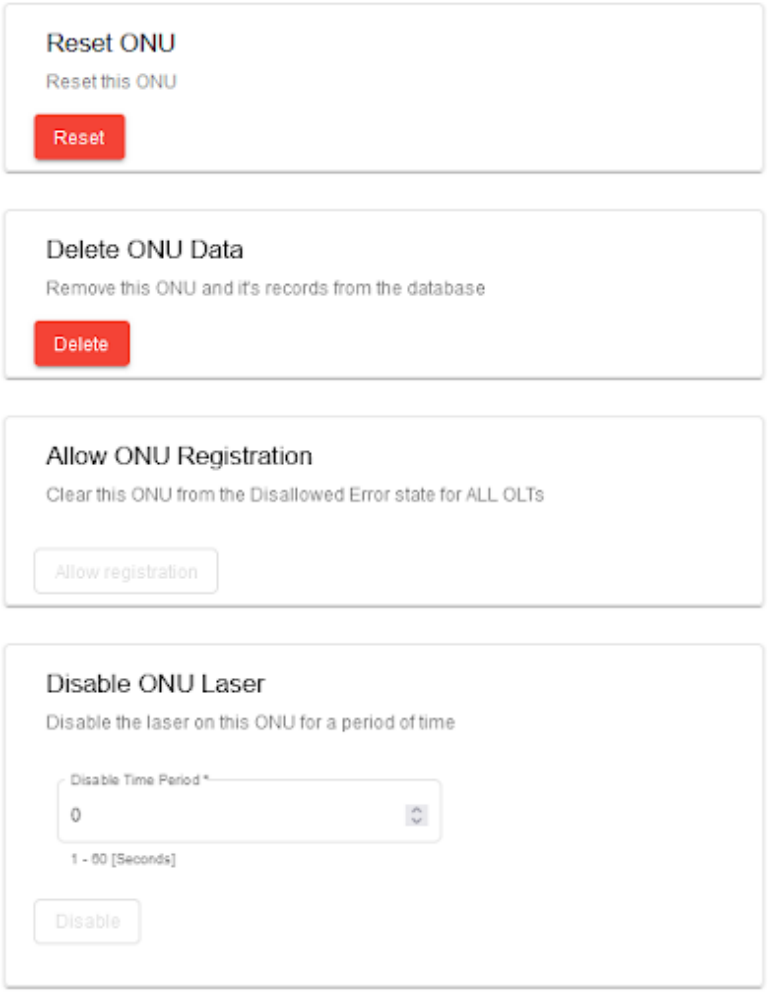
The final sub-tab for ONU Monitoring is the Debug tab. Clicking the "Generate All" button will generate and download a JSON formatted dump of the ONU debug information.



Operations

There are up to five (depending on the PON Mode) actions available for an ONU: Reset, Allow ONU Registration, Disable ONU Laser, Restart ONU Automation, and Delete.

© 2024 Cisco and/or its affiliates. All rights reserved.



Reset the ONU

Click the ‘RESET’ button to reset an ONU. When clicked, the Reset button prompts the user to confirm the Reset action with a popup. Once confirmed, this will trigger the ONU to restart. This process may take several minutes.

Allow ONU registration

When an OLT detects a faulty ONU on the PON (e.g., ONU transmitting over other ONUs), the OLT restricts the ONU’s access to the PON and transitions the ONU to the Disallowed Error state. The Allow ONU Registration operation clears the Disallowed Error State condition for this ONU. Click the ‘ALLOW REGISTRATION’ button to clear the Disallowed Error for this ONU. The ‘ALLOW REGISTRATION’ button is disabled when the ONU is not in the Disallowed Error state.

© 2024 Cisco and/or its affiliates. All rights reserved.

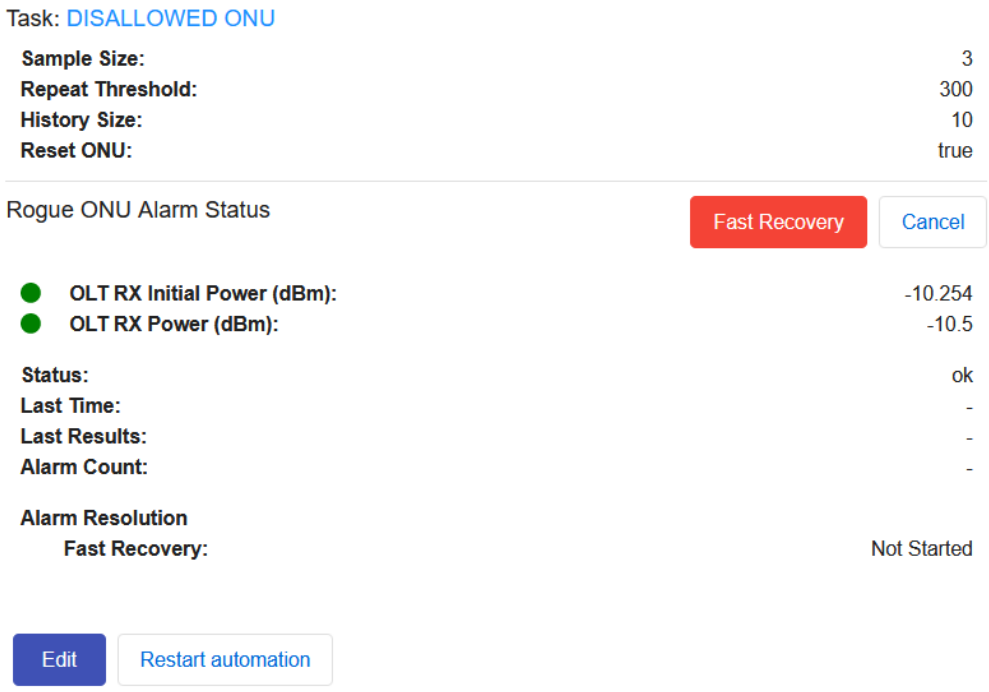
If the OLT is busy in the process of allowing registration for a different ONU, the message ‘Allow ONU Registration operation is in progress . . .’ is displayed and the ‘ALLOW REGISTRATION’ button is disabled. Wait for the OLT to complete the pending Allow ONU Registration operation before attempting the Allow Registration operation for this ONU.

Disable ONU Laser

The Disable ONU Laser operation is available for EPON devices only. To disable the ONU laser for a period of time, enter an integer within 1 to 60 in seconds into the field ‘Disable Time Period’. Then, click the ‘DISABLE’ button to disable the ONU laser for the period of time defined above.

Delete the ONU

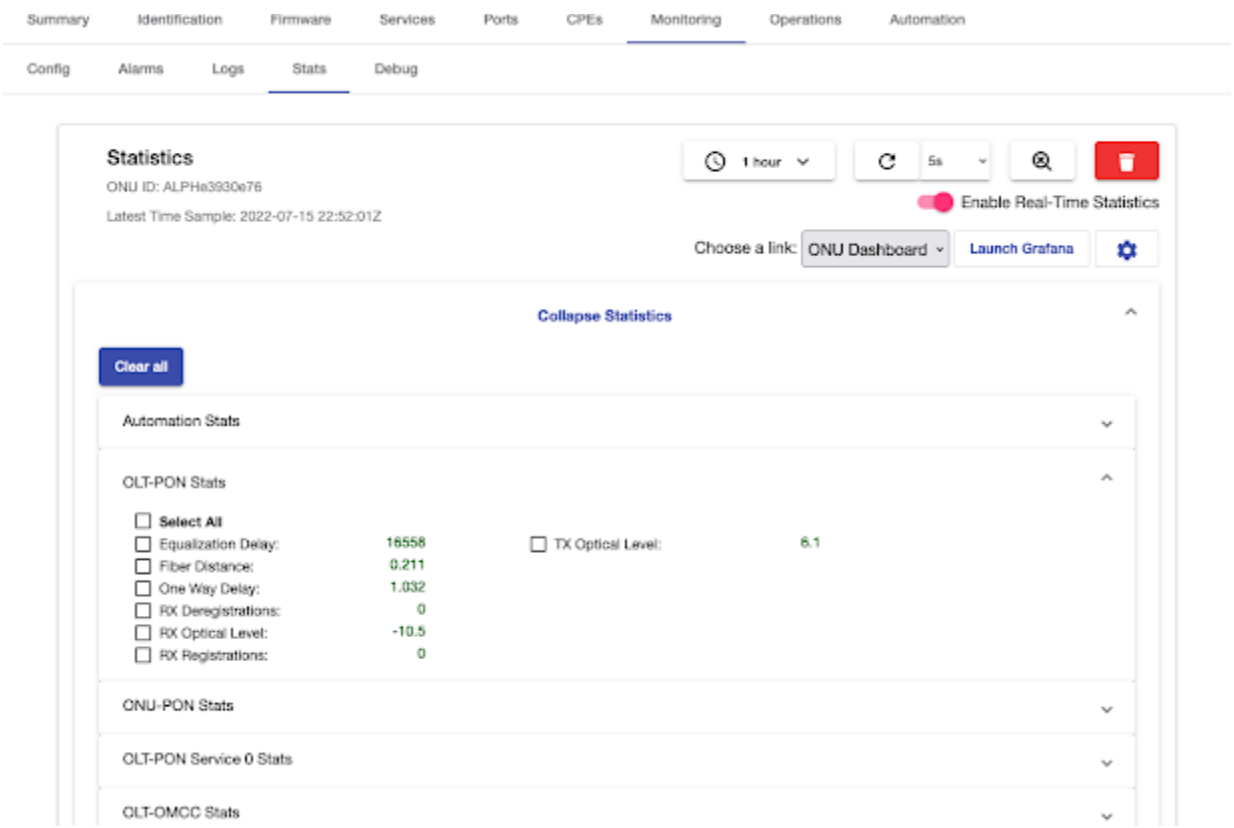
Click ‘DELETE’ to remove the ONU from the system. The Delete action removes all configuration, state, statistics, and logging data for this ONU from the database. This also removes the ONU from any OLT Inventories. After the delete action is confirmed, it cannot be undone.



© 2024 Cisco and/or its affiliates. All rights reserved.

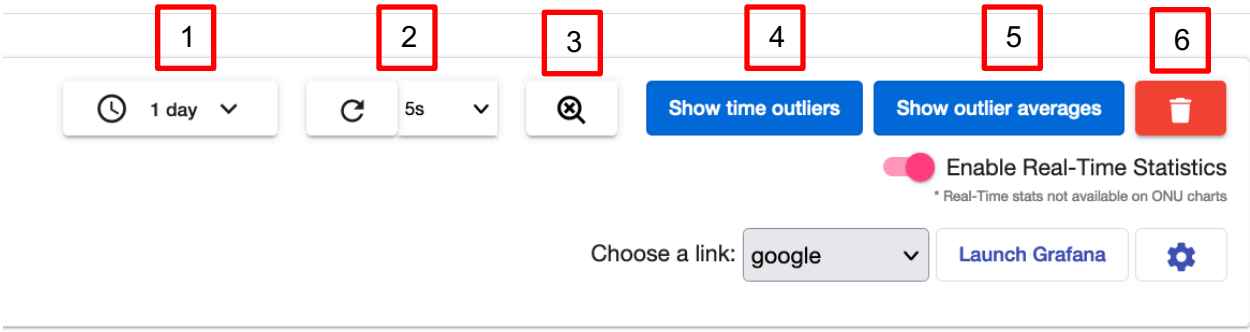
Statistics

The stats sub-tab is available under the Monitoring tab for PON Controllers, OLTs, and ONUs. It presents a view of the statistics generated about the device's operation. All available statistics are shown within the accordions for each stats group. To display the graph for any given statistic, mark the checkbox 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.



© 2024 Cisco and/or its affiliates. All rights reserved.

The Stats tab has advanced controls for selecting the time range, refresh interval, and other statistics display controls. The controls are numbered in the figure below and described in the sections below.



1) ***Time selection***. Selecting the dropdown for time range selection offers the following options to the user. A custom time range can be specified by selecting the start and end date inputs, which present a calendar for the user to choose the day to start or stop the range at. Choosing a set “To” date will stop the graphs from automatically updating. Simple, predefined ranges from 15 minutes to the last month can be applied with one click. After choosing a time period, click “Apply time change” to see it in the graphs.

2) ***Refresh***. The refresh icon with the drop down allows the user to configure how often to refresh the statistics data. The data may be manually refreshed by clicking the refresh icon button here or it can be paused by selecting “Off”.

3) ***Reset zoom***. The reset or clear zoom button restores the X/Y axis zoom on graphs to their default, zoomed-out values.

4) ***Show time outliers.*** Although the PON Controller tries to gather stats at consistent time intervals, many scenarios can occur where there may be a long period of time between 2 or more stat gathering cycles. Often when this happens a large spike or drop can be seen on the line graphs which would be confusing if the user assumes that period between stats (x-axis) is consistent with the other time periods on the graph. Clicking “Show time outliers” will find these 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.

5) ***Show outlier averages***. This can only be used after “Show time outliers” is clicked. This feature will then use what is 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

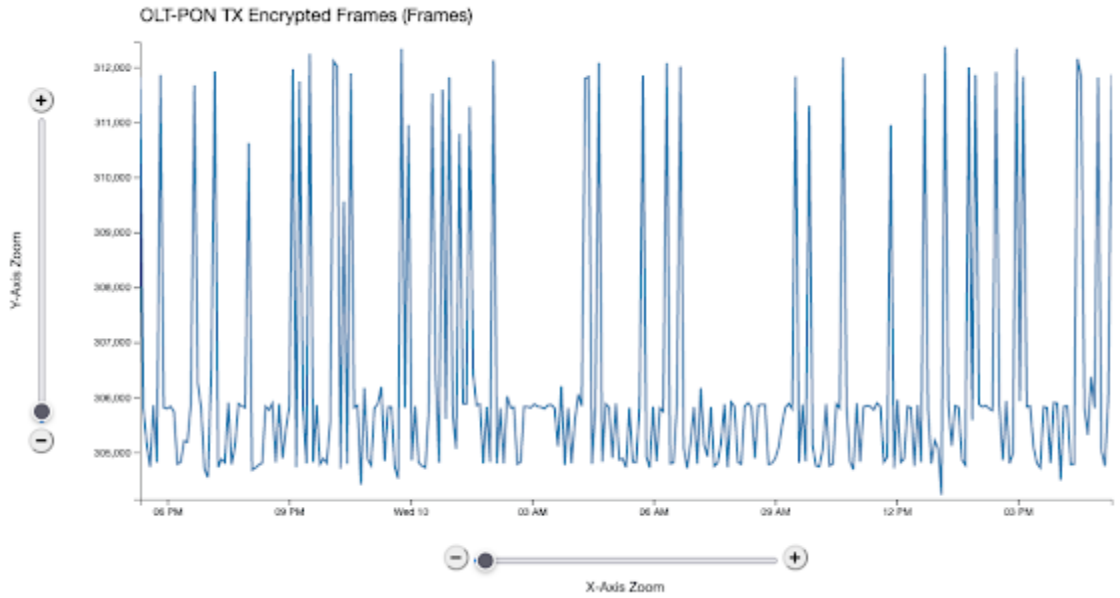
© 2024 Cisco and/or its affiliates. All rights reserved.

should have occurred. It will then use 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. This will often lower the spike on the graph and show a more accurate measurement of the y-axis values.

6) ***Clear statistics***. Click the trash can to clear all statistics for this device. Upon clicking the trash can button the user is prompted to confirm. When confirmed, all statistics for this Controller are deleted from the database. This cannot be undone.

Displaying Graphs

All graphs on the Stats 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 shown in the figure below.



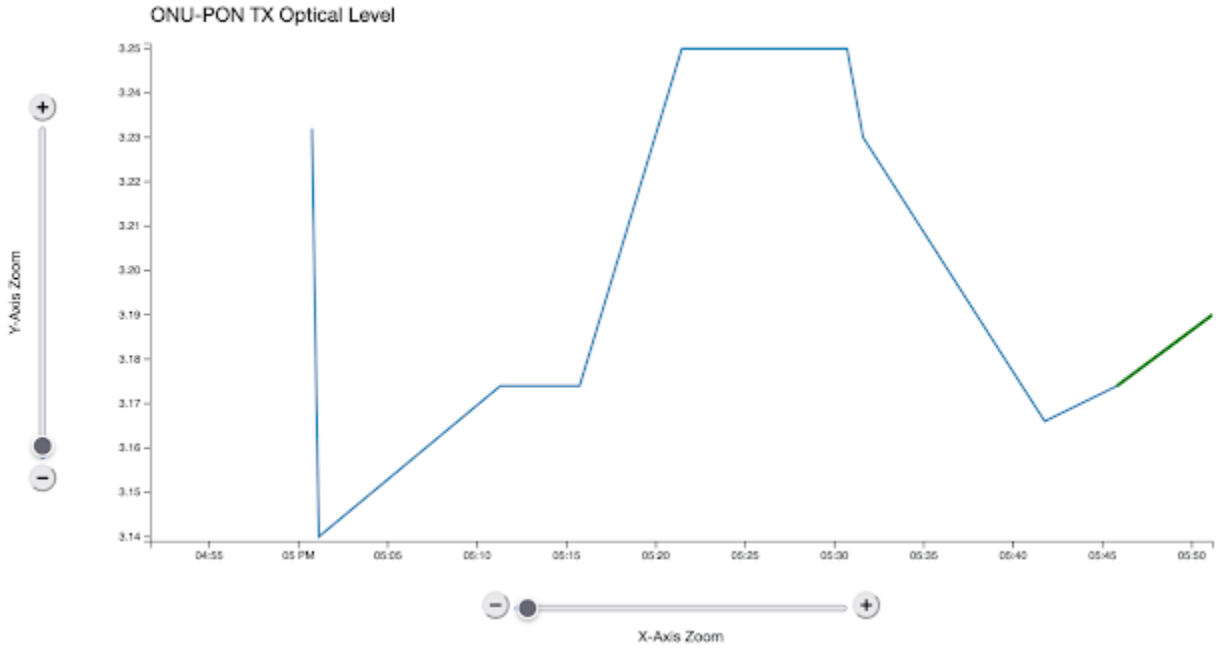
Each graph has controls for zooming and viewing data. Clicking the plus and minus buttons on the Axis Zoom, zooms in and out of the graphs for a more detailed view of the data. When zoomed in on graph data, click and drag the graph to view different data in the series. The Y-Axis Zoom and vertical click-and-drag is controlled individually for graphs. X-Axis Zoom and 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.

© 2024 Cisco and/or its affiliates. All rights reserved.

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 viewing statistics for an ONU or OLT, there is a special 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 counts will update steadily as the current values are reported for each PON Controller real-time statistics sample interval. These can be seen 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.

ONUs under OLT stats

The OLT stats page is unique in that it shows 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 will show both a line chart containing all the ONUs on one chart 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, just click on its address at the top of the page. More information can be found in the OLT Monitoring Stats portion of this document.

© 2024 Cisco and/or its affiliates. All rights reserved.

Grafana

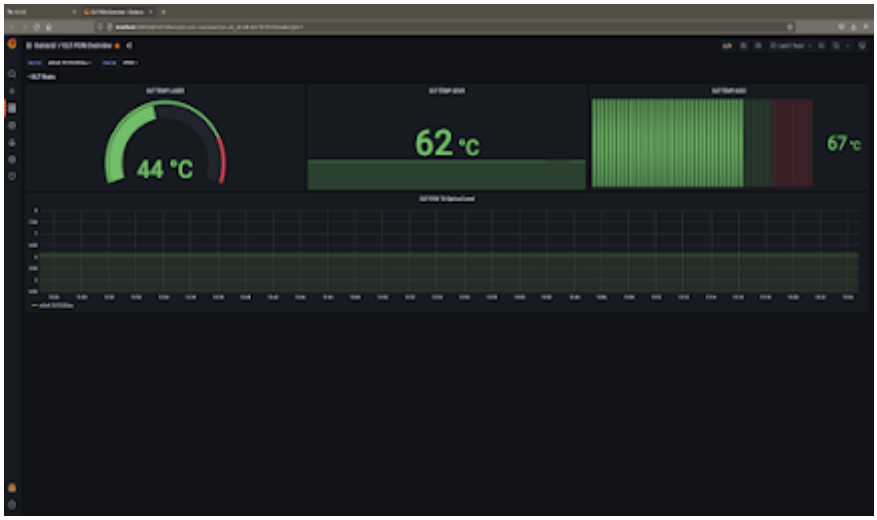
NOTE: Grafana must be installed prior to using the features described in this section.

Grafana is an open source data visualization tool that runs separately from the Cisco Routed PON. The Stats Exporter in conjunction with Prometheus, an open-source data collection software tool-kit, is available for Routed users (See TN073 for more information). The OLT and ONU statistics pages provide a way to link users to a Grafana server for a more in-depth view of statistics.

Prerequisites

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

1. Install the Grafana server on a supported operating system within the network accessible from PON Manager. See the Grafana documentation for more information on installing.
2. Install and configure the Stats Exporter which is packaged with the PON Controller.
3. Create dashboards for OLT and ONU devices in Grafana that PON Manager can link to.



Grafana Dashboard Links

Users can create up to 50 links to preconfigured Grafana dashboards. When creating links, users have the option to add query parameters into their links to help pre-populate their dashboards with the ONU and OLT's names and IDs. The query parameters will automatically take information about whatever device a user is on and include it in the link, so there's no need

© 2024 Cisco and/or its affiliates. All rights reserved.

to specify devices when creating the links as they can be used across all devices of the same type.

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 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.

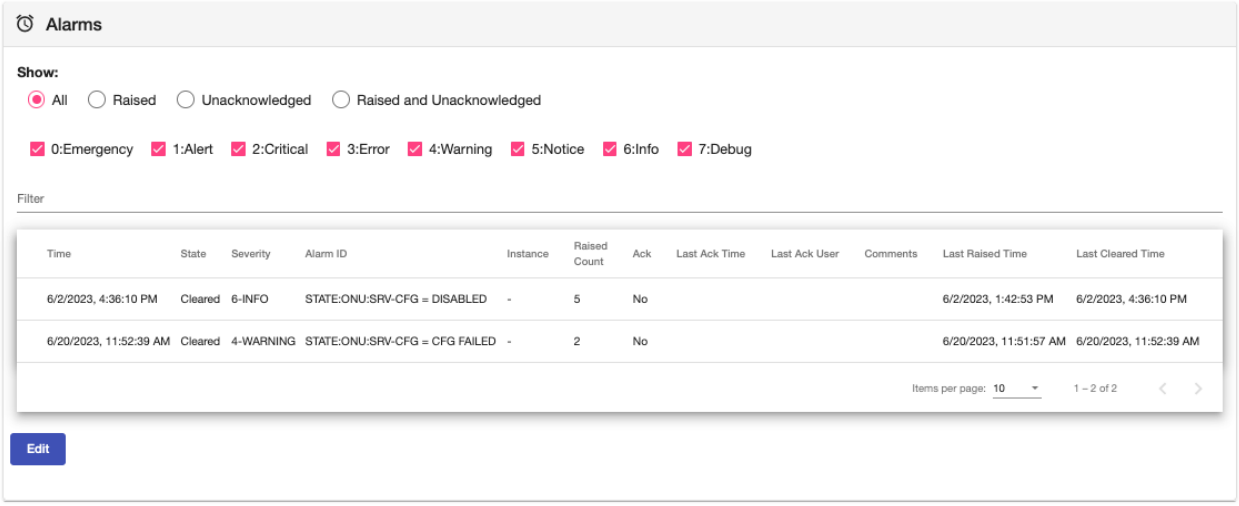
© 2024 Cisco and/or its affiliates. All rights reserved.

Include ONU ID	{{ONU ID}}	GPON Serial Number or EPON MAC Address identifying the ONU device. Available when displaying OLT or ONU statistics.
Include ONU Name	{{ONU Name}}	User configurable name identifying the ONU device (ONU-CFG.ONU.Name). Available when displaying OLT or ONU statistics.

Upgrading Routed PON Manager

Users should take note that a database schema change took place in R3.1.0 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 several scripts located in the “tools/” directory that will merge old collections and then delete them from the database. If users do not, they will only be able to see data collected from the time the upgrade took place and not before. This only ever needs to be done once per database. Directions are located in the README.txt file in the Routed PON Manager package.

Alarms



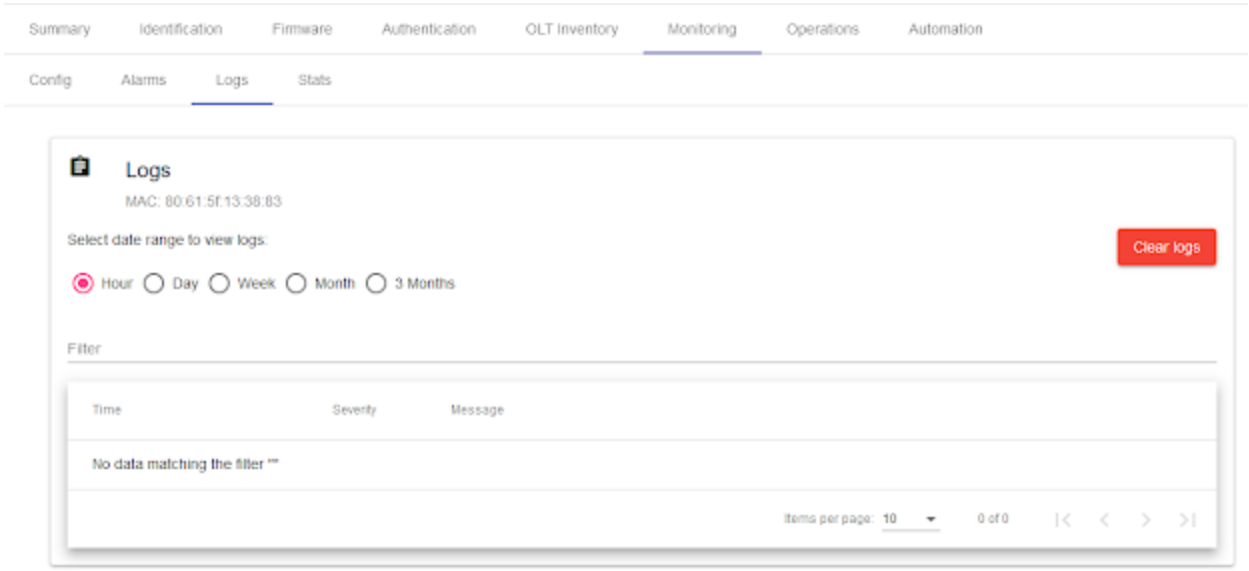
The alarms sub-tab displays a history of alarms on that device as well as controls to acknowledge and purge alarms from the database. Alarms in the table can be filtered based on their state; *Raised* for active alarms, *Unacknowledged* for alarms that haven’t been acknowledged by an operator or by both *Raised and Unacknowledged*. They can also be filtered based on their severity.

© 2024 Cisco and/or its affiliates. All rights reserved.

The *Time* column will either display the time the alarm was last raised if it is still active or the time it was cleared if it is no longer active. The *State* column displays either *Raised* for active alarms or *Cleared* for alarms that have stopped. The *Raised Count* column shows users how many times the alarm was triggered. *Last Ack Time* and *Last Ack User* will display the last time the alarm was acknowledged and the user that acknowledged it, updating whenever a new user acknowledges the alarm. Comments can also be added to the alarm without the need to acknowledge it. The comments section can be used to add notes, resolution info, user assignments and more to help with collaboration between team members.

Logs

The Logs sub-tab contains a table of logs the devices have entered the database. The user may select a time range of one Hour, Day, Week, Month, or three Months to retrieve all logs from within that range. Logs can then be sorted by time or severity, as well as filtered by time, severity, and message. To delete all logs, click on the “Clear Logs” button. This prompts the user to confirm the action. After this is performed it cannot be undone.



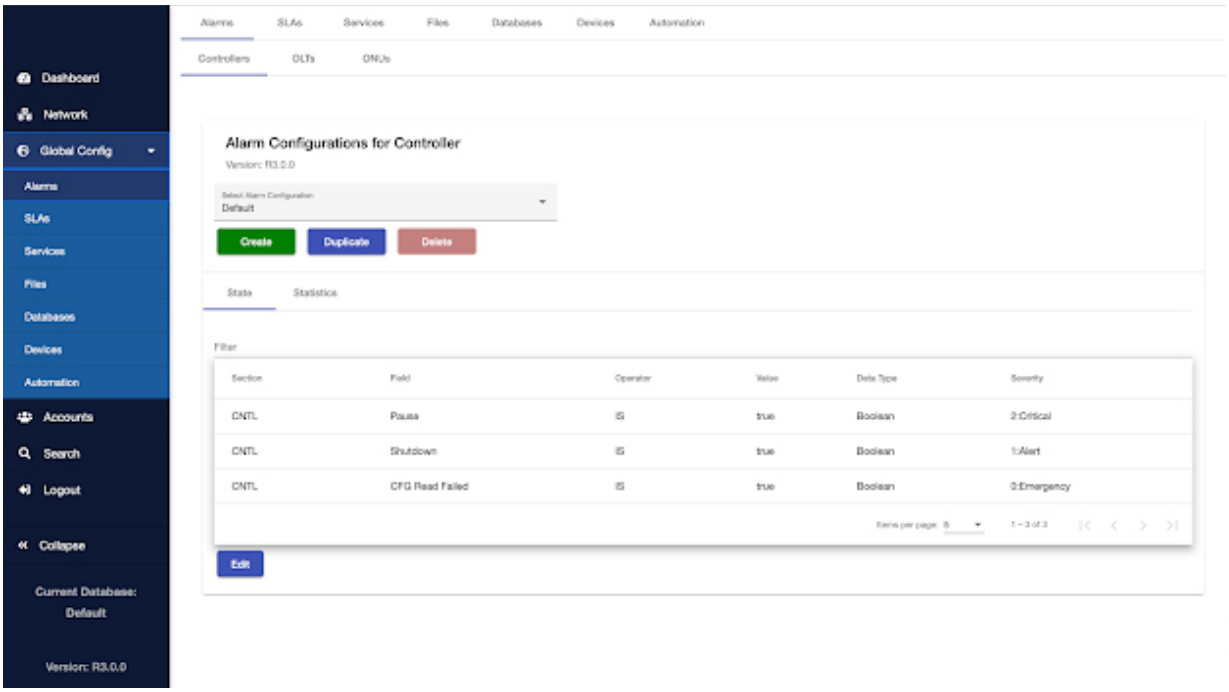
Global Config

Global configurations can be created, configured, and deleted from the Global Config tab.

Alarms

The Alarms tab and relevant device sub tabs are used for viewing, creating, editing, and deleting alarm configurations that can be set in a device’s configuration.

© 2024 Cisco and/or its affiliates. All rights reserved.



View and Edit Alarm Configurations

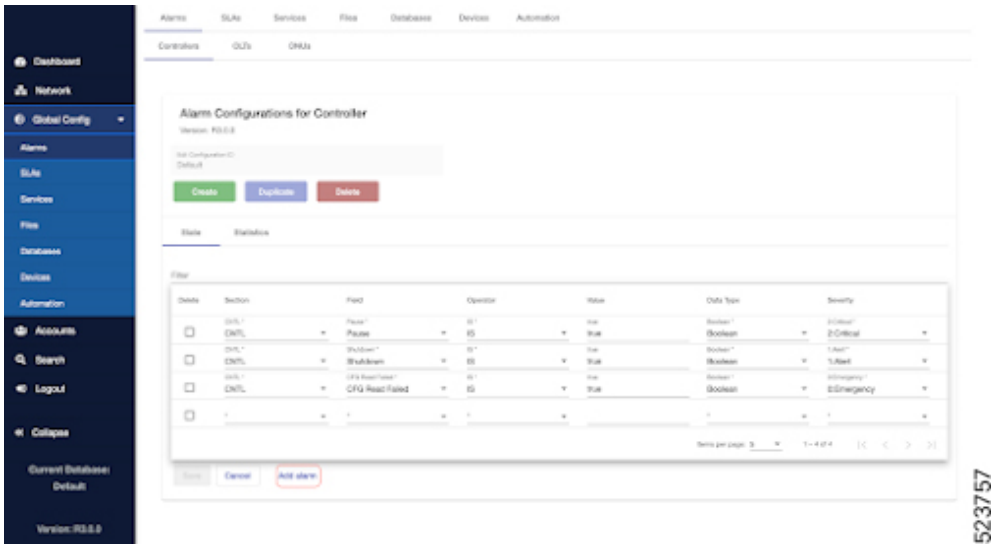
Select an existing alarm configuration via the ‘Select Alarm Configuration’ dropdown.

Along the top of the alarm table, there will be a tab group that allows for navigation between the different alarm types for a given device. Only State and Statistics alarms can be added or deleted from an alarm configuration. OLT Device alarms for an OLT and XGS-PON and 10G-EPON Alarms for an ONU are static and can only be edited, not created or deleted. These device specific alarms can have their Severity edited, as well as the ability to suppress the alarm if it’s not desired.

To add a new alarm criteria within the selected configuration, select the ‘Edit’ button on the bottom panel. Then, select the tab for the alarm type to be viewed, edited, or added. Following this, select the ‘Add’ button also located on the bottom panel. This inserts a new alarm entry row into the table for the selected alarm type that can then be configured. The ‘Save’ button is disabled until this additional row is completely configured. Once the alarm configuration has been edited, select the ‘Save’ button to update this configuration.

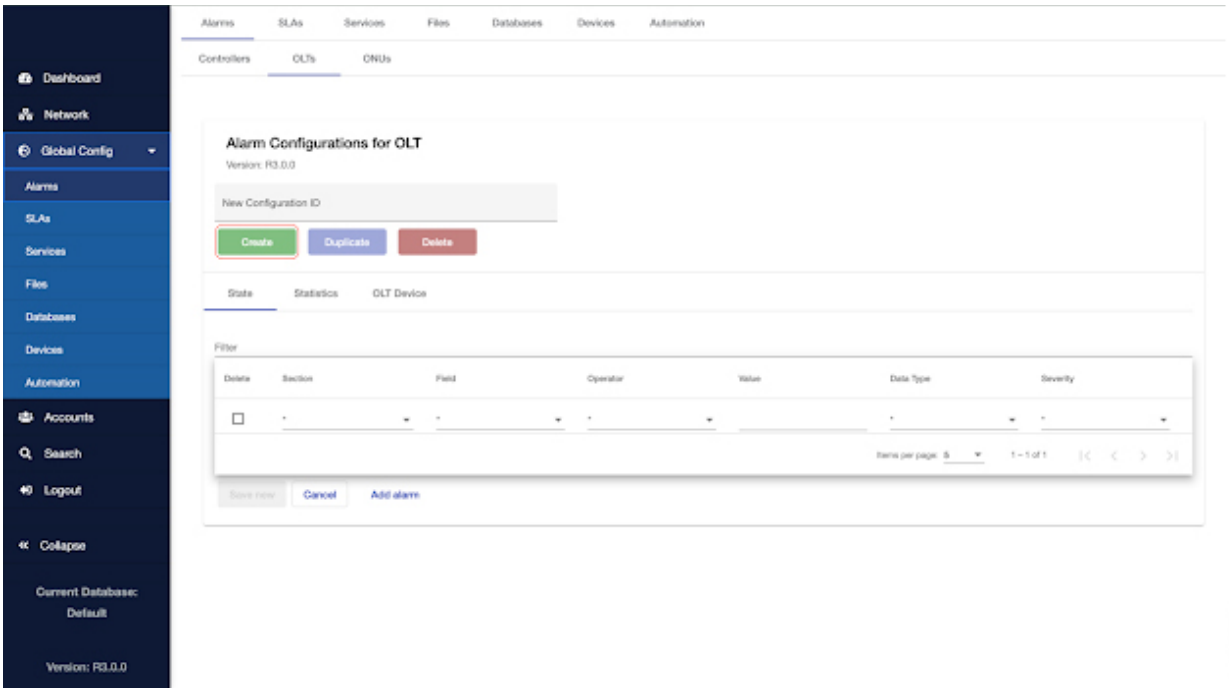
To delete an existing alarm criteria within a configuration, toggle the checkbox in the left-most column titled ‘Delete’. When the ‘Save’ button is selected or the table is navigated to a different alarm type, the alarm criteria is removed from the configuration.

© 2024 Cisco and/or its affiliates. All rights reserved.



Create an Alarm Configuration

On the top panel, select the button ‘Create’ to start a new alarm configuration. A configuration ID must be entered into the ID field for the configuration to be saved. The ‘Create’ button is disabled if currently creating a new configuration or when actively editing a configuration.



© 2024 Cisco and/or its affiliates. All rights reserved.

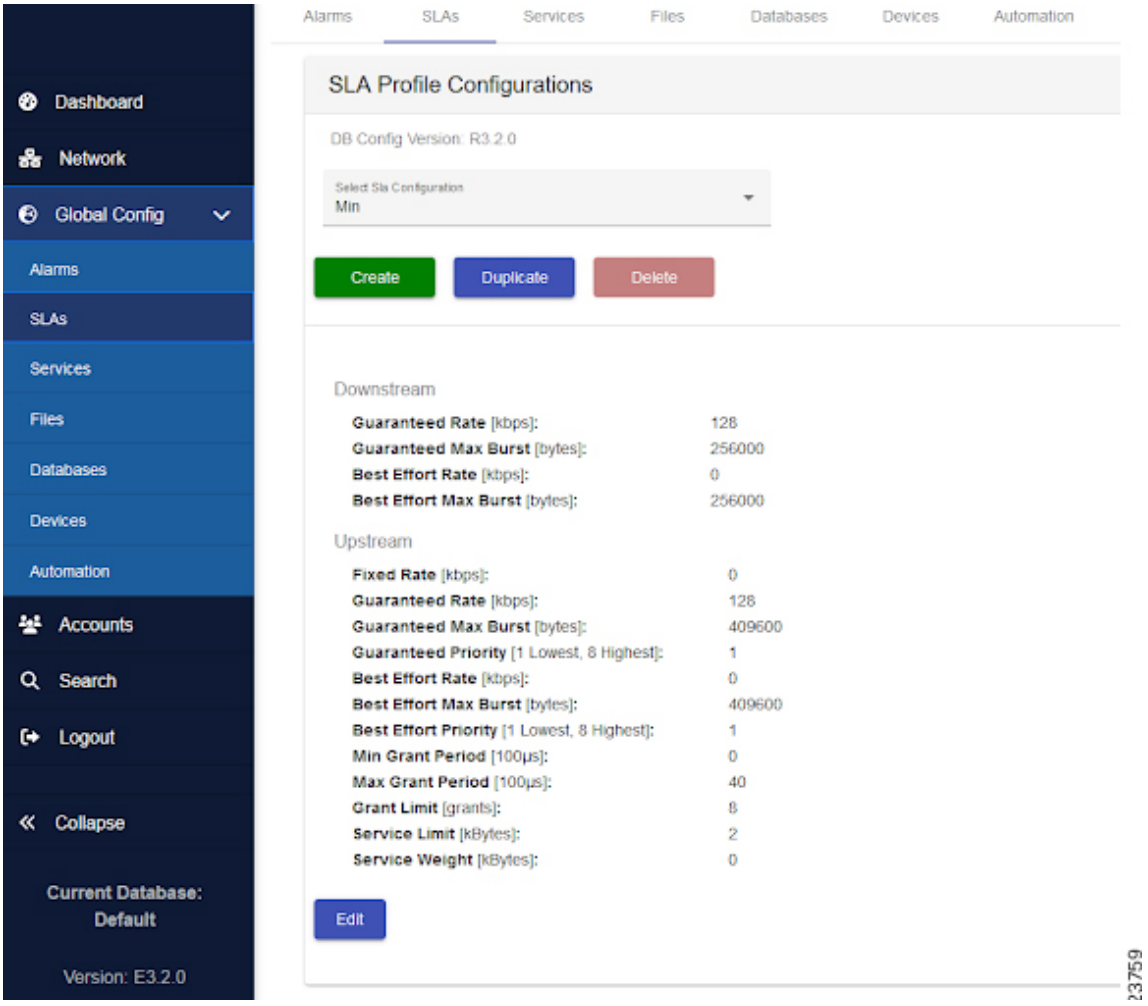
A new alarm configuration can be based on an existing Alarm configuration. Select the ‘Duplicate’ button on the top panel with the alarm configuration to be duplicated selected. The new ID for this duplicated configuration is the original ID with ‘-copy’ appended to the end. Update the configuration ID and fields as desired, and save. The Duplicate button is disabled if currently duplicating a configuration or when actively editing a configuration.

Delete an Alarm Configuration

To delete an existing alarm configuration, select the ‘Delete’ button on the top panel with the alarm configuration to be deleted selected. The Delete button is disabled if the ‘Default’ configuration is selected or when actively editing a configuration.

SLAs

The SLAs tab is used for viewing, creating, editing, and deleting SLA profiles that can be set in a device’s configuration.



© 2024 Cisco and/or its affiliates. All rights reserved.

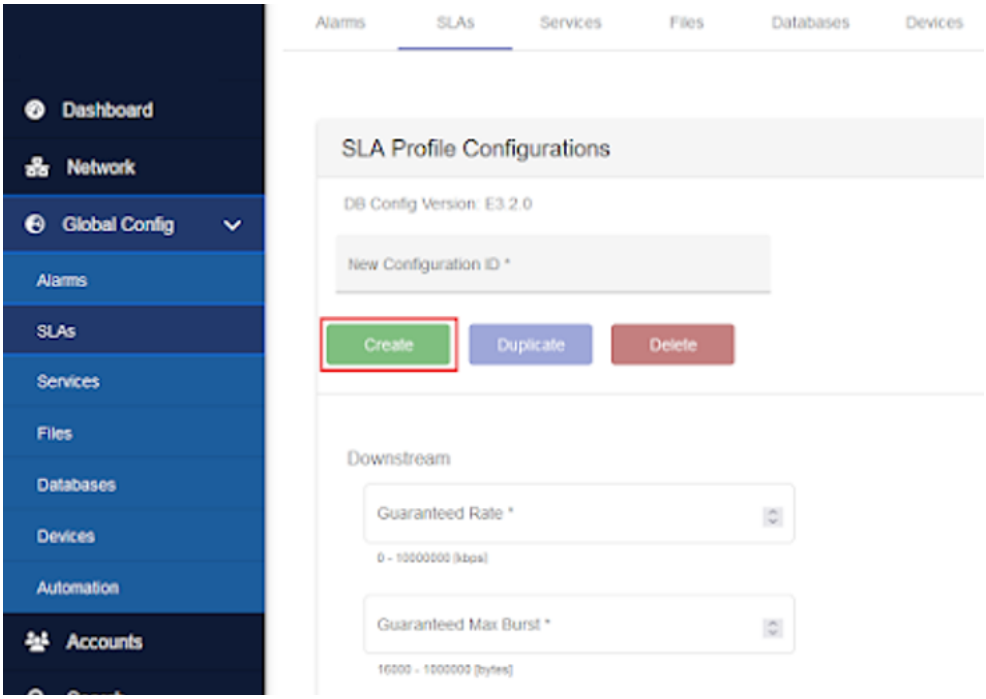
View and Edit SLA Configurations

Select an existing SLA configuration via the ‘Select Sla Configuration’ dropdown.

To edit an SLA configuration, select the ‘Edit’ button on the bottom panel. Once the SLA configuration has been edited, select the ‘Save’ button to update this configuration.

Create an SLA Configuration

On the top panel, select the ‘Create’ button to create a new SLA configuration. A configuration ID must be entered into the ID field for the configuration to be saved. The ‘Create’ button is disabled if currently creating a new configuration or when actively editing a configuration.



A new SLA configuration can be based off of an existing SLA configuration. Select the ‘Duplicate’ button on the top panel with the SLA configuration to be duplicated selected. The new ID for this duplicated configuration is the original ID with ‘-copy’ appended to the end. Update the configuration ID and fields as desired, and save. The Duplicate button is disabled if currently duplicating a configuration or when actively editing a configuration.

© 2024 Cisco and/or its affiliates. All rights reserved.

Delete an existing configuration

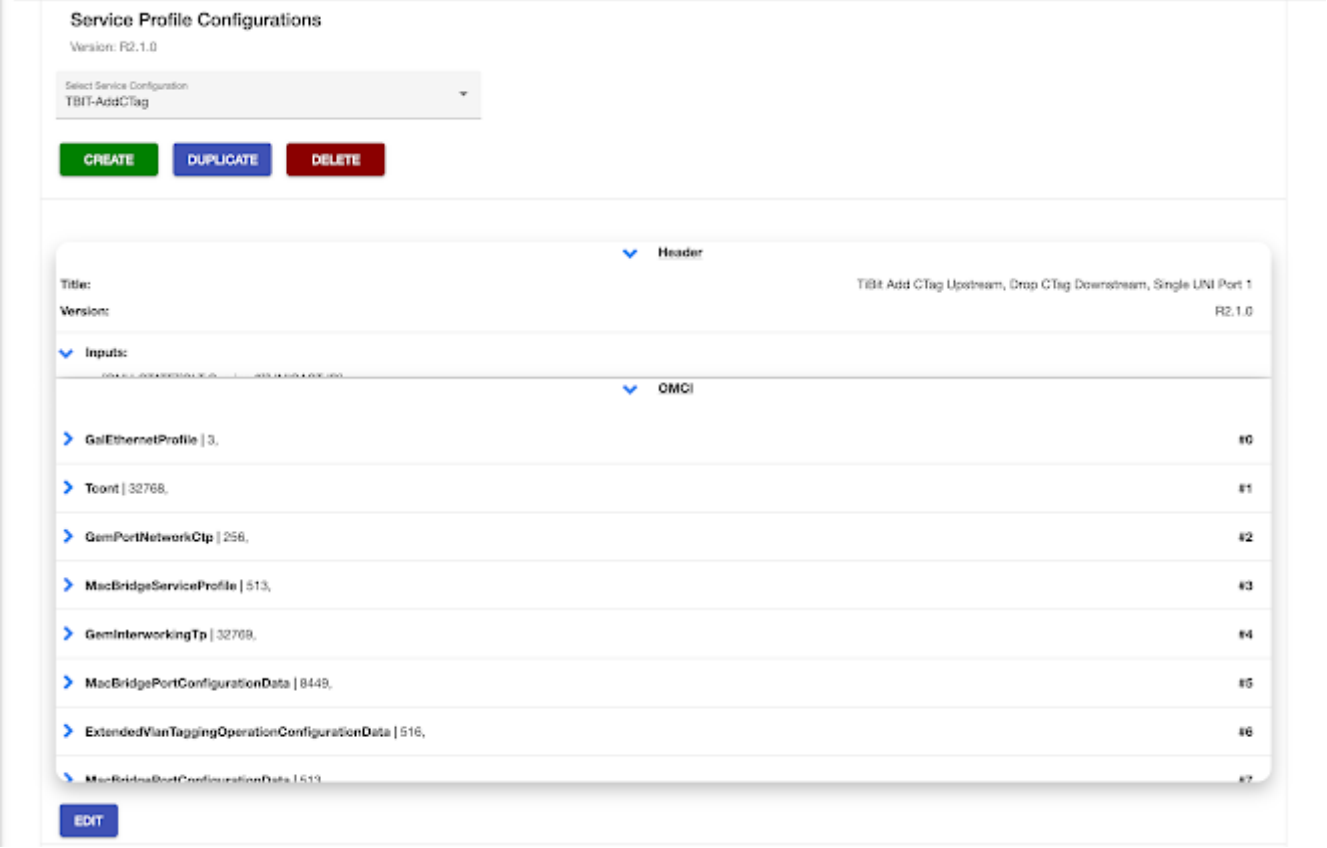
To delete an existing SLA configuration, select the ‘Delete’ button on the top panel with the SLA configuration to be deleted selected. The Delete button is disabled if the ‘Min’ or ‘Max’ configuration is selected or when actively editing a configuration.

Services

The Services tab is used for creating/editing/viewing various service based configurations and profiles.

Profiles

The Profiles tab is used for creating/editing/viewing Service Profile Configurations that can be later set in an ONU configuration.



© 2024 Cisco and/or its affiliates. All rights reserved.

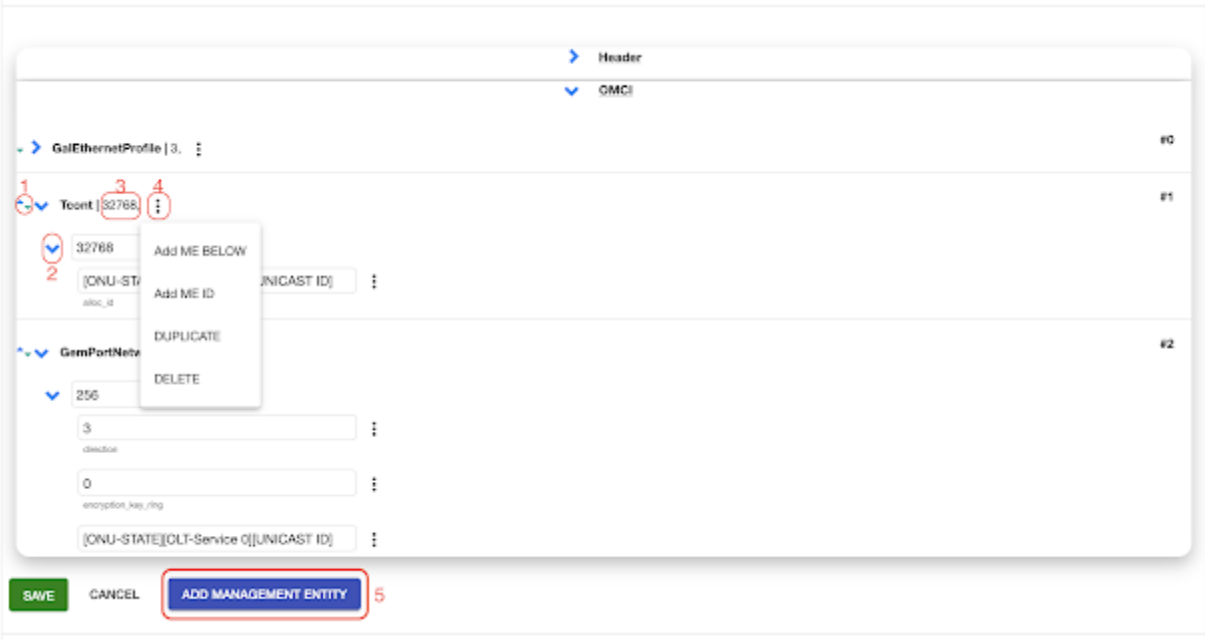
View and Edit Service Profile Configurations

Select an existing service configuration via the ‘Select Service Configuration’ dropdown.

To edit a Service configuration, select the ‘Edit’ button on the bottom panel. Once the Service configuration has been edited, select the ‘Save’ button to update this configuration.

The top configuration section titled “Header” can be used to edit the title, add inputs, add ports, as well as create and add to Compatibility tables.

The bottom configuration section titled “OMCI” can be used to traverse a Service configuration. The ME, IE, Attribute, and value can be viewed and edited.



1. To shift the position of an ME within the service configuration, toggle the up and down arrows left-most of the Management Entity

2. Expandable sections have a blue chevron next to them. Clicking this chevron toggles expansion and collapsing of the section.

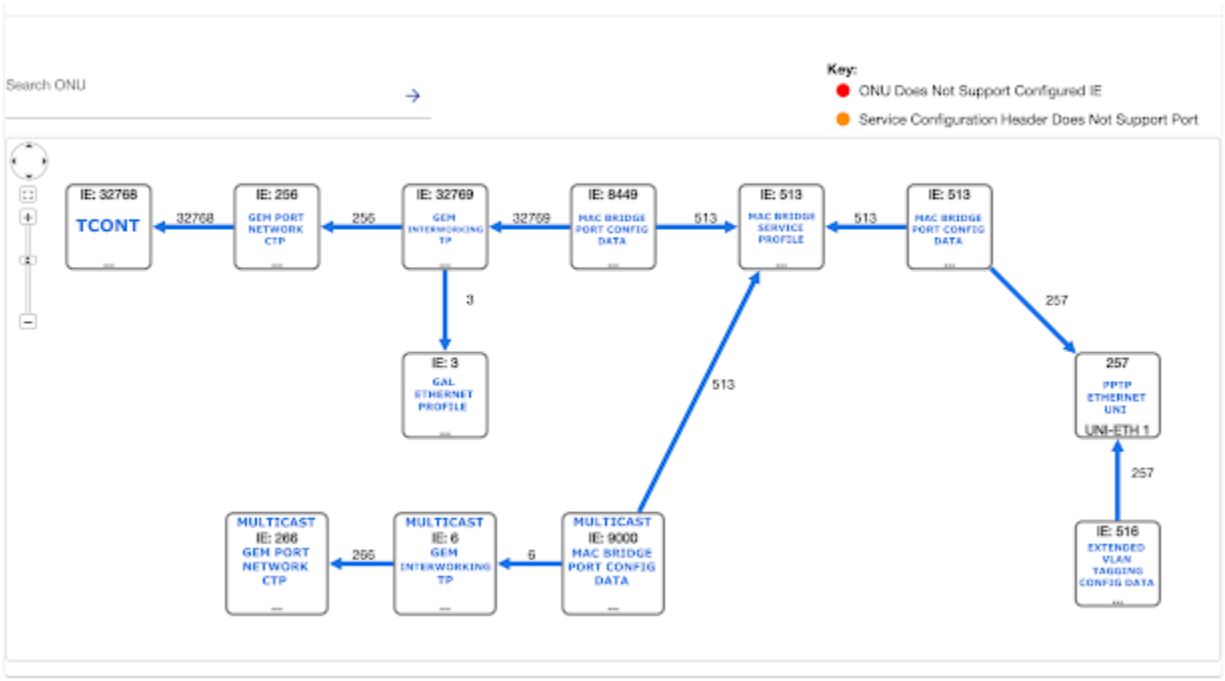
3. Currently configured ME IDs can be quickly viewed to the right-most position of the Management entity.

4. Service configuration elements that support multiple actions beyond editing have a clickable ellipsis next to them that displays a menu of actions.

© 2024 Cisco and/or its affiliates. All rights reserved.

5. To add a new management entity to the selected configuration, select the ‘edit’ button on the bottom panel. Following this, then select the ‘Add Management Entity’ button also located on the bottom panel. This brings up a popup that steps through configuring an ME. After the ME has been added via the popup, select the ‘Save’ button to update this configuration.

When a valid service configuration is selected, a diagram depicting the data flow path can be viewed. If desired, using the search bar in the top-left hand corner of the diagram pane, a specific ONU can be applied to see the behavior with that ONU MIB configuration. To do so, search for the desired ONU and select it within the dropdown that appears when typing in the “Search ONU” field. After selecting the ONU, click the blue arrow to the right of the field. It may take a few moments for the ONU-specific information to be applied to the diagram.



© 2024 Cisco and/or its affiliates. All rights reserved.

Create a Service Profile Configuration

On the top panel, select the ‘Create’ button to start a new Service configuration. A configuration ID must be entered into the ID field for the configuration to be saved. The ‘Create’ button is disabled if currently creating a new configuration or when actively editing a configuration.

A new Service configuration can be based off of an existing Service configuration. Select the ‘Duplicate’ button on the top panel with the Service configuration to be duplicated selected. The new ID for this duplicated configuration is the original ID with ‘-copy’ appended to the end. Update the configuration ID and fields as desired, and save. The Duplicate button is disabled if currently duplicating a configuration or when actively editing a configuration.

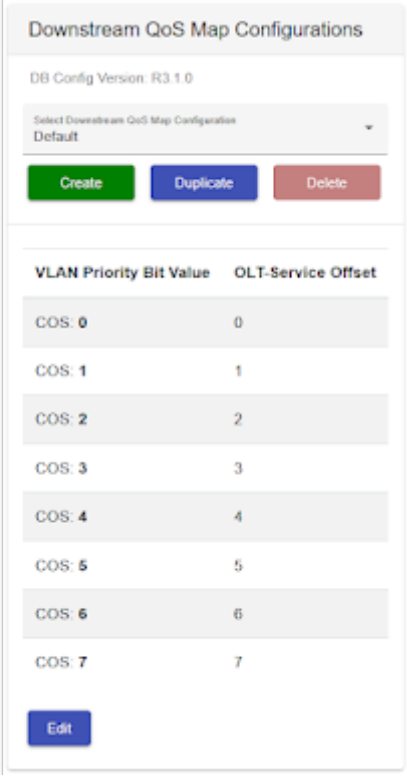
Delete an existing Service Profile Configuration

To delete an existing Service configuration, select the ‘Delete’ button on the top panel with the Service configuration to be deleted selected. The Delete button is disabled when actively editing a configuration.

© 2024 Cisco and/or its affiliates. All rights reserved.

Downstream QoS Map

The Downstream QoS Map tab is used for creating/editing/viewing QoS Mappings for downstream traffic received by the OLT on the NNI port. These profiles are referenced by GPON ONU Multi-XGem configurations and define the mapping between priority bits in the VLAN tag to OLT Service Ports (i.e., XGem Ports).



The mapping is defined as a list of VLAN Priority Bit (CoS) values 0..7 to OLT-Service Offsets 0..7, where the OLT Services represent a T-CONT and a group of associated XGem Ports. The OLT-Service Offset is the relative location of the OLT Service Port in the group of OLT Service ports representing the T-CONT and XGem Ports. This allows downstream traffic being sent to the ONU to be carried on different XGem Ports based on the CoS values. The Downstream QoS Map is referenced by the ONU Service configuration on the OLT Service Port operating in ‘T-CONT and XGEM’ mode.

The use of the Downstream QoS Map carries several restrictions which must be kept in mind when configuring the service:

- All Alloc-IDs assigned to the OLT-Services referenced by the Downstream QoS Map must be in consecutive order.
- A Downstream QoS Map cannot be assigned to an OLT-Service if its Service Offsets refer to XGEM-only OLT-Services which do not exist on the ONU.

© 2024 Cisco and/or its affiliates. All rights reserved.

- Before disabling an OLT-Service which is referred to by a Downstream QoS Map, the Downstream QoS Map reference MUST be cleared from the ‘T-CONT and XGEM’ OLT-Service.
- Only three unique Downstream QoS Maps can be assigned to a single OLT but the same Downstream QoS Map can be used across different OLTs.
- A Downstream QoS Map where all OLT-Service Offset values are set to zero cannot be assigned to an OLT Service as this is the same as having no downstream CoS mapping.

View and Edit Downstream QoS Mappings

Select an existing Downstream QoS Map via the ‘Select Downstream QoS Map Configuration’ dropdown.

To edit a Downstream QoS Map, select the ‘Edit’ button on the bottom panel. Once the Downstream QoS Map has been edited, select the ‘Save’ button to update this configuration.

Create a Downstream QoS Mapping

On the top panel, select the ‘Create’ button to start a new Downstream QoS Map. A configuration ID must be entered into the ID field for the configuration to be saved. The ‘Create’ button is disabled if currently creating a new configuration or when actively editing a configuration.

A new Downstream QoS Map can be based off of an existing mapping. Select the ‘Duplicate’ button on the top panel with the Downstream QoS Map to be duplicated selected. The new ID for this duplicated configuration is the original ID with ‘-copy’ appended to the end. Update the configuration ID and fields as desired, and save. The Duplicate button is disabled if currently duplicating a configuration or when actively editing a configuration.

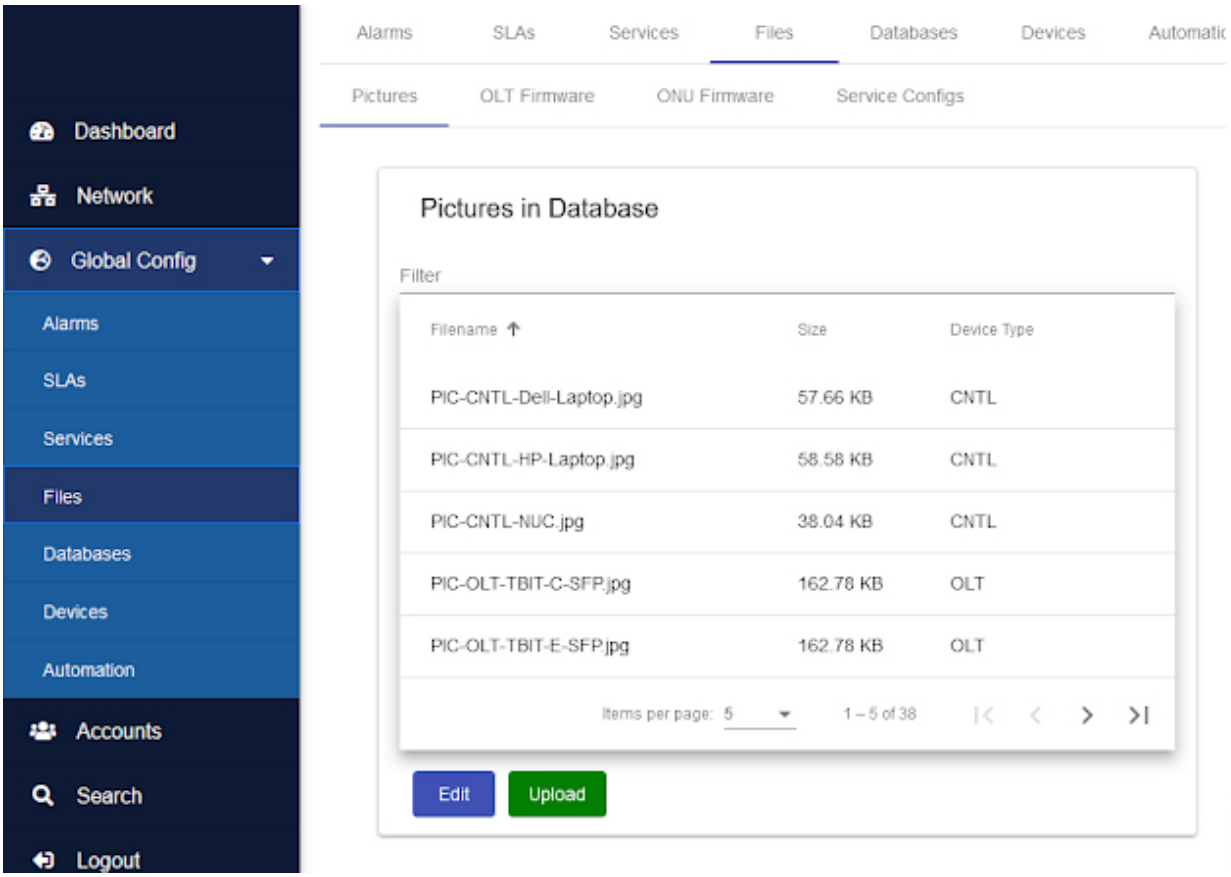
Delete an existing Downstream QoS Mapping

To delete an existing Downstream QoS Map, select the ‘Delete’ button on the top panel with the mapping to be deleted selected. The Delete button is disabled when actively editing a configuration.

Files

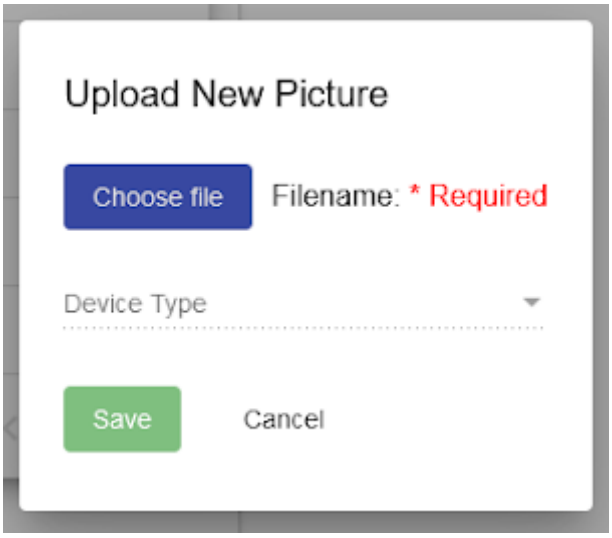
The Files tab is used for uploading and deleting files as well as editing the metadata of firmware and pictures.

© 2024 Cisco and/or its affiliates. All rights reserved.



Uploading

The following section describes the upload process for each type of file;



© 2024 Cisco and/or its affiliates. All rights reserved.

Pictures

To upload a picture, select the ‘Upload’ button along the bottom panel. Then, select the “Choose File” button to bring up a file browser to select the desired image. Any file with a MIME type of ‘image/*’ can be used.

Firmware

To upload a firmware image, select the ‘Upload’ button along the bottom panel on the relevant OLT or ONU tab. Then, select the “Choose File” button to bring up a file browser to select the desired image. The OLT firmware upload accepts files of type ‘.bin’. The ONU firmware upload accepts files of any type.

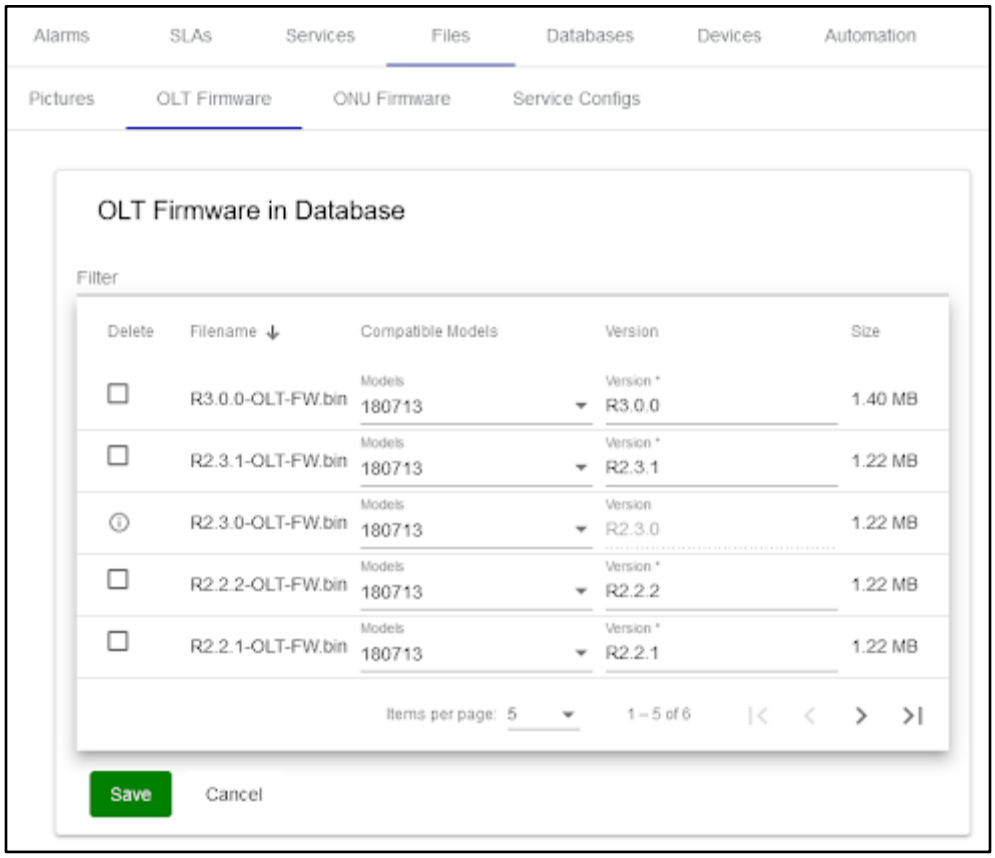
Services

To upload a service configuration, select the ‘Upload’ button along the bottom panel. Then, select the “Choose File” button to bring up a file browser to select the desired configuration. Any file of type ‘.json’ is accepted.

Editing and Deleting

The following section describes the editing and deletion process for each type of file;

© 2024 Cisco and/or its affiliates. All rights reserved.



Pictures

It is possible to delete or edit the device type of an uploaded picture. To do so, select the ‘Edit’ button along the bottom panel.

To delete a picture, toggle the checkbox in the left-most column titled ‘Delete’. When the ‘Save’ button is selected, this picture is removed from the database. If the file is currently saved to a device’s configuration then instead of a checkbox an info icon will be displayed. Clicking this icon will open a popup that lists up to ten devices that have that file assigned in their configurations. This file will not be deletable unless it is removed from all device configurations.

To edit the device type of a picture, change the dropdown in the right-most column titled ‘Device Type’ to the desired type. Select ‘Save’.

Firmware

It is possible to delete or edit the supported models and version of an OLT firmware image. It is also possible to delete or edit the vendor, supported models, and version of an ONU firmware image. To do so, select the ‘Edit’ button along the bottom panel on the appropriate tab.

© 2024 Cisco and/or its affiliates. All rights reserved.

To delete an OLT or ONU firmware image, toggle the checkbox in the left-most column titled ‘Delete’. When the ‘Save’ button is selected, this image is removed from the database. If the file is currently saved to a device’s configuration then instead of a checkbox an info icon will be displayed. Clicking this icon will open a popup that lists up to ten devices that have that file assigned in their configurations. This file will not be deletable unless it is removed from all device configurations.

To modify the supported models of an OLT or ONU firmware image, change the checked options in the dropdown in the column titled ‘Compatible Models’ to the desired options. Select ‘Save’.

Services

It is possible to delete or modify the version and title of a service configuration. To do so, select the ‘Edit’ button along the bottom panel on the appropriate tab.

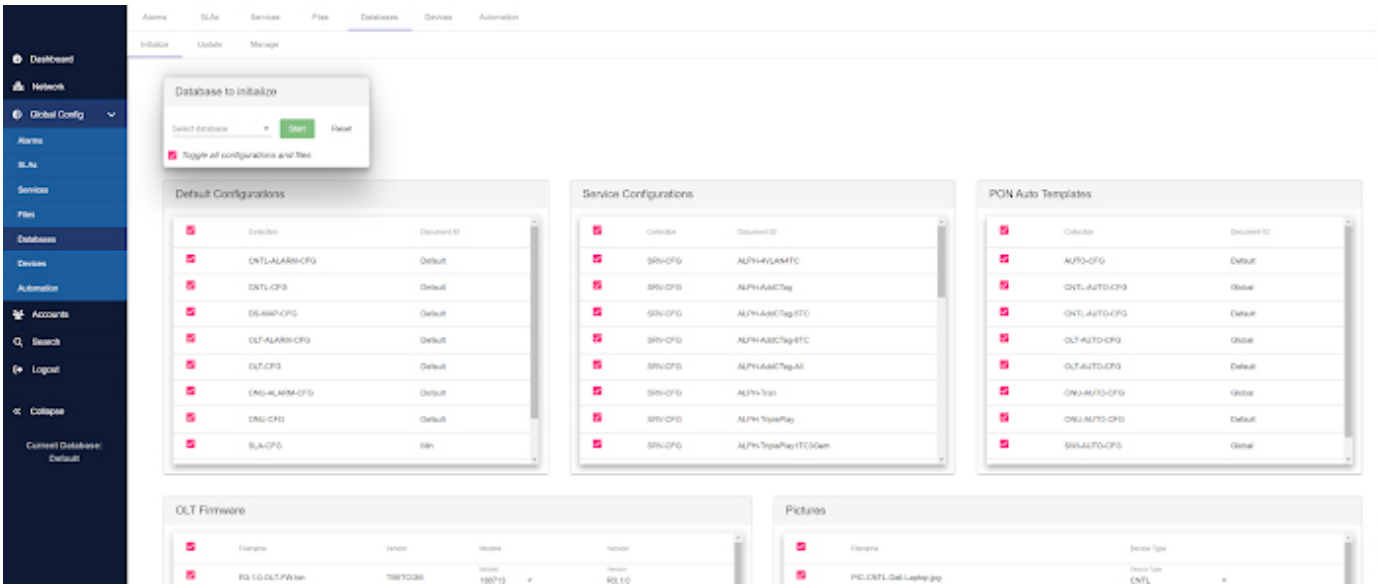
To delete a service configuration, toggle the checkbox in the left-most column titled ‘Delete’. When the ‘Save’ button is selected, this configuration is removed from the database. If the file is currently saved to a device’s configuration then instead of a checkbox an info icon will be displayed. Clicking this icon will open a popup that lists up to ten devices that have that file assigned in their configurations. This file will not be deletable unless it is removed from all device configurations.

Databases

The Databases tab is used for adding, removing, modifying, initializing, and updating databases for Routed PON Manager.

© 2024 Cisco and/or its affiliates. All rights reserved.

Initialize

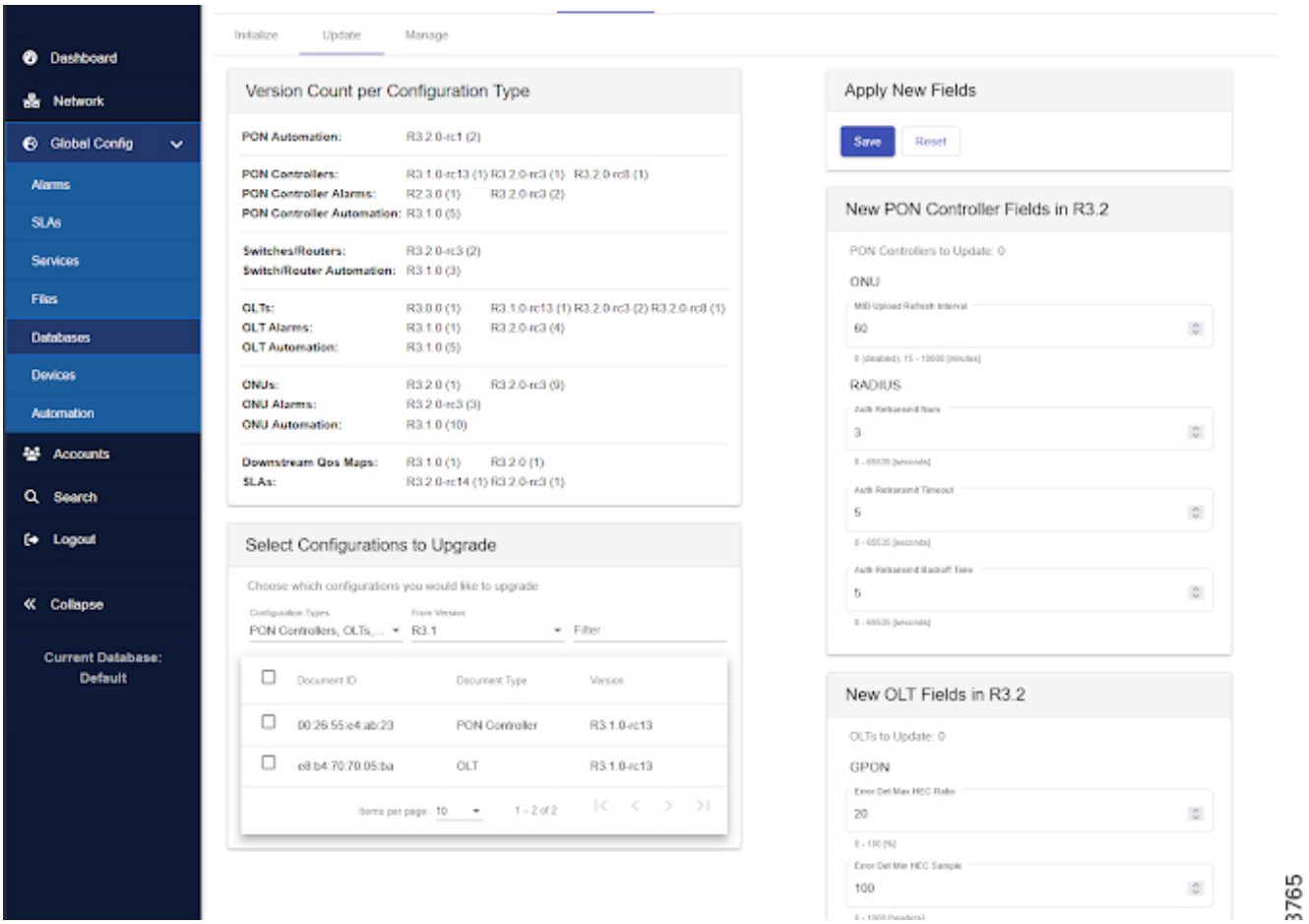


523764

The Routed PON Manager allows a user to initialize a database with default configurations, pictures, and firmware images. The user may select any of the SLA, Service, PON Controller, Switch, OLT, ONU and PON Auto default configuration documents as well as default device pictures and firmware images that come with the install package. The user may then choose a database from the existing list of configured databases. It is important to note that when inserting pictures, firmware or other large files, it may take a few minutes to complete the upload. After initialization, the inserted documents and files may be edited or modified as normal.

© 2024 Cisco and/or its affiliates. All rights reserved.

Update



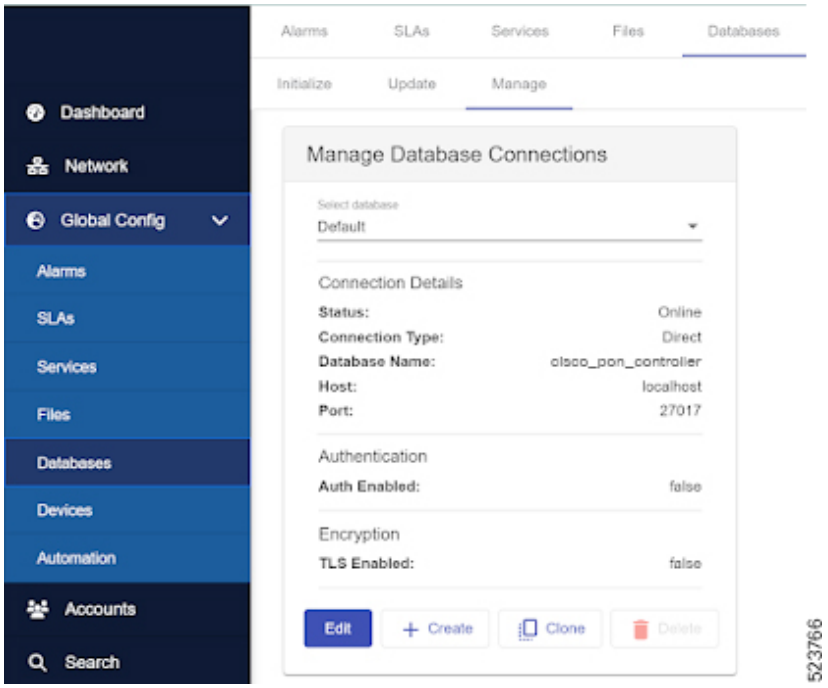
3765

Note: Only one version update is allowed at a time. It is not possible to skip versions.
The Databases Update tab supports upgrading a database to use the latest configuration schemas. This allows a network to access the full capabilities of the PON Controller. This should be done for all devices, SLAs and alarm configurations on the network for each release.

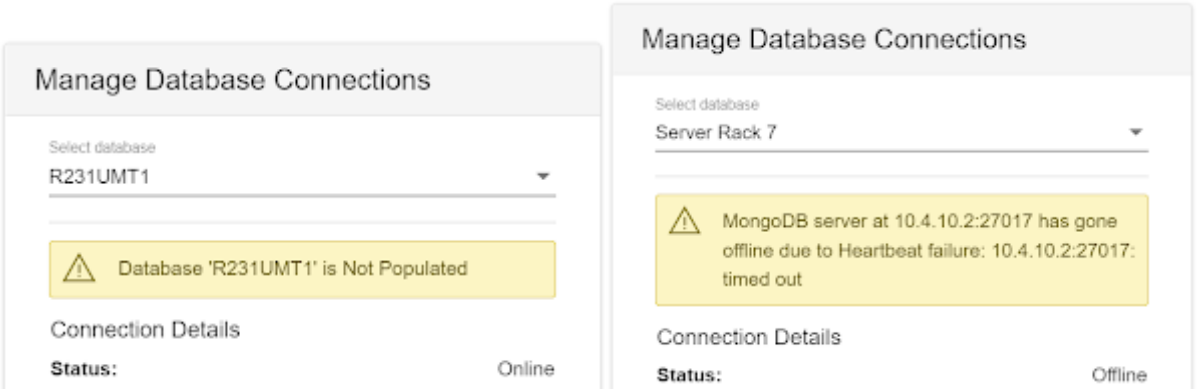
There is an option to update every configuration on the network, by selecting the checkbox in the top left-hand corner of the table, in the header. Choosing this option overwrites any existing configurations already using the version to which you are upgrading.

© 2024 Cisco and/or its affiliates. All rights reserved.

Manage



The Databases Manage tab supports adding, modifying existing, cloning, and deleting database connections from Cisco Routed PON Manager. To view the data for a database connection, select the ID from the drop down at the top of the tab. If the MongoDB server is offline or cannot be reached, the “Status” will show Offline and a ‘Heartbeat failure’ warning panel appears under the drop down. If a server is Online but has not been initialized yet (blank or non-existent), a ‘Not Populated’ warning panel appears under the dropdown.



Note: PON Manager users and user profiles are stored in the users database (e.g., tibit_users). The users database connection settings cannot be modified using the Web App.

© 2024 Cisco and/or its affiliates. All rights reserved.

Add a New Database Connection

On the bottom of the panel, select the ‘Create’ button to create a new MongoDB database connection. A Database ID must be entered into the Database ID field on the top of the panel for the connection to be saved. The Database ID field is the name of the database as it appears in Routed PON Manager. This does not necessarily have to be the Name of the database as it exists in MongoDB. See the section Configurable Fields to properly configure the new database connection. Click the save button to create the connection.

Modify an Existing Database Connection

Select the database connection to be modified in the dropdown ‘Select Database’.

On the bottom of the panel, select the button ‘Edit’ to modify the selected database connection. See the section; Configurable Fields to properly configure the new database connection. Click the Save button to update the connection.

Clone an Existing Database Connection

Select the database connection to be cloned in the dropdown ‘Select Database’.

Click the ‘Clone’ button on the bottom of the panel and enter a new “Database ID” for new database connection. If desired, modify connection information for the cloned database connection. See the section Configurable Fields for a description of the connection fields. Click the Save button to create the connection.

Delete an Existing Database Connection

Select the database connection to be deleted in the dropdown ‘Select Database’.

On the bottom of the panel, select the button ‘Delete’ to remove the selected database connection. The Delete button will be disabled when the ‘Default’ database connection is selected. This connection cannot be removed.

Configurable Fields

The configurable fields for a database connection are as follows:

Key	Description
Database ID	Name of the database as it appears in the UI.

© 2024 Cisco and/or its affiliates. All rights reserved.

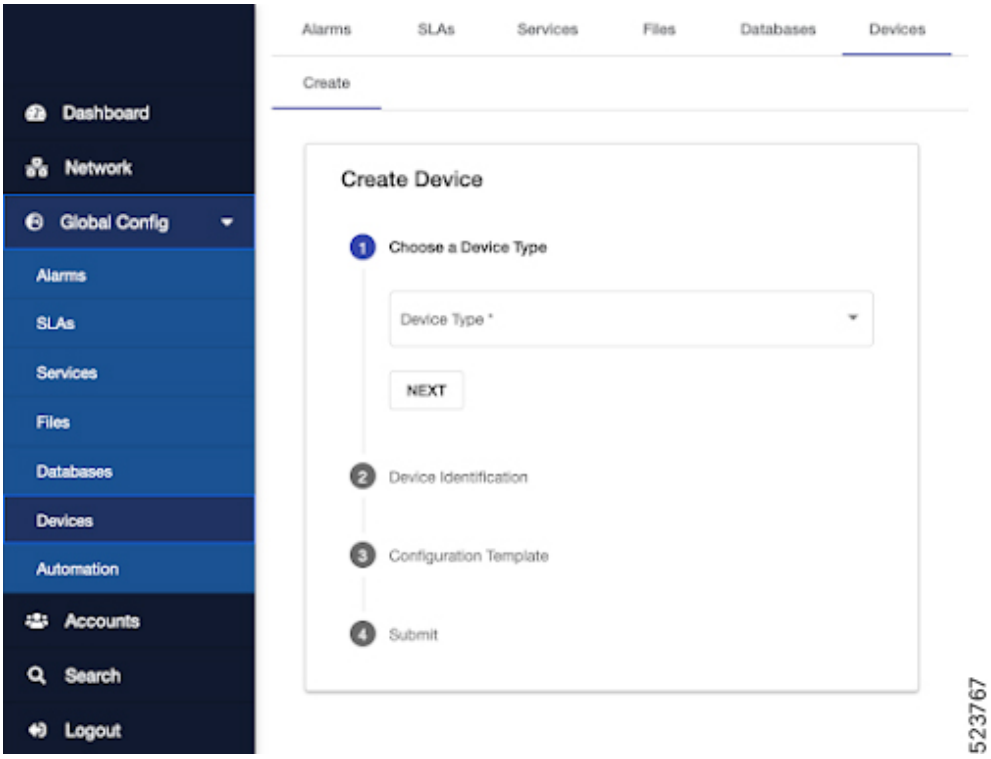
Connection Type	**Direct** - Connect to MongoDB instance via UI guided host, port and name **Replica Set** - Connecting to MongoDB replica set **URI** - Connect to MongoDB via raw URI
Database URI	MongoDB connection URI string. *(If used, all other fields except for Database Name are ignored)*
Database Name	Name of PON Controller database.
Host	Hostname/IP Address of your MongoDB server hosting the MongoDB instance.
Port	MongoDB server port number.
Enable Auth	Boolean specifying if the MongoDB server at *host:port* is using authentication.
Auth Database	Name of your MongoDB authentication database. *(Available when Enable Auth is true)*
Username	The username of the MongoDB user to authenticate with. *(Available when Enable Auth is true)*
Password	The password of the specified MongoDB user. *(Available when Enable Auth is true)*
Enable TLS	Boolean value specifying if the MongoDB server at *host:port* is using encryption.
CA Certificate Path	Path to the encryption certificate.
Enable Replica Set	Boolean specifying if the MongoDB server is a replica set.
Replica Set Name	The name of the MongoDB replica set. *(Available when Enable Replica Set is true)*
Replica Set Hosts	List of host servers that are a part of the replica set. *(Available when Enable Replica Set is true)*

© 2024 Cisco and/or its affiliates. All rights reserved.

Devices

Create

The Devices Create tab is used for pre-provisioning PON Controllers, Switches, OLTs, and ONU device configurations.



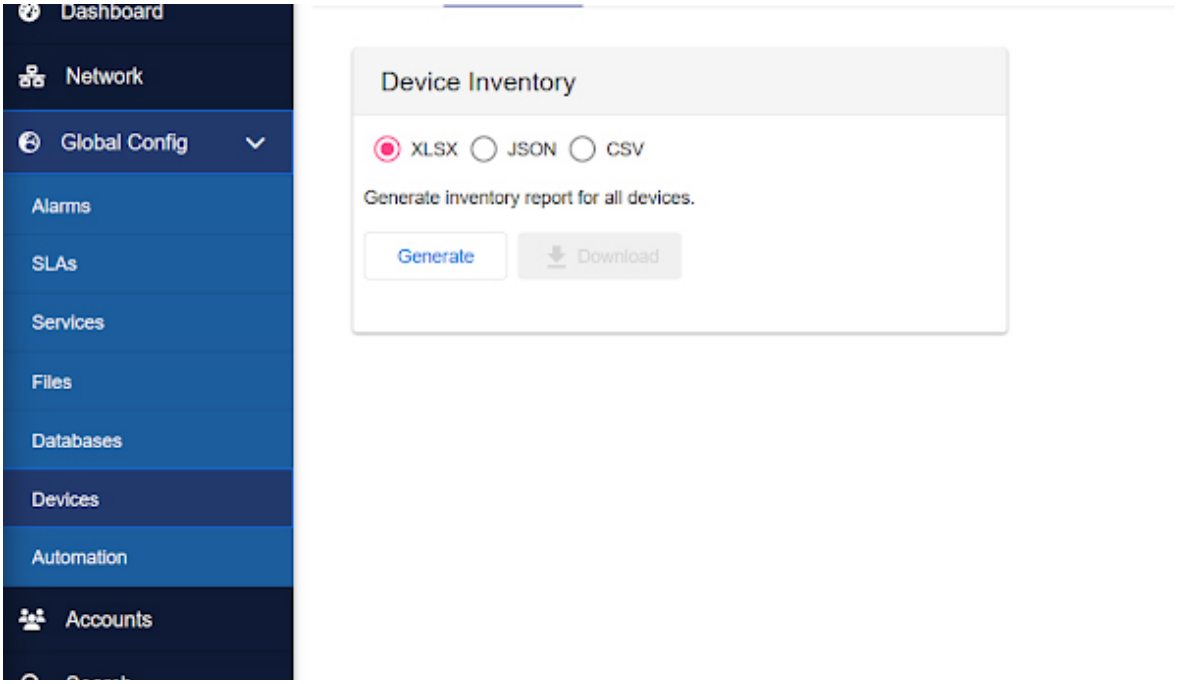
A base configuration template is selected when configuring a new device. The new device being created is based on this base configuration template.

A new OLT and ONU configuration may be inventoried under a PON Controller and Switch or OLT, respectively, but is not required.

© 2024 Cisco and/or its affiliates. All rights reserved.

Inventory

The Devices Inventory tab is used for generating an inventory report for all Switches, PON Controllers, OLTs, and ONUs on the system.



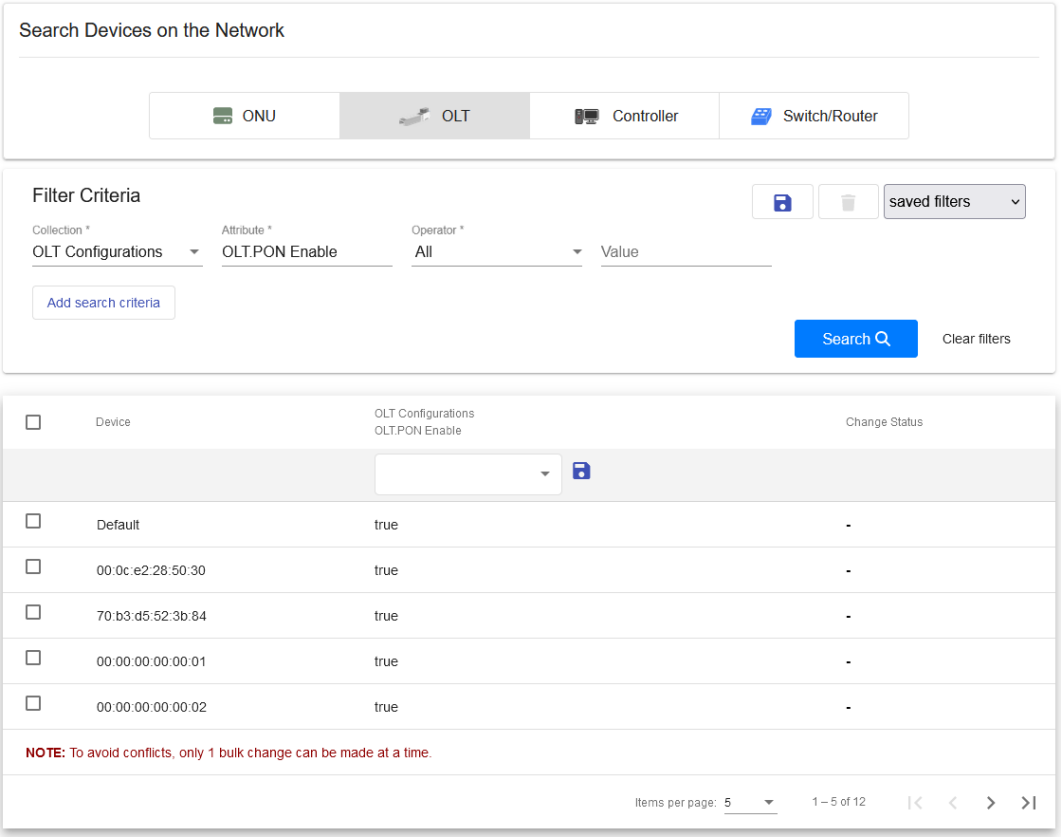
Clicking the “Generate” button will start the process. To generate a device inventory, state and configuration documents are collected for all devices managed by PON Manager from the current database. This process can take several minutes for larger databases.

After the inventory report has been generated it can be downloaded directly to the user’s local computer. There are three file type options: XLSX, JSON, or CSV. If XLSX is selected, one Excel Worksheet will be downloaded consisting of one sheet for each device type. If JSON or CSV is selected, a Zip file will be downloaded consisting of one file for each device type. Alternate file formats may be selected and downloaded without re-generating the inventory report.

Search

The Search tab is a user's view into the database. From here, users can query the database 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.

© 2024 Cisco and/or its affiliates. All rights reserved.



Values that are returned from the database are placed in a table along with the MAC address of the device that matches the specified query. By clicking on the device ID in the table row, users can navigate to that 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 and loaded to prevent the user from having to rebuild common searches each time they come to the page. Multiple criteria can be added to one search. These saved searches can also 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.

© 2024 Cisco and/or its affiliates. All rights reserved.

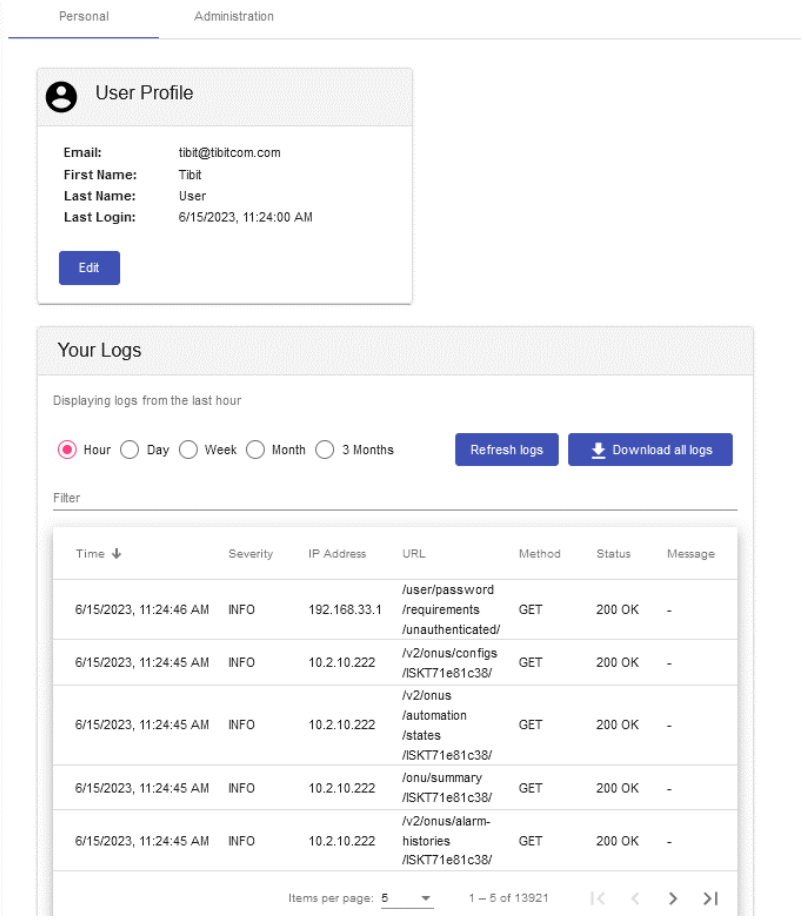
Note: Only 1 attribute can be updated at a time.

Accounts

The Accounts tab is used for creating, editing, viewing, and managing user profiles and roles. All users have the ability to update their first and last names as well as passwords. However, only a user that has been assigned the built-in Administrators role may view and edit the information of other users.

Personal

The default view of the Accounts page is the Personal tab. This tab presents the email address, first name, last name, last login time, and user logs of the currently logged in user. The first tile allows the user to edit their first and last name as well as their password. The second tile displays the user action logs. All of the logs shown here are relevant to the logged in user only. It is possible to retrieve all logs within the last hour, day, week, or month and to sort and filter by the values in the table.



© 2024 Cisco and/or its affiliates. All rights reserved.

Change Password

To change the password of the currently logged in user click the Edit button of the first tile. To update the password, enter the new desired password in the Password field. To see what was entered as plain text, click on the eye icon at the right of the field. To view the chosen passwords status, hover the cursor over the Password input field. See Password Requirements for more detailed information. Re-enter the new password in the Confirm Password field. Click SAVE to confirm and accept the changes. These changes will take effect immediately and the new password will be required the next time the user logs in.

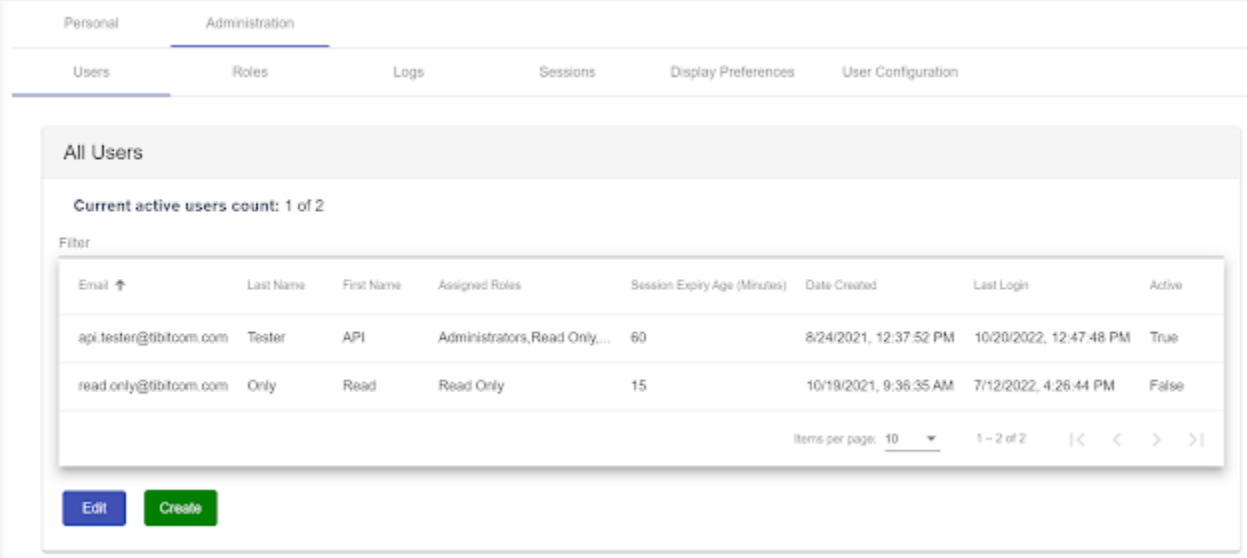
Administration

This tab is used to manage all user profiles, roles, as well as the user session timeout. It is only visible and available to users assigned to a role with the Accounts, Admin Read permission.

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.

© 2024 Cisco and/or its affiliates. All rights reserved.



Create a New User

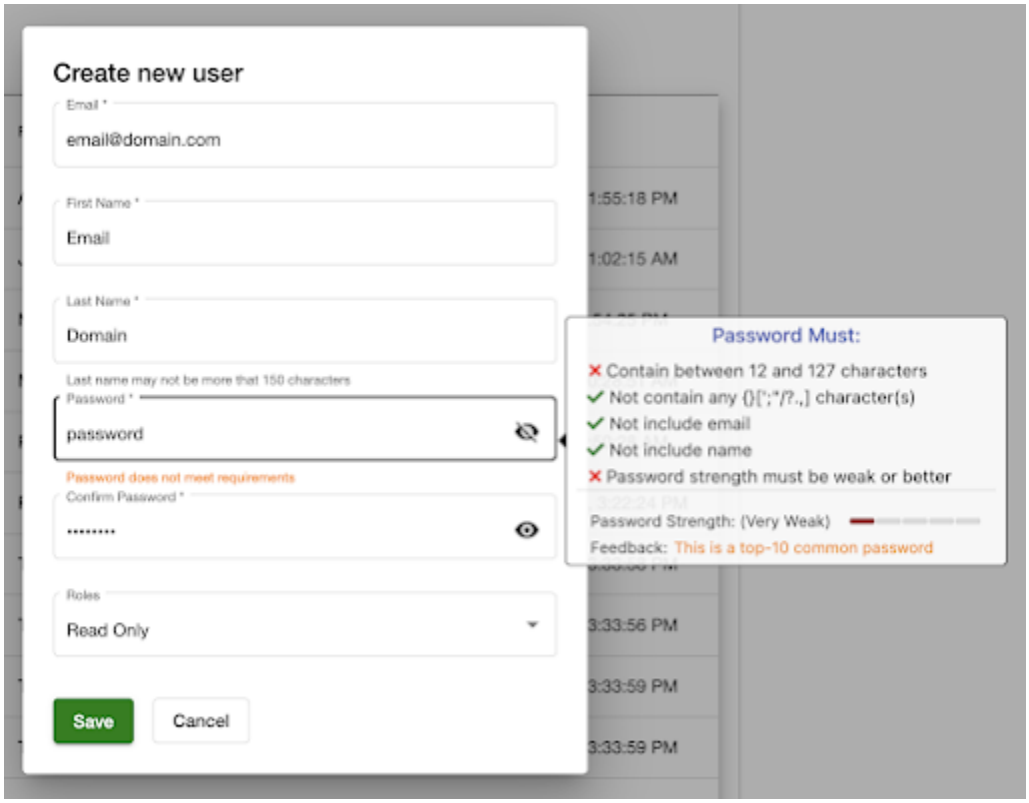
Next to the Edit button on the main view, there is also a Create button. Clicking this button opens a dialog with inputs for a new user account. Email, first name, last name, roles, and a

© 2024 Cisco and/or its affiliates. All rights reserved.

password must be provided for a new user account. However, it is optional to assign roles to a new user.

It is recommended, but not required, that the chosen password adheres the configured requirements. To view the chosen passwords status, hover the cursor over the Password input field. See Password Requirements for more detailed information.

It is highly recommended that a user changes their password from the Personal tab after their first login with the created password. Once all required files have been filled in and are valid, the new account may be created.



Modify an Existing User

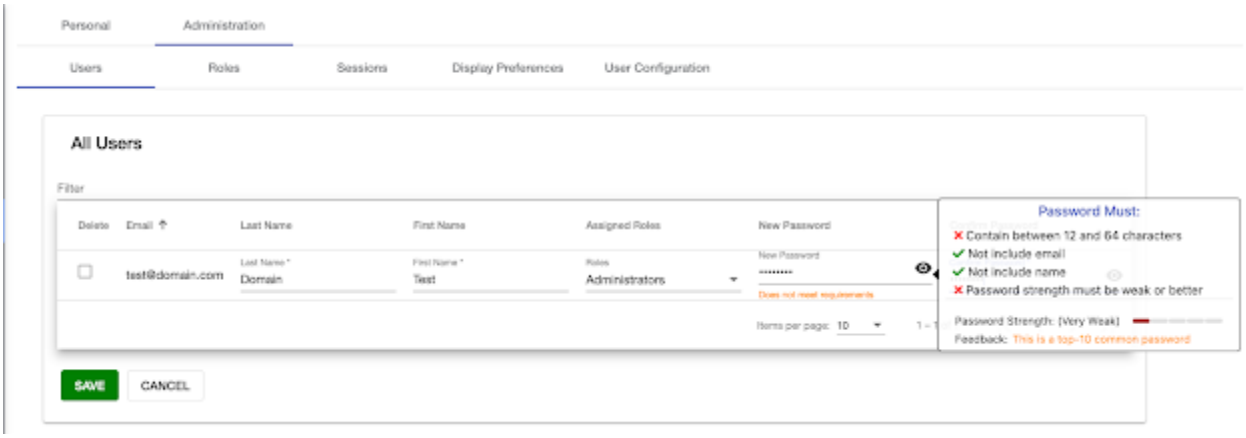
To edit existing users, click the Edit button at the bottom left of the table. The table columns vary slightly during edit, as the Date Created and Last Login values are not editable and new password fields are also added.

From this view, a user with the Accounts Admin Update permission may edit the first and last names, assigned roles, and passwords of all users at once.

© 2024 Cisco and/or its affiliates. All rights reserved.

It is recommended, but not required, that the chosen password adheres the configured requirements. To view the chosen passwords status, hover the cursor over the New Password input field. See Password Requirements for more detailed information. The Confirm Password field is required once a value has been entered in the New Password field for that row.

Once all desired changes have been entered and are valid, the Save button is enabled and the user may click Save. To clear these changes without saving click Cancel.



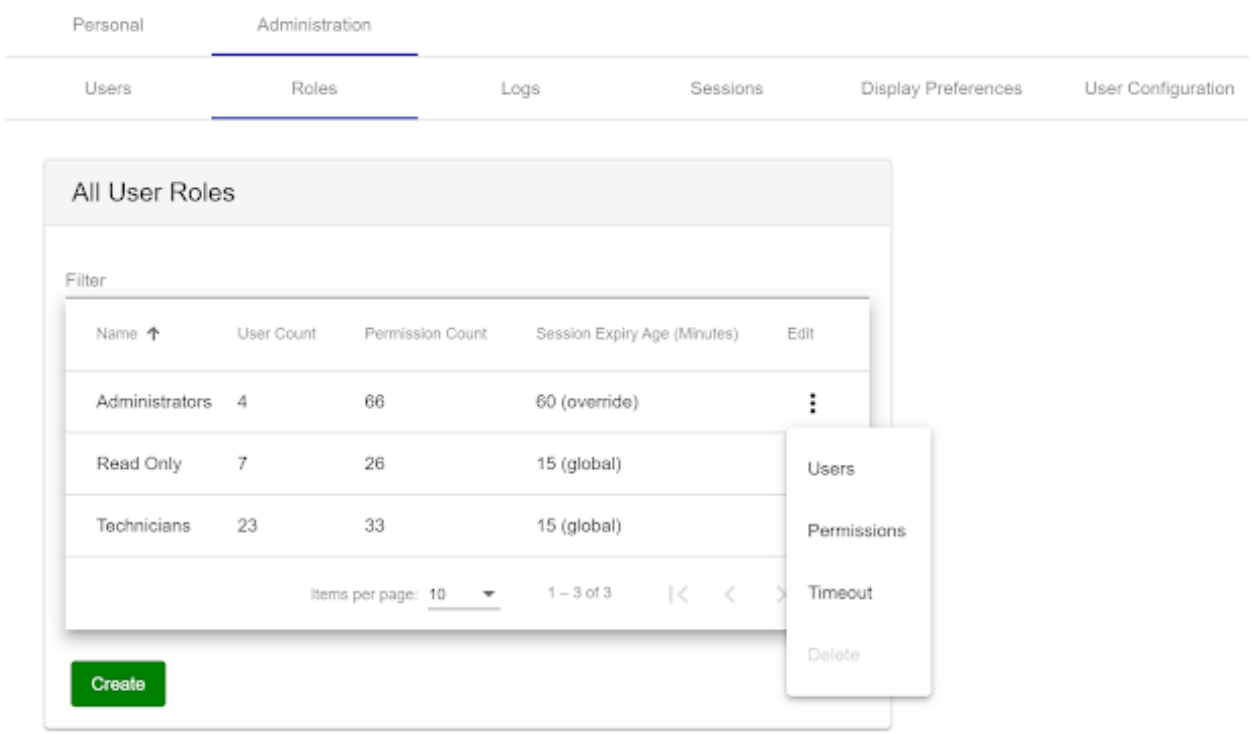
Delete a User

A user account can also be deleted from this view if the logged-in user has the Accounts Admin Delete permission. Deleting a user is done in the same view as editing. Click Edit at the bottom left of the table. For every user to delete, select the checkbox in the left-most Delete column. The inputs for that user's information become disabled. Upon save, any users with this box checked are deleted. Once saved, the deletion cannot be undone.

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.

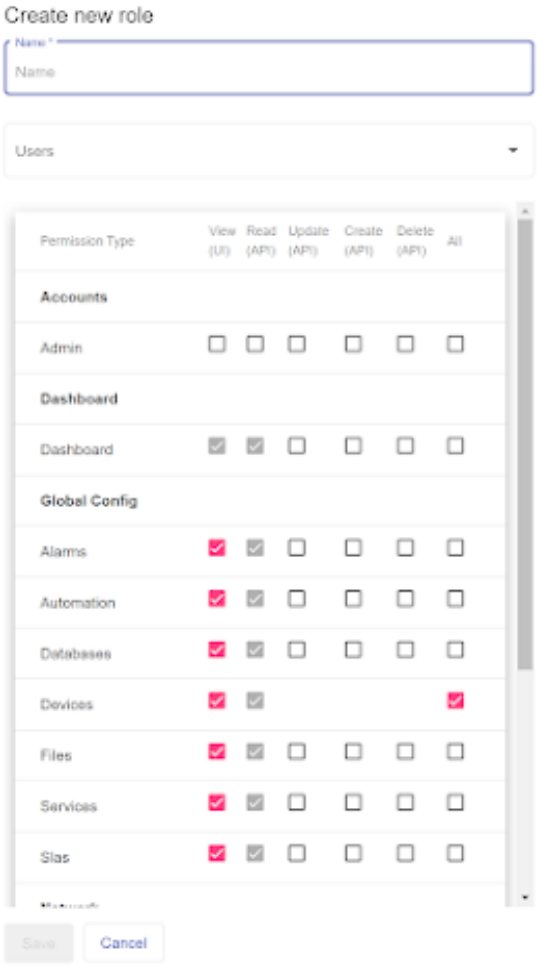
© 2024 Cisco and/or its affiliates. All rights reserved.



© 2024 Cisco and/or its affiliates. All rights reserved.

Create a New Role

To create a new role, click on the green Create button at the bottom of the main Roles tab view. This opens a dialog with two inputs and a permissions table. The new role must be assigned a unique name. It is optional to assign users to the role upon creation. All read permissions except for Accounts Admin are selected by default and not removable. After a unique name has been input, the new role can be created. The users and permissions can always be changed.



© 2024 Cisco and/or its affiliates. All rights reserved.

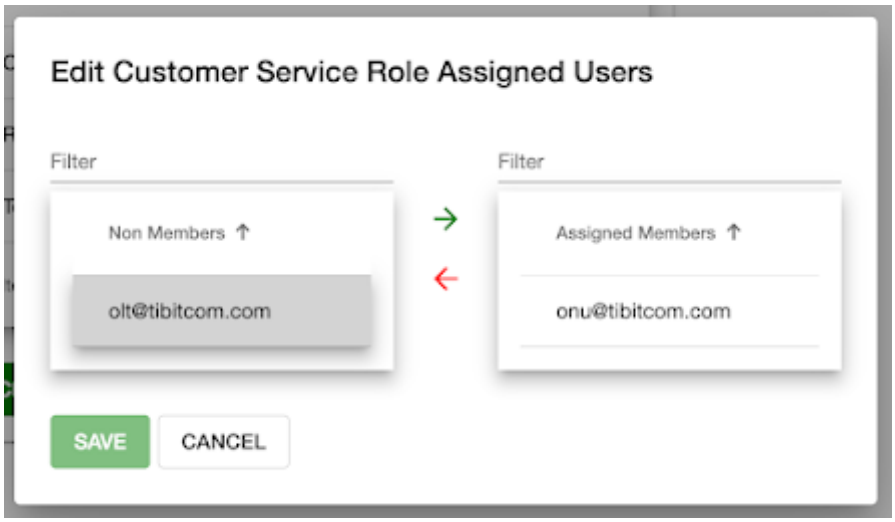
View Permissions

Note: View permissions only control what is displayed in the UI and DOES NOT restrict API access to users.

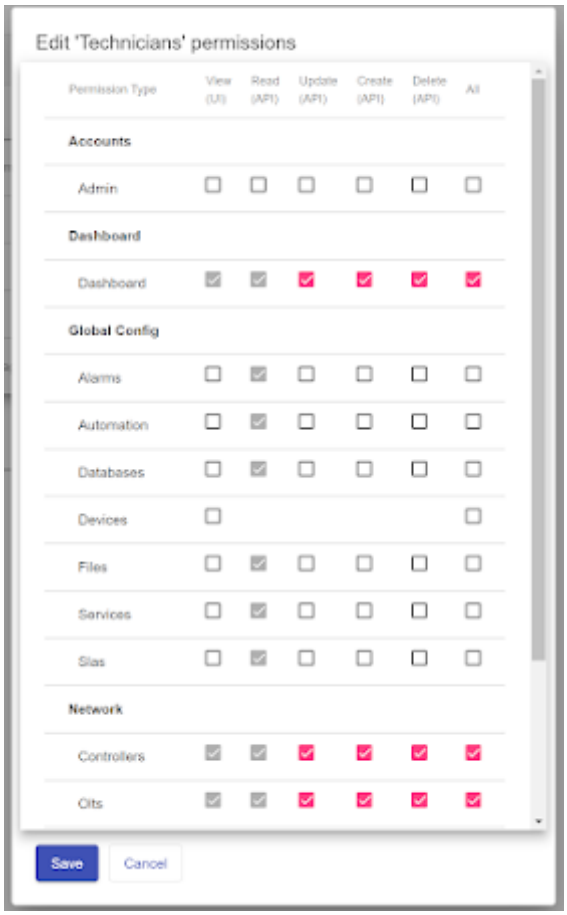
View permissions are used to show or hide sections of the UI from a group of users. Disabling view permissions will hide the tabs and reroute users back to login if they navigate to the pages. View permissions other than Admin, are enabled by default and can only be disabled for the Global Config.

Modify an Existing Role's Users

By selecting the users option from the edit menu a dialog is displayed with two tables. The left table shows all users that are not a member of that role. The right shows all users that are. Users may be added to the role by selecting each user to add from the non members table, then the green right-facing arrow. They may also be removed by choosing the users from the members table and selecting the red left-facing arrow. The Save button is enabled once changes are made.



© 2024 Cisco and/or its affiliates. All rights reserved.



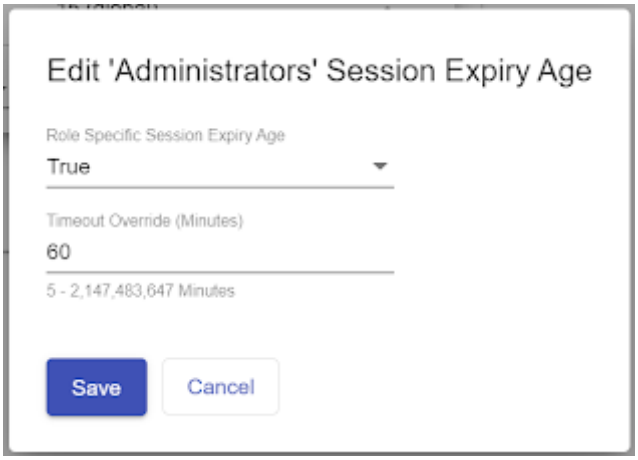
Modify an Existing Role's Permissions

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.

© 2024 Cisco and/or its affiliates. All rights reserved.

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.



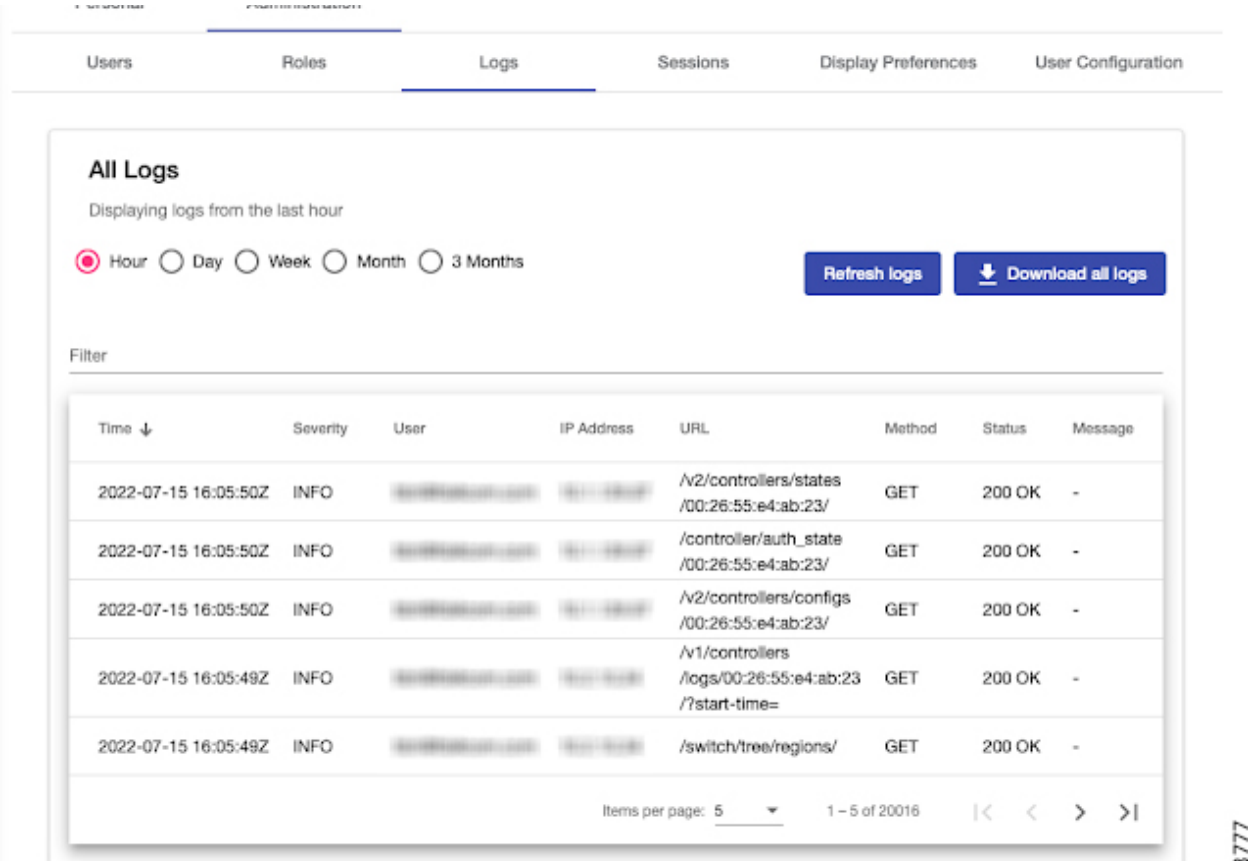
Delete a Role

To delete a user role, select the menu icon in the Edit column of the main Roles view table. Click on the Delete option. If the role contains no users, a prompt to confirm the deletion is displayed. Upon confirmation the role is deleted, This cannot be undone. If there are users assigned to the role, a warning message is displayed alerting the user that a role can not be deleted if it contains users. All users must be removed from the role before deleting. **Note:** the built in Administrators and Read Only roles can not be deleted at any time.

Logs

The Logs tab displays a table of PON Manager log entries for all users. An Administrator may choose to see the logs for the last Hour, Day, Week, or Month. 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. Clicking "Download all logs" will save the logs to the user's computer in json format. Clicking "Refresh logs" will get the latest logs from the database.

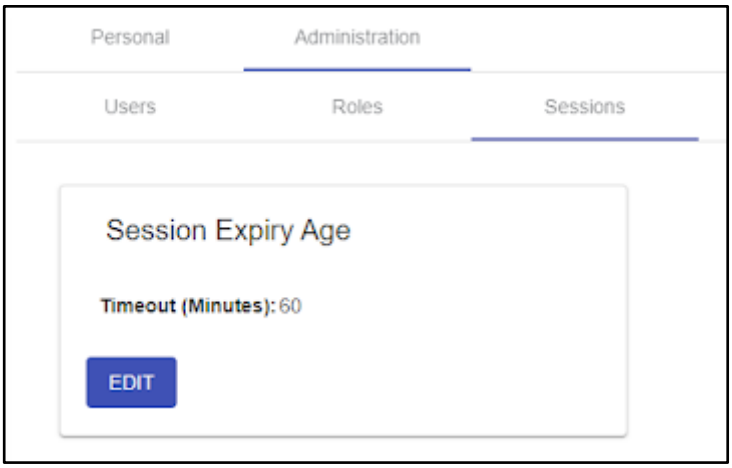
© 2024 Cisco and/or its affiliates. All rights reserved.



Sessions

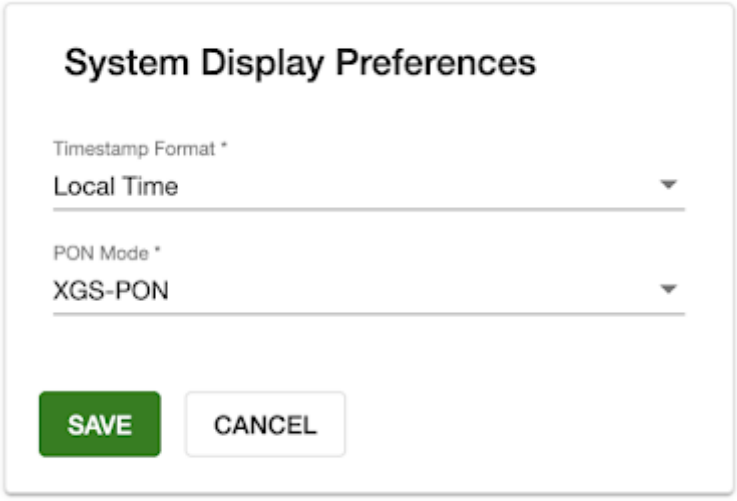
The Sessions tab contains a single option to set the length of time in minutes for how long a user should remain logged in without activity. If a user is logged in and there is no activity from them within the time limit defined here, then they are automatically logged out and their session is invalidated.

© 2024 Cisco and/or its affiliates. All rights reserved.



Display Preferences

The Display Preferences tab provides the ability to configure Timestamp Format and PON Mode of Routed PON Manager system wide for all users.



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.

© 2024 Cisco and/or its affiliates. All rights reserved.

PON Mode

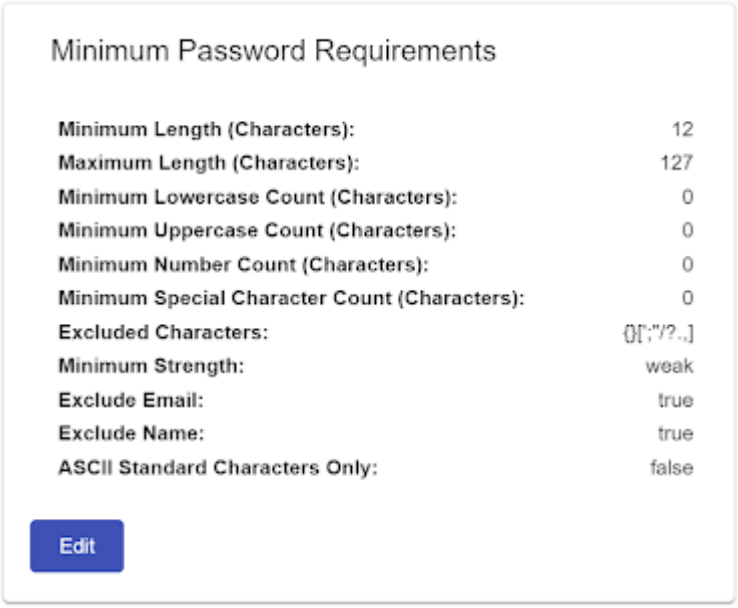
There are three options for PON Mode; XGS-PON, 10G EPON, and XGS-PON & 10G EPON. This setting controls what PON Mode specific configurations will be available to modify within the UI. When a PON Mode is selected, all configurations in the interface that do not apply to the given PON Mode will be removed.

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.

User Configuration

The User Configuration tab provides the ability to configure the password requirements for new users and existing users changing passwords.

See Password Requirements for more details.



Various aspects of user password composition requirements can be configured, including;

- Minimum and maximum length
- Minimum amount of lowercase, uppercase, numbers, and special characters
- A blacklist of excluded characters
- Minimum Strength

© 2024 Cisco and/or its affiliates. All rights reserved.

    - Password strength utilizes an entropy-based algorithm in conjunction with a blacklist of most common passphrases that predicts how insecure a given password is.
- Disallow passwords from containing the users name or email
- Disallow any characters not contained with the Standard Range ASCII character set

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2024 Cisco and/or its affiliates. All rights reserved.